Centre for Human Rights
UNIVERSITY OF PRETORIA

THE DIGITAL RIGHTS LANDSCAPE IN SOUTHERN AFRICA

AUGUST 2022

USAID
FROM THE AMERICAN PEOPLE

ADVANCING RIGHTS IN SOUTHERN AFRICA
ARISA

TABLE OF CONTENTS

Authors
S'lindile Khumalo and Murray Hunter on behalf of ALT Advisory.

Editors
Hlengiwe Dube, Marystella Simiyu, and Dr. Tomiwa Ilori on behalf of the Centre for Human Rights, University of Pretoria.

ISBN: 978-1-7764116-4-1

Photo acknowledgments
Cover by Christina @ wocintechchat.com/Unsplash
Pages i, 53, 63 by Aidah Namukose/ALT Advisory | Page 1 by Graham van de Ruit/ALT Advisory
Page 5, 12, 17, 27 by Opara Gods'promise/ALT Advisory
Page 36 by Charles Deluvio-Dilfan/Unsplash | Page 44 by Brandy Kennedy/Unsplash
Page 55, Bruce Mars/Unsplash | Page 71, LinkedIn Sales Solutions/Unsplash

Designed by
Wilna Combrinck

About the Centre for Human Rights
The Centre is an internationally recognised institution based at the Faculty of Law at the University of Pretoria. It is both an academic and human rights organisation that aims to contribute to advancing human rights through education, research, and advocacy.

About ALT Advisory
ALT Advisory is a public interest advisory and research firm based in South Africa which questions convention and works for positive change in Africa, and the world. It assists socially responsible organisations with advisory & analysis, research, impact, training, and communications & design services in the areas of public law & policy, information rights, data privacy, and emergent tech & innovation.

About the ARISA Programme
This work was conducted with the support of Freedom House under the Advancing Rights in Southern Africa (ARISA) programme. The goal of the ARISA programme is to improve the recognition, awareness, and enforcement of human rights in the region and a cross-cutting emphasis on protecting the region's most vulnerable and marginalised groups, including indigenous peoples, women, and youth.

PREFACE

While there are positive developments in the adoption and use of digital technologies in Southern Africa, such as internet connectivity and adoption of the relevant legal framework, there are worrisome gaps in the manner in which human rights are exercised in the digital age. These disparities were exposed and exacerbated in the wake of the COVID-19 pandemic. While those that are digitally connected shifted to virtual alternatives, a large segment of Southern Africa remains unconnected. Digital inequalities manifest from, among other factors, poor infrastructure, lack of or inadequate supply of electricity, and high cost of data. An examination of the dimensions of the digital divide reveals that vulnerable and disadvantaged groups such as women, children, rural populations, and persons with disabilities are disproportionately affected. Also, the use of digital technologies comes with vulnerabilities such as arrests of journalists and activists for speaking out on online platforms against corruption and impunity; misinformation and disinformation; online violence against women, children, and other vulnerable groups; and violations of the right to privacy in an environment with weak data protection laws and policies. Some of the cyber laws being adopted in the Southern African Development Community (**SADC**) region infringe on human rights owing to the flawed regional framework that was developed under the Harmonisation of the ICT Policies in Sub-Saharan Africa (**HIPSSA**) project.

In January 2022, the Centre for Human Rights, University of Pretoria (**the Centre**) commissioned a study on digital rights in Southern Africa with the objective to assess the status of digital rights in the sub-region. The foundational instrument for this research is the African Charter on Human and Peoples' Rights, with a focus on article 9, which provides for the right to freedom of expression and access to information. Soft law instruments that have been developed under article 9 of the African Charter (the Model Law on Access to Information for Africa, the Guidelines on Access to Information and Elections in Africa, and the revised Declaration of Principles on Freedom of Expression and Access to Information in Africa) provide an opportunity to work towards enhancing freedom of expression and access to information in the digital age. This project is an opportunity for the adoption of 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. The output of this project is a report titled "The Digital Rights Landscape in Southern Africa".

The report builds onto existing digital rights research on the continent and provides an insight into the status of digital rights in Southern Africa. It draws examples from the sub-region and highlights milestones and gaps in the exercise of digital rights. The report also proposes comprehensive recommendations for regional bodies, governments and policymakers, civil society actors, and other stakeholders. The proposed recommendations include legislative and policy reforms, research initiatives, and advocacy to enhance the promotion and advancement of digital rights in Southern Africa. I trust that this report will be a useful resource for African stakeholders (civil society actors, public officials, regulatory bodies, and media organisations) in advancing digital rights.

Finally, I wish to acknowledge the commendable effort of our partners, ALT Advisory, for drafting this report. I would also like to extend my sincere gratitude to the Centre's Expression, Information and Digital Rights Unit for the excellent work in conceptualising, editing, and reviewing this report.

Prof Frans Viljoen
Director, Centre for Human Rights
1 August 2022

ACRONYMS & ABBREVIATIONS

ACHPR	African Commission on Human and Peoples' Rights
APC	Association for Progressive Communications
ACRWC	African Charter on the Rights and Welfare of the Child
ACERWC	African Committee of Experts on the Rights and Welfare of the Child
AU	African Union
AUC	African Union Commission
CBO	Community-Based Organisation
CDC	Centres for Disease Control and Prevention
CSO	Civil Society Organisation
DCC	Digital Complaints Committee
DCT	Digital Contract Tracing
DTS	Digital Transformation Strategy
FRT	Facial Recognition Technology
FSD	Financial Sector Deepening
GDPR	General Data Protection Regulation
GNI	Gross National Income
HIPSSA	Harmonisation of the ICT Policies in Sub-Saharan Africa
ICASA	Independent Communications Authority of South Africa
ICT	Information and Communications Technology
IOT	Internet of Things
ISP	Internet Service Provider
ITU	International Telecommunication Union
MINTIC	Ministry of Information Technologies and Communications
MNO	Mobile Network Operator
NADPA	Network of African Data Protection Authorities
NIDA	National Identification Authority
NHRI	National Human Rights Institution
NRIS	National Registration and Identification System
OECD	Organisation for Economic Co-operation and Development
OHCHR	Office of the United Nations High Commissioner for Human Rights
POPIA	Protection of Personal Information Act
PORTAZ	Postal and Telecommunications Regulatory Authority of Zimbabwe
PWD	Persons with Disabilities

QR	Quick Response
REC	Regional Economic Community
RICA	Regulation of Interception of Communications and Provision of Communication-related Information Act
SADC	Southern African Development Community
SDG	Sustainable Development Goal
SIM	Subscriber Identity Module
SLAPP	Strategic Litigation Against Public Participation
SOE	State-owned Enterprise
STEM	Science, Technology, Engineering, and Mathematics
UN	United Nations
UNHCR	United Nations High Commissioner for Refugees
ZESA	Zimbabwe Electrical Supply Authority

GLOSSARY

4IR	The Fourth Industrial Revolution, coined by Klaus Schwab refers to a theorised leap forward in economic and social development enabled by emergent technologies such as Artificial Intelligence and the Internet of Things. The Fourth Industrial Revolution blurs the lines between the physical, digital, and biological spheres.[1]
Artificial Intelligence	The capacity for computer systems to be programmed to complement, mimic, or replace human 'thinking', for example by spotting patterns, making decisions, or predicting likely outcomes on a particular task.[2]
Biometrics	A natural person's physical, physiological, or behavioural information which can be used to identify them,[3] such as fingerprints, face, iris of the eye, or voice. A *biometrics system* is a mechanical system designed to record and identify a person based on one or more biological and behavioural characteristics. Such systems may be used for security measures.
Broadband	High-speed transmission by means of wired and wireless networks which operate faster than analogue dial-up.[4]
Bulk interception	The process of intercepting and analysing electronic communications (which may include both content and metadata) where the interception is not targeted to specific individuals or parties who are subject to an investigation. Also known as mass surveillance or untargeted interception.
Cyberspace	The online or digital world created by the internet and within which electronic communication occurs.
Data subject	A natural or juristic person whose personal information may be subject to processing.
Digital divide	The gap between those with access to ICTs and those without, as a result of socio-economic differences.[5]
Digital literacy	The learned ability or skill to use ICTs to find, assess, create, research, or communicate.[6]
Digital rights	The extension of a range of fundamental human rights into the digital sphere or digitally networked spaces. These spaces may be created physically through infrastructure, protocol, devices, or virtually constructed through online identities and communities as well as other forms of expression.[7]

1 Philip Ross, 'Towards a 4th industrial revolution, Intelligent Buildings International', March 2021, at page 159, accessible here.
2 UN, A/HRC/48/21, 'The right to privacy in the digital age', 13 September 2021, at page 2, accessible here.
3 Article 4(14), General Data Protection Regulation (**GDPR**).
4 Britannica web dictionary, accessible here.
5 Sekoetlane Phamodi *et al*, 'Making ICT Policy in Africa: An Introductory Handbook', Fesmedia Africa, August 2021, at page 2, accessible here.
6 UN, 'General Comment 25: Children's rights in relation to the digital environment', February 2021, at page 2, accessible here.
7 Jessica Dheere, 'A methodology for mapping the emerging legal landscapes for human rights in the digitally networked sphere. In Global information society watch 2017. Unshackling expression: a study on laws criminalising expression online in Asia', Special edition, India: Association for Progressive Communications, 2017, accessible here.

Encryption	The process of converting data or information to an unreadable format for anyone except the intended recipient.[8]
e-Government	The use of digital technology to support the government in carrying out its duties.[9]
Facial recognition technology	Technology that is designed to record and analyse digital images of people's facial features, in order to try to identify them by matching them to pre-existing images.[10]
Information Communication Technologies	A wide range of digital technology and infrastructure connecting people to the digital world., inclusive of devices, telecommunications networks, software, and systems.
Intermediary	An entity that provides or enables access to the internet by acting as a conduit or a host.[11]
Internet shutdown	The deliberate disruption of the internet or electronic communications to impede the free flow of information within a specific location.[12]
Network throttling	The deliberate slowing down of internet speed or performance through the use of low bandwidth.[13]
Personal information or Personal data	A wide range of information that can be used to identify or trace a person, such as their race, gender, sexual orientation, pregnancy, marital status, national, ethnic or social origin, colour, age, physical or mental health, well-being financial status, political affiliation, religious beliefs, or biometric information.[14]
Processing	An umbrella term used to describe virtually any handling of personal information or data for example collection, receipt, recording, organisation, collation, storage, updating, modification, retrieval, alternation, consultation, use, dissemination, distributing, linking, restricting, degrading, erasing, or destruction.[15]
Spectrum	Radio frequencies which are used by mobile telecommunications providers and other industries to connect individuals to networks.[16]
Zero-rating	Enabling internet access without financial cost to users.[17]

8 Above n 5 at page 2.
9 *Id.*
10 Jawahitha Sarabdeen, 'Protection of the rights of the individual when using facial recognition technology', March 2022, at page 1, accessible here.
11 *Id.*
12 *Id.*
13 MDN, 'Web Docs Glossary: Definitions of web-related terms', undated, accessible here.
14 Section 1, Protection of Personal Information Act 4 of *2013*.
15 *Id.*
16 Above n 5 at page 2.
17 *Id.*

EXECUTIVE SUMMARY

This report aims to contribute to existing works on the status of digital rights in Southern Africa, and act as a resource for civil society actors, public officials, regulatory bodies, and media organisations in the region. The report builds on contributions from researchers, activists, journalists, and public institutions. It maps out the status of digital rights and provides an overview of how digital rights are exercised in Southern Africa. It also assesses common themes and differences across the region. This exercise is especially important in the Southern African context, where many countries are now seeing progress in connecting more people to the internet and other digital technologies.

Overall, this report highlights that there is significant progress in the promotion and protection of digital rights in Southern Africa. Most notably, after many years of delays, there is a proliferation of laws that are relevant to the digital age such as cybersecurity, cybercrimes, and data protection laws in the region. There has also been increased advocacy from civil society actors on this set of rights. However, digital rights violations persist. Some of the challenges that the report highlights include the divide in its various forms; poor governance over personal data and privacy rights breaches; network disruptions including internet shutdowns; and other government perpetrated actions that limit freedoms of expression, assembly and association online. Attacks on the media and the use of Strategic Litigation Against Public Participation (**SLAPP**) suits are other examples of the concerns which threaten the enjoyment of human rights in the digital age. The COVID-19 pandemic also had a significant impact on the digital rights landscape in the region. It prompted an acceleration in digitisation for some sectors, but exposed ongoing inequalities in digital access and participation for others.

This report also identified gaps in available information and analysis on particular digital rights themes in Southern Africa, such as gender inequalities in accessing Information Communication Technologies (**ICTs**), and unequal access to ICTs for marginalised groups such as Persons with Disabilities (**PWDs**) and rural communities. Issues relating to children's digital rights in the region are also underdeveloped and under-researched. Addressing these information gaps will be vital in assessing the true nature of these issues in Southern Africa and making positive changes.

Unfortunately, in many Southern African countries, slow progress in digital rights development often coincides with a poor democratic climate and weak protections for human rights. While many Southern African States have recognised the need for enhanced digital policy and improved access to ICTs for citizens, this is often articulated only in terms of narrow economic objectives and geopolitical positioning, rather than opportunities to advance digital rights and promote the broader public interest.

In view of the identified gaps and challenges across a range of digital rights issues in the region, recommendations are proposed for policymakers, civil society actors, and other stakeholders. The proposed recommendations include legislative and policy reforms, research initiatives, and processes of societal change through advocacy to promote and advance digital rights.

SADC COUNTRIES

INTRODUCTION

Digital rights are a vital and evolving subject in contemporary human rights research and policymaking. This report aims to contribute to existing work on the status of digital rights in Southern Africa and serves as a resource for civil society bodies, public officials, regulatory bodies, and other stakeholders seeking to advance digital rights in the region.

Methodology and objectives

The drafting of this report entailed a comprehensive desktop review of international, regional, and domestic digital rights literature, inclusive of legal and policy documents, research reports, and other scholarly resources.

Through a balanced and nuanced assessment of key topics related to digital rights, this research report aims to achieve four goals:

- To examine digital rights in Southern Africa through the lens of key regional and international human rights laws and standards;
- To assess important trends and developments in respect of digital rights in Southern Africa;
- To identify gaps and challenges to digital rights in the region; and
- To propose recommendations for various stakeholders involved in the advancement of digital rights, including regional bodies, relevant government stakeholders, civil society organisations, and private actors.

Key findings

Key findings documented in this report include:

- Substantial barriers to internet access for many communities, including excessive data costs, unstable supply of electricity, and other social and technological digital divides;
- Notable progress in many Southern African countries to develop data protection laws and policies – though implementation remains a challenge. Overall, there are inadequate domestic and regional frameworks to safeguard personal information and the right to privacy;
- New policies and technologies for the collection of personal information in response to the COVID-19 pandemic have often prompted concerns over insufficient oversight and unknown efficacy of the policies;
- Other impacts of the COVID-19 pandemic on the digital rights landscape, including positive contributions, such as policies to accelerate access to the internet in some sectors, and negative impacts including a deepening of digital divides in other sectors;
- Inadequate lawful safeguards in many countries for the use of communications surveillance by States and insufficient regulation for the use of other emerging technologies, which may impact the right to privacy, freedom of expression online, digital inclusion, and other digital rights;
- Interference with freedom of expression, assembly, and association online by state and nonstate actors, including the use of internet shutdowns;
- Ongoing censorship and attacks on news media, despite statutory protections for freedom of the press; and
- Gaps in research and data on a range of critical digital rights issues in the region, such as inequalities in access, and concerns around safety for vulnerable and marginalised groups such as children, women, and Persons with Disabilities (**PWDs**) as well as those in rural communities.

This report notes progress in many Southern African societies to advance digital rights but there is a need for significant changes in access, policy, infrastructure development, and social practices, to meaningfully fulfil States' commitments to protect and promote digital rights in the region. As a point of departure, **Angola**, **Mozambique**, **Mauritius**, **Namibia** and **Zambia** are the only SADC signatories of the African Union Convention on Cyber Security and Personal Data Protection (**Malabo Convention**), despite the Convention's adoption in June 2014. The internet penetration rate remains comparatively low. In 2020, it was only in the **Seychelles**, **South Africa**, **Mauritius**, and **Botswana** that half the population had access to the internet. Further, there are also patterns of serious digital rights violations in many Southern African countries, which are of grave concern. For instance, there are a couple of examples of unlawful surveillance practices, which

are particularly harmful in the absence of adequate oversight mechanisms. Only eight SADC countries, **Angola, Botswana, Democratic Republic of Congo, Eswatini, Lesotho, South Africa, Namibia, and Zambia** require the appointment of a judge to authorise the interception of communications. Silencing tactics such as the use of Strategic Litigation Against Public Participation (**SLAPP**) suits and network throttling during times of heightened political tensions are still a reality. As of July 2022, the Constitutional Court of **South Africa** is expected to hand down a judgment on the judicial recognition of the SLAPP defence. In **Zimbabwe**, an independent research and advocacy body conducted studies showing deliberate attempts by the State to impede access to social media during what it termed an insurrection in July 2019.[18] Further, with the exception of the **Seychelles** and **Namibia,** media freedom generally deteriorated in SADC during the COVID-19 pandemic.

Examples of positive developments for digital rights include the enactment, albeit delayed, of data protection legislation and policy in many parts of the region, the development of jurisprudence on digital rights, and increased advocacy from civil society actors on this set of rights. Yet, despite these advancements, digital rights violations persist throughout the region. Poor governance over personal data and privacy rights breaches, internet shutdowns, limitations on the freedom of expression, assembly and association online, attacks on the media, and the use of SLAPP suits are just some examples of the concerns which threaten digital rights.

This report also explores the impact on digital rights of the COVID-19 pandemic, which has both occasioned an increase in digitisation and also exposed existing inequalities in digital access and participation. While there is a lack of publicly available data for Southern Africa specifically, between 2019 and 2021, the International Telecommunication Union (**ITU**) recorded a 23% growth in internet use in Africa – an increase, at least in part, attributed to the impact of the pandemic.[19] This increase in digitisation raised concerns about consequent increases in the tracking of data records, social media usage, and users' location.[20] Yet for those without access to the internet, the trend towards digitisation has resulted in even more obstacles to participation in public life, such as education, work, or access to news media. Research shows that these challenges disproportionately affected marginalised groups such as women, children, and PWDs.

18 NetBlocks, 'Zimbabwe internet disruption limits coverage of planned protests,' 31 July 2020, accessible here.

19 ITU, 'Measuring digital development: Facts and figures 2021', 2021, at page 4, accessible here.

20 CIPESA, 'State of Internet Freedom in Africa 2020 – Resetting Digital Rights Amidst the COVID-10 Fallout', September 2020, at page 1, accessible here.

Framing digital rights in Southern Africa

Broadly, digital rights refer to human rights in the digital realm or cyberspace, or in interaction with technology.[21] This framing of digital rights is firmly entrenched in international human rights law. Human rights instruments under the United Nations (**UN**)[22] and in the African human rights framework affirm that the same rights people have offline should also be protected online.[23] These rights are enshrined in several foundational international law instruments, including the Universal Declaration of Human Rights (**UDHR**),[24] the International Covenant on Civil and Political Rights (**ICCPR**),[25] and the African Charter on Human and Peoples' Rights (**the African Charter**).[26] Digital rights have been further developed through the work of regional and international human rights bodies, such as the Joint Declaration on Freedom of Expression and the Internet by the UN Special Rapporteur on Freedom of Opinion and Expression and their regional counterparts in Africa, Europe, and the Americas.[27]

Over the years, digital rights instruments at the regional and domestic levels have been developed throughout Southern Africa. The 2014 African Union (**AU**) Malabo Convention seeks to create a harmonised legal framework for data protection and cybersecurity for all AU Member States.[28] It includes provisions to protect the free flow of personal data, privacy, and associated rights in cyberspace.[29] As of July 2022, the Convention had been ratified by only thirteen AU Member States,[30] five of which are SADC Member States (**Angola, Mozambique, Mauritius, Namibia,** and **Zambia**). Article 36 stipulates that the Convention will enter into force once it has been ratified by at least 15 AU Member States.[31]

---

21 UNHRC, 'The promotion, protection and enjoyment of human rights on the Internet', A/HRC/32/L.20, 2016.

22 *Id.*

23 ACHPR, 'Resolution on the right to freedom of information and expression on the internet in Africa', ACHPR/Res.362(LIX), 2016, accessible here.

24 UN, 'Universal Declaration of Human Rights', 1948.

25 UN General Assembly, 'International Covenant on Civil and Political Rights', 1966.

26 African Charter on Human and People's Rights, accessible here.

27 United Nations, 'Joint Declaration on Freedom of Expression and the Internet', 2011, accessible here.

28 African Union, 'Convention on Cyber Security and Personal Data Protection', 2014, accessible here.

29 *Id.* See Article 8 which notes that the objective of the Malabo Convention is two-fold. First, it requires State Parties to commit themselves to establishing a legal framework which strengthens the protection of physical data and privacy and upholds the principle of free flow of personal data. Second, the Convention is a mechanism to ensure that the processing of data is done in a manner which respects fundamental rights and freedoms, "...while recognising the prerogatives of the States, the rights of local communities and the purposes for which the businesses were established."

30 African Union, 'Status List: List of countries which have signed, ratified/acceded to the Malabo Convention', 23 June 2022, accessible here. At the time of writing, the Convention had been ratified by 13 countries: Angola, Cabo Verde, Congo, Ghana, Guinea, Mozambique, Mauritius, Namibia, Niger, Rwanda, Senegal, Togo, and Zambia.

31 Article 36 of the Malabo Convention states that the Convention will enter into force after 30 days once at least 15 AU Member States have ratified it.

"The tripod of enabling rights – privacy, freedom of expression, and freedom of access to information – existed before the advent of digital technologies. So did the right to dignity and the free, unhindered development of one's personality. Digital technology has however resulted in a huge impact on these rights both off-line and online where, today, netizens generate tens of thousands of more data-sets about themselves than they did two decades ago."

– JOSEPH A. CANNATACI, FORMER UN SPECIAL RAPPORTEUR ON THE RIGHT TO PRIVACY*

* OHCHR, 'Statement by Mr. Joseph A. Cannataci, Special Rapporteur on the right to privacy, at the 31st session of the Human Rights Council', 2017, accessible here.

The 2016 Resolution on the Right to Freedom of Information and Expression on the Internet by the African Commission on Human and Peoples' Rights (**ACHPR**) gives explicit recognition to the importance of digital rights protections to give effect to article 9 of the **African Charter**.[32] Article 9 grants every individual the right to receive information and to express and disseminate their opinions within the law. The Resolution called on States to respect and protect citizens' right to freedom of information and expression through access to the internet.

The 2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa (**ACHPR Declaration**) further developed protections for these rights in the internet age.[33] The Declaration was initially adopted in 2002 and underwent revision in 2019. It sets out 43 principles that anchor the right to freedom of expression and access to information in the digital age and offline. The 2019 ACHPR Declaration essentially consolidates the continent's standards on freedom of expression offline and online. Further, and importantly, it elaborates on the meaning and scope of article 9 of the African Charter.

The Special Rapporteur on Freedom of Expression and Access to Information in Africa (**the Special Rapporteur**) is tasked with, among other things, monitoring Member States' compliance with freedom of expression and access to information standards, and investigating and providing recommendations to the African Commission on systemic violations of freedom of expression and access to information.[34] Since its establishment in 2004, the mechanism has developed normative standards and issued statements on a range of issues that relate to digital rights. These include elections and democratic governance,[35] internet and social media shutdowns,[36] and the importance of these rights amidst the COVID-19 pandemic.[37]

While Southern African States recognise the need for enhanced digital policy and improved access to ICTs, this is often articulated in terms of economic objectives and geopolitical positioning, rather than in terms of equally important – and often complementary – goals of advancing digital rights, empowering all people, and strengthening of democratic institutions.[38]

---

32 ACHPR, 'Resolution on the Right to Freedom of Information and Expression on the Internet in Africa,' ACHPR'ACHPR/Res. 362(LIX), 2016, accessible here.

33 ACHPR, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa', 2019, accessible here.

34 See ACHPR 'Special Rapporteur on Freedom of Expression and Access to Information' webpage, accessible here.

35 ACHPR, 'Special Rapporteur on Freedom of Expression and Access to Information in Africa, Guidelines on access to information and elections in Africa', 2017, accessible here.

36 ACHPR, 'Special Rapporteur on Freedom of Expression and Access to Information in Africa on the Continuing Trend of Internet and Social Media Shutdowns in Africa, 2019: Press Release', 1 July 2022, accessible here.

37 ACHPR, 'Special Rapporteur on Freedom of Expression and Access to Information in Africa: Statement on the Importance of Access to the Internet in Responding to the COVID-19 Pandemic, 2020', accessible here.

38 See for example, SADC, 'e-SADC strategic framework', 2010, accessible here.

INTERNET ACCESS

Internet access at a glance:

- Inadequate access to the internet is a huge obstacle to the fulfilment of digital rights in Southern Africa.
- Costs associated with internet access remain excessive in parts of the region, placing a serious barrier to access especially for indigent communities.
- While policymakers have recognised the risks of a gender-specific digital divide, there has been a lack of decisive policy initiatives to address it.

Although there is presently no express right to the internet under international and regional law, there is consensus that the internet enables a host of other human rights. These include, but are not limited to, the rights to freedom of expression, access to information, freedom of assembly, freedom of thought, and education, as well as cultural and religious rights.[39] Despite this consensus, many Southern African countries have concerningly low internet access rates,[40] which is an indicator of a significant digital divide in the region. Consequently, this may result in a violation of the various human rights cited above.

Statistics from the International Telecommunication Union (**ITU**) suggest that only four countries in the SADC region (**Seychelles**, **South Africa, Mauritius,** and **Botswana**) had internet access for more than half the population in 2020. In many SADC countries, the reported access rate was 30% or less. (See Table 1.)

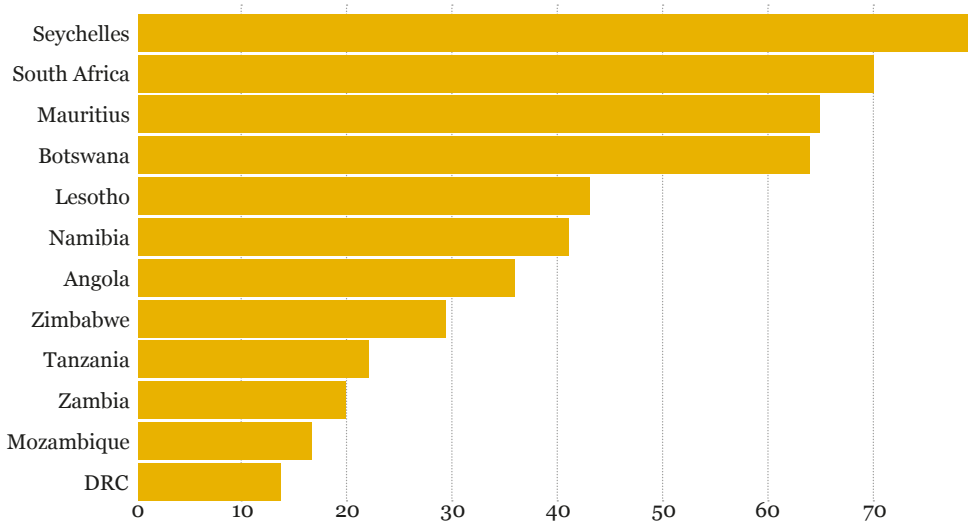


TABLE 1: *PERCENTAGE OF POPULATION WITH INTERNET ACCESS IN 2020, ITU WORLD TELECOMMUNICATION/ICT INDICATORS DATABASE*

39 Preamble of African Declaration on Internet Rights and Freedoms, accessible here.
40 Research ICT Africa, 'SADC not bridging digital divide', Policy Brief 6, 2017, accessible here.

More encouraging data exists on access to mobile phones in the region. In 2021, Sub-Saharan Africa saw the biggest increase in mobile broadband coverage globally, but it still stands at 19%.[41] However, many SADC countries report a high rate of mobile phone access, with seven SADC countries reporting more mobile phone subscriptions than people as highlighted in Table 2.

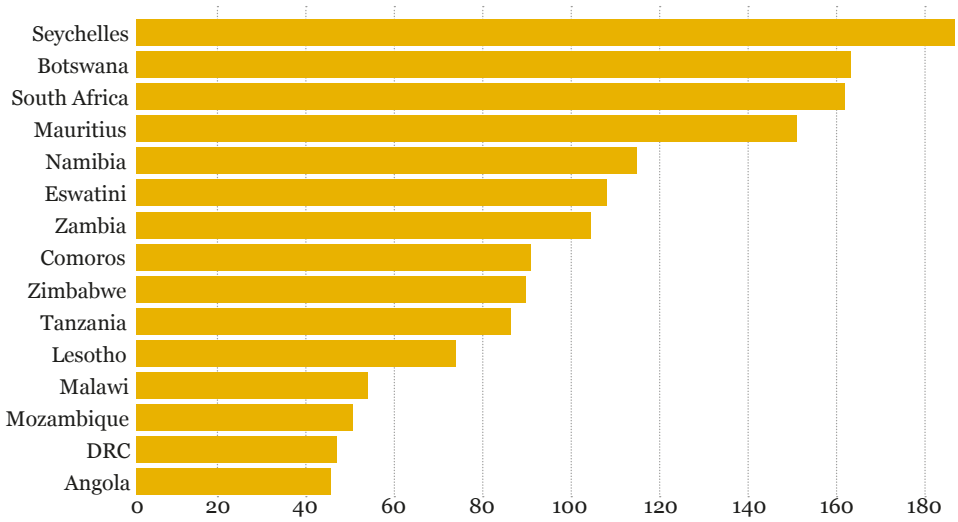


TABLE 2: *MOBILE PHONE SUBSCRIPTIONS PER 100 PEOPLE IN SADC COUNTRIES, ITU WORLD TELECOMMUNICATION/ICT INDICATORS DATABASE*

Yet, in order for the right of access to be progressively realised, mere access to the internet and telecommunications is not sufficient; instead, countries need to examine whether there is meaningful access. Meaningful access to the internet requires an assessment of factors such as connectivity, affordability, access to the necessary devices, and digital literacy skills. While some African States grapple with these challenges, they are not insurmountable. Below are the causes of these challenges.

The state of ICT infrastructure

Much of Southern Africa faces the same challenges as the rest of Africa in terms of the lack of enabling infrastructure, such as hardware, software, and networking components.[42] The necessity of reliable infrastructure was particularly emphasised after the onset of the COVID-19 pandemic in 2020, as it highlighted several divides along the lines of gender, economic status, and rural-urban communities when it comes to access to broadband.[43]

41 The GSMA, 'The State of Mobile Internet Connectivity 2021', at page 6, accessible here.
42 Alex Makulilo, 'Privacy and data protection in Africa: a state of the art, International Data and Privacy Law', 2012, Volume 2, No. 3, at page 164.
43 OECD, 'Digital transformation in the age of COVID-19', 2020, at page 4, accessible here.

Further, the lack of consistent access to electricity continues to impede access to the internet in the region. Sustainable Development Goal (**SDG**) 7 calls for universal access to reliable, affordable, and modern energy sources. Yet, this is far from a reality in Africa. It has been reported that 45% of African households reside further than 10 kilometres from the nearest network infrastructure.[44] The internet penetration rate in **Zimbabwe's** rural and peri-urban areas is particularly impacted by a lack of enabling infrastructure.[45] The country's national electricity supplier, Zimbabwe Electrical Supply Authority (**ZESA**), interminably implements power outages.[46] The country's largest mobile operator, Econet Wireless reported difficulty with maintaining its network.[47] In 2019, half of the **Mozambican** population did not have access to electricity.[48] The **Zambian** situation is also dire. Less than 6% of the Zambian population has access to electricity.[49] Since 2007, **South Africa's** state-owned electricity supplier, Eskom, has implemented loadshedding - scheduled power outages to deal with an inability to meet demand. Loadshedding has been linked to a history of mismanagement and lack of long-term investment by Eskom.[50] As of July 2022, Eskom was estimated to record its most severe year of loadshedding as it had cut 2 276 gigawatt-hours of electricity (at the halfway mark of the year), which is slightly lower than the 2 521 gigawatt-hours it cut during the entirety of 2021.[51] Electricity woes aside, in **South Africa**, there is generally a higher rate of internet penetration. However, the notable inadequacies in infrastructure provision are, in part linked to the legacy of apartheid.[52] These infrastructure deficiencies compromise access to the internet and related technologies that enable the exercise of digital rights. A case in point is that of the education sector in which, under the apartheid system, white-owned and dominated middle-class schools were better resourced and this resulted in infrastructure backlogs that are still present in public schools.[53]

---

44 Paul Kimumwe, 'Towards an Accessible and Affordable Internet in Africa: Key Challenges Ahead', CIPESA, accessible here.
45 *Id.*
46 *Id.*
47 Nelson Banya, 'Power crisis turns night into day for Zimbabwe's firms and families', Reuters, 1 August 2019, accessible here.
48 Above n44 at page 4.
49 *Id* at page 5.
50 Marta Nowakowska and Agnieszka Tubis, 'Loadshedding and the energy security of Republic of South Africa', October 2015, at page 106, accessible here.
51 Bloomberg, 'Eskom nears record for worst year of loadshedding ever - and there's still 6 months to go', 2 July 2022, accessible here.
52 ALT Advisory *et al,* 'Access denied: Internet in Schools', 2020, at page 25, accessible here.
53 *Id* at page 25.

Affordability

Comparative to other continents, and with the exception of North America, the cost of mobile data in Africa is the least affordable.[54] However, even in comparison to North America, in November 2020 the ITU reported that since incomes in Africa are low, the cost of data is even more disproportionate.[55] Mobile data costs in Botswana, for example, account for 2% to 3% of Gross National Income (**GNI**) per capita.[56]

Costs have fallen significantly across Southern Africa in recent years, although this does not necessarily render data affordable. Data collected by Research ICT Africa suggests that the average price for 1GB of data across SADC markets fell from over US$10 in 2016 to less than $5 by 2020.[57] There are big price differences from country to country. In 2020, 1GB of mobile data costs less than US$2 in **Mozambique**, and less than US$2.50 in **Tanzania** and **Zambia**, while in **Eswatini** and **Namibia,** 1GB cost as much as US$10.[58] Excessive data prices have been attributed to poor infrastructure, which may necessitate costly upgrades and investments (such as upgrades to 5G), and the limited pool of telecommunications companies in the market, which reduces competition.[59] Further, the low-income status of many communities across the region leads to a higher ratio of spending on items such as mobile phones and data.[60]

Digital divide and non-discrimination

In addition to what has been outlined above, there are other factors which exacerbate barriers to access for specific demographics, including women and children, rural communities, and PWDs. These factors include illiteracy, inherent biases in the technology industry, and social, cultural, and economic norms which reinforce harmful divisions.[61]

2.3.1 Gender digital divide

From an educational standpoint, there is generally a lower enrolment rate for girls in modules that would enhance their digital and technological literacy skills, for instance, Science, Technology, Engineering, and Mathematics (**STEM**) and ICTs.[62] There is ample data on how the gender digital divide widens the gap of inequality, particularly in disadvantaged areas. In Africa, women are less likely to have a smartphone and internet access when

54 DW, 'Why mobile internet is so expensive in some African nations', undated, accessible here.
55 *Id.*
56 ITU, 'Digital trends in Africa 2021: Information and communication technology trends and developments in the Africa region 2017 - 2020', 2021, at page 14, accessible here.
57 Authors' own analysis from data provided by Research ICT Africa, 'Cheapest prepaid broadband product by country (in USD)', accessible here.
58 *Id.*
59 DW, 'Why mobile internet is so expensive in some African nations', undated, accessible here.
60 *Id.*
61 Above n 43 at page 11.
62 *Id.*

compared to men.[63] While there is limited data on gender disparities in ICT in Southern Africa, country surveys in **South Africa, Tanzania, Mozambique,** and **Lesotho** consistently found that women are less likely to have internet access, smartphones, and social media than men.[64] Additional research suggests that 14% of women in Sub-Saharan Africa are less likely to own a basic mobile phone and that 34% of women are less likely to own a smartphone with internet connectivity capabilities.[65] On a positive note, there are some States in SADC, namely, **Mauritius**, **Namibia,** and **South Africa** which have been recorded as having the fastest-growing regular internet use by women.[66]

In 2001, the SADC passed its Declaration on Information and Communications Technology (**SADC Declaration**).[67] **Comoros** is the only SADC country that is not a signatory to the SADC Declaration. The SADC Declaration aims to bridge the digital gender divide with three areas of action: community participation and governance, ICT in business development, and human resources capacity for ICT development.[68] Importantly, the SADC Declaration also recognises that the digital divide does not only manifest itself economically or technologically but also culturally. In 2019, the SADC hosted its first gender workshop in Johannesburg, **South Africa**, with a session dedicated to the use of technology to advance the financial inclusion of women.[69] Two conclusions drawn from the session were that empowering women by closing the digital gender divide would ripple into the greater community and that support from regulators is needed.

2.3.2 Rural-urban digital divide

Low internet connectivity rates in Southern Africa should be assessed through an intersectional lens, which goes beyond gender barriers. It is well-documented that the digital divide is also significant along class and economic lines, owing to disproportionate levels of development between urban, peri-urban, and rural areas.[70] The extent of rural-urban digital divides in the region remains relatively under-researched, but the available data paints a worrying picture. For example, in 2021, the **ITU** estimated that for Africa as a whole, close to 30% of its rural populations lacked access to mobile broadband coverage, and 18% had no mobile network coverage at all.[71] The ITU estimated that Africa had the most significant urban-rural divide of any region, with an estimated 50% of urban

63 *Id* at page 13.
64 Research ICT Africa, 'After Access survey presentation', IGF, 2017, accessible here.
65 Organisation for Economic Co-operation and Development (OECD), 2018, 'Bridging the Digital Gender Divide: Include, Upskill, Innovate', accessible here.
66 Afrobarometer, 'Africa's digital gender divide may be widening, Afrobarometer survey finds', 4 November 2019, at page 4, accessible here.
67 SADC, 'Declaration on Information and Communications Technology (**ICT**)', 2001, accessible here.
68 *Id.*
69 SADC, 'Report of the First SADC Gender Workshop Held on 28 – 29 March 2018 in Johannesburg, South Africa', at page 2, accessible here.
70 Lester Henry, 'Bridging the urban-rural digital divide and mobilizing technology for poverty eradication: challenges and gaps', 2017, accessible here.
71 ITU, 'Measuring digital development: Facts and figures 2021', 2021, at page 12, accessible here.

populations using the internet compared to 15% of rural populations.[72] Country-specific data further suggests that a rural-urban digital divide persists. For example, in **Angola**, communities living in rural areas are less likely to be in a position to access the internet due to high costs and lower quality infrastructure and services.[73] In **Malawi**, the geographic location creates a notable digital divide, with an estimated 9.3% of people in rural areas having access to the internet compared to 40.7% of those based in urban settings.[74]

Recommendations

- State actors should pursue more stringent policies to reduce mobile data costs, with due regard to inflation.
- There is a need for growth in the pool of (grassroots) Internet Service Providers (**ISPs**) which prioritise affordability over profit.
- Innovative and easy-to-maintain infrastructure should be introduced in peri-urban and rural communities.
- The establishment of dedicated agencies and bodies tasked with gender-mainstreaming in STEM.
- Alternative sources of energy should be explored and adopted to enhance access to the internet.
- Introduction of digital literacy programmes targeting vulnerable and marginalised groups.

72 *Id* at page 6.
73 Freedom House, 'Freedom of the Net 2021: Angola', 2021, accessible here.
74 *Id.*

PRIVACY AND DATA PROTECTION

Data Protection at a glance:

- While the region lags in adopting data protection laws, positive steps have been noted in recent years.
- The poor implementation of existing laws infringes on citizens' rights to adequate data protection.
- Poor resourcing for data protection institutions is another obstacle to effective implementation.

As of 2022, 61% of African States have enacted data protection and privacy legislation.[75] Despite debates on whether 'privacy' and 'data protection' are interchangeable terms,[76] the two should certainly be viewed in tandem. From a regional standpoint, the right to privacy has often been couched in vague terms. The African Charter, for example, does not expressly provide for the right to privacy, despite being the continent's primary binding human rights instrument. However, human rights groups have argued that the right to privacy is a crucial component of other basic rights embedded in the African Charter, such as the right to dignity, the right to access information, and free expression.[77] Several other regional instruments provide for the right to privacy and data protection, including in the ACHPR 2019 Declaration. These instruments are considered below.

Regional standards on data protection

Through the ACHPR 2019 Declaration, the African Commission adopted a progressive stance on privacy and data protection. The key provisions are noted hereunder.

- Principle 40. Privacy and the protection of personal information provides:

> *"1. Everyone has the right to privacy, including the confidentiality of their communications and the protection of their personal information.*
>
> *2. Everyone has the right to communicate anonymously or use pseudonyms on the internet and to secure the confidentiality of their communications and personal information from access by third parties through the aid of digital technologies.*
>
> *3. States shall not adopt laws or other measures prohibiting or weakening encryption, including backdoors, keys escrows, and data localisation requirements unless such measures are justifiable and compatible with international human rights law and standards."*

75 United Nations Conference on Trade and Development, 'Data Protection and Privacy Legislation Worldwide', 2021, accessible here.

76 Above n48 at page 164.

77 Legal Resources Centre, 'Statement to the African Commission on Human and Peoples' Rights', 2018, accessible here.

- Principle 41: Privacy and communication surveillance, provides:

  "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 with 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:

    a. the prior authorisation of an independent and impartial judicial authority;

    b. due process safeguards;

    c. specific limitation on the time, manner, place and scope of the surveillance;

    d. notification of the decision authorising surveillance within a reasonable time of the conclusion of such surveillance;

    e. proactive transparency on the nature and scope of its use; and

    f. effective monitoring and regular review by an independent oversight mechanism."

- Principle 42: Legal framework for the protection of personal information, provides:

  1. States shall adopt laws for the protection of personal information of individuals in accordance with international human rights law and standards.

  2. The processing of personal information shall by law be:

    a. with the consent of the individual concerned;

    b. conducted in a lawful and fair manner;

    c. in accordance with the purpose for which it was collected, and adequate, relevant, and not excessive;

    d. accurate and updated, and were incomplete, erased or rectified;

    e. transparent and disclose the personal information held, and

    f. confidential and kept secure at all times.

  3. States shall ensure, in relation to the processing of a person's personal information, that the person has the rights to:

    a. be informed in detail about the processing;

    b. access personal information that has been or is being processed;

    c. object to the processing; and

d. rectify, complete or erase personal information that is inaccurate, incomplete or prohibited from the collection, use, disclosure or storage.

4. Every person shall have the right to exercise autonomy in relation to their personal information by law and to obtain and reuse their personal information, across multiple services, by moving, copying or transferring it.

5. Any person whose personal information has been accessed by an unauthorised person has the right to be notified of this fact within a reasonable period and of the identity of the unauthorised person unless such identity cannot be established.

6. The harmful sharing of personal information, such as child sexual abuse or the non-consensual sharing of intimate images, shall be established as offences punishable by law.

7. Every individual shall have legal recourse to effective remedies in relation to the violation of their privacy and the unlawful processing of their personal information.

8. Oversight mechanisms for the protection of communication and personal information shall be established by law as independent entities and include human rights and privacy experts."

The African Commission's 2016 Resolution on the Right to Freedom of Information and Expression on the Internet also expressly recognised that privacy online "*is important for the realization of the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association.*"[78]

The Malabo Convention, adopted in 2014, provides a framework for e-transactions, cyber security, and personal data protection. 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.[79] As outlined in section 1, as of July 2022, the Malabo Convention still required at least two more ratifications to come into force. Given that the Convention was adopted in 2014, it is presently outdated and has received criticisms on certain aspects which are vague, for example, its criminalisation of "insulting language".[80]

- The SADC Model Law on Data Protection is not a binding instrument but provides guidance to States on the essential components of data protection legislation to prevent violations.[81] The Model Law, in its preamble, recognises that data protection is fundamental to the protection of an individual and to "*...the construction of well-being*."

78 Above n 23.
79 Article 25 of the African Union Convention on Cyber Security and Personal Data Protection (**Malabo Convention**), accessible here.
80 Article 3(g) of the Malabo Convention.
81 SADC, 'Data Protection: Southern African Development Community Model Law', 2013, accessible here.

Additionally, children's rights to privacy and data protection find expression in a variety of regional instruments, including the ACHPR 2019 Declaration, the African Charter on the Rights and Welfare of the Child (**ACRWC**),[82] which is the principal regional treaty protecting children's rights in Africa, and through the ongoing work of the African Committee of Experts on the Rights and Welfare of the Child (**ACERWC**). The Committee was established in 2001 and derives its mandate from the ACRWC.[83] Composed of 11 experts, the Committee's main responsibility is to protect the rights and welfare of children in Africa in accordance with the ACRWC. Its responsibilities have been described as both promotional and protective.[84] In 2016, the Committee adopted Africa's Agenda for Children 2040 (**Agenda 2040**),[85] which lists ten aspirations for States to achieve by 2040. Although none of the aspirations speaks directly to protecting children as they navigate digital spaces, one could read this into, for example, the following aspirations

- Aspiration 2: an effective child-friendly national legislative, policy, and institutional framework is in place in all Member States.
- Aspiration 4: Every child survives and has a healthy childhood.
- Aspiration 6: Every child benefits fully from quality education.
- Aspiration 7: Every child is protected against violence, exploitation, neglect, and abuse.
- Aspiration 10: African children's views matter

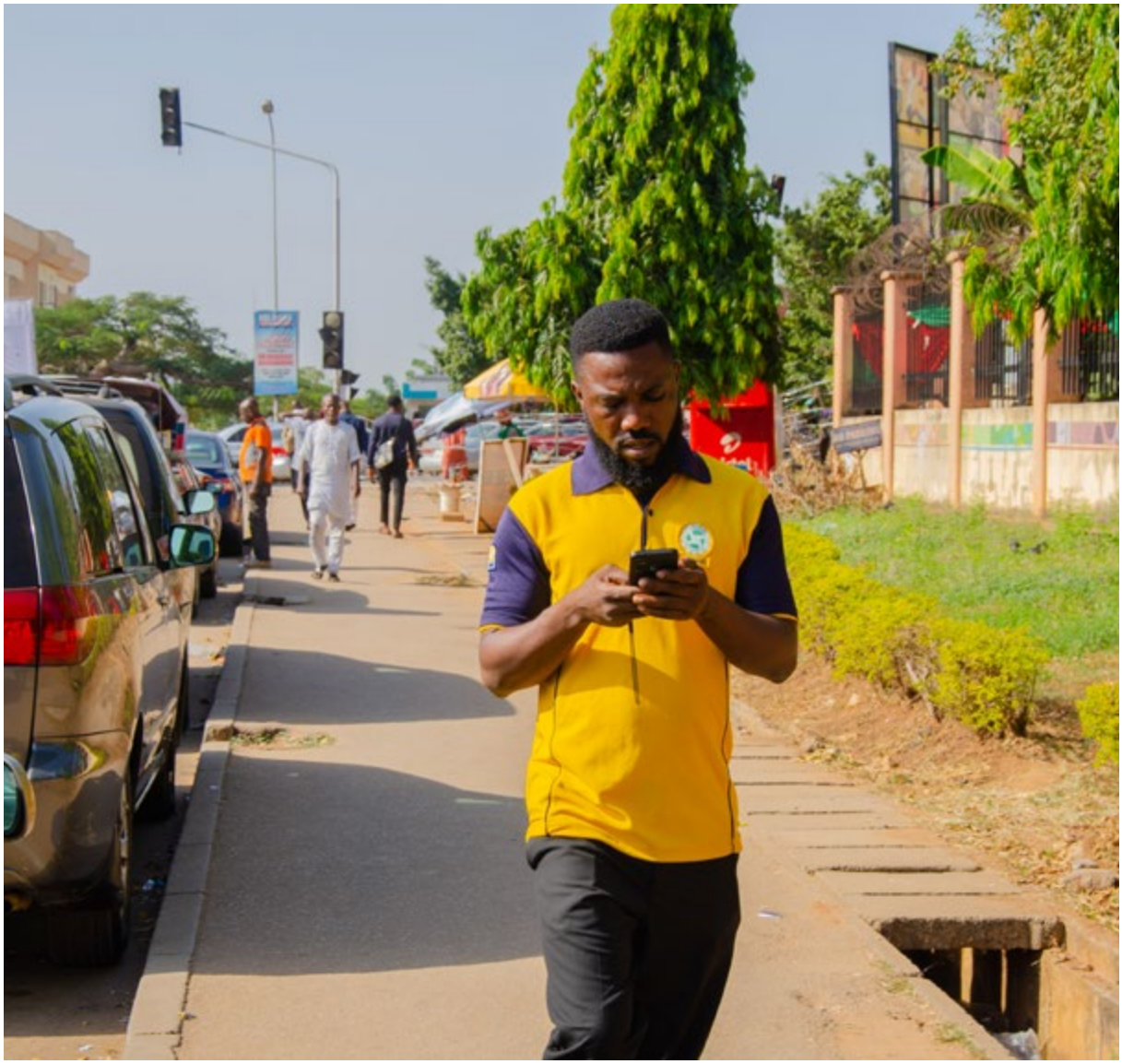
In March 2022, the Committee's Working Group on Children's Rights and Business adopted a resolution on the Protection and Promotion of Children's Rights in the Digital Sphere in Africa.[86] Significantly, the Resolution calls on States to, amongst other things, report to the Committee on the domestic measures taken to protect children in the digital age; to enact legislation, and establish regulatory bodies that place responsibilities on the private sector for the protection of children in advertising and marketing practices; to facilitate cross-border collaboration to support survivors of online child sexual exploitation (**OCSE**).

The overall picture of children's digital rights in Southern Africa is explored in section 7 of this report.

82 African Union, 'African Charter on the Rights and Welfare of the Child', 1990, accessible here.
83 See Articles 32 to 46 which deal with the establishment and organisation of the Committee including *inter alia* its composition, the election of its members, terms of office, and the appointment of a secretariat.
84 Ulkrie Kahbila Mbuton, 'The role of the African Committee of Experts on the Rights and Welfare of the Child in the follow-up of its decisions on communications', University of Pretoria, 2017, accessible here.
85 African Committee of Experts on the Rights and Welfare of the Child, 'Africa's Agenda for Children 2040,' 2016, accessible here.
86 ACERWC, 'The Protection and Promotion of Children's Rights in the Digital Sphere in Africa', Resolution No. 17/2022, accessible here.

National standards and oversight mechanisms on data protection

Constitutions in Southern Africa protect the right to privacy. The countries (listed in the table below) in Southern Africa have enacted data protection legislation giving effect to the right to privacy through data protection legislation (see Table 3). These laws typically contain standard data provisions including minimum requirements for consent, data minimisation, objection provisions by data subjects, limitations on data retention, the notification of data subjects, as well as remedies in case of a breach. At the time of publication, many of the laws are regarded as non-compliant with international human rights standards.[87] For instance, some of the laws enacted do not properly establish oversight mechanisms and they fall short when it comes to remedies.



87 CIPESA, 'Mapping and analysis of privacy laws in Africa in 2021', 2021, at page 8, accessible here.

Table depicting data protection legislation in SADC:

Country	Data protection legislation	Status
Angola	Laws No. 22/11, 2011[88]	Passed
Botswana	Data Protection Act, 2018[89]	Passed
Comoros	N/A	N/A
Democratic Republic of Congo	N/A	N/A
Eswatini	Data Protection Act, 2022[90]	Passed
Lesotho	Data Protection Act, 2012[91]	Passed
Madagascar	Law No. 2014-038 (DP Law), 2015[92]	Passed
Malawi	Data Protection Bill, 2021[93]	In progress
Mauritius	Data Protection Act, 2017[94]	Passed
Mozambique	N/A	N/A
Namibia	Draft reportedly in progress	N/A
Seychelles	Data Protection Act, 2003[95]	Passed, but not in force
South Africa	Protection of Personal Information Act, 2013[96]	Passed
Tanzania	Draft reportedly in progress.	N/A
Zambia	Data Protection Act, 2021[97]	Passed
Zimbabwe	Data Protection Act, 2021[98]	Passed

TABLE 3: *STATUS OF DATA PROTECTION LEGISLATION IN SADC*

88 Laws No. 22/11, 2011, accessible here.
89 Data Protection Act, 2018, accessible here.
90 Data Protection Act, 2022, accessible here.
91 Data Protection Act, 2012, accessible here.
92 Law No. 2014-038 (DP Law), 2015, accessible here.
93 Data Protection Bill, 2021, accessible here.
94 Data Protection Act, 2017, accessible here.
95 Data Protection Act, 2003, accessible here.
96 Protection of Personal Information Act, 2013, accessible here.
97 Data Protection Act, 2021, accessible here.
98 Data Protection Act, 2021, accessible here.

Although the development of data protection laws in Southern Africa lagged behind many parts of the world, the region has made significant progress in recent years, particularly since 2020. **Zambia** and **Zimbabwe** enacted their data protection laws in 2021,[99] and **Eswatini** enacted the law in 2022.

However, data protection laws in the region have often shown a track record of 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.[100] **South Africa's** data protection law,[101] the Protection of Personal Information Act (**POPIA**), was signed into law in 2013.[102] Its different provisions came into force incrementally until the entire Act came into effect in July 2021.[103] During this period, the lack of funding and operational capacity of South Africa's DPA, the Information Regulator, became a source of public frustration for civil society bodies, Members of Parliament, and members of the Information Regulator itself.[104]

Among those countries without a data protection law in place, the **Democratic Republic of Congo** has opted for a slightly divergent approach by adopting a Digital Code which includes provisions relating to data protection; however, limited information is available on progress made towards its implementation.[105]

Recommendations:

- Data protection authorities should be adequately resourced, staffed with skilled personnel, and subject to capacity building at a national and regional level.
- More consistent intervention and guidance from the ACHPR on how Member States should implement the ACHPR 2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa.

99 Aisaatou Sylla, 'Recent developments in African data protection laws – Outlook for 2022', 1 February 2022, accessible here.
100 ALT Advisory, Data Protection Africa: Angola Factsheet, 2020, accessible here.
101 Brian Daigle, 'Data Protection Laws in Africa: A Pan-African Survey and Noted Trends', 2021, at page 7, accessible here.
102 *Id.*
103 ALT Advisory, 'Data Protection Africa: South Africa Factsheet, 2021', 2021, accessible here.
104 Parliamentary Monitoring Group, 'Meeting minutes: Portfolio Committee on Justice and Correctional Services', 2019, accessible here.
105 Lexology and Hogan Lovells, 'Recent developments in African data protection laws – Outlook for 2022', undated, accessible here.

REGULATION OF EMERGING TECHNOLOGIES

Emerging technologies at a glance:

- Lack of clear regulation for new and emerging technologies may result in the infringement of privacy rights, exacerbate existing digital divides, and enable private technology developers to operate in legal grey areas or pre-empt policymaking.
- States often treat new technologies as 'silver bullets' to a range of policy problems, which leads to uncritical endorsement of complex technologies such as artificial intelligence **(AI)** or biometrics, with limited attention to potential risks to human rights.
- Despite significant progress in developing data protection legislation, most States' legal frameworks and practices on surveillance and associated technologies are extremely fragmented, vague, and in contradiction with international standards.

States and policymakers across the world are navigating the appropriate use of emergent technologies. These include explicitly invasive technologies, such as those used for communications interception, security, and policing, and technologies that industry actors and policymakers may see as benign or for civic good. However, these technologies pose certain risks to human rights, as is the case for many uses of AI and biometric technology.

In recent years, increased awareness about bulk interception of communications and the abuse of surveillance technologies has highlighted severe implications for the right to privacy, freedom of expression, and other digital rights, especially in light of mounting examples of state and non-state actors using surveillance technology.[106] This section examines the regulatory landscape for a variety of emergent technologies in Southern Africa, such as those which are used for surveillance and interception of communications and the collection of health data and other personal information during the COVID-19 pandemic. It also considers the use of facial recognition technology, biometrics, and artificial intelligence.

The novel and dynamic nature of these technologies presents an inherent challenge for regulation, both through international and regional instruments, and domestic law and policy. One notable measure is the Budapest Convention on Cybercrime,[107] which seeks to create a harmonised international framework for domestic cybercrime laws. Parties to the Convention are required to develop domestic laws which establish certain cybercrime offences, including 'hacking' offences, child sexual abuse material, and copyright infringements. The Convention also requires domestic laws to contain minimum safeguards to protect freedom of expression, the right to privacy, and other digital rights, from infringement during investigations.[108] Although the Convention does not regulate

106 Above n 82 at page 8.
107 Council of Europe, 'Convention on Cybercrime (ETS No. 185),' 2001, accessible here.
108 *Id* at Article 15.

specific types of technology, it prohibits certain uses for the technology. For example, in terms of offences defined under the Convention, national laws should prohibit the use of any technology to gain illegal access to a computer system, or to illegally intercept computer data, if the act was "without right" or with "dishonest intent".[109] It should be noted that although article 15 of the Convention requires safeguards for human rights in the enforcement of domestic cybercrime law, no further guidance or detail is given on how this should be approached by States.[110] Only one Southern African country, **Mauritius**, is currently a party to the Convention, with **South Africa** being listed among the parties who have been invited to accede.[111]

Regionally, the ACHPR Resolution 473, adopted in 2021, addresses the use of AI, robotics, and other emerging technologies in order to mitigate human rights violations.[112] Through the Resolution, albeit brief, the Commission calls on States, and in some instances the AU, to take various steps towards the regulation of these technologies. These steps include:

- ensuring that the development of these technologies is compatible with the rights and duties contained in the African Charter and other regional and human rights instruments;
- ensuring that imported technologies for the African context and Africa's needs given the prevalence of global epistemic injustice;
- ensuring that there is transparency when such technologies make an automated decision;
- creating comprehensive legal and ethical governance frameworks;
- for the AU to rapidly place these technologies on its agenda and work towards developing a regional regulatory framework;
- ensuring that these technologies remain under meaningful human control to avert any threats they may post; and
- to commit to undertaking a study to further develop guidelines which pertain to AI, robotics, and other new and emerging technologies.

109 *Id* at Articles 2 and 3.
110 Human Rights Watch, 'Abuse of Cybercrime Measures Taints UN Talks', 2021, accessible here.
111 Council of Europe, 'Parties/Observers to the Budapest Convention', n.d., accessible here.
112 ACHPR, 'Resolution on the need to undertake a Study on human and people's rights and artificial intelligence (AI), robotics and other new and emerging technologies in Africa'. ACHPR/Res. 473(Ext.OS/XXXI)2021, accessible here.

Surveillance and interception of communications

It is a basic feature of modern human rights law that States' capacity to intercept communications and conduct digital surveillance may only be used in highly restricted ways. Such conduct may only be justifiable to combat the most serious crimes and national security threats, and only with adequate safeguards, oversight, and transparency. This is articulated in principle 41 of the ACHPR Declaration, concerning privacy and communication surveillance (see textbox).

ACHPR 2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa

Principle 41

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 with 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.*

Such safeguards include the prior authorisation of any interception of communications by a judge; the provision of various safeguards for due process; post-surveillance notification; adequate transparency; and the monitoring of operations by an independent oversight mechanism.

Numerous examples of how States both in the region and elsewhere abuse their surveillance powers in ways that violate the right to privacy (and other civil rights) elucidate the need for safeguards. Without appropriate safeguards, such violations cast a chilling effect on freedom of expression, and may generally undermine the democratic climate. Existing research on surveillance in Southern Africa documented evidence and suspicion of such abuses in many parts of the region, and that the most common targets are journalists, opposition politicians, and human rights activists and groups.[113] A few noteworthy features are highlighted here.

First, the majority of surveillance laws in the region are woefully out of step with regional and international standards (see Table 4). Only 8 of 12 SADC countries surveyed (**Angola, Botswana, Democratic Republic of Congo, Eswatini, Lesotho, South Africa, Namibia, and Zambia**) had any legal requirement for a judge or court to authorize the interception of communications, which is considered a basic oversight feature of

113 Murray Hunter and Admire Mare, 'A Patchwork for Privacy: Mapping communications surveillance laws in Southern Africa', 2020, at page 6, accessible here.

interception laws. With the exception of **Angola** and **South Africa**, the laws surveyed typically did not have any semblance of proportionality, in that they do not restrict the use of interception to investigations of more serious criminal offences. **Eswatini** recently passed a law enabling and regulating the state's right to conduct communications surveillance.[114]

	Is there a law?	Is there judicial oversight?		Is it restricted to serious offences?	Is there user notification?	Are metadata and content given equal protection?	Does law require metadata t o be retained?	SIM registration?
		Police	Intel					
South Africa				*	†		36 Months	
DRC								
Tanzania		*						
Angola				*				
Mozambique	*							
Malawi								
Zambia							3 Months	
Zimbabwe							6 Months*	
Namibia	*							
Botswana								
Lesotho		*					36 Months†	
Eswatini								

Yes
No

* Only access to content is restricted o serious offences. Metadata may be accessed for any offence

† Courts may overturn this

* Except using the terror law

*Restricted to offences with a maximum prison penalty of more than two years

*There is a law but it is deemed non-functional

* De facto – no clear legal provision

* There is a law but it is only partly implemented

* Some scope for warrantless access

† De facto – no clear legal provision

TABLE 4: *SOUTHERN AFRICAN SURVEILLANCE LAWS*[115]

114 Computer Crime and Cybercrime Act No.6 of 2022, accessible here.
115 Above n 114 at page 6.

While there is limited information about States' actual surveillance capacities, due to the lack of transparency in this sector, there is evidence that some Southern African States use emerging surveillance technologies without regulation. In 2020, researchers found evidence that the governments of **Botswana**, **Zambia**, and **Zimbabwe,** were clients of an Israeli spyware firm, Circles.[116] Previous research found evidence that **Mozambique** and **Zambia** may have been clients of the NSO Group, a related spyware firm that developed the military-grade spyware known as Pegasus.[117] **Zambia** is also among a growing list of African States whose relationship with Chinese communications giant Huawei has raised suspicions of surveillance trade after it was reported that Huawei technicians tracked and intercepted digital communications of suspected criminals, opposition politicians, and dissident bloggers for Zambian authorities.[118] These incidents highlight a worrying lack of controls, both domestically, regionally, and internationally, on the export, procurement, and use of such surveillance tools.

A few positive developments should be noted on surveillance issues in the region. In 2021, **South Africa's** Constitutional Court struck down several provisions in the country's interception law, the Regulation of Interception of Communication and Provision of Communication-Related Information Act (**RICA**), as unconstitutional.[119] The court ordered the law to be amended to improve oversight and protections against abuse in state surveillance operations, including the right for targets of surveillance to be notified after the fact, greater safeguards of management of data obtained through surveillance, and the need for specific protections when the subject under surveillance is a lawyer or journalist.

The grounds on which the South African Constitutional Court's declared the RICA unconstitutional:

- Failure to provide safeguards to ensure that a sufficiently independent judge is designated for oversight;
- Failure to provide safeguards specifically for surveillance targets who have a professional duty to confidentiality, such as a practising lawyer or journalist;
- Absence of post-surveillance notification;
- Failure to include safeguards to address *ex parte* requests or directions for interception; and
- Absence of procedures to ensure proper management of surveillance data.

116 Marczak, Scott-Railton and others 'Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles' Citizen Lab Research Report No. 133, 2020, accessible here.

117 Marczak, Scott-Railton and others 'Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries', Citizen Lab Research Report No. 113, 2018, accessible here.

118 Wall Street Journal 'Huawei technicians helped African governments spy on political opponents' 2019, accessible here.

119 *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others* (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) 2021.

In 2022, due to pressure from media freedom groups, **Botswana's** new Bill on police interception powers was amended to include a requirement for prior approval from a judge in all police surveillance operations to prohibit warrantless and arbitrary interception.[120]

Technology and COVID-19

The COVID-19 pandemic prompted the widespread introduction of digital contact-tracing (**DCT**) applications and other technologies to automate contact tracing, monitor or enforce stay-at-home orders, and otherwise bolster public responses to the pandemic. By May 2020, at least 40 countries had decided to use DCT applications.[121] These technologies have simultaneously been praised for their role in using digital technology to improve health outcomes and criticised for potentially violating privacy rights and exacerbating digital divides.[122] The use of digital contact tracing was in line with global public health guidelines and the Africa Centres for Disease Control and Prevention (**CDC**) recommended contact tracing to help limit the spread of COVID-19 and advised States to use "the characteristics of the epidemic in their country to decide when and how to do contact tracing."[123] Moreover, the CDC Guidance stated that at the time it was prepared, there was no clear evidence-based threshold for contract tracing to be reduced or halted.

However, the digital rights impact and public health efficacy of each specific DCT tool is often a subject of debate.[124] Observers noted a tendency for technological solutions to be embraced uncritically.[125]

In June 2020, **Botswana** launched the Bsafe contact tracing app, which was donated to the government by a local company.[126] The app allowed for digital registration and checking infection statuses through the use of QR codes.[127] Privacy activists initially raised concerns about the app, which was the first government-issued contact tracing app in sub-Saharan Africa.[128] One such concern is that at the time during which the app was rolled out, **Botswana** had still not established a DPA.[129] To allay these concerns, the COVID-19 government task force advised that measures would be taken to anonymise users' data and that limited government departments would have access to this data.

---

120 Jonathan Rozen, 'Botswana journalists remain 'vigilant' under new surveillance law' 2022, accessible here.
121 Sonia Cisse, '40 countries ploughing ahead with contact-tracing apps as debate intensified on differing approaches' 15 May 2020, accessible here.
122 Above n 43 at page 1.
123 ACDC, 'Guidance on Contacting Tracing for COVID 19 Pandemic', April 2020, accessible here.
124 See Privacy International, 'Apps and Covid-19', n.d., accessible here; Privacy International, 'Telecommunications data and Covid-19', n.d., accessible here.
125 See Jonathan Klaaren and Brian Ray, 'South Africa's Technologies Enhancing Contact Tracing for COVID19: A Comparative and Human Rights Assessment' *South African Journal on Human Rights,* 2022, accessible here.
126 Above n 43 page 22.
127 *Id.*
128 Morgan Meaker, 'African countries' growing app-etitie for Coronavirus apps gets mixed results', The Correspondent, 20 July 2020, accessible here.
129 *Id.*

The **Democratic Republic of Congo** utilised an app previously developed to tackle the Ebola crisis.[130] The app, Polio GIS platform, was reportedly repurposed, however, information on the re-use of data collected for Ebola and used for the COVID-19 pandemic is unclear.

As a low-income country, **Malawi** proves to be an interesting case study on the use of mobile phone data to gather health information. Limited testing kits per capita and reliance on unfeasible traditional means of contact tracing resulted in the collection of mobile data for contact tracing (as opposed to the use of an app).[131] In 2020, Telekom Networks Malawi, the country's second-largest Mobile Network Operator (**MNO**), entered into an agreement to share anonymised data to call detail records with a private company, Cooper/Smith, to reportedly support the Ministry of Health in tackling the COVID-19 crisis.[132] Telekom Networks Malawi and Cooper/Smith entered into an agreement governing how the data collected between the two would be protected.[133] Moreover, information on the anonymisation process has been made available to the public.[134]

The **Seychelles** Health Ministry launched a DTC app called Proximity developed by Ernst & Young and a Seychellois professor. The app recorded proximity and contact time between individuals using Bluetooth technology.[135] From thereon, the app would load anonymised data onto a database and enable health authorities to determine contacts to be investigated based on other positive test results in the database.

In **South Africa**, health officials first attempted to use sensitive mobile location data for contact tracing, before pivoting to a more conventional Bluetooth-based proximity app and messaging interfaces. Policymakers were lauded for adopting regulations that increased oversight and safeguards over the collection and use of personal data in the government's pandemic response, which included the appointment of a retired judge to oversee the implementation of the policy and make recommendations to improve it.[136] However, subsequently, analysts expressed concern that there is little evidence that certain regulations were properly implemented or enforced and there was limited engagement with the policy oversight from Parliament and regulators.[137] Health authorities and lawmakers have been urged to conduct a public review and assessment of the policy, to improve public

130 Emmanueal Arakpogun, 'Digital contact-tracing and pandemics: Institutional and technological preparedness in Africa', World Development Journal, 2020, at page 1, accessible here.
131 Dylan Green *et al*, 'Using mobile phone data for epidemic response in low resource settings – A case study of COVID-19 in Malawi', Data & Policy, 3, at page 19, 2021, accessible here.
132 *Id.*
133 Rachel Sibande and Tyler Smith, 'Using mobile phone records to improve public health: evidence from Malawi', Centre for Global Development, 10 December 2021, accessible here.
134 *Id.*
135 Seychelles Nation, 'New contact-tracing app against the spread of Covid-19' 2021, accessible here.
136 Klaaren and Ray, 'South Africa's Technologies Enhancing Contact Tracing for COVID-19: A Comparative and Human Rights Assessment' *South African Journal on Human Rights,* 2022; Hunter, 'Track and Trace, Trial and Error: Assessing South Africa's Approaches to Privacy in COVID-19 Digital Contact Tracing', Media Policy and Democracy Project, 2020, accessible here.
137 Murray Hunter, 'Don't impose new health policy until we understand impact of Covid data collection', News24, 2022, accessible here.

understanding of how it impacted South Africa's pandemic response, if at all, and any potential impact on digital rights.[138] The Information Regulator released a guidance note for public and private bodies and their operations supporting the processing of personal information in the management and containment of the COVID-19 pandemic.[139] In terms of the note, specific conditions for responsible, lawful, and justifiable processing were still applicable during this time.

138 ALT Advisory and Jonathan Klaaren, 'Joint comment on draft regulations relating to COVID-19 data collection', 2022, accessible here.

139 Information Regulator South Africa, 'Guidance note on the processing of personal information in the management and containment of COVID-19 pandemic in terms of the Protection of Personal Information Act 4 of 2013', n.d., accessible here.

Facial recognition technology, biometrics, and SIM card registration

Principle 40 of the ACHPR 2019 Declaration provides that, *"Everyone has the right to privacy, including the confidentiality of their communications and the protection of their personal information.*" Furthermore, principle 42 requires States to enforce laws to protect individuals' personal information in accordance with prevailing international law standards. Although the use of biometrics, including facial recognition technology (**FRT**), is nascent, States have not enacted adequate regulatory measures. Rather, in several instances explored below, authorities are pursuing efforts to integrate biometric surveillance into SIM card registration. Mandatory SIM card registration is another long-standing concern for digital rights advocates.

As in the rest of the continent, all countries in Southern Africa have either implemented or are seeking to implement mandatory SIM card registration, which requires every person to link their electronic communications to their legal identity.[140] Although SIM card registration is typically presented by policy makers as vital to combating crime, there remains little evidence of the policy's effectiveness as a crime-fighting measure.[141] On the contrary, critics contend that SIM card registration enables more pervasive surveillance, increases the costs and barriers to accessing communication, especially for marginalised groups, and fuels identity theft and other risks to data protection.[142]

In **Malawi**, the National Registration and Identification System (**NRIS**) is a centralised system for the processing of biometric data.[143] NRIS has been in use since 2017 and is linked to a broad scope of information: voter registration, revenue collection, immigration information, and SIM card registration. It is also connected to banking and financial inclusion programmes. The system was also used to support COVID-19 vaccination efforts and has been criticised for the mass collection of personal data in the absence of data protection legislation, a situation which enables mass surveillance.[144]

South Africa's RICA requires network operators to register all SIM cards to the identity of the user. The registration requires the recording of the user's full name, address, and identity number or passport. Regarding biometric information, South Africa's Protection of Personal Information Act generally prohibits the collection of such data except where the data's subject gives consent, where processing is necessary for the exercise of a right or legal obligation, or where processing is for historical, statistical or research purposes where this would serve a public interest. However, in this case, it also appears that there

140 Above n 43 at page 57.
141 Nicola Jentzsch, 'Implications of mandatory registration of mobile phone users in Africa', Telecommunications Policy 36, 2012, at page 609.
142 Privacy International, 'Africa: SIM Card Registration Only Increases Monitoring and Exclusion', 2019, accessible here.
143 Above n 82 at page 37.
144 Jimmy Kainja, 'Are Malawians Sleep-Walking into a Surveillance State?', CIPESA, 12 August 2019, accessible here.

is policy interest in linking biometrics and SIM card registration. In 2022, South Africa's Independent Communications Authority of South Africa (**ICASA**), sought public comment on draft regulations that would require MNOs to collect biometric information from users for the purpose of SIM registration, as an anti-fraud measure.[145] Digital rights groups criticised the proposal as an example of "surveillance creep",[146] which refers to the use of surveillance systems which, over time, become more expansive and invasive of individuals' data.[147]

In **Tanzania,** the registration of SIM cards is mandated by the Electronic and Postal Communications (SIM Card Registration) Regulations, 2020. The Act does not allow SIM card registration unless a user's photographs and fingerprints have been verified against the National Identification Authority (**NIDA**) database**.**[148] Beyond this, the use of biometrics has become commonplace as public institutions – such as the Higher Education Loans Board, the Tax Revenue Authority, and the Government Recruitment Agency rely on National IDs, facilitated by the NISA database.[149] The justification provided for this is that the process improves public service delivery.

In early 2021, the **Zimbabwean** cabinet announced that it had contracted an unnamed company to implement a National Biometric Database for the production of documents such as e-passports, national IDs, and birth certificates.[150] This followed a 2018 agreement between the government and CloudWalk, a Chinese firm specialising in facial recognition, to create a national face database.[151] The Cyber Security and Data Protection Act, passed in 2021, prohibits the processing of biometric, genetic, and health data without consent from a data subject.[152] However, this does not mean that large-scale data collection has been eliminated. The 2014 Postal and Telecommunications (Subscriber Registration) Regulations require all telecommunications companies to create a centralised subscriber database,[153] which should reflect the user's full name, residential address, nationality, gender, identity number, and subscriber identifying number. In 2016, the Postal and Telecommunications Regulatory Authority of Zimbabwe (**PORTAZ**) alerted the public that persons responsible for "*abusive and subversive*" material in respect of the database would be prosecuted.[154] The use of such ambiguous language (in its press statements, PORTAZ did not provide further detail on what would constitute abusive and subversive material) undoubtedly fails to accord with best practice when it comes to States enabling the realisation of freedom of expression (dealt with in section 5 of this report).

145 ICASA, Draft Numbering Plan Regulations, 2022, GG 46080, accessible here.
146 Amabhungane, 'Submission on draft ICASA regulations, 2022, accessible here.
147 *Id.*
148 Above n 82. at page 40.
149 *Id.*
150 *Id* at page 41.
151 Global Voices, 'How Zimbabwe's biometric ID scheme (and China's AI aspirations) threw a wrench into the 2018 election', 2020, accessible here.
152 Section 14 of Cyber Security and Data Protection Act.
153 Zimbabwe, '2014 Postal and Telecommunications (Subscriber Registration) Regulations to Act 95 of 2014', 2014, accessible here.
154 Above n 44 at page 41.

Artificial intelligence

As is the case with other forms of emergent technology, the region lacks a comprehensive framework for AI governance. As discussed above, the African Commission made an important contribution to addressing this gap with the adoption of ACHPR Resolution 473.

Notably, SADC's Data Protection Model Law also provides some regulation to AI, including provisions for algorithmic transparency, by providing that the model law's provisions are applicable to automated processing of personal information, and that data subjects' rights include the right to information *"about the basic logic involved in any automatic processing of data relating to him/her in case of automated decision making"*.[155]

Nevertheless, given the significant potential for AI technologies to impact human rights, there is a need for further regulation and guidance to govern the design and use of such technology.[156] Despite the complexities of policymaking in this realm, there is a growing body of research and policy guidance to inform the creation of regional and domestic policies. For example, an Independent Group of Experts of the European Commission produced ethical guidelines for trustworthy AI,[157] which promote four foundational principles:

- respect for human autonomy;
- prevention of harm;
- fairness; and
- explicability.

In 2019, two notable AI-related meetings occurred at a regional level. The first was a meeting of various African Communication and ICT Ministers in Sharm El Sheik, Egypt to discuss the African Digital Transformation Strategy (**DTS**), amongst others.[158] One of the objectives of the DTS is to secure a digital single market in Africa by 2030 to digitally empower all persons. In relation to AI, the DTS requires policy makers and regulators to keep pace with advancements in AI and promote the use and innovation of this technology. The second meeting was the African Union Working Group on AI holding its first session in Cairo, Egypt to craft a single continental strategy on AI as well as to exchange expertise between States.[159]

---

155 ITU, 'Data Protection: SADC Model Law', 2013, Section 31, accessible here.

156 Above n 44 at page 22.

157 European Commission, 'Ethics Guidelines for Trustworthy AI – High-Level Expert Group on Artificial Intelligence', April 2019, accessible here.

158 African Union Press Release, 'African Digital Transformation Strategy and African Union Communication and Advocacy Strategy among major AU initiatives in final declaration of STCCICT', 26 October 2019, accessible here.

159 See Media Centre at Egypt Ministry of Communications and Information Technology webpage, 6 December 2019, accessible here.

The rapid pace of development and implementation of AI technology in the region by a wide range of public and private actors, require policymakers, civil society actors, and the general public to weigh up the many perceived and real benefits of AI. These include possible economic benefits, improved innovation, and consumer outputs[160] – with possible risks and implications for human rights, such as lack of accountable and transparent decision-making, and discriminatory profiling.[161] Some of the key developments in AI on a domestic front are documented below.

Angola's Ministry of Telecommunications, Information Technologies, and Media (**MINTIC**) described AI as one of the central pillars of Angola's digital transformation.[162] Recently, the country launched its Digital Transformation Plan.[163] Additionally, a recent development in **Angola** is the formulation of Portal IT, which is an AI platform for the acceleration of digital transformation.[164] The platform consolidates news on ICT developments and technological innovation in Africa, posts job vacancies in these fields, and shares details of upcoming ICT events. The **Angolan** government has been vocal about its plans to promote a single digital market in Africa, which serves to modernise public services and promote good governance.[165]

Botswana has reportedly developed a national policy on AI. Although the policy has not been published, the government has declared its readiness for the 4IR.[166] Beyond policy, other initiatives introduced by the state include a strategy for e-commerce development, called SmartBots, [167] and an action plan which is centred on the digitization of the public sector.[168]

Mauritius' AI Strategy[169] appears to be at an advanced stage. The comprehensive strategy was formulated by a working group of experts and the Finance and Economic Development Ministry. Although the Strategy does not contain extensive content on the human rights implications of AI, it acknowledges the implications for privacy, data protection, and vaguely, "*...the rights of individuals*".[170] Notably, the Strategy was prepared through an economic lens and it thoroughly details the potential impact of AI on a variety of sectors – for instance, the manufacturing sector, the food, and beverage sector, and healthcare and biotechnology.[171]

---

160 University of Pretoria, 'Artificial Intelligence for Africa: An Opportunity for Growth, Development, and Democratisation,' at page 46, undated, accessible here.
161 Alex Najibi, '*Racial Discrimination in Face Recognition Technology*', Harvard University, Blog, Science Policy, Special Edition: Science Policy and Social Justice', 24 October 2020, accessible here.
162 Above n 20 page 10.
163 *Id.*
164 *Id.*
165 AllAfrica, 'Africa: Angolan Government wants to promote digital single market in Africa', 7 May 2022, accessible here.
166 Above n 20 at pages 30 and 31.
167 UNCTAD, 'Launch of the ICT Policy Review and National E-commerce Strategy for Botswana', 21 October 2021, accessible here.
168 Andrew Maramwidze, 'Botswana intensifies SmartBots digitisation strategy', ITWeb, 25 November 2021, accessible here.
169 Mauritius Artificial Intelligence Strategy, 2018, at page 16, accessible here.
170 *Id.*
171 Above n 162 at page 5.

In section 71, South Africa's POPIA deals with automated decision-making. This provision prohibits automated decision-making where this results in legal consequences for the data subject which:

a. affect the data subject to a substantial degree; and

b. where the decision is based solely on the automated processing of personal information which pertains to the data subject's work performance, credit worthiness, reliability, location, health, personal preferences, or conduct.

There are exceptions to this - the prohibition does not apply where the decision has been taken in connection with the conclusion or execution of a contract or where the decision is governed by law or a code of conduct wherein appropriate measures have been included to protect the legitimate interests of the data subject.

Recommendations:

- In light of the complexities and potential human rights impacts of emergent technologies, States should fund research into the ethics and appropriate regulation of emergent technology.
- States should undertake a full reform of domestic laws for the interception of communication, to align with the applicable principles in the ACHPR 2019 Declaration and other international human rights laws and standards.
- States should convene multi-stakeholder assessments of the human rights implications, cost-effectiveness, and necessity, of national biometrics policies, SIM registration, and related policies.
- In addition, any public-private partnership involving the rollout of technology-driven services which make use of biometrics, health information, or other sensitive data collection, should be subject to public participation, human rights impact assessments, and minimum standards for the accountability and transparency of the private implementing partners.
- States should develop clear national policies, guidelines, and laws, to regulate the appropriate use of AI, which are centred on human rights. Where States have formulated AI policies in the absence of human rights considerations, these policies should be revised.

RESTRICTIONS ON FREEDOM OF EXPRESSION

Restrictions on freedom of expression at a glance:

- States' ongoing use of internet shutdowns and other network disruptions to stifle dissent, enforce public order, or for any other purpose, results in serious infringements to digital rights, as well as harm to public safety, business, the economy, and the broader democratic climate.
- Regulation of harmful speech, including hate speech and defamation, should aim to protect vulnerable parties from harm while striking an appropriate balance for freedom of expression. Yet the regional trend is often for these regulations to be used by powerful actors to stifle critics and target vulnerable parties.

The right to freedom of expression is a foundational element of any democratic society and is well protected under international and regional law. Article 19 of the UDHR guarantees that freedom of expression includes the freedom to hold opinions without interference and to seek, receive and impart information "*...through any media and regardless of frontiers*". The ICCPR, in article 19, mirrors the wording of the UDHR, although the ICCPR further mentions that the right carries special duties and responsibilities. On a regional front, 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. The right to freedom of expression is not absolute and may be limited in certain circumstances. For example, it is not unusual for speech that incites violence or constitutes harassment to be subject to regulation.[172] However, where speech is regulated arbitrarily, this poses a threat to free speech and freedom of expression. For such regulation to be justifiable, it should meet certain criteria stipulated under international human rights law. Article 19(3) of the ICCPR provides clear guidance on the two circumstances under which speech may be restricted. First, where a restriction is necessary out of respect for the rights or reputations of others. Second, where this restriction is necessary for the protection of national security, public order, or public health or morals. In 2011, the UN adopted General Comment 34 on how States should give effect to article 19(3).[173] We extract some guiding principles from General Comment 34:

- There are two limitations and areas of restrictions on freedom of speech. These areas are when the restriction is out of respect for the rights/reputation of others or in the interests of national security, public order, public health, or morals;
- Even when States impose restrictions on freedom of expression, such restrictions should not jeopardise the rights themselves;

172 Section 36, Constitution of the Republic of South Africa, 1996.
173 UNHRC, 'General Comment No. 34. Article 19: Freedoms of opinion and expression', CCPR/C/GC/34, 12 September 2011, accessible here.

- States should make plans to protect against attacks that serve to silence individuals from exercising their freedom of speech;
- Restrictions should serve a legitimate purpose and should be proportionate to the circumstances;
- Any laws which restrict freedom of expression should not confer unfettered discretion on those charged with executing such restrictions; and
- The onus falls on the state to demonstrate the legal justification for restricting this right.

Closer to home, principle 23 of the ACHPR also explains which type of speech should be prohibited by States. Speech that advocates for national, racial, religious, or other forms of discriminatory hatred which incites discrimination, hostility, or violence may be prohibited. Where speech merely lacks civility or is offensive or disturbing, this is not sufficient ground to prohibit it. According to principle 23(2), the criminalisation of prohibited speech should be deemed as a last resort by States and where this is a consideration, States should take into account six factors: prevailing social and political context; the status of the speaker in relation to the audience; the existence of a clear intent to incite; the content and form of the speech; the extent of the speech, including its public nature, size of audience and means of dissemination; and the real likelihood and imminence of harm caused by the speech.

Over the course of June and July 2022, the UN Human Rights Council adopted a resolution on the freedom of opinion and expression[174] and a separate resolution[175] on the right to freedom of peaceful assembly and of association. The first resolution calls on States to promote and protect the right to freedom of opinion and expression exercised both on- and offline. It also notes several challenges related to digital rights such as the gender digital divide, online harassment and violence particularly against women and girls, and internet shutdowns. The resolution goes on to stress that undue restrictions on the right to freedom of opinion and expression undermine democracy and the rule of law. In the same spirit as the first, the second resolution calls on States to guard the rights of all individuals to peacefully assemble and associate freely on- and offline. It unequivocally condemns action which disrupts these rights as this may amount to censorship. Over and above this, the resolution calls on States to refrain from the arbitrary or unlawful use of force by law enforcement officials against those exercising the rights in question.

Yet across Southern Africa, there are examples of restrictions on speech that go beyond the aforementioned limited criteria, guidelines, and standards. These include censorship through internet shutdowns and network disruptions in the certain African States, especially during elections and periods of civil unrest.[176] Other examples include defamation proceedings and SLAPP suits. These concepts are dealt with below.

---

174 UNHRC, 'Freedom of opinion and expression', A/HRC/50/L.11, 30 June 2022, accessible here.
175 UNHRC, 'The right to freedom of peaceful assembly and association', A/HRC/50/L/20, 4 July 2022, accessible here.
176 Giles and Mwai, 'Africa internet: Where and how are governments blocking it', 14 January 2021, accessible here.

Internet shutdowns

Deliberate disruptions to internet access and social media interfere with a range of rights, including freedom of expression, the right of access to information, freedom of assembly and protest rights, freedom of the press, electoral freedoms, freedom and security of the person, and religious freedoms.

In July 2021, the UN passed a resolution condemning internet shutdowns,[177] which expressed deep concern, "*…at all human rights violations and abuses committed against persons for exercising their human rights and fundamental freedoms on the Internet, and the impunity for these violations and abuses.*" It further called on States to cease such measures. In May 2022, the Office of the High Commissioner for Human Rights (**OHCHR**) issued a report on the causes and legal implications of internet shutdowns,[178] which notes that between 2016 and 2021, the majority of internet shutdowns reported took place in Asia and Africa.[179]

According to #KeepItOn, a civil society coalition documenting and advocating against internet shutdowns, these shutdowns are more likely to occur during periods of social and political contention, such as elections, or amid civil unrest. These shutdowns can take the form of the blocking of websites or apps, network throttling, and partial or full disruptions to mobile or broadband services. The #KeepItOn coalition has documented fewer shutdowns between 2019 and 2021, though the length of shutdowns has increased in a few cases.[180] The harm resulting from these types of restrictions includes limiting civic participation, undermining the ability of groups to mobilise, preventing journalists from producing or sharing news stories, impeding people's access to education or health information, and disrupting commerce and digital banking.[181] While a limited number of internet shutdowns have been documented in certain Southern African countries – examples of which are documented below – these constitute serious infringements of digital rights in those societies.

177 UN, 'Resolution on the promotion, protection and enjoyment of human rights on the Internet', A/HRC/32/L.20, 27 June 2016, accessible here.

178 UN, , 'Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights', A/HRC/50/5513, May 2022, accessible here.

179 *Id* at page 3.

180 Access Now, '#KeepItOn update: who is shutting down the internet in 2021', 7 June 2021, accessible here.

181 Human Rights Watch, 'Shutting Down the Internet to Shut Up Critics', 2020, accessible here.

Given their indiscriminate and widespread impacts, Internet shutdowns very rarely meet the proportionality test. Any form of Internet shutdown impairs countless legitimate and beneficial activities. Shutdowns also directly put people's safety and well-being at risk, for example, when they make it impossible to warn people against impending danger or for people to call for vital services."

– OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS*

* Office of the United Nations High Commissioner for Human Rights, 'Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights', A/HRC/50/55, accessible here.

The internet and social media were blocked on 31 December 2018 in the **Democratic Republic of Congo** during elections.[182] Restrictions were enforced in areas with a strong opposition presence. A senior advisor to the President stated that the disruptions were intended to preserve public order after "fictitious results" were shared on social media.[183] Connectivity was restored on 20 January 2019, twenty days later, upon the announcement of the election results.

Similarly, in October 2020, the **Tanzania** Communications Regulatory Authority suspended bulk SMS for over two weeks ahead of the national elections.[184] In 2021, during elections in **Zambia,** there was a partial internet shutdown, with apparent network slowdowns targeting social media and messaging platforms, though access was restored after a civil society organisation, the Chapter One Foundation, secured a court order.[185] Notably, in March 2022, Chapter One Foundation entered into an agreement with the Zambia Information Communications Authority (**ZICTA**) in terms of which ZICTA has agreed not to act outside its legal authority and/or control or interrupt the flow or access to the internet going forward.[186]

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, online communications were blocked.[187] It has been reported that during this period, mobile operators such as TelOne, Liquid Telecom Zimbabwe, Telecel, and Econet succumbed to state and/or external political pressure for implementing the shutdown. 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.[188] The Minister was found not to have the requisite authority to issue the directive. Thus, the relevant mobile operators were ordered to immediately reinstate the connection. 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.[189] The state-owned network provider, TelOne, has been reported to have throttled connectivity speeds. Shortly after the incident, NetBlocks, an independent organisation monitoring digital rights, cybersecurity, and internet governance, mapped out the IP address space of Zimbabwe in real-time and publicly released metrics showing the throttling coincided with

182 MISA-Zimbabwe, 'Beyond a Click: Regional assessment on state of digital rights: Southern Africa', undated, at page 22, accessible here.
183 Joseph Kabila, 'DRC internet restored after 20-day suspension over elections', 20 January 2019, accessible here.
184 MISA-Zimbabwe, 'The State of Press Freedom in Southern Africa 2019-2020', 2021, at page 8, accessible here.
185 Londa, 'Digital Rights and Inclusion Africa Report: 2021', 2022, accessible here.
186 Chapter One Foundation, 'Consent Judgment between Chapter One Foundation and ZICTA over Internet Shutdowns' March 200, accessible here.
187 Juliet Nanfuka, 'Zimbabwe becomes the latest country to shut down social media', CIPESA, 7 July 2016, accessible here.
188 MISA-Zimbabwe, 'High Court sets aside internet shutdown directives', 21 January 2019, accessible here.
189 Above n 20 at page 28.

the timing of the planned protests.[190] This throttling occurred after Zimbabwe's government had issued a warning that participation in the protest would be considered insurrection.[191] More recently, in February 2022, NetBlocks confirmed that there was a "significant slowing of internet service for many users in Zimbabwe" which happened to coincide with a major political opposition rally.[192] At a later stage, the Media Institute of Southern Africa (**MISA**) Zimbabwe brought this to the attention of the Ministry of Information Communications Technology, Postal and Courier Services, and PORTAZ.[193]

Content moderation

While less indiscriminate than internet shutdowns, content moderation can also have significant impacts on people's right to access information and freedom of expression. Content moderation can result 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. While social media companies may invoke their community guidelines to restrict or censor specific posts, ranging from extremism to false news, the application of these guidelines has been criticised for being inconsistent, non-transparent, and in certain instances, harmful.

The negative effects of untargeted or disproportionate content moderation have been shown to disproportionately impact marginalised persons, mainly through disregarding their experiences on social media.[194]

The principles of legality, legitimacy, necessity, and proportionality are essential in the moderation of content.[195] The United Nations High Commissioner for Refugees (**UNHCR**) identified several types of content moderation, with the most common being:[196]

190 NetBlocks, 'Zimbabwe internet disruption limits coverage of planned protests,' 31 July 2020, accessible here.
191 *Id.*
192 NetBlocks, 'Internet slowdown limits coverage of Zimbabwe opposition rally' 20 February 2022, accessible here.
193 African Freedom of Expression Exchange, 'Statement on the recently reported internet throttling in Zimbabwe', 22 February 2022, accessible here.
194 Eugenia Sipaer, 'AI Content Moderation, Racism and (de)Coloniality', International Journal of Bullying Prevention', August 2021, at page 61 accessible here.
195 Electronic Frontier Foundation, 'RightsCon: Contemplating content moderation in Africa: disinformation and hate speech in focus', June 2021, accessible here.
196 UNHCR, 'Using Social media in Community Based Protection: A Guide', at pages 114 to 116, January 2021 accessible here.

Type of moderation	Meaning
Pre-moderation	The moderation of content before it is publicly displayed or posted on a site.
Post-moderation	This level of moderation involves the detection and removal of content that has already been publicly shared.
Reactive moderation	Normally facilitated by user engagement and may involve a breach of community guidelines.
Supervisor moderation	Grants select moderators the power to unilaterally remove content.
Commercial Content Moderation (**CCM**)	Outsources moderation to specialists, which may involve human rights organisations and NGOs. Particularly useful in highly polarised environments.
Distributed moderation	Relies more heavily on flagging, reporting, and voting on content by the community.
Automated moderation	Makes use of AI to make decisions related to the display of content. This type of moderation is best paired with some degree of human moderation and a broadened linguistic scope.

Principle 39 of the ACHPR 2019 Declaration compels States to require internet intermediaries to enable access to internet traffic equally. Where internet intermediaries moderate or filter online content, they should mainstream human rights safeguards into these processes. States themselves are discouraged from approaching internet intermediaries to remove online content. Where such requests are made, principle 39(4) provides that the request should be: clear and unambiguous, imposed by an independent and impartial judicial authority, subject to due process safeguards, justifiable and compatible with international human rights law, and implemented through a transparent process that allows a right of appeal.

Zimbabwe serves as a notable case study of restrictive state-sponsored action against social media content.[197] While state justifications of social media regulation include protecting national security and disseminating information for disaster management, it appears that restrictions in **Zimbabwe** have exceeded this. According to MISA Zimbabwe, fear of criticising the government has led to self-censorship on social media.[198]

197 Tomiwa Ilori, 'Content moderation is particularly hard in African countries', 21 August 2020, accessible here.

198 MISA-Zimbabwe, 'Zimbabwe Input for Report on Disinformation', undated, accessible here.

Misinformation and disinformation

As in many other parts of the world, disinformation and misinformation have become an increasing focus of debates and policy measures on the regulation of speech in Southern Africa.

Misinformation is generally understood as false or misleading information without the intention to cause harm (i.e. it may involve an element of mistakenness), whilst disinformation is false or misleading information that is deliberately created and disseminated to cause confusion, stoke divisions, or spread falsehoods.

Measures taken in Southern Africa to curb the spread of false information have received mixed reviews.

Eswatini enacted regulations that criminalise disinformation. Where such information is related to COVID-19 and is shared without the Health Ministry's permission, this could result in a sanction. The use of the term 'rumour' in the regulations, which is ill-defined, leaves room for doubt on the necessary standards.

Likewise, **South Africa** prohibited the spread of false information in the wake of the COVID-19 pandemic. While the country was under a national state of disaster, the Department of Cooperative Governance and Traditional Affairs published regulations criminalising the publication of COVID-19-related disinformation.[199] These regulations were met with mixed reviews, with some civil society actors criticizing the regulations for their failure to meet the test of legality, necessity, and proportionality.[200] In the event that anyone was found to have published any disinformation, including on the infection status of any other person or a measure taken by the government to address the virus, they would potentially be liable for a fine or a maximum of six months imprisonment. Outside of these regulations, other steps have been taken to combat disinformation. The Real411 initiative is a reporting channel for tackling disinformation. The public is encouraged to report disinformation, among other types of digital harm, for investigation by a Digital Complaints Committee (**DCC**). To enable inclusivity, complaints may be reported in any of South Africa's official languages. Upon receipt of a complaint, the Secretariat of the DCC forwards it to the Sub-Committee which may make an array of decisions. Possible outcomes include that the complaint falls outside the scope of the DDC, no action is required, and referral of the complaint to the relevant body (for example, the Press Ombud, the South African Human Rights Commission, or the South African Police Service.) The **DCC** can also advise that assistance should be sought directly from the online platform, that a case should be instituted before the Equality Court or another appropriate court or tribunal, or that a counter-narrative should be published. The process includes an appeal mechanism.

199 South Africa, 'Regulations issued in terms of section 27(2) of the Disaster Management Act 2002, GN 43107, GG 318, 18 March 2020, accessible here.

200 Article19, 'South Africa: Prohibitions of false COVID-19 information must be amended,' 23 April 2021, accessible here.

Hate speech, harassment, and incitement to violence

An increase in internet access has given rise to online harms which may, on circumscribed occasions, necessitate a limitation of freedom of expression. Freedom of expression may be limited to thwart hate speech, harassment, propaganda, and incitement to discrimination, hostility, or violence. Several provisions in international law instruments speak to harmful and inflammatory speech. Article 2 of the UDHR prohibits discrimination on the basis of *"…race, colour, sex, language, religion, political or other opinions, national or social origin, property, birth or other status."* Article 19 of the UDHR goes on further to provide guidelines on the limitation of freedom of expression where, for example, the impugned speech is discriminatory and unlawful. The ICCPR explicitly places an obligation on States to prohibit hate speech. Article 20(2) provides that, *"[a]ny advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law."* The International Convention on the Elimination of All Forms of Racial Discrimination also calls upon States to declare hate speech an offence punishable by law. Thus, it is well-established in international law that not all speech is protected speech. It is not unusual for domestic legislatures to adopt a similar stance.

Tanzania introduced hate speech regulations titled the Online Content Regulation of 2020. Through the use of licenses, the country also introduced systems to regulate the publication of online content outside of public communications. These regulations have rightly been described as harmful, particularly in the context of COVID-19.[201] In particular, the 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.'

In **South Africa**, the protection against hate speech is established through the Promotion of Equality and Prevention of Unfair Discrimination Act, 2000 (**the Equality Act**). The Act allows for both civil and criminal remedies against hate speech and other harmful speech, both offline and online. The Constitutional Court in **South Africa** recently handed down two landmark judgments on hate speech. In *Qwelane v South African Human Rights Commission and Another*,[202] the Court explained that hate speech undermines human dignity and substantive equality. In *South African Human Rights Commission on behalf of the South African Jewish Board of Deputies v Masuku and Another*,[203] the Court assessed whether a specific provision in South Africa's Equality Act would result in an unjustifiable limitation on freedom of expression. Notably, in both cases, the Court affirmed that the rights to equality, human dignity, and freedom of speech and expression are indispensable to a healthy constitutional order.

---

201 Article 19, 'Tanzania: Online Content Regulations 2020 extremely problematic in the context of COVID-19', 19 January 2021, accessible here.

202 *Qwelane v South African Human Rights Commission and Another* (CCT 13/20) [2021] ZACC 22, accessible here.

203 *Masuku and Another v South African Human Rights Commission obo South African Jewish Board of Deputies* (1062/2017) [2018] ZASCA 180., accessible here.

Defamation online and SLAPP suits

Defamation, which is the publication of false statements which harm a person's reputation, is regarded as another mechanism to stifle freedom of expression and dissent. It is employed particularly in the media.[204] While a number of Southern African countries retain defamation laws, in recent years, courts in **Zimbabwe** and **Lesotho** struck down those countries' criminal defamation laws.[205] This accords with the ACHPR's Resolution 169 on Repealing Criminal Defamation Law in Africa.[206] The resolution speaks to state actors and members of the media. On the one hand, in recognising the gravity of unlawfully restricting the right to freedom of expression, the resolution calls on States to repeal criminal defamation laws and refrain from imposing general restrictions which violate this right. On the other hand, the resolution urges journalists and media practitioners to uphold ethical journalism "*...so as to avoid restriction to freedom of expression, and to guide against the risk of prosecution.*"[207] It is appropriate, at this point, to highlight principle 21 of the ACHPR 2019 Declaration, which also speaks to this issue. Principle 21 states:

> *"1. States shall ensure that laws relating to defamation conform with the following standards:*
>
> *a. No one shall be found liable for true statements, expressions of opinions or statements which are reasonable to make in the circumstances.*
>
> *b. Public figures shall be required to tolerate a greater degree of criticism.*
>
> *c. Sanctions shall never be so severe as to inhibit the right to freedom of expression.*
>
> *2. Privacy and secrecy laws shall not inhibit the dissemination of information of public interest."*

Media freedom advocates have documented instances of journalists being detained or charged under criminal defamation laws in the region, including in **Angola,**[208] the **Democratic Republic of Congo**,[209] and **Zambia**.[210]

Defamation proceedings may also take the form of SLAPP suits. These types of legal proceedings have been recognised as a silencing tactic in jurisdictions such as the United

---

204 Media Defence, 'Module 5: Summary Modules on Litigating Digital Rights and Freedom of Expression Online', 2020, at page 1, accessible here.

205 Nyane Hoolo, 'Abolition of criminal defamation and retention of scandalum magnatum in Lesotho' *19* African Human Rights Law Journal, 2019, at page 753, accessible here.

206 ACHPR. 'Resolution on Repealing Criminal Defamation Laws in Africa, 'ACHPR/Res.169(XLVIII) 2020', accessible here.

207 *Id.*

208 Committee to Protect Journalists, 'Angola charges 2 more journalists with criminal defamation over corruption reporting', 2021, accessible here.

209 Committee to Protect Journalists, 'DRC journalist Pius Romain Rolland Ngoie detained since December over criminal defamation complaint', 2021, accessible here.

210 Committee to Protect Journalists, 'Zambian police arrest five radio journalists', 2016, accessible here.

States.[211] They are generally deemed to be litigation proceedings with little to no merit, instituted by powerful entities against more vulnerable individuals and groups, with the goal of intimidating critics, draining their resources, or exacting a "price" for speaking out.[212] Judicial recognition of SLAPP suits is still new in the region and outside of South Africa, there is yet to be jurisprudential guidance on this topic. The Constitutional Court of **South Africa** recently heard its first SLAPP in *Mineral Sands Resources Proprietary Limited and Another v Christine Reddell and Others*.[213] Briefly, the case is an appeal of a judgment by the Western Cape High Court wherein the SLAPP defence was accepted for the first by the South African judiciary. The defence was raised by a group of environmental activists and academics, who had shared their views against the activists of a mining company, Mineral Sands Resources (Pty) Ltd. The mining company subsequently brought a defamation suit against the respondents and sought damages amounting to just shy of R15 million. As of August 2022, the judgment had not yet been handed down.

Recommendations:

- Domestic and regional human rights bodies, media organisations, and civil society actors should continue to document the use and impact of internet shutdowns, and regional bodies should establish mechanisms to ensure compliance with international human rights laws and standards.
- National laws should provide for greater transparency in network licensing agreements in order to improve public oversight of the relationships between state agencies, and public and private telecommunications providers.
- Regional and domestic bodies should develop clear standards and policies for content moderation, especially in relation to disinformation and misinformation, which safeguard freedom of expression.
- Domestic and regional human rights bodies and civil society actors should explore opportunities for strategic litigation to develop jurisprudence against the use of SLAPP lawsuits.

211 George Pring, 'SLAPPs: Strategic Lawsuits against Public Participation, 7 Pace Envtl. L. Rev. 3 (1989) accessible here.
212 *Id.*
213 *Mineral Sands Resources Propriety Limited and Another v Christine Reddell and Others* CCT 66/21 and CCT 67/21, accessible here.

MEDIA FREEDOM AND REGULATION

Media regulation at a glance:

- Most of the broader challenges to digital rights in Southern African countries, such as restrictions on freedom of expression and risks of surveillance, are especially applicable to journalists and other media practitioners – who are often primary targets for state mechanisms to stifle dissent on- and offline.
- Generally, the media in Southern Africa face an immensely hostile environment, legally, politically, and economically. Journalists face a range of threats from governments, political parties, and other powerful actors.
- While direct attacks, legal threats, and acts of censorship are viewed as primary concerns for media freedom in many parts of Southern Africa, obstacles to media sustainability and development are also vital to consider.

Vibrant, free and critical media are a hallmark of any democratic society. It is therefore concerning to note that many Southern African countries continue to experience a host of infringements on media freedom, including through laws and policies that stifle critical reporting or weaken journalistic institutions, and through direct harassment and attacks on individual journalists.[214]

214 MISA-Zimbabwe, 'The State of Press Freedom in Southern Africa 2019-2020', 2021, accessible here.

Media freedom in the context of digital rights

Exercising freedom of expression should encompass the ability of individuals to express themselves over a broad range of media, including print, broadcast, and online media.[215] The stifling of media freedom interferes with a host of rights, including the right to political participation, freedom of expression, access to information, and freedom of association. In many instances, where harassment or violence against journalists occurs during protests or gatherings, there is also an infringement on freedom of assembly. Further, where journalists' communications are monitored or devices seized, their right to privacy is violated. The impact of this interference flows in two ways. First, it prevents the media from exercising their rights. Second, it prevents the public from receiving information.

The role of the media should be understood as multi-faceted, including reporting on current affairs, acting as a watchdog over the conduct of public administrations and the private sector, and fulfilling a general duty to educate and inform.[216] This aligns with the media's mandate to enable the public to exercise the right to access information. Yet it should be noted that media freedom – and media regulation – do not only pertain to professional journalists and newsrooms, but a much wider range of digital publishers, social media users, and other content producers.[217]

Regional and domestic protections for media freedom

At the continental level, article 9 of the African Charter guarantees the right to freedom of expression and access to information. In 2002, the African Commission adopted the Declaration of Principles of Freedom of Expression and Access to Information in Africa to safeguard these rights. The Declaration, which underwent revision in 2019 (this report refers to the 2019 version), aims to promote principles of freedom of expression, and access to information online and offline. It recognises internet rights in Africa. Principle 1 of the 2019 Declaration highlights that:

> *"Freedom of expression and access to information are fundamental rights protected under the African Charter and other international human rights laws and standards. The respect, protection, and fulfilment of these rights is crucial and indispensable for the free development of the human person, the creation and nurturing of democratic societies, and for enabling the exercise of other rights."*

Most countries in Southern Africa provide constitutional protections for media freedoms such as freedom of expression and access to information. Nevertheless, there are restrictive laws that undermine these assurances of media freedom. The persistent attacks of journalists online and offline as well as harassment, assault, arrests, and detentions

215 Justine Limpitlaw, 'Media Law Handbook for Southern Africa', Second Edition, Konrad-Adenauer-Stiftung, 2021, at page 11, accessible here.
216 *Id* at page 14.
217 *Id* at pages 11 and 12.

undermine their contributions to the information ecosystem. There is still significant work to be done in the region to create an environment that enables journalists to effectively carry out their mandate without fear.

Media freedom rankings

The 2022 Reporters Without Borders Index indicates that the media freedom climate in Southern Africa ranges widely. The **Seychelles** and **Namibia** rank especially highly – yet most countries in the region are ranked in the bottom half of the global index.[218] Media freedom in most Southern African countries remains severely under threat, and has, in some cases, deteriorated during the recent COVID-19 pandemic. A visual representation of how States in Southern Africa have scored is shown below.[219]

Country	World Press Freedom Score, 2021-2-20	Freedom House: Are there free and independent media? 2021-2-21
1. Angola	99	1/4
2. Botswana	95	2/4
3. Comoros	83	1/4
4. Democratic Republic of Congo	125	1/4
5. Eswatini	131	1/4
6. Lesotho	88	2/4
7. Madagascar	98	2/4
8. Malawi	80	2/4
9. Mauritius	64	3/4
10. Mozambique	116	2/4
11. Namibia	18	3/4
12. Seychelles	13	2/4
13. South Africa	35	3/4
14. Tanzania	123	1/4
15. Zambia	109	1/4
16. Zimbabwe	137	1/4

218 Reporters Without Borders, '2022 World Press Freedom Index', accessible here.

219 As a guidance note, the first column uses a ranking of out of 180 countries, with higher rankings indicating greater restrictions on media freedom. In the second column, a higher score out of 4 represents a freer and independent media.

Domestic restrictions

A range of domestic laws in many Southern African countries contributes to these low rankings. These include new content-regulation measures, such as laws 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."[220]

The proliferation of cybercrime laws in the region has also introduced broad new content restrictions in several countries which are regarded as media freedom concerns, with recent laws enacted in **Eswatini**, **Tanzania,** and **Malawi,** and similarly concerning bills under consideration in **Zambia** and **Zimbabwe**.[221]

In other instances, longstanding laws are used to harass publishers and broadcasters, including defamation law as discussed in Section 5.5 of this report. **Eswatini**, as one of the lowest-ranked countries for media freedom in Southern Africa, is estimated to have over 30 laws that restrict media rights, including laws relating to state secrecy, obscenity, sedition, and insults.[222] Dissenting opinions in the media, particularly those which challenge the monarchy, have been stifled in **Eswatini**.[223] The government currently exercises control over broadcast media, with the Minister of ICT being a member of the royal family, [224] which, from a political perspective, has implications on the free flow of information and ICT governance.

The need for diverse voices in the media

In diverse countries such as those in Southern Africa – in language, politics, and identities – that face continuing inequities in divides such as race, class, gender, urban-rural positioning, or political orientation, media diversity is a crucial component of media freedom. A diverse media that represents different people and voices helps guarantee that a plurality of viewpoints and interests are represented in the public domain, including those that may not be aired through media that are dominated by mainstream commercial or government influence.[225]

---

220 MISA-Zimbabwe, 'Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights', 2021, at page 6, accessible here.
221 *Id.*
222 Above n 201, at page 6.
223 Reporters Without Borders, 'Eswatini' country profile, n.d., accessible here.
224 Id.
225 Jane Duncan and Julie Reid, 'Toward a measurement tool for the monitoring of media diversity and pluralism in South Africa: A public-centred approach,' Communication: South African Journal for Communication Theory and Research, 2013, accessible here.

This echoes provisions in the ACHPR 2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa, principle 17 of which states:[226]

> *"States shall take positive measures to promote a diverse and pluralistic media, which shall facilitate the promotion of free flow of information and ideas, access to media and other means of communication, access to non-discriminatory and non-stereotyped information, access to the media by poor and rural communities, the promotion of transparency and diversity in media ownership, the promotion of local African languages, content, and voices, and the promotion of the use of local languages in public affairs."*

Despite this clear imperative, there is scope for improvement when it comes to media diversity in Southern Africa In **South Africa,** an independent industry inquiry into media ethics chaired by retired judge Kathleen Satchwell (the Satchwell Report) found that "[o]ligopoly and lack of diversity persist, narrowing the public space for access to information and debate in a socio-political and economic landscape where English and Afrikaans dominate all platforms, pay-walls encroach, data is expensive and online access limited."[227] In **Angola**, an assessment of the press freedom climate indicates that many private media outlets were owned by high-ranking state officials and other political elites, which compromised critical coverage of the government in those newsrooms.[228]

The need for enabling environments for media freedom

The intensifying sustainability challenges for news media globally, and in Southern Africa specifically, present a major challenge for freedom of expression and associated rights. As media organisations shrink or shutter, the barriers to the diversification of media landscapes increase, and those journalistic institutions that remain are less likely to be able to fulfil their duties to the broader public, and are more likely to rely on the largesse of government institutions or corporate advertisers for survival. These concerns became even more apt following the COVID-19 pandemic, which ratcheted up the sustainability crisis for many media organisations both regionally and globally.[229]

Media freedom advocates suggested that States should establish public, non-partisan funding for independent media organisations or a range of other policy conditions that explicitly enable media sustainability as part of their positive obligation to enable freedom of expression and associated rights.[230] The prospects for this policy option in most of Southern Africa seem slim. This is in light of limited public resources in the region and

226 African Commission on Human and People's Rights, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa', 2019, accessible here.
227 Kathleen Satchwell *et al,* 'Independent Panel Report: Inquiry into Media Ethics and Credibility', 2021, accessible here.
228 Above n 204 at page 6.
229 MISA-Zimbabwe, 'Impact of COVID-19 on media sustainability', 2021, at page 35, accessible here.
230 See for example South African National Editors' Forum, 'Media Sustainability and Universal Access to Public Interest Journalism', 2021, at page 13, accessible here.

especially given that a number of countries have actively pursued policies that restrict the growth and development of diverse media sectors. Moreover, media sustainability is impeded by reliance on donor funding, internal tensions, and unequal capacities amongst media houses.[231]

For example, at least ten SADC countries – **Botswana**, the **Democratic Republic of Congo**, **Lesotho**, **Malawi**, **Mauritius**, **Mozambique**, **Namibia**, **Seychelles**, **Eswatini, Tanzania,** and **Zambia** – impose registration requirements on print media organisations, meaning that publishers should pay the state a fee to establish or maintain a newspaper.[232] In **Zimbabwe**, both newsrooms and individual journalists are required to pay an annual registration or accreditation fee in order to work in the media, which media freedom groups have described as "exorbitant" and designed to exclude certain journalists from accreditation.[233] Similar accreditation fees were introduced in **Mozambique** in 2018.[234] In parallel to these fees on the journalism profession, certain Southern African countries have adopted policies that place a financial barrier on citizen journalists. For example, in recent years authorities in **Tanzania** and **Zambia** faced public criticism after introducing 'taxes' on bloggers and other online content producers, which were predicted to silence citizens and deepen digital divides in those countries.[235] In **Malawi**, the high cost of registering web domains has been identified as an obstacle to publishing locally produced content.[236] This does not align with the principle 15(2)(b) of the ACHPR 2019 Declaration, which provides as follows:

> *"The regulation of community broadcasting shall be governed in accordance with the following principles:*
>
> *(b) Licensing processes shall be simple, expeditious and cost-effective, and guarantee community participation."*

On a more positive note, **Zambia**, which is subject to a range of press freedom concerns, has recently made encouraging moves towards self-regulation for the news media and official recognition of journalism as a profession, which are seen as progress towards developing and securing the media sector.[237]

---

231 Herman Wasserman, 'The Untapped Potential for Regional Cooperation for Media Reform in Southern Africa', March 2021, at page 9, accessible here.
232 *Id.*
233 ALT Advisory, 'Zimbabwe: Newsrooms face "exorbitant" fee increase', 2022, accessible here.
234 Global Voices, 'In Mozambique, new licensing fees have raised the cost of doing journalism — and may threaten media freedom', 2018, accessible here.
235 Global Voices, 'Netizen Report: Internet taxes are sweeping sub-Saharan Africa — and silencing citizens', 2018, accessible here.
236 Freedom House, 'Freedom of the Net 2020: Malawi', 2021, accessible here.
237 Above n 201 at page 8.

Recommendations:

- States should limit interference with media reporting, through traditional or digital channels, and promote an independent and diverse press that is protected through clear and accessible laws.
- Regional bodies and regulatory authorities should challenge the restriction of journalistic activities through the use of privacy, decency, or cybercrime laws.
- States should remove barriers to establishing and maintaining news organisations, monetary or otherwise (such as licensing requirements and pay-walls to credible online news sources), and explore policies that promote the development of independent and critical news media.

MEANINGFUL INCLUSION AND EQUALITY IN THE DIGITAL ENVIRONMENT

Meaningful inclusion and equality at a glance:

- Despite the importance of this issue, and early research by human rights groups, children's rights in the digital age remain underdeveloped in the policy landscape in Southern Africa. This is compounded by a lack of detailed data and statistics regarding children's access to ICTs in the region. Domestically, States should pay particular attention to children's privacy, online safety, and digital literacy and develop policies and educational resources for parents, guardians, and educators.
- Despite global improvements in bridging the gender digital divide, the opposite is true in the African context. Limited access to opportunities in Science, Technology, Engineering, and Mathematics (**STEM**) perpetuates gender inequality. Moreover, recent regional research suggests developing trends regarding the use of technology and online spaces to perpetuate gender-based violence. Collective action across the region is necessary to ensure the digital environment is safe, accessible, and empowering.
- Limited disaggregated data presents a challenge in understanding the number of PWDs without equitable access to ICTs and where access is not an issue, statistics on meaningful access are scarce. SADC's current declaration does not speak to the digital inclusion of PWDs in particular and requires revision. A lack of access to ICTs impedes PWDs from participation in ordinary civil life, particularly when health-related movement restrictions are in force.

Children and the digital environment

A critical part of digital rights discourse is children's right to privacy, given that the internet and digital technology are likely to be embedded in many children's lives from their earliest years.[238] There is a lack of precise figures on the extent of children's access to the internet in Southern Africa, though the United Nations International Children's Fund (**UNICEF**) and the ITU report that by 2021, only 13% of children in both East and Southern Africa were online.[239] This low percentage indicates that children's rights to access are an equally important dimension to consider.

From an international law perspective, the UN General Comment 25 on the Convention on the Rights of the Child (**CRC**) affirms that children's rights shall be respected, protected, and fulfilled in the digital environment.[240] In full recognition of the vulnerabilities of children, the General Comment expressly mentions the evolving capacities of the child, which acknowledges children's gradual acquisition of competencies, understanding, and agency as they develop. The General Comment suggests the following action from States:

238 Children's Rights International Network, 'Briefing: Children's rights in the digital age', undated., accessible here.
239 UNICEF, 'How many children and young people have internet access at home: estimating digital connectivity during the COVID-19 pandemic', December 2021, accessible here.
240 Above n 6.

- The inclusion of child rights impact assessments in national data legislation;
- The integration of children's online protection sections in child protection policies;
- The establishment or designation of a public body specifically mandated to deal with children's rights in the digital environment;
- The allocation of the appropriate public resources to realise children's digital inclusion; and
- The provision of appropriate remedies to bolster access to justice for children who experience online harms, including monetary compensation, restitution, removal of the impugned content, apologies, therapy, follow-up care, and social reintegration.

It is therefore clear that States should take proactive and reactive measures to safeguard children's digital rights.

7.1.1 Best interests of the child principle and user education

International law requires that 'the best interests of the child' should be a primary consideration of any policy or practice relating to the processing of children's personal data, or other aspects of children's digital rights.[241] Article 3 of the CRC binds a host of actors to uphold this principle including public and private welfare institutions, courts of law, administrative authorities, and legislative bodies. Article 3 provides as follows:

> *"1. In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities, or legislative bodies, the best interests of the child shall be a primary consideration.*
>
> *2. States Parties undertake to ensure the child such protection and care as is necessary for his or her well-being, taking into account the rights and duties of his or her parents, legal guardians, or other individuals legally responsible for him or her, and, to this end, shall take all appropriate legislative and administrative measures.*
>
> *3. States Parties shall ensure that the institutions, services, and facilities responsible for the care or protection of children shall conform with the standards established by competent authorities, particularly in the areas of safety, health, in the number and suitability of their staff, as well as competent supervision."*
>
> A balanced approach is necessary given that the internet offers a plethora of benefits for children, including "access to information, opportunities for self-expression, wider horizons of awareness, and a radically extended scope for social interaction."[242] On the other hand, online spaces may pose real risks to children's wellbeing, such as online sexual abuse and exploitation; cyberbullying; the misuse of their data, identity theft; and exposure to inappropriate content.

241 Article 3(2) of the CRC.
242 Child Rights International Network, 'Briefing: Children's rights in the digital age', undated, accessible here.

> The former UN Special Rapporteur on the right to privacy found that "age appropriateness" and "evolving capacity" are both essential considerations for regulatory and educational interventions on children's digital rights.[243]

As more and more children and young people participate in the online world "the right to privacy has come to the forefront of children's rights discourse."[244] Unfortunately, children's right to privacy, and other children's digital rights, remain underexplored in the policy arena in much of Southern Africa, where legislation and policies governing children's rights cater almost exclusively to rights offline.

However, there have been several developments worth noting in the region, especially in relation to measures geared toward protecting children from online sexual exploitation.

7.1.2 Online content protections for children

Without proper safeguards in place, children are at risk of exposure to various types of exploitation and abuse, such as online grooming, the live streaming of child sexual abuse, and online sexual extortion and coercion.[245] Resultantly, it is crucial for stakeholders to remain cognizant and responsive to such harms. The African Union has published a Plan of Action on strengthening regional and national capacity and action against OCSE in Africa.[246] The Plan of Action was created in response to the ACRWC, which, in article 27, requires States to enact measures to prevent the inducement, coercion, or encouragement

243 UN Special Rapporteur on the Right to Privacy, 'AI, privacy and children's privacy,' A/HRC/46/37, 2021, accessible here.

244 Centre for Human Rights, 'A study on children's right to privacy in the digital sphere in the African region' 2022, accessible here.

245 Power Singh Incorporated, 'Deconstruct: Online Gender-Based Violence (OGBV) - Children's Online Safety Toolkit,' 2021, at page 5, accessible here.

246 African Union, 'Online Child Sexual Exploitation and Abuse (OCSEA) Strengthening Regional and National Capacity and Action against Online Child Sexual Exploitation and Abuse in Africa Strategy and Plan of Action 2020 – 2025', accessible here.

of children to engage in sexual activity, the use of children in sex work, or other sexual practices including pornographic activities, performances, and materials. It identifies the Ministries of Social Affairs or Welfare as responsible for enacting the policy while acknowledging that the prevalence and scope of OSCE is still unknown in Africa. Some domestic responses are dealt with below.

Various government agencies in **Mauritius** developed a Child Safety Online Action Plan from 2009 to 2019.[247] The objective of the Action Plan was to prevent the digital sexual exploitation of children and deliver awareness-raising measures aimed at children, parents, and educators. However, there has been a lack of information about the extent of its implementation.[248] Children's rights groups have raised concerns about the lack of coordination between agencies and lack of consultation with civil society[249] to provide support for implementation. A separate report by ECPAT International, a network of civil society organisations working to end child sexual exploitation and trafficking, notes with concern that although Mauritius acknowledges the increasing prevalence of OCSE, the country's laws on key questions, such as whether restrictions on publishing indecent 'photographs' of children apply to videos, audio material, or live streaming of child abuse, remain unclear.[250]

South Africa's Film and Publications Board (**FPB**) is responsible for establishing guidelines and content and age classifications for a wide range of media. The FPB has established a Child Protection team which, among other things, maintains a hotline for users to report any examples of child sexual abuse material online.[251] Several other countries have launched similar initiatives: for example, the government of **Tanzania** launched its reporting portal in 2017, and **Malawi** followed suit in 2018.[252] The **Malawi** Communication Regulatory Authority (**MACRA**) also published a national Child Online Protection framework in 2017 and the Postal and Telecommunications Regulatory Authority of **Zimbabwe** (**POTRAZ**) launched its Child Online Safety Guidelines in 2020.[253]

Not all countries in the region have followed this path. For instance, it has been noted that some States lack legal provisions that are aimed at limiting the online 'grooming' of minors, or a requirement for internet service providers to report child sexual abuse material to authorities.[254]

---

247 Mauritius National Computer Board, 'Child Safety Online Action Plan for Mauritius', 2009, archive version, accessible here.

248 See for example US Department of Labour, 'Findings on the Worst Forms of Child Labour: Mauritius country report', 2019, at page 5, accessible here.

249 Halley Movement, 'Pan-Mauritius Coalition and ECPAT International, Submission on Sexual Exploitation of Children in Mauritius to the UN Committee on the Rights of the Child', 2020, accessible here.

250 ECPAT International, 'A report on the scale, scope and context of the sexual exploitation of children, Mauritius: Country overview', 2019, at page 18, accessible here.

251 Film and Publications Board, 'Child Protection', undated, accessible here.

252 Above n 248.

253 *Id*.

254 *Id* at page 33.

7.1.3 Privacy protections for children

As progress is made in connecting more children in the region to ICTs, there will be even greater urgency to ensure adequate protection for children's data and their right to privacy. Given the mounting challenges associated with the handling of children's data, a multi-stakeholder approach is valuable to promote children's right to privacy, as well as other children's rights that may be affected online.[255]

Under international law, the two relevant instruments on children's rights are the CRC[256] and the ACRWC. The CRC, in article 16, provides that:

> *"1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home, or correspondence, nor to unlawful attacks on his or her honour and reputation.*
>
> *2. The child has the right to the protection of the law against such interference or attacks."*

255 Avani Singh & Tina Power, 'Children's privacy rights in the digital era', 2021, at page 4, accessible here.

256 UN, 'Convention on the Rights of the Child', 1989, accessible here.

> Article 10 of the ACRWC adopts a more nuanced framing of the right and makes reference to "reasonable supervision" on the part of parents or legal guardians. It states:
>
> *"No child shall be subject to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks."*

In **South Africa**, POPIA recognises that children are deserving of particular protection when it comes to the processing of their personal data, and stipulates that a child's personal information may not be processed without a competent person's prior consent.[257] In the event that consent has not been provided, one may process children's personal information by relying on one of the other justifications set out in section 35.[258] These justifications are: if the processing is necessary for the establishment, exercise or defence of a right or obligation in law; if the processing is necessary to comply with an international law obligation; if the processing is for historical, statistical or research purposes where the purpose serves a public interest purpose (and processing is necessary for the fulfilment of the purpose) or where it would be impossible or require disproportionate effort to obtain consent; and if the child's personal information has deliberately been made public by the child with the consent of a competent person.

While there has been limited focus on the implementation of these provisions, the Information Regulator, **South Africa's** data protection authority, issued a guidance note on the processing of children's personal data.[259] The guidance note is to be used by public and private who are required, in terms of POPIA, to obtain authorisation from the Information Regulator before processing children's personal data. In order to process such data, the Information Regulator must be satisfied that the processing is in the public interest and that appropriate safeguards have been put in place to protect the data. Section 4.3. of the guidance note provides clarity on what will be assessed by the Information Regulator when considering whether appropriate safeguards have been put in place. For example, sufficient risk management systems used by the responsible party. In **Mauritius**, a similar amendment Bill has been introduced to give explicit protection to children's right to privacy in law, which provides that *'no person shall do an act which affects the privacy of a child.'*[260]

257 *Id* at page 34.
258 Section 35 of POPIA.
259 Information Regulator South Africa, 'Guidance Note: Processing Personal Information of Children', 2021, accessible here.
260 Above n 238 at page 34.

In addition to observing how other States in Southern Africa have dealt with children's digital rights, UNICEF has collated a rights-by-design standard for data used by technology companies, which recommends the promotion of meaningful and non-monetisable digital experiences, data minimisation, and the use of parent controls of mediation. A combination of these tips, coupled with practical steps for implementation and monitoring and evaluation systems, can assist stakeholders to form a holistic, human-rights-based approach to digital rights.

Recommendations for the digital inclusion of children:

- Data Protection Authorities should develop policies and guidelines that give effect to children's data protection. Further, DPAs should be seen to be enforcing the applicable laws to promote compliance.
- Legislatures should ensure adequate resourcing and capacity-building for public agencies to raise awareness of the need to safeguard children's data, consent, and the importance of children's participation.
- CSOs and Community-based Organisations (**CBOs**) should monitor, and ensure, the implementation of laws on child online protection and privacy.
- Legislatures should consider criminalising acts which amount to the digital sexual exploitation of children and ensure that such legislation evolves as new forms of technologies and harms emerge.

Women and the digital environment

On a global scale, the gender digital divide appears to be closing, yet regrettably, the opposite is true in the African context.[261] This divide is often attributed to lack of access, affordability, and/or economic status, geographical location, racial or ethnic origin, age, and an under-representation of women and girls in educational programmes which would expose them to the digital world.[262] To reaffirm the importance of gender mainstreaming when it comes to digital innovation and inclusion, in July 2022, the UN Human Rights Council adopted a resolution on the elimination of all forms of discrimination against women and girls.[263] Holistically, the resolution expresses concern over the abuse and violence faced by women and girl activists inclusive of defamation and smear campaigns both on- and offline. The resolution also encourages States to make use of an intersectional lens when reviewing proposed and existing legislation which impacts gender equality. Kimberlé Crenshaw, African-American civil rights and race studies academic and feminist, frames intersectionality as the conceptualising and analysing of differing intersecting systems of oppression that individuals may be subjected to as a result of their multi-layered identities.[264]

261 UN Women, 'Addressing the digital gender divide in Africa through the African Girls Can Code Initiative', 21 October 2021, accessible here.
262 OECD, 'Bridging the Digital Gender Divide: Include, Upskill, Innovate', 2022, at page 5, accessible here.
263 UN HRC, 'Elimination of all forms of discrimination against women and girls', A/HRC/50/L.22Rev. 1, 7 July 2022, accessible here.
264 Anna Carathathis, 'The Concept of Intersectionality in Feminist Theory', Philosophy Compass, Volume 9, Issue 5, 7 April 2014, accessible here.

7.2.1. Meaningful participation and empowerment

There is scope for improvement in the creation of practical gender-specific laws and policies to promote the participation of women in the digital environment. Alongside law and policy reform, practical considerations around meaningful opportunities, particularly in STEM fields, require urgent prioritisation. Studies from **South Africa** show that only 20% of women in the ICT sector occupy formal jobs.[265] Further research suggests that of the 22% of computer science graduates that are women, only 2.9% get jobs in the technology sector.[266]

A study conducted by researchers at the Faculty of Economics and Management Science at North-West University in **South Africa** illustrates flagrant disparities between male-led and women-led firms.[267] Interestingly, the study also finds that partly women-owned businesses are more likely to incorporate digital technologies into their operations.

The AU has formulated a strategy in relation to women's empowerment.[268] The strategy seeks to achieve continental gender equality by 2028, in line with the African Union's Agenda 2063. However, apart from noting the factors contributing to the gender digital divide, the strategy is vague on how it intends to achieve e-inclusion. It mentions that the AU will, "Advocate for and lobby tech firms and financial institutions to fund start-ups and innovation hubs which promote gendered solutions and increase women and girls' equal and effective participation in the technology space." Principle 3 of the ACHPR Declaration is particularly relevant here. It prohibits non-discrimination on several grounds, including gender identity, sex, and sexual orientation. While the AU strategy provides a useful base, more specificity is needed as well as further efforts to ensure gender mainstreaming in the education and employment sectors.

7.2.2 Promoting online safety

It is well accepted that online harms are in many ways part of the continuum of violence against women, girls, and gender and sexual monitories that occurs offline.[269] Examples of harassment and threats of physical and sexual violence are increasingly found to seep into online spaces across the region.[270] A recent research report on online gender-based violence (**OGBV**) in Southern Africa revealed concerning trends regarding the proliferation of online

265 Makola. & Kgosinyane, 'How Women End Up in the Information Technology Sector: The Perspectives of South African Women', Academy of Strategic Management Studies, 2020 at page 19, accessible here.

266 South African Institute of International Affairs (SAIIA), 'No women left behind: The gender digital divide technology', 2021, accessible here.

267 Emmanuel Orkoh and Wilman Viviers, 'Gender composition of ownership and management of firms and the gender digital divide in Africa' , July 2021, accessible here.

268 African Union, 'AU Strategy for Gender Equality & Women's Empowerment', 2022, accessible here.

269 Association for Progressive Communication (APC), 'Online gender-based violence: A submission from the Association for Progressive Communications to the United Nations Special Rapporteur on violence against women, its causes and consequences, 2017 at page 3, accessible here.

270 Neema Iyer et al, 'Alternate Realities, Alternate Internets African Feminist Research for a Feminist' 2020, accessible here.

harm in the region.[271] The report reviews trends and policy frameworks relating to OGBV in eight SADC countries, namely, **Angola**, **Botswana**, **Malawi**, **Mozambique**, **Namibia**, **South Africa**, **Zambia,** and **Zimbabwe**. The report further provides country-specific recommendations and finds that the region is not insusceptible to the burgeoning scourge of OGBV. Of interest, insufficient legal protections and inadequate government actions were highlighted as key concerns. In conclusion, the report recommends that collective effort, from various stakeholders, including governments, intermediaries, civil society, the media, and academia, is needed in order to create safe online experiences for all. Further efforts are being explored to monitor responses to OGBV, and in time, identify gaps in law and policy and advocate for change.[272]

In recent months there have been positive law reform efforts in **South Africa**, with the signing of three acts into law which deal with GBV.[273] For present purposes, the most relevant one is the Domestic Violence Amendment Act. Through an expanded definition of 'harassment', the Act caters for online GBV, including, inter alia, the non-consensual tracking of a person's movements, and using social media to send abusive messages which may violate the sexual integrity or dignity of a person. The Cybercrimes Act criminalises the non-consensual sharing of intimate images.[274] From a procedural standpoint, the Domestic Violence Amendment Act allows individuals to apply for protection orders online - a progressive step to expedite the reporting channels of GBV. At this stage, it is unclear what implications, if any, this will have on the enforcement of protection orders.

Of concern, the failures of the criminal justice system have undoubtedly contributed to online 'naming and shaming'. A few examples of this have been seen, for example with the #RUReference List in **South Africa**. This was a social media campaign wherein Rhodes University students circulated the names of alleged perpetrators in order to protest what they deemed to be an inadequate response to sexual violence from the institution. Of further concern are trends relating to litigious efforts aimed at silencing victims and survivors who speak out online. **South Africa** has seen several cases in recent months that, to differing degrees, highlight the "tensions that exist when alleged perpetrators approach the Courts to gag women and prevent them from exercising their right to freedom of expression".[275]

---

271 Centre for Human Rights et al, 'Understanding Online Gender-based violence in Southern Africa', 2022, accessible here.

272 ALT Advisory, Endgbv.Africa, 2021, accessible here.

273 Tina Power, 'New law protects women against online abuse,' GroundUp, 22 February 2022, accessible here.

274 South Africa, 'Cybercrimes Act 19 of 2020', accessible here.

275 See Women's Legal Centre, ','The WLC encouraged by WCHC landmark decision against an interdict seeking to silence rape survivor', 2021, accessible here; See also *Nkosi v Mazwai* [2022] ZAGPJHC 129, accessible here, *S v P and Others* [2022] ZAWCHC 42, accessible here, and Women's Legal Centre, 'High Court vindicates women's rights to speak about their rape experience as a critical way to combat the scourge of violence against women' 2022, accessible here.

Recommendations for the digital inclusion of women and girls:

- States should urgently revise legislation and policy which take reasonable measures to guard against discrimination on the basis of gender.
- The participation of women and girls in the development of these laws and policies should be prioritised.
- Private actors should regulate their price points to increase access to mobile technology for women and girls to facilitate their connection to the internet and link them to educational and labour opportunities.
- Private actors are further responsible for monitoring harmful conduct online and facilitating appropriate complaint and redress mechanisms to address such conduct.

Persons with Disabilities and the digital environment

Regrettably, PWDs are not always front of mind when it comes to digital inclusion and a number of barriers persist when it comes to equitable access to ICTs including the cost of suitable devices and equipment and inadequate measures to incorporate disability-friendly formats and services. The COVID-19 pandemic brought with it a multiplicity of issues when it comes to equitable access for PWDs. During the pandemic, the African Declaration on Internet Rights and Freedoms Coalition released a position paper on efforts, or a lack thereof, by States to promote the enjoyment of rights online.[276] The paper found that PWDs are excluded in terms of access to information, in part due to a lack of access to affordable assistive technologies, and in other parts, due to news and media not being broadcast with accessibility in mind.[277] For instance, individuals with visual and hearing impairments did not receive critical health-related information as quickly, if ever, as others. In light of their categorisation as vulnerable persons during public health emergencies, this is particularly worrisome.

7.3.1 Equal access

As early as 2006, the UN adopted the Convention on the Rights of Persons with Disabilities (CRPD),[278] which places a positive obligation on States to ensure that PWDs can exercise the right to freedom of expression, including the right to access information on an equal basis with others and through all forms of communication of their choice. This should be read together with the Protocol of the ACHPR's on the Rights of Persons with Disabilities (which is not yet in force but may be consulted for guidance).[279] The protocol speaks to, for example, access (article 15), access to health services in particular (article 17), the right to freedom of expression and opinion, (article 23), access to information (article 24), women

276 African Declaration on Internet Rights and Freedoms Coalition, 'Position paper in response to the COVID-19 pandemic, 2020, accessible here.

277 *Id*. at 13-14.

278 UN, 'Convention on the Rights of Persons with Disabilities; A/RES/51/106', 2006, 13 December 2006, accessible here.

279 ACHPR, 'Protocol to the African Charter on Human and People's Rights of Persons with Disabilities in Africa', n.d., accessible here.

and girls with disabilities (article 27), and children and youth with disabilities (articles 28 and 29). Interestingly, the Marrakesh Treaty to Facilitate Access to Published Works for Persons Who Are Blind, Visually Impaired, or Otherwise Print Disabled recognises, "*the positive impact of new information and communication technologies on the lives of persons with visual impairments or with other print disabilities*".[280]

Regionally, States should support PWDs in an ever-evolving digital landscape. Article 18(4) of the African Charter states that:

> *"The aged and the disabled shall also have the right to special measures of protection in keeping with their physical or moral needs."*

The ACHPR 2019 Declaration affirms that everyone, which includes PWDs, shall have the right to exercise freedom of expression and access to information without distinction of any kind. Principle 7 requires States to:

> *"...take specific measures to address the needs of marginalised groups in a manner that guarantees the full enjoyment of their rights to freedom of expression and access to information on an equal basis with others. Marginalised groups include women, children, persons with disabilities, older persons, refugees, internally displaced persons, other migrants, ethnic, religious, sexual or gender minorities."*

Practically speaking, the steps that SADC has taken to foster digital inclusion for PWDs, in particular, are difficult to access. The SADC Declaration falls short of proper recognition of the unique challenges faced by PWDs in accessing ICTs. While the Declaration recognises the existence of a digital divide, it goes no further than this. Accordingly, the natural starting point is for law and policy reform to prioritise the mainstreaming of PWDs in, at the very least, public spaces. To this end, guidance could be sought from the Web Content Accessibility Guidelines (**WCAG**).[281] The WCAG raises important considerations around user interfaces, operable systems, and versatile content that can be interpreted reliably by a wide range of assistive technologies. Drawing on guidelines such as these is important when considering law and policy efforts geared towards meaningful and inclusive access for PWDs. As noted below, this will require input from PWDs in order to fully gauge appropriate and adequate accessibility measures.

280 Marrakesh Treaty to Facilitate Access to Published Works for Persons Who Are Blind, Visually Impaired, or Otherwise Print Disabled (2013).

281 Web Content Accessibility Guidelines, accessible here.

7.3.2 The participation of PWDs in the creation of law and technology

Tanzania is a useful case study on how to properly accommodate the digital rights of PWDs. The country enacted the Person with Disability Act in 2020, which includes access to information, communication, and the physical environment in its definition of accessibility.[282] Further, the establishment of the National Advisory Council for PWDs enables specific public officials and experts to advise the state on realising the rights of PWDs.

Similarly, **South Africa**'s Department of Communications developed a Disability and ICT Strategy,[283] which sets out the status of disability mainstreaming in specific state-owned enterprises (**SOEs**). The strategy identifies priorities to better support PWDs. For example, creating a mainstreaming strategy for the ICT sector and amending existing policies, developing a communications strategy with sufficient budget and reasonable timeframes to promote awareness of legislative and policy changes, building capacity in public departments, and SOEs to implement disability mainstreaming, and coordinating training at focal points.

Recommendations for the digital inclusion of PWDs:

- States should develop ICT strategies which specifically cater for the needs of PWDs.
- To the extent possible, individual state ministries should promote e-accessibility for administrative tasks in which ordinary citizens are obliged to partake in. For example, online taxing systems and e-voting should be explored. The need for this was clear during the COVID-19 pandemic.
- In collaboration with each other, state and private actors should create accessible digital literacy programs for PWDs, particularly where they may receive training on utilising assistive technology.
- CSOs and National Human Rights Institutions (NHRIs) may consider collating more precise and updated data on the specific needs of PWDs. This collection may also be done through government-managed Census surveys.
- DPAs should enable data subjects to exercise their rights electronically and orally should they so elect.

282 Patricia Boshe, 'eAccessibility for persons with disability in Tanzania: an assessment of policy and legal frameworks', Open University Law Journal, Volume 4, Number 1, at page 109, 2013, accessible here.

283 South Africa, The Department of Communications, 'Disability and ICT Strategy', 'n.d., accessible here.

CONCLUSION

The challenges outlined above may paint a bleak picture. It is clear that Southern African countries still have some way to go before digital rights are fully protected in line with international law and best practices. However, there is some hope. A number of States in the region have demonstrated increased awareness of the socio-economic advantages of digitisation and enhanced protection for digital rights. Broadly, there has been a slow but steady trend toward the enactment of laws that are relevant to the digital environment including data protection legislation. States should continuously prioritise these legislative reforms. Other stakeholders, the judiciary, regulatory data authorities, the media, and the private sector all have a contribution to make towards the advancement of digital rights and freedoms. The presence of a vibrant civil society, and human rights institutions across the region is a positive attribute that is key to promoting and defending digital rights.

RECOMMENDATIONS FOR STAKEHOLDERS

As outlined above, progress in Southern Africa in realising digital rights has been halting, though there are improvements nonetheless. These improvements include:

- The enactment of data protection legislation and standards in most SADC States;
- An overall trend, albeit slow, in most SADC States towards improved access to ICTs for many parts of the population, including through improved internet penetration rates, and lower costs for mobile and broadband internet;
- Reform in the surveillance laws of several countries. This reform has manifested through policymaking and jurisprudence, to improve oversight and safeguards in the interception of communications;
- Early developments in jurisprudence to safeguard against the use of tactics such as SLAPP suits to stifle dissent and criticism of the powerful public and private actors;
- In select parts of the region, moves towards progressive media development, including self-regulation of the news media sector, including online media actors; and
- Through the enactment of legislation and policy, increased awareness of the need to strengthen children's online protections including their privacy.

However, there is a wide range of policies and practices throughout the region that restrict or infringe on digital rights. The infringements impact fundamental rights such as freedom of expression, the right to privacy and data protection, the right of access to information, and dignity and equality.[284] These require concerted attention from diverse stakeholders across each country and at a regional level. The enormity and complexity of these challenges call for a multi-stakeholder approach that facilitates participatory decision-making with an understanding of the various interests to be balanced. A multi-stakeholder approach ensures the inclusion of voices and concerns of marginalised groups; allows for technical expertise over multiple areas; and ensures broad public support for the outcomes of policy processes and other decisions.[285]

284 African Declaration on Internet Rights and Freedoms, 'The struggle for the realisation of the right to freedom of expression in Southern Africa', 2020, accessible here.

285 Ashnah Kalemera, 'How applicable is the multi-stakeholder approach to Internet Governance in Africa', CIPESA, 23 December 2016, accessible here.

From a continental perspective, the importance of collaboration on internet governance processes has already been identified. For example, proceedings at the 11th Internet Governance Forum noted considerable challenges to multi-stakeholder approaches at a domestic and regional level, including a lack of political will and limited expertise on internet governance issues.[286] Despite these surmountable challenges, the digital rights space requires a level of uniformity and partnership to ensure meaningful access to the internet and other digital technologies. Uniformity and partnership are also critical for the purposes of combating the abuse and exploitation of individuals online and protecting their personal information.

Regional bodies

Through existing regional and continental instruments, regional bodies and policymakers already have a foundation for strengthening digital rights governance. These regional bodies, which include the SADC Secretariat and relevant SADC Directorates, structures of the African Union, and other regional leadership forums, should consider the following strategies to strengthen this foundation.

Encourage States to enact and implement data protection and privacy legislation

- States and legislatures should expedite the enactment and enforcement of data protection laws. As outlined in section 3, several States have not yet enacted these laws, and many of those that have enacted laws are still in the process of implementing them with limited public reporting on progress. The continued processing of personal information in many parts of the region outside the parameters of a clear or enforceable framework is a cause for concern. Finalising these processes would trigger the duties of regulatory bodies to monitor, enforce and test the strength of the legislation.
- At a regional level, the Southern African States and legislatures should prioritise ratification of the Malabo Convention, which requires at least two more state ratifications to be brought into operation. Doing so would create a harmonising framework for data protection policy across the continent, and enhance the efforts to embed data protection law at domestic levels. It is also necessary to review outdated provisions of the Convention given that it was adopted almost a decade ago.

286 *Id.*

Raising awareness

The lack of alignment to international and regional frameworks in many state-level laws and practices speaks to significant gaps in knowledge and understanding of digital rights by state actors and policymakers.

- States and applicable regional bodies should establish regional working groups and expert panels to draw on expertise from CSOs, the media, and industry to fill in knowledge gaps on the intricacies and implications of emerging technologies from a human rights perspective. These bodies should include diverse stakeholders and incorporate perspectives from vulnerable and marginalised groups.
- These regional groups should foster learning and awareness-raising among public servants and elected officials on the applicable regional and domestic digital rights instruments in accessible and affordable ways.
- These regional groups should foster public awareness of these mechanisms for citizens, and ensure access to information about digital rights is readily available in central information portals. Presently, the instruments are fragmented online and are often inaccessible to the average citizen. Readability also forms a critical aspect of access. This would necessitate the development of simple, easy-to-read versions of the instruments.
- Working with States and legislatures, and the applicable SADC Units, the SADC Secretariat should establish regular reporting and monitoring of compliance with existing mechanisms at a domestic and regional level, and track updates and developments to existing frameworks. Such updates should be available across the spectrum of the official languages spoken in Southern Africa, at the very least.

Government bodies and policymakers

There is room for significant improvement with respect to the internet penetration rate and digital literacy skills in Southern Africa. This requires sufficient investment in improving network infrastructure, supporting research initiatives, and capacity building to enable continuous learning on the harnessing of digital skills for States, collaboration with Data Protection Authorities, and introducing and improving digital literacy and access in education.

Initiatives to improve access to the internet

- States should allocate sufficient funding and resources toward universal, equitable, and meaningful internet access, through the development and expansion of ICT infrastructure.
- If this requires States to explore public-private partnerships, it should be prefaced with rigorous public participation, and the development of clear standards and safeguards to ensure the delivery of secure and meaningful access, and to ensure all public and

private entities are subject to robust oversight and governance.

- States should take specific steps to deliver reliable and affordable digital access in peri-urban and rural communities, including improved internet and energy infrastructure. This may include the exploration of alternative and renewable energy to support ICT infrastructure in non-urban areas.
- States should also explore policy and licensing arrangements to enable cheaper, better mobile broadband provision in urban, peri-urban, and rural areas.

Bridging digital divides

Moreover, specific policies should be undertaken across the region to address the gender divide.

- States should prioritise accessible educational opportunities for girls and women, including modules to boost their digital and technological literacy skills. There should be an availability of educational opportunities beyond the formal schooling period.
- States should seek to create job opportunities for women in STEM and ICTs, create gender-specific goals and programmes which are accessible, and ensure adequate monitoring and evaluation occurs.

Collaboration with and capacitating Data Protection Authorities

- States and Data Protection Authorities in the region should promote regional collaboration, including through bodies such as the Network of African Data Protection Authorities (**NADPA**), to share strategies and best practices at a regional level, and lower the barriers to the implementation of data protection policies at a domestic level.
- In order for DPAs to carry out their functions, they should be properly resourced and operationalised. This includes the employment of independent data privacy experts and providing them with the requisite tools to effectively manage large volumes of work related to compliance and enforcement. To the extent possible, DPAs should be empowered to operate online.

Research and capacity building

The establishment of structures and committees tasked to manage digital rights issues enables states to build capacity for individuals to contribute to solutions on prevalent issues as well as to empower themselves. It is also necessary to ensure adequate research, training, and knowledge management issues in order to foster proper policy making and implementation on key digital rights issues.

- States and policymakers should ensure adequate funding for ICT research and innovation across the public sector, with a strong emphasis on digital rights, to remain alert to the potential harms which new technologies may cause and better understand

the ethics around these advancements.

- States should prioritise accurate research and data collection on key metrics related to digital rights, such as assessing the extent of gender inequalities in ICT access, children's access, and the access of PWDs to the internet. These findings should be publicly available and shared at a regional level to address information gaps.

Policy reforms to enable free expression and media development

- States and policymakers should recognise the importance of creating an enabling environment for media freedom and freedom of expression, including dissent and criticism of public bodies and officials, as a means of strengthening democracy and accountable governance.
- In pursuit of this, States and policymakers across Southern Africa should urgently suspend, reform, and repeal policies that frustrate free expression and undermine freedom of the press. This may include provisions in criminal and civil law, fiscal policy, and communication policy.
- States should establish and improve mechanisms for non-partisan, public funding of news media organisations, which is free from political interference.
- States should also explore other policy interventions to create a more enabling environment for media development, including the waiving of media registration fees, the reduction of publishing costs such as domain registrations, and business-policy reforms to foster the development of small media enterprises.

The judiciary

As custodians of the rule of law, the judiciary plays a unique role in upholding digital rights.

Building the capacity for courts to engage in digital rights issues

- Judicial officers should foster training and capacity building for all members of the judiciary to ensure adequate knowledge and understanding of emerging digital rights issues, and applicable international standards and best practice.
- Where appropriate, courts should uphold the anonymity of victims of digital rights violations, particularly where such persons have limited legal capacity.

Striking down harmful laws and standards

Where the facts of a matter before a court show an unlawful or unconstitutional breach of digital rights, the judiciary should maintain its independence from powerful state or private actors, and ensure any decision of the court upholds the rule of law, safeguards protected rights, and creates any necessary progressive precedent.

Data Protection Authorities

The main function of DPAs is to protect the rights and interests of data subjects and enforce domestic legislation. DPAs play an indispensable role in working towards sound digital governance.

Enforcing data protection legislation

DPAs should actively monitor and enforce regulatory compliance across all industries, and publish guidance notes and directives on existing and emerging data protection issues.

Regular and accessible communication with the public

- DPAs should build public trust and awareness of data protection law by ensuring their work is visible and accessible to the public and available in easy-to-access formats, including through up-to-date websites and all applicable languages.
- To the extent possible, DPAs may consider partnering with the relevant domestic communications authorities and various ombudsmen across different sectors to alleviate strained capacity.

Civil society and NHRIs

CSOs, NHRIs, and digital rights activists have made valuable progress in advancing digital rights across the region and should deepen work to empower communities and build the social capital to hold institutions to account.

Public participation and treaty-body reporting

- Prior to the enactment of law and policy, CSOs and NHRIs can leverage public participatory processes to ensure that diverse perspectives are taken into account by policy-makers.
- CSOs and NHRIs should pay particular attention to enabling the participation of marginalised and under-represented groups in such processes, including rural communities, children, persons with disabilities, and sexual minorities, to ensure that digital rights policies are inclusive of their needs.

Advocacy

The importance of CSO-led advocacy campaigns in achieving existing advances in digital rights cannot be overstated. Given the significant ongoing challenges for digital rights in the region that this report has flagged, these efforts should continue.

- CSOs and NHRIs should expand research and awareness-raising on key digital rights issues, especially to ensure adequate framing of gender and PWDs within digital rights. While social media campaigning is an apt platform for digital rights advocacy, given

the low rates of internet access and digital literacy in Southern Africa, CSOs and NHRIs may consider exploring multi-layered approaches that include adequate provisions for offline or 'analogue' engagement and messages that are inclusive of communities with limited access to ICTs.

- CSOs and NHRIs should continue to build regional collaborations and alliances with civil society groups in other Southern African communities. This should foster learning to ensure that the relevant communities with existing expertise in one country can offer capacity-building and support to partner organisations in another. Most importantly, by strengthening regional alliances, CSOs and NHRIs can increase their collective influence on digital rights issues across Southern Africa.
- In order to foster positive dialogue and learning on key digital rights issues, CSOs and NHRIs should explore the use of multi-stakeholder forums to develop strategic opportunities for policy change and other advances on digital rights.
- While much digital rights advocacy in Southern Africa is necessarily directed towards the powers and prerogatives of state bodies, CSOs and NHRIs should also seek to develop advocacy strategies that address the growing power and influence of global technology companies in the region.

Strategic litigation

Vital advances in digital rights in the region often result from strategic litigation, including legal challenges to internet shutdowns, and test case litigation on defamation, hate speech, and other speech-related offences. These successes do not only have an impact domestically but can often inform further litigation and jurisprudence in other countries regionally and internationally.

- CSOs and NHRIs should continue to identify opportunities for strategic litigation that will develop progressive jurisprudence, especially in instances where engagement with policymakers and other stakeholders is not possible or has not yielded results.
- In particular, these bodies should explore avenues for strategic litigation on digital rights matters which have the widest impact on the population and where there are significant common patterns across the region. Examples of these include internet shutdowns, abuse of defamation mechanisms, and data protection violations.
- CSOs and NHRIs, especially those focused on human rights law, should share research and coordinate across borders in order to support litigation strategies in other jurisdictions and develop regional jurisprudence.
- Where possible, these bodies should support awareness-raising and capacity-building among court officials and other members of the legal community to enhance understanding of emerging issues of human rights and digital technology.

Media organisations

Whether traditional or digital, the media exists to inform, educate, and entertain the public. To uphold freedom of expression, access to information, and associated rights, the media should be independent of state actors, influential private sector actors, and politicians. To do so, journalists and other media practitioners should be well-resourced and protected by the judiciary, legislature, and executive.

Lobbying for the development of public funding for journalism

- Media organisations should research and advocate for policy reforms and funding mechanisms to enable independent, sustainable, and quality journalism. This may include new measures for non-partisan public funding for independent and community news organisations.
- Media organisations should also pursue other enabling policy reforms, such as measures to reduce operating and compliance costs for independent news organisations and journalists, including registration fees levied on media workers and organisations in certain Southern African countries.

Monitoring and evaluating

Media organisations can also play an enabling role for digital rights through journalism and news making. The media can also hold regional bodies, government actors, DPAs, and the private sector to account for their respective roles and responsibilities in digital rights governance, and reporting on digital rights violations to the public.

Private actors

The private sector has an integral part to play in the advancement of digital rights. In view of increasing advancements in digital technology, private technology companies are likely to grow in influence in the region. Given the role of ISPs, social media companies, and other private actors in shaping how people access and share information, and the process of people's most personal information, they hold a dual role in both public and private spheres. Accordingly, it is critical for private actors to adopt a rights-based approach and operate on clearly outlined principles of social responsibility in conformity with the normative framework established in the UN's Guiding Principles on Business and Human Rights.[287]

Content regulation

- Where private technology companies are called to engage in content moderation, they should develop policies and processes that promote a diversity of political views and perspectives. They should undertake to moderate content online on grounds that are in line with international law and best practices.[288]
- Private actors should minimise automated filtering of content, and should rather opt for systems that enable end-user control.[289] Any system established to monitor for or adjudicate complaints of legitimately harmful content, such as hate speech, should be transparent, responsive, and adequately resourced to ensure it is catered to local contexts and languages.

Cooperation with other stakeholders and commitment to digital rights

Private actors have an opportunity to support meaningful and transparent engagement with States as they develop digital rights laws and policies.[290]

- Private enterprises should use their reach and influence to spotlight human rights violations and abuse of power.[291]
- Private actors should not succumb to political pressure which leads to unlawful and unjustifiable limitations on digital rights. In particular, ISPs and network operators should not enable internet shutdowns, or engage in state-enforced removal of content that is legitimate dissent or criticism.

---

287 United Nations, 'Principles on Business and Human Rights', 2011, accessible here.
288 The Danish Institute for Human Rights, 'Tech Giants and Human Rights: Investor Expectations', 2021, at page 19, accessible here.
289 Pedro Hartung, 'The children's right-by-design standard for data use by tech companies', November 2020, accessible here.
290 Molly Galvin, 'Human rights in age of social media, big data, and AI' , National Academis, 2019, accessible here.
291 *Id.*

- Private technology companies should make regular, proactive disclosures of statistics and other information about the use of their services, and any requests or processes by state actors or other parties that affect the digital rights of their users. Such transparency measures are vital to ensuring CSOs, policymakers, and the broader public are informed on key aspects of digital rights compliance at a national or regional level.
- Above all, private actors should operate ethically and lawfully in their own business activities, including minimising the collection of personal data and ensuring the overall digital wellbeing and safety of their users.

REFERENCE LIST

Case law

- *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others* (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) 2021, accessible here.
- *Masuku and Another v South African Human Rights Commission on behalf of South African Jewish Board of Deputies* (1062/2017) [2018] ZASCA 180, accessible here.
- *Mineral Sands Resources Propriety Limited and Another v Christine Reddell and Others* CCT 66/21 and CCT 67/21, accessible here.
- *Nkosi v Mazwai* [2022] ZAGPJHC 129, accessible here.
- *Qwelane v South African Human Rights Commission and Another* (CCT 13/20) [2021] ZACC 22, accessible here.
- *S v P and Others* [2022] ZAWCHC 42, accessible here.

Journal articles

- Alex Makulilo, 'Privacy and data protection in Africa: a state of the art, International Data and Privacy Law', 2012, Volume 2, No. 3, accessible here.
- Alex Najibi, 'Racial Discrimination in Face Recognition Technology', Harvard University, Blog, Science Policy, Special Edition: Science Policy and Social Justice', 2020, accessible here.
- George Pring, 'SLAPPs: Strategic Lawsuits against Public Participation, 7 Pace Envtl. L. Rev. 3 (1989), accessible here.
- Jane Duncan and Julie Reid, 'Toward a measurement tool for the monitoring of media diversity and pluralism in South Africa: A public-centered approach,' Communication: South African Journal for Communication Theory and Research, 2013, accessible here.
- Jessica Dheere, 'A methodology for mapping the emerging legal landscapes for human rights in the digitally networked sphere. In Global information, society watch 2017. Unshackling expression: a study on laws criminalising expression online in Asia', (Special edition, pp. 6–17), India: Association for Progressive Communications, 2017, accessible here.
- Klaaren and Ray, 'South Africa's Technologies Enhancing Contact Tracing for COVID-19: A Comparative and Human Rights Assessment' South African Journal on Human Rights, 2022; Hunter, 'Track and Trace, Trial and Error: Assessing South Africa's Approaches to Privacy in COVID-19 Digital Contact Tracing', Media Policy and Democracy Project, 2020, accessible here.

- Nyane Hoolo, 'Abolition of criminal defamation and retention of scandalum magnatum in Lesotho' 19 African Human Rights Law Journal, 2019, accessible here.

Legal instruments and policies

- ACERWC, 'The Protection and Promotion of Children's Rights in the Digital Sphere in Africa', Resolution No. 17/2022, accessible here.
- ACHPR, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa', 2019, accessible here.
- ACHPR, 'Resolution on the right to freedom of information and expression on the internet in Africa', ACHPR/Res.362(LIX), 2016, accessible here.
- ACHPR. 'Resolution on Repealing Criminal Defamation Laws in Africa, 'ACHPR/Res.169(XLVIII) 2020', accessible here.
- ACHPR, 'Protocol to the African Charter on Human and Peoples' Rights on the rights of persons with disabilities in Africa', n.d, accessible here.
- African Charter on Human and People's Rights, accessible here.
- African Committee of Experts on the Rights and Welfare of the Child, 'Africa's Agenda for Children 2040,' 2016, accessible here.
- African Declaration on Internet Rights and Freedoms, 'The struggle for the realisation of the right to freedom of expression in southern Africa', 2020, accessible here.
- African Union Convention on Cyber Security and Personal Data Protection, 2014, accessible here.
- African Union, 'AU Strategy for Gender Equality & Women's Empowerment', 2022, accessible here.
- Angola Law No. 22/11, 2011, accessible here.
- Botswana Data Protection Act, 2018, accessible here.
- Children's Amendment Bill, B18-2020, accessible here.
- Constitution of the Republic of South Africa, 1996, accessible here.
- Eswatini Data Protection Act, 2022, accessible here.
- Information Regulator South Africa, 'Guidance Note on the Processing of Personal Information in the Management and Containment of COVID-19 Pandemic in terms of the Protection of Personal Information Act 4 of 2013 (POPIA)', n.d., accessible here.
- Joint Declaration on Freedom of Expression and the Internet, 2011, accessible here.
- Lesotho Data Protection Act, 2012, accessible here.
- Madagascar Law No. 2014-038 (DP Law), 2015, accessible here.
- Malawi Data Protection Bill, 2021, accessible here.
- Mauritius Data Protection Act, 2017, accessible here.
- Protection of Personal Information Act 4 of 2013, accessible here.

- SADC Declaration on Information and Communications Technology, 2001, accessible here.
- SADC, 'Data Protection: Southern African Development Community Model Law', 2013, accessible here.
- SADC, 'Declaration on Information and Communication Technology, 2001, accessible here.
- Seychelles, 'Data Protection Act, 2003', accessible here.
- South Africa, 'Cybercrimes Act 19 of 2020', accessible here.
- South Africa, The Department of Communications, 'Disability and ICT Strategy', 'n.d., accessible here.
- South Africa, 'Protection of Personal Information Act, 2013', accessible here.
- South Africa, 'Regulations issued in terms of section 27(2) of the Disaster Management Act 2002, GN 43107, GG 318, 18 March 2020, accessible here.
- UN Committee on the Rights of the Child, 'General Comment 25: Children's rights in relation to the digital environment' CRC/C/GC25 (2021), accessible here.
- UN, 'Convention on the Rights of Persons with Disabilities; A/RES/51/106', 2006, 13 December 2006, accessible here.
- UNHRC, 'Elimination of all forms of discrimination against women and girls', A/HRC/50/L.22/Rev. 1, 7 July 2022, accessible here.
- UN General Assembly, 'International Covenant on Civil and Political Rights, 1966, accessible here.
- UN Human Rights Committee, 'General Comment No. 34. Article 19: Freedoms of opinion and expression', CCPR/C/GC/34, 12 September 2011, accessible here.
- UN, A/HRC/50/55, 'Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights', 13 May 2022, accessible here.
- UNHRC, 'Freedom of opinion and expression', A/HRC/50/L.11, 30 June 2022, accessible here.
- UN Human Rights Council, 'The promotion, protection and enjoyment of human rights on the Internet', A/HRC/32/L.20, 2016, accessible here.
- UN Human Rights Council, 'The right to freedom of peaceful assembly and association', A/HRC/50/L/20, 4 July 2022, accessible here.
- UN, 'Special Rapporteur on the right to privacy, in a report on AI, privacy, and children's privacy', A/HRC/46/37, 25 January 2021, accessible here.
- United Nations, 'General Comment 25: Children's rights in relation to the digital environment', February 2021, accessible here.
- United Nations, 'Guiding Principles on Business and Human Rights, 2011, accessible here.
- United Nations, 'The right to privacy in the digital age', A/HRC/48/21, 3 September 2021, accessible here.

- United Nations, 'Resolution on the promotion, protection and enjoyment of human rights on the Internet', A/HRC/32/L.20, 27 June 2016m accessible here.
- United Nations, 'Universal Declaration of Human Rights', 1948, accessible here.
- Zambia Data Protection Act, 2021, accessible here.
- Zimbabwe Data Protection Act, 2021, accessible here.

Research reports, theses, and reference texts

- African Declaration on Internet Rights and Freedoms, 'The struggle for the realisation of the right to freedom of expression in Southern Africa', 2020, accessible here.
- African Freedom of Expression Exchange, 'Statement on the recently reported internet throttling in Zimbabwe', 22 February 2022, accessible here.
- ALT Advisory *et al*, 'Access denied: Internet in Schools', 2020, accessible here.
- Anna Carathathis, 'The Concept of Intersectionality in Feminist Theory, Philosophy Compass, Volume 9, Issue 5, 7 April 2014, accessible here.
- Andrew Maramwidze, 'Botswana intensifies SmartBots digitisation strategy', ITWeb, 25 November 2021, accessible here.
- Article 19, 'Tanzania: Online Content Regulations 2020 extremely problematic in the context of COVID-19', accessible here.
- Ashnah Kalemera, 'How applicable is the multi-stakeholder approach to Internet Governance in Africa', CIPESA, 23 December 2016, accessible here.
- Avani Singh & Tina Power, 'Children's privacy rights in the digital era', 2021, accessible here.
- Bill Marczak *et al*, 'Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries' Citizen Lab Research Report No. 113, 2018, accessible here.
- Bill Marczak *et al,* 'Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles' Citizen Lab Research Report No. 133, 2020, accessible here.
- Centre for Human Rights, 'A study on children's right to privacy in the digital sphere in the African region,' Pretoria University Law Press, 2022, accessible here.
- Dylan Green *et al*, 'Using mobile phone data for epidemic response in low resource settings—A case study of COVID-19 in Malawi', Data & Policy, 3, 2021, accessible here.
- Electronic Frontier Foundation, 'RightsCon: Contemplating content moderation in Africa: disinformation and hate speech in focus', June 2021, accessible here.
- Emmanuel Orkoh and Wilman Viviers, 'Gender composition of ownership and management of firms and the gender digital divide in Africa' , July 2021, accessible here.
- Eugenia Sipaer, 'AI Content Moderation, Racism, and (de)Coloniality', International Journal of Bullying Prevention, August 2021, accessible here.

- Halley Movement, Pan-Mauritius Coalition and ECPAT International, Submission on Sexual Exploitation of Children in Mauritius to the UN Committee on the Rights of the Child, 2020, accessible here.
- Herman Wasserman, 'The Untapped Potential for Regional Cooperation for Media Reform in Southern Africa', March 2021, accessible here.
- Human Rights Watch, 'Shutting Down the Internet to Shut Up Critics', 2020, accessible here.
- Information Regulator South Africa, 'Guidance Note: Processing Personal Information of Children', 2021, accessible here.
- ITU, 'Digital trends in Africa 2021: Information and communication technology trends and developments in the Africa region 2017 - 2020', 2021, accessible here.
- ITU, 'Measuring digital development: Facts and figures 2021', 2021, accessible here.
- Jentzsch, 'Implications of mandatory registration of mobile phone users in Africa', Telecommunications Policy 36, 2012, accessible here.
- Jimmy Kainja, 'Are Malawians Sleep-Walking into a Surveillance State?', CIPESA, 12 August 2019, accessible here.
- Justine Limpitlaw, 'Media Law Handbook for Southern Africa', Second Edition, Konrad-Adenauer-Stiftung, 2021, accessible here.
- Kathleen Satchwell *et al*, 'Independent Panel Report: Inquiry into Media Ethics and Credibility', 2021, accessible here.
- Legal Resources Centre, 'Statement to the African Commission on Human and Peoples' Rights', 2018, accessible here.
- Lester Henry, 'Bridging the urban-rural digital divide and mobilizing technology for poverty eradication: challenges and gaps', 2017, accessible here.
- Lexology and Hogan Lovells, 'Recent developments in African data protection laws – Outlook for 2022', undated, accessible here.
- Londa, 'Digital Rights and Inclusion Africa Report: 2021', 2022, accessible here.
- Marta Nowakowska and Agnieszka Tubis, 'Loadshedding and the energy security of Republic of South Africa', October 2015, accessible here.
- Mauritius Artificial Intelligence Strategy, 2018, accessible here.
- Media Defence, 'Module 5: Summary Modules on Litigating Digital Rights and Freedom of Expression Online', 2020, accessible here.
- MISA-Zimbabwe, 'Beyond a Click: Regional assessment on state of digital rights: Southern Africa', undated, accessible here.
- MISA-Zimbabwe, 'Zimbabwe Input for Report on Disinformation', undated, accessible here.
- Molly Galvin, 'Human rights in age of social media, big data, and AI', National Academies, 2019, accessible here.

- Murray Hunter and Admire Mare, 'A Patchwork for Privacy: Mapping communications surveillance laws in southern Africa', 2020, accessible here.
- Murray Hunter, 'Don't impose new health policy until we understand impact of Covid data collection', News24, 2022, accessible here.
- Nelson Banya, 'Power crisis turns night into day for Zimbabwe's firms and families', Reuters, 1 August 2019, accessible here.
- Neema Iyer et al, 'Alternate Realities, Alternate Internets African Feminist Research for a Feminist' 2020, accessible here.
- OECD, 'Bridging the Digital Gender Divide: Include, Upskill, Innovate', 2022, accessible here.
- OECD, 'Digital transformation in the age of COVID-19',2020, accessible here.
- OHCHR, Statement by Mr. Joseph A. Cannataci, Special Rapporteur on the right to privacy, at the 31st session of the Human Rights Council, 2017, accessible here.
- Patricia Boshe, 'eAccessibility for persons with disability in Tanzania: an assessment of policy and legal frameworks', Open University Law Journal, Volume 4, Number 1, 2013, accessible here.
- Paul Kimumwe, 'Towards an Accessible and Affordable Internet in Africa: Key Challenges Ahead', CIPESA, accessible here.
- Pedro Hartung, 'The children's right-by-design standard for data use by tech companies', November 2020, accessible here.
- Philip Ross, 'Towards a 4th industrial revolution,', Intelligent Buildings International, March 2021, accessible here.
- Power Singh Incorporated, 'Deconstruct: Online Gender-Based Violence (OGBV) - Children's Online Safety Toolkit,' 2021, accessible here.
- Privacy International, 'Africa: SIM Card Registration Only Increases Monitoring and Exclusion', 2019, accessible here.
- Privacy International, 'Apps and Covid-19', n.d., accessible here.
- Privacy International, 'Telecommunications data and Covid-19', n.d., accessible here.
- Rachel Sibande and Tyler Smith, 'Using mobile phone records to improve public health: evidence from Malawi', Center for Global Development, 10 December 2021, accessible here.
- SACDC, 'Guidance on Contacting Tracing for COVID 19 Pandemic', April 2020, accessible here.
- Sekoetlane Phamodi *et al*, 'Making ICT Policy in Africa: An Introductory Handbook', Fesmedia Africa, August 2021, Page 2, accessible here.
- Southern African Development Community, 'e-SADC strategic framework', 2010, accessible here.
- Special Rapporteur on Freedom of Expression and Access to Information in Africa,

Guidelines on access to information and elections in Africa, 2017, accessible here.

- Special Rapporteur on Freedom of Expression and Access to Information in Africa, Statement on the Importance of Access to the Internet in Responding to the COVID-19 Pandemic, 2020, accessible here.
- The Danish Institute for Human Rights, 'Tech Giants and Human Rights: Investor Expectations', 2021, accessible here.
- The GSMA, 'The State of Mobile Internet Connectivity 2021', accessible here.
- Tina Power, 'New law protects women against online abuse,' GroundUp, 22 February 2022, accessible here.
- Tomiwa Ilori, 'Content moderation is particularly hard in African countries, 21 August 2020, accessible here.
- Ulkrie Kahbila Mbuton, 'The role of the African Committee of Experts on the Rights and Welfare of the Child in the follow-up of its decisions on communications', University of Pretoria, 2017, accessible here.
- UN Women, 'Addressing the digital gender divide in Africa through the African Girls Can Code Initiative', 21 October 2021, accessible here.
- UNHCR, 'Using Social media in Community Based Protection: A Guide', January 2021 accessible here.
- UNCTAD, 'Launch of the ICT Policy Review and National E-commerce Strategy for Botswana', 2021, accessible here.
- UNICEF, 'How many children and young people have internet access at home: estimating digital connectivity during the COVID-19 pandemic', December 2021, accessible here.
- United Nations Conference on Trade and Development, 'Data Protection and Privacy Legislation Worldwide', accessible here.
- University of Pretoria, 'Artificial Intelligence for Africa: An Opportunity for Growth, Development, and Democratisation', undated, accessible here.
- US Department of Labour, 'Findings on the Worst Forms of Child Labour: Mauritius country report', 2019, accessible here.

Media sources and other

- Access Now, '#KeepItOn update: who is shutting down the internet in 2021?', 7 June 2021, accessible here.
- African Union Press Release, 'African Digital Transformation Strategy and African Union Communication and Advocacy Strategy among major AU initiatives in final declaration of STCCICT', 26 October 2019, accessible here.
- African Union, 'Status List: List of countries which have signed, ratified/acceded to the Malabo Convention', 23 June 2022, accessible here.

- Afrobarometer, 'Africa's digital gender divide may be widening, Afrobarometer survey finds', 4 November 2019, at page 4, accessible here.
- Aisaatou Sylla, 'Recent developments in African data protection laws – Outlook for 2022', 1 February 2022, accessible here.
- Alex Moltzau, 'The AI Strategy of Mauritius', 11 February 2020, accessible here.
- ALT Advisory 'Zimbabwe: Newsrooms face "exorbitant" fee increase' 7 April 2022, accessible here.
- ALT Advisory, 'Data Protection Africa: Angola Factsheet', 2020, accessible here.
- ALT Advisory, 'Data Protection Africa: South Africa Factsheet', 2021, accessible here.
- Article19, 'South Africa: Prohibitions of false COVID019 information must be amended,' 23 April 2021, accessible here.
- Bloomberg, 'Eskom nears record for worst year of loadshedding ever - and there's still 6 months to go', 2 July 2022, accessible here.
- Film and Publications Board, 'Child Protection', undated, accessible here.
- Freedom House, 'Freedom of the Net 2020: Malawi', 2021, accessible here.
- Jonathan Rozen 'Botswana journalists remain 'vigilant' under new surveillance law', News24, 2022, accessible here.
- Joseph Kabila, 'DRC Congo internet restored after 20-day suspension over elections', 20 January 2019, accessible here.
- Juliet Nanfuka, 'Zimbabwe becomes the latest country to shut down social media', CIPESA, 7 July 2016, accessible here.
- Mauritius National Computer Board, 'Child Safety Online Action Plan for Mauritius', 2009, archive version accessible here.
- MDN, 'Web Docs Glossary: Definitions of web-related terms', undated, accessible here.
- Media Centre at Egypt Ministry of Communications and Information Technology webpage, 6 December 2019, accessible here.
- MISA-Zimbabwe, 'High Court sets aside internet shutdown directives', 21 January 2019, accessible here.
- MISA-Zimbabwe, 'The State of Press Freedom in Southern Africa 2019-2020', 2021, accessible here.
- Morgan Meaker, 'African countries' growing app-etite for Coronavirus apps gets mixed results', The Correspondent, 20 July 2020, accessible here.
- Netblocks, 'Zimbabwe internet disruption limits coverage of planned protests,' 31 July 2020, accessible here.
- Parliamentary Monitoring Group, 'Meeting minutes: Portfolio Committee on Justice and Correctional Services', 2019, accessible here.
- Reporters Without Borders, 2022 World Press Freedom Index, accessible here.

- Research ICT Africa, 'After Access survey presentation', IGF, 2017, accessible here.
- Research ICT Africa, 'Cheapest prepaid broadband product by country (in USD)', accessible here.
- Research ICT Africa, 'SADC not bridging digital divide', Policy Brief 6, 2017, accessible here.
- SADC, 'Report of the First SADC Gender Workshop Held on 28 – 29 March 2018 in Johannesburg, South Africa', undated, accessible here.
- Seychelles Nation, 'New contact-tracing app against the spread of Covid-19', 2021, accessible here.
- Sonia Cisse, '40 countries ploughing ahead with contact-tracing apps as debate intensified on differing approaches', 15 May 2020, accessible here.
- Wall Street Journal, 'Huawei technicians helped African governments spy on political opponents, 2019, accessible here.