



SUMMARY REPORT

INFORMATION ECOSYSTEM ASSESSMENT (IEA) ON
THE IMPACT OF CYBER SECURITY AND
CYBERCRIME LAWS ENACTED BY SOUTHERN
AFRICA GOVERNMENTS ON MEDIA FREEDOM AND
DIGITAL RIGHTS



USAID
FROM THE AMERICAN PEOPLE



Internews
Local voices. Global change.



ADVANCING RIGHTS
IN SOUTHERN AFRICA
ARISA



ADVANCING RIGHTS IN SOUTHERN AFRICA (ARISA) INFORMATION ECOSYSTEM ASSESSMENT (IEA)

IMPACT OF CYBER SECURITY AND CYBERCRIME LAWS ENACTED BY SOUTHERN AFRICA GOVERNMENTS ON MEDIA FREEDOM AND DIGITAL RIGHTS

ARISA CONSORTIUM PARTNERS



About ARISA

ARISA is a five-year USAID funded human rights program being undertaken by a consortium of four partners - Freedom House, ABA Rule of Law Initiative, Pact and Internews. ARISA works in select Southern Africa Development Community (SADC) countries to improve the recognition, awareness, and enforcement of human rights in the region, including protecting the region's most vulnerable and marginalized groups.

CONNECT WITH US



About Internews

Internews is an international media support nonprofit organization operating in 100+ countries. Operating since 1982 and with international headquarters in Washington DC and Africa headquarters in Nairobi, Internews believes everyone deserves trustworthy news and information to make informed decisions about their lives and hold power to account. Within the ARISA consortium, Internews leads on the implementation of programs to support media to promote human rights public education programs, in the areas of media freedom and digital rights, women's customary land rights, indigenous peoples' rights, and the protection of human rights defenders.

CONNECT WITH US



This report is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The contents are the responsibility of ARISA and do not necessarily reflect the views of USAID or the United States Government.



ABOUT THE AUTHORS

Author: Dianne Hubbard has degrees in English from the University of North Carolina-Chapel Hill and Stellenbosch University in South Africa and a law degree from Harvard Law School. She was the Coordinator of the Gender Research & Advocacy Project of the Legal Assistance Centre in Windhoek, Namibia for 30 years. She has also served on Namibia’s statutory Law Reform and Development Commission, and carried out consultancy work for various international agencies including the ILO, the World Bank, UNICEF and UNHCR.

Contributors: Frederico Links is a Namibian journalist, researcher, trainer and freedom of expression advocate. In both his journalism and research, Links has a strong focus on good governance, human rights (including digital rights), state surveillance, corruption, rule of law, and transparency and accountability. Chaacha Mwita is a consultant at Internews and compiled the IEA Summary Report.



ACKNOWLEDGEMENTS

Internews and the researchers, Dianne Hubbard and Frederico Links, would like to acknowledge and thank the following individuals for their contributions and inputs, through interviews and/or reviewing of manuscripts, towards deepening and strengthening the accuracy and credibility of this report with their informed perspectives and insights.

Heartfelt thanks to Dr. Allen Munoriyarwa and Prof. Tachilisa Balule, both of the University of Botswana, for their insights on relevant political, legislative and electoral matters playing out in Zimbabwe and Botswana, respectively.

Similarly, we would like to thank Prof. Tresor Musole Maheshe, of the Catholic University of Bukavu, in the Democratic Republic of the Congo (DRC), for granting an interview to discuss unfolding events in that country; Christina Chan-Meetoo, Senior Lecturer in Media and Communication at the University of Mauritius, for her insights regarding the situation in Mauritius; Murray Hunter, Interim Director of Intelwatch and also of ALT Advisory in South Africa; Armando Nhatumbo of MISA Mozambique; Richard Mulonga, CEO of Bloggers of Zambia; and, Ndimphiwe Shabangu of the Coordinating Assembly of NGOS (CANGO) in Eswatini.

We further acknowledge and thank the following people for taking the time to review the country specific sections: Gregory Gondwe, Director of the Platform for Investigative Journalism (PIJ), and Moses Chitsulo, Program Officer at MISA Malawi, in Malawi; Prof. Rui Verde, Chief Legal Adviser at MakaAngola and researcher at Oxford University’s Center for African Studies; Andrew Marawiti, Executive Director of MISA Tanzania; and Mzimkhulu Sithetho, consultant and adviser at MISA Lesotho. Perri Caplan, a layout consultant based in Namibia, who provided volunteer assistance with the conversion and processing of various documents in French and Portuguese to make them suitable for the application of online translation tools.

To the Internews team, Rosemary Viljoen, and Molly Hove who provided support and guidance and to Chaacha Mwita for preparing the IEA Summary Report.



CONTENTS

SUMMARY REPORT	5
BACKGROUND	6
SADC COUNTRY REVIEWS	8
ANGOLA	8
BOTSWANA	10
COMOROS	12
THE DEMOCRATIC REPUBLIC OF THE CONGO (DRC)	13
eSWATINI	15
LESOTHO	16
MADAGASCAR	18
MALAWI	19
MAURITIUS	21
MOZAMBIQUE	22
NAMIBIA	24
SEYCHELLES	25
SOUTH AFRICA	27
TANZANIA	29
ZAMBIA	31
ZIMBABWE	32
KEY FINDINGS	34
RECOMMENDATIONS	36
CONCLUSION	37

Whereas there is need to combat cybercrime, it should not happen at the expense of established human rights practices – as continues to be the case in the SADC region to the dire detriment of journalism practice in the region. Donor programming, advocacy efforts, and the legislative agenda within the SADC countries should focus on bringing laws regulating freedom of expression and media freedom, and practice thereof, in line with best practice guidance and standards, making them compliant with international and continental instruments that speak to protecting and enhancing such freedoms.



BACKGROUND

In 2023, Advancing Rights in Southern Africa (ARISA) through its consortium partner, Internews, undertook the most comprehensive review yet of laws affecting media practice and the freedom of expression, including cyber laws, penal codes, constitutions and acts of parliament, in the sixteen Southern African Development Community (SADC) countries. The result was a thorough 450-page tome. That work has been distilled into this Summary Report.

This report, as well as the comprehensive research document it is distilled from, is meant to give the reader an objective picture of the state and impact of cybersecurity laws on media and civic freedoms in SADC. For ease of use, the Summary Report does not include the extensive copies of the laws under review, references, citations and case studies. It is best read in consultation of the comprehensive Information Ecosystem Assessment (IEA) report, which is publicly available for [download here](#). Additionally, links to the individual full country chapters are provided in the summary chapters.

Although all laws on media practice are covered in the research, there is a specific focus on cyber laws, as they relate to international conventions, agreements, and best practice, including the SADC Model Law. After comprehensive research, analysis of the specific wording of the various laws and offences is largely guided by the Comprehensive Study on Cybercrime drafted by the United Nations Office on Drugs and Crime (UNODC).

Cybercrime – being criminal activities carried out by means of computers or the internet – has three components to it: Crimes where an information system, such as a computer, is the object of the crime (e.g. hacking); crimes where an information system is used as a tool to facilitate the crime (e.g. fraud); and crimes committed by the content the system carries (e.g. child pornography). In this analysis, the first two categories are grouped together as “technical offences” in contrast to “content-related offences” of the third.

To ensure adherence to international standards, models and guidelines, the research undertook a comprehensive review of the relevant laws, agreements and international conventions, including a review of the relevant SADC laws and conventions. These include: the SADC Model Law on Computer Crime and Cyber Crime, 2012¹; the Universal Declaration of Human Rights; the International Covenant on Civil and Political Rights; the African Charter on Human and Peoples’ Rights, in particular the Declaration on the Principles of Freedom of Expression and Access to Information; the Convention on Cybercrime (Budapest Convention), 2001, and supplemented by the Additional Protocol to the Convention on Cybercrime, 2003, and the Second Additional Protocol to the Convention on Cybercrime, 2022; the Commonwealth Computer and Computer Related Crimes Model Law; and the African Union Convention on Cyber Security and Data Protection (Malabo Convention), 2014.

¹ In 2012, SADC developed the “SADC Harmonised Cyber Security Legal and Regulatory Framework” which is made up of three model laws: the Computer Crime and Cybercrime Model Law, the Data Protection Model Law and the E-Commerce/E-Transaction Model Law. The SADC Model Law has been criticised for including provisions that “actively infringe on the fundamental right to privacy” and “can easily be used to justify intrusive communications surveillance”, with insufficient safeguards.

Of particular interest are the provisions on criminal defamation, privacy and freedom of expression, Subscriber Identity Module (SIM) card registration of subscribers, mass surveillance and data retention, access to information, and provisions governing democratic elections.

A 2015 report on encryption, anonymity, and the human rights framework by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression considered encryption and anonymity in communications in light of the rights to privacy and freedom of opinion and expression, noting that these options “provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks”. The Report also notes that laws requiring SIM card registration directly undermine anonymity and “may provide Governments with the capacity to monitor individuals and journalists well beyond any legitimate government interest”.

In summary, the ARISA IEA report provides an in-depth overview of the legal provisions that have been enacted, or are in various stages of becoming laws in the region, being used by SADC governments to stifle and limit press freedom or public debate. Each of the sixteen SADC countries have been included as individual country chapters, providing country-specific legal analyses of the relevant Cyber security and related laws used by the respective country’s governments to stifle freedom of expression. Importantly, the report highlights the interconnected laws being enacted to enable the abuse and or overreach of state surveillance, especially through mass surveillance. This has become a primary concern, particularly for media freedom advocates, in the context of cybersecurity and/or cybercrime laws and regulatory crafting and drafting in the SADC region. Through this research, ARISA seeks to contribute to the improved understanding of the cyber security and cybercrime laws, and regulatory landscapes, that impact the work of journalists and other media workers in the SADC region, and in doing so, advance and strengthen media rights and counter oppressive practices across Southern Africa.





SOUTHERN AFRICA DEVELOPMENT COMMUNITY COUNTRY REVIEWS



ANGOLA

There are several content-based offences in the law that could inhibit the freedom of expression, including some that have been applied against journalists for this purpose.

Access the full country chapter [here](#)

The Angolan media does not provide sufficient access to free, diverse, and impartial information. A country without community radio stations, the information gaps are gaping. Five stringent media laws were promulgated in January 2017. They introduced a media regulatory body and tight controls on journalism and the internet.

Introduced under the Social Communication Legislative Package of 2017, these were Law no.1/17 (Press Law), which grants the President and his appointee the legal powers to limit press freedoms in the name of the public interest; Law no. 2/17 (Regulatory Entity of the Angolan Media), which establishes the Regulatory Entity of the Angolan Media (ERCA), an entity that ensures that web content is under state control; Law no. 3/17 (Exercise of Television Activity), which has controlling power over television and audiovisual social communication activities; Law no. 4/17 (Exercise of Broadcasting Activity), which regulates radio broadcasting; and Law no. 5/17 (Journalists' Statute), which regulates journalists' work.

There are additional laws relevant to the communications sector. Law no. 23/11 (Electronic Communications and Information Services), which provides foundational regulations for electronic communications and establishes the Electronic Communications Authority to regulate and supervise electronic communications stands out. Others are Presidential Decree no. 202/11: Regulation on Information Technologies and Services; Presidential

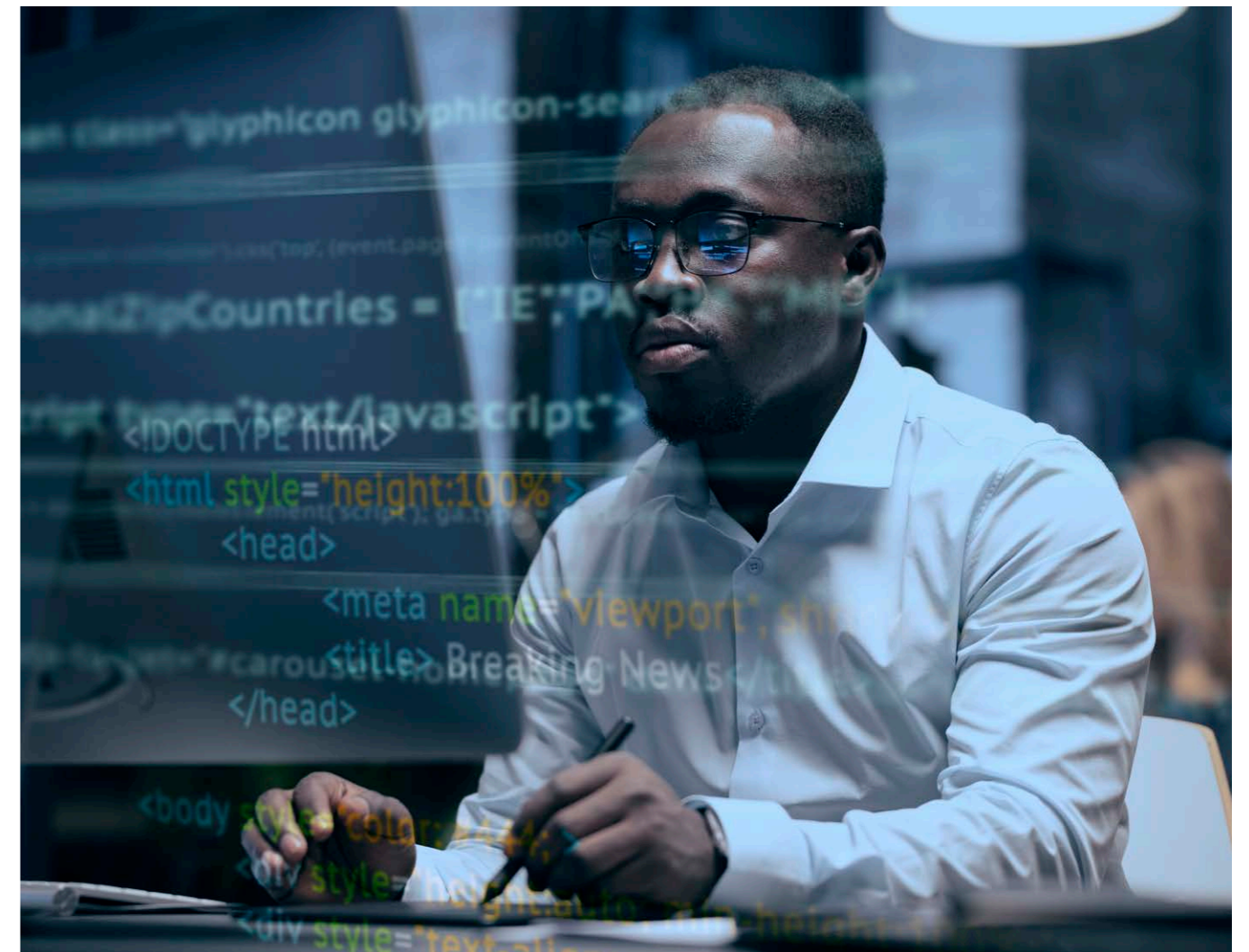
Decree no. 243/14: National Institute of Telecommunications; Presidential Decree no. 108/16: General Electronic Communications Regulation; Law no. 7/17: Protection of Networks and Information Systems; Law no. 27/17: Electronic Communications; Law no. 38/20: Angolan Penal Code.

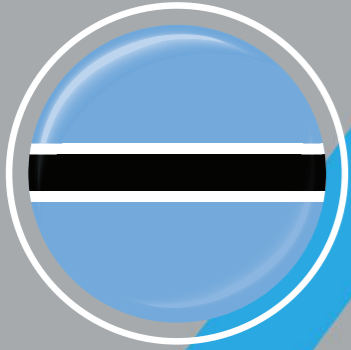
These laws have been used to clamp down on investigative reporting touching on subjects involving governance, including corruption, with journalists often being heavily punished. Journalists in Angola are always alive to violence, threats of violence, unjustified arrests, censorship, and criminal libel as occupational hazards in the country. In Angolan law, there are direct provisions on and steep penalties for criminal defamation, insult, publication of false information, abuse of press freedom, propaganda against national defence and the armed forces, outrage to the State, its symbols and organs, incitement to discrimination, incitement to genocide, criminal defamation.

In addition, there's legalised State surveillance, limited data protection provisions, mandatory SIM card registration, take-down enforcements and interception of communication signals are all legally mandated in Angola despite a constitution that guarantees the freedom of expression.

Also, politically, under the law, it is prohibited to disclose opinion polls during the electoral campaign period in Angola.

Angolan media and cybercrime laws are, therefore, very broad and ambiguous, giving the government broad discretion to control and censor the media and individuals against using available platforms for any free expression that could be perceived to be anti-government.





BOTSWANA

Certain provisions of the Penal Code that criminalise specific forms of expression seem to have been used repeatedly against media practitioners, in respect of both online and traditional media.

Access the full country chapter [here](#)

Botswana will hold general and presidential elections in October 2024. The country has a relatively vibrant media landscape, populated by a variety of print, broadcast and online media. The country's Constitution authorises broad grounds for restrictions to freedom of expression on the basis of defence, public security, public order, public morality and public health. Otherwise, it protects free speech.

Nonetheless, the media landscape has deteriorated in a two-fold manner over the last decade: On one hand media capture by politically associated interests and political bias have led to the loss of credibility of mainstream media and journalists. On the other hand, the government has become increasingly intolerant of free journalism.

Newspapers are registered under the Printed Publications Act 15 of 1968. The definition of newspaper is very broad and includes any publication, released with regularity or irregularity, for free or for sale, that carries news and information on Botswana in Botswana.

Other relevant laws include the Cinematograph Act 73 of 1970; the Electronic Communications and Transactions Act 14 of 2014; the Broadcasting Act 6 of 1999; the Communications Regulatory Authority Act 19 of 2012; the Intelligence and Security Services Act 16 of 2007; the Counter-Terrorism Act 24 of 2014; the Criminal Procedure and Evidence (Controlled Investigations) Act 14 of 2022; the Penal Code; and the Cybercrime and Computer Related Crimes Act 18 of 2018. The Media Practitioners Association Act, 2022, to regulate the media, has been passed by Parliament but is yet to come into force.

These laws separately, and sometimes collectively, authorise government interference in media operations. They regulate publications, films, broadcasting, telecommunications, and postal services; legalising the interception of post, electronic mail, computer or telephonic communications; authorising surveillance and interception of private communications; and imposing heavy penalties for transgressions.

These laws criminalise publishing alarming publications, offensive electronic communication, publishing with intention to deceive, violation of the COVID-19 Emergency Regulations, common nuisance, cyber harassment, cyber stalking, child pornography, obscene material relating to children, revenge pornography, hate speech, criminal defamation, undermining the authority of public officers, defamation of foreign princes, the use of abusive, obscene or insulting language (against senior politicians), improper use of a public telecommunications system, criminal trespass, and sedition. There also exist strict SIM card registration and content take-down provisions.

Journalists have been charged with some of these 'crimes'. They also face threats, surveillance, detention without trial, police violence, and confiscation of essential equipment. All this is in addition to State-sanctioned extra-judicial social media smear campaigns.

In light of the upcoming elections, concerns have been raised that restrictions based on "public order" might be interpreted in a broad way that inhibits media freedom and whistleblowing. Elections in Botswana are governed by the electoral law contained in Chapter 02:09 of the Laws of Botswana and their coverage by the Broadcasters' Code of Practice (2018).





COMOROS

Comoros is one of the few countries in the world (and the only SADC country) that has not ratified the International Covenant on Civil and Political Rights (ICCPR). The rule of law is considered weak and journalists are frequently arrested and intimidated over their reporting.

Access the full country chapter [here](#)

Generally, Comoros' Law is based on both Sharia (Islamic law) and the French legal code. The 2021 Code of Information and Communication of the Union of Comoros, which was promulgated in January 2022, is the key statute that regulates journalists and sets out their qualifications, duties, and rights. Although the Constitution protects freedom of expression as well as the freedom of information, communication, and the press, no illustrations of the application of these rights could be ascertained in this research. Besides, ominously, the enjoyment of these rights is subject to a caveat: "within the conditions established by law", which include broad powers of decree wielded by the President. Notably, Comoros has not ratified the International Covenant on Civil and Political Rights (ICCPR).

The operative media environment in Comoros is hostile for journalists as serious restrictions on free expression and media exist. Journalists and individuals are detained for making public statements, including online statements, that are critical of the President. Thus self-censorship is rife, journalists are often pressured to reveal their sources while in police custody, and over-dependence on state advertising contributes to media compliance with political whims.

However, with conservative religious influence on the wane, the media, increasingly, are able to cover hither-to taboo subjects related to sex and sex work, with the public's support.

Specifically, the Penal Code and the Law on Cyber Security and the Fight Against Cybercrime place grand restrictions on media practice. Journalists can be – and have been – charged with defamation, insult, participating in protests against the government, spreading false news, disturbing public order, incitement to violence, use of false materials, espionage, and offence against religion. These provisions limit free expression, including whistleblowing.

In Comoros, state surveillance is legal and the 'duties' of surveillance extend to businesses and citizens. Cybercafés, for instance, may be required to carry out targeted monitoring of activities carried out through their services.

Everyone accessing internet services from a cybercafé must provide identification; minors must be accompanied by authorized adults; online communication service providers must offer filtering options; and service providers must retain data that can be used to identify persons who have contributed to the creation of content on the service for three years... and so on.

Furthermore, provisions on take-down notifications and searches and seizures (by decree, the government may conduct searches and seizures of computer equipment and computer storage media, according to the procedures in the Code of Criminal Procedure), ensure that Comoros journalists operate in a very tight legal and practical environment. This is despite the Constitution giving the State the duty to promote "the diffusion and the utilisation of new technologies".

Interestingly, Comoros does not have a law on mandatory SIM card registration. Elections are held under tight government control and, instructively, in 2019, three privately-owned newspapers (La Gazette des Comores, Al-Fajr, and Masiwa Komor) had their print runs for specific days seized before they could reach newsstands because they carried reports related to post-election disputes.



THE DEMOCRATIC REPUBLIC OF THE CONGO (DRC)

The Digital Code regulates online media, and (amongst other things) provides prison sentences and heavy fines for offences related to social networks. It gives authorities power to imprison journalists for sharing information electronically.

Access the full country chapter [here](#)

Political ownership and control of the media in the DRC is perverse; here, there's nothing like independent media. Congolese journalists and media lead a precarious existence. Employment contracts are rare and corruption in media is widespread. Journalists are attacked for any reason including, strangely, ethnic origins. A media rights watchdog in the DRC, Journalistes en Danger, reports that in 2022 alone there were at least 124 cases of attacks against journalists and media organisations, including one death, two abductions, 37 arrests, 18 assaults, and 17 closures of media organisations or programmes. In addition, internet shutdowns are common in a country with only six per cent internet penetration.

Article 212 of the DRC Constitution and Organic Law no. 11/001 establish the High Council for Broadcasting and Communication (CSAC) which is the key media regulatory body. The high-handed CSAC operates alongside the extremely partial Regulatory Authority for Posts, Telecommunications and Information Technologies of Congo (ARPTIC), which is responsible for processing licence applications and permits and overseeing adherence to the laws and regulations relating to telecommunications as set out in Law no. 20/17 of 2020, which also contains provisions on cybercrime.

The DRC Constitution acknowledges the rights to freedom of expression and freedom of information and the press subject to respect for the law, public order and morality. In 2023, the DRC enacted the Press Freedom Law and the Digital Code, which, respectively, set out procedures for the exercise of freedom of the press and freedom of information and cover all digital activities and services, including electronic commerce, electronic signatures, digital government services, the regulation of digital platforms, the protection of personal data, cybersecurity and cybercrime. In addition, the Penal Code, Ordinance 81/050 of 1981, Ministerial Order No. CAB/MIN/PT&NTIC/AKIM/KL/Kbs/002 of 2020, Decree-Law No. 003-2003, Decree-Law 1-61 of 1961, and Ordinance-Law no. 23/010 of 2023 contain provisions on broadcasting, cryptology, cybersecurity, and cybercrime.

The Penal Code criminalises defamation, public insult, slanderous denunciation, instigation of disobedience to the laws, provocation of soldiers to turn away from their military duties and from the obedience they owe to their leaders, publication of false information, anonymous publications, attack through the press, acting in bad faith, and falsely claiming to be a media professional. Additionally, it is forbidden to offer, give or sell to minors publications of any kind inciting to debauchery, prostitution, crime or the consumption or trafficking of drugs, alcohol or tobacco.

The DRC does not have a single dedicated cybercrime law. However, together, these laws and ordinances legalise state surveillance, SIM card registration, regulate cybercafés, demand of network operators and service providers to preserve connection and traffic data for security agencies, ban operators from ‘facilitating’ any undermining of state security, require network content providers to provide filters, and spell out take down procedures.

The DRC will hold a General Election on December 20, 2023. Elections in DRC are regulated by the Independent National Electoral Commission (CENI), which is established by the Constitution but, decidedly, lacks in independence.



eSWATINI

The eSwatini media and civil society landscapes, as well as the general human rights climate, are characterised by continuous repression. Arbitrary arrest and detention of journalists have become commonplace. In addition to government arrests and intimidation, there is an increasing trend of civil defamation cases against the media particularly by the powerful.

[Access the full country chapter here](#)

eSwatini is the last absolute monarchy in Africa, where the rule of law and respect for human rights are only meaningful in so far as the king, Mswati III, allows it to happen. Elections are meaningless as no institution – parliament and the judiciary included – has any capacity whatsoever to hold power to account. Mswati III is the law.

Nonetheless, the country has a constitution which recognises the freedom of expression with restrictions placed on public officials thereby limiting the ability of whistle blowers in the public service to bring illegal conduct, including corruption, to the attention of the media in the public interest.

The publication of newspapers requires registration under the Books and Newspapers Act 20, 1963. Newspaper editors must be resident in eSwatini. The Swaziland Communications Commission Act 10, 2013 establishes the eSwatini Communications Commission (the SCC), which regulates all communications services in the country, including postal services, broadcast media and the internet. The creation of this Commission catalysed the enactment of a trio of related laws in 2022: the Computer Crime and Cyber Crime Act, 2022; the Data Protection Act, 2022; and the Electronic Communications and Transactions Act, 2022.

Although regulation of the broadcasting sector is in the process of being updated by the eSwatini Broadcasting Bill 20, 2019 (which has been repeatedly revised and delayed for years and is, as of mid-2023, awaiting Royal Assent), the state broadcaster, the eSwatini Television Authority (STA), is established by the Swaziland Television Authority Act, 1983. The new law would create a three-tier broadcasting system for public, commercial and community broadcasting.

In eSwatini, the intimidation of journalists, assaults, arrests, and arraignments are common fare. Sedition, high treason, and civil defamation cases against the media are frequent. Without a doubt, any criticism of the monarchy is likely to lead to a trial and result in punitive penalties. Internet shutdowns too happen the best example of which was on June 29, 2021 as protests against King Mswati III spread nationwide. These acts are made possible by a raft of draconian laws including the Penal Code; the Suppression of Sedition and Subversive Activities Act, 1938; the

Suppression of Terrorism Act, 2008 as amended in 2017; the Public Order Act, 2017; the Official Secrets Act 30, 1968; the Obscene Publications Act 20, 1927; the Proscribed Publications Act 17, 1968; and the Cinematograph Act 31, 1920.

These laws – applied separately or in tandem as the case may be – also make it an offence to publish any information that is likely to be even indirectly useful to an enemy, they legalise surveillance, mandate SIM card registration (registration of electronic communications and mobile customers), and liberally operationalise take-down of ‘offending’ content.

Under the supervision of the Elections and Boundaries Commission (EBC), which is established by the Constitution, eSwatini held parliamentary elections in September 2023 and the results are unlikely to change the political scene in the Kingdom for the better. Furthermore, the wording of the Election Act 6, 2013 leaves enough room to limit journalism practice within the “vicinity” of polling stations.



LESOTHO

Although laws on access to data and take-down notifications are in abeyance, Lesotho’s Penal Code and Communications Act have been used to target, arrest and prosecute journalists in recent times, adversely limiting the freedom of expression in the country.

Access the full country chapter [here](#)

On the freedom of expression, the Constitution of Lesotho is unusual in the region in that it goes as far as enshrine everyone’s right of reply; any person who feels aggrieved by statements or ideas disseminated to the public has that right in the same medium of communication where the statements appeared. Another Lesotho rarity is that in 2021, parliament adopted the National Media Policy 2021 as part of the overarching media reforms that are underway in Lesotho. This policy was developed by media practitioners and its adoption was a very positive and progressive step.

That is where the rosy story ends. Deathly violence against journalist Ralikonelo ‘Leqhashasha’ Joki in May 2023 shocked the whole country. Journalists have been threatened, barred from covering courts, detained, interrogated and allegedly tortured by police, studios have been raided in gung-ho style, and at least one media house’s licence has been suspended. The crimes of incitement to violence; sedition; disrespect, contempt or irreverence for the national flag or anthem; intent to violate the dignity or injure the reputation of anyone in the Royal Family; hate

speech; and publishing an untrue statement calculated to bring any judicial officer or court into disrepute are menacingly sufficient to make any journalist engage in self-censorship.

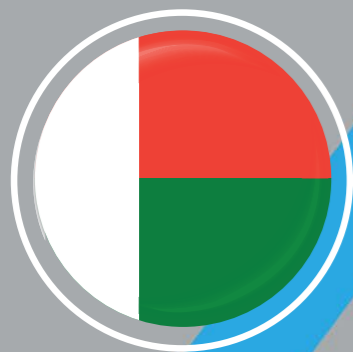
Although criminal defamation has been declared unconstitutional by the judiciary, it remains in the Penal Code as amendments have not been made to repeal the offending clauses.

Newspapers, magazines and other periodicals are required to register under the Printing and Publishing Act 10, 1967. The telecommunications, broadcasting and postal sectors are regulated by the Communications Act 4, 2012, under which the government can issue an emergency media licence suspension order. State surveillance is made possible by the National Security Services (NSS) Act, 1997. Also, Lesotho has a provision on crimes specific to computers in its Penal Code: Section 62(2) criminalises unlawful access to a computer or an electronic storage device. Other laws that adversely impact the freedom of expression include the Sedition Proclamation 44, 1938; the Official Secrets Act, 1967; and the Internal Security (General) Act, 1984.

On a positive note, although the Communications (Subscriber Identity Module Registration) Regulations 2021 require customers to present a national identity document or other identification verification to a service provider to obtain or retain a SIM card, there is no requirement for biometric verification. Also, access to traffic data and requirements on take-down notifications are in abeyance.

The legal terrain on media practice in Lesotho is still evolving. For example, as of July 2023, Lesotho’s Computer Crime and Cyber Security Bill had been passed by Parliament and was awaiting Royal Assent. It might be withdrawn for further refinement. The Bill contains a long list of cybercrime offences.





MADAGASCAR

Although Madagascar has ratified and domesticated most of the regional and international instruments on freedom of expression and press freedom, it does not enforce them. Defamation and insult clauses in the country's cybercrime law have been used to arrest, charge and prosecute journalists on a number of occasions.

[Access the full country chapter here](#)

The key legal framework for the communications sector is contained in Law no. 2016-029: Code of Media Communication, adopted in 2016 and amended in 2020 by Law no. 2020-006. It prohibited the publication of government documents until a constitutional court found this provision in violation of the right to information enshrined in the Constitution as well as Madagascar's international commitments through the ratification and domestication of regional and international instruments.

There are licence requirements for broadcasters, and film production and dissemination both require prior authorisation. Print media outlets do not require licensing or prior authorisation, but must provide a declaration to the Public Prosecutor that includes identifying details of the publication director (including information on his or her criminal record) and the printer. The same applies to professional online press with internet access providers and any other online service providers being required to verify the content of the sites. The Regulatory Authority of Communication Technologies (ARTEC), under Law no. 2005-023, regulates telecommunications networks.

The Constitution of Madagascar limits the freedom of expression, communication, and the press on the basis of respect for the freedoms and rights of others, and safeguarding the public order, national dignity and security of the state. Accordingly, the constitutional right to freedom of expression and its limitations have been interpreted in a manner that is consistent with international treaties, but in practice, press freedom has been undermined by criminal libel laws and other restrictions. While physical attacks on journalists are rare, public verbal attacks and smear campaigns on social media by politicians are not uncommon.

Also, the offices of La Gazette de la Grande Île have been raided and the owner arrested on charges related to attempted extortion, defamation, threats, insults, and for being in arrears with water and electricity payments. Other journalists have been arrested, and at least one imprisoned, on charges of defamation and the humiliation of Members of Parliament and civil servants. Spreading false information, insulting an institution, inciting hatred and public unrest, infringement of the life and security of the President and his family, the disclosure of confidential

information considered to be a state secret, and offence to the fulfilment of a state mission are all, by law, criminal offences and journalists have suffered all of them. Death threats and blackmail are also features of journalism in Madagascar.

The Penal Code, Law no. 2014-006 on the Fight Against Cybercrime as amended by Law no 2016-031, Law no. 2005-023, and the Code on Media Communications separately and severally allow state surveillance, equipment seizures, telephone tapping and recordings to uncover journalists' sources, regulate take-downs, and mandates SIM card registration.

Presidential elections are scheduled for November 9, 2023 and, given Madagascar's weak political institutions, it can only be hoped that the Independent National Electoral Commission (CENI) will obey provisions of Election Law is Law no. 2018-008, which allows the use of electronic media during campaigns. Increasingly, politicians in Africa are resorting to shutting down electronic media, including social media, during elections.



MALAWI

Numerous incidents since 2020 show how cybercrime offences under the Electronic Transactions and Cyber Security Act have been applied against journalists and persons who post on social media.

[Access the full country chapter here](#)

Newspapers and periodicals must be registered under the Printed Publications Act 18, 1947. Under the Censorship and Control of Entertainments Act 11, 1968, no one may direct or take part in the making of any film or show one without a permit. Plays, concerts, art exhibitions and other public entertainments require an entertainment permit. The Communications Act 34, 2016, regulates broadcasting, telecommunications and postal services. All these are under the Malawi Communications Regulatory Authority (MACRA).


Unlike many other constitutions in the SADC regions, the grounds for limiting the freedom of expression and other fundamental rights are not specified with reference to concerns such as national security or public morals. Notably, the Constitution explicitly guarantees the right to report and publish freely, within Malawi and abroad. Official efforts to infringe on various freedoms (of association, to demonstrate etc.) have been overturned in court.

Since 2019, several TV channels have been vandalised and radio phone-in programmes interrupted. There's no whistle blower protection law in Malawi, and journalists are sometimes attacked, subjected to threats and online intimidation, and arrested and detained arbitrarily. There are also searches and seizures of equipment, and, at least in one case, demands that a journalist provides his cell phone's and laptop's passwords. In addition, internet freedom is in decline, despite a new administration promising better days.

Online content is regulated by the Penal Code and the Electronic Transactions and Cybersecurity Act 33 of 2016, which has been applied against journalists and persons who post on social media. With broad interpretative possibilities, criminal libel, offensive communication, under the cybercrime law, spamming, cyber harassment, cyberstalking, publication of offensive communication, criminal insult of the President, attempting to undermine the authority of the head of state, photographing some people without permission, conduct likely to cause a breach of peace, obstructing police officers on duty, and working without permission from the police, disseminating false information, speaking or writing words with the intention of wounding religious feelings, are all criminal offences. The Act includes provisions for take-down notifications, and SIM card registration.

On surveillance, no legal authority for interception of communications by government or law enforcement officers was located, nor any authority for the retention of traffic data by service providers for access by government authorities – but there are indications that state monitoring of communications takes place in practice, as evidenced by arrests related to online activities.

The Preservation of Public Security Act 11, 1960; the Protected Flag, Emblems and Names Act, and the Prisons Act, the Aviation (Airport Security) Regulations issued in terms of the Aviation Act, also limit to varying degrees the freedom of expression, whistle blowing, and ultimately therefore, journalism practice. For instance, in 2020, three journalists were detained for two hours at Kamuzu International Airport in Lilongwe, after attempting to cover the arrival of an EU delegation due to present their final report on the disputed election. Their equipment was confiscated and their footage deleted, and they were locked in a police cell in the airport, speaking to how touchy authorities can be against journalists at election time.



MAURITIUS

The Independent Broadcasting Authority Act allows a judge in Chambers to require journalists to reveal their sources without any legal safeguards, while in recent times the Information and Communication Technology Act has been used repeatedly to arrest and prosecute social media users.

[Access the full country chapter here](#)

The Newspapers and Periodicals Act 6, 1837 regulates newspapers and periodicals, while radio and television are regulated under the Independent Broadcasting Authority Act 29, 2000. The Act prohibits the issuance of a broadcasting licence to any political party or association or any person actively engaged in politics, or to any religious group. Any entity “found liable for defamation or sedition” is prohibited from getting a broadcasting licence. License renewals are not guaranteed; “past conduct” is taken into consideration before a license is renewed. Information and communication technologies, including internet service providers are licenced under the Information and Communication Technologies (ICT) Act 44, 2001. The Media Trust Act 9, 1994, creates a media trust running a media and documentation centre, organising seminars, conferences, workshops and trainings, and fostering relationships with international media. It is complemented by the Mauritius Digital Promotion Agency established under the Mauritius Digital Promotion Agency Act 4, 2023 to boost the growth of the ICT sector.

The Supreme Court has held that the freedom of expression is protected by the Constitution. In reality there are restrictions. For one, journalists can be legally compelled to reveal their sources. This jeopardises the confidentiality of journalists’ sources without any legal safeguards. In recent years threats and acts of intimidation against journalists have increased.

Under both the Cybersecurity and Cybercrime Act 16, 2021 and the ICT Act 44, 2001, police, using investigatory powers the laws provide, can seek authorisation to search and seize equipment, and intercept real time data and communications. Also, a Safe City project currently underway, would make high-tech state surveillance possible, and probably a norm. Provisions on moderation allow take-downs and the ICT Act 44, 2001 requires forfeiture of any equipment, as well as allows suspension of a service, and cancellation of the licence. This law also gives disturbing powers of interception and censorship to service providers. The recent Information and Communication Technologies (Registration of SIM) (Amendment) Regulations 2023 mandates SIM card registration. The laws examined are silent on encryption.

Although there's no evidence that it has been applied against journalists, the Criminal Code features criminal defamation, outrage against public and religious morality, stirring up racial hatred, inciting to disobedience or

resistance to law, insult, and publishing false news as criminal offences. Also, the National Assembly (Privileges, Immunities and Powers) Act 22, 1953 outlaws contempt of the National Assembly, which includes sending a member of the National Assembly an insulting or threatening letter – which frustrates accountability by shielding the National Assembly from probity.

Mauritius will hold general elections in November 2024, after which the newly-elected National Assembly will elect the President, who appoints the Prime Minister. The Mauritian Constitution establishes an Electoral Supervisory Commission and an Electoral Commissioner to supervise elections. The Representation of the People Act 14, 1958 and the National Assembly Elections Regulations 2014 as amended by the National Assembly Elections (Amendment) Regulations 2019 regulate elections. There is a broad right of reply that applies specifically to newspapers in the Criminal Code, and in election time, the Mauritius Broadcasting Corporation Act 22, 1982 explicitly provides for this right.



MOZAMBIQUE

The Penal Code has been used to arrest and charge journalists with engaging in terrorism. Harassment, assault and intimidation of journalists, and civil society actors, have become part of the country's media and civic spaces. Although there are strong constitutional guarantees against state surveillance, some civil society activists have reported that government intelligence services and ruling party operatives have monitored telephone calls and emails, conducted surveillance of their offices, and followed members of opposition parties.

Access the full country chapter [here](#)

On paper, Article 50 of the Constitution of Mozambique establishes the Superior Council of the Mass Media (CSCS). However, lacking in any direct regulatory powers, the council is reduced to an advisory caucus of Executive-friendly individuals while the Executive branch of government carries out the “real” media regulation. The Council is governed by the 1991 Press Act. A more significant body is the Government Press Office (GABINFO), which operates as an arm of the Executive from the Office of the Prime Minister, with a Director. GABINFO took over the functions of the Minister of Information in 1995, and, as per Diploma 2/2005, accredits and registers foreign correspondents and publications and takes responsibility for the registration and licensing of the mass media. Decree no. 9/93 (The Broadcasting Decree) regulates Radio Mozambique and Mozambique TV. Law no. 8/04 on Telecommunications, as

amended by Law no. 4/2016, governs telecommunications networks and services, including the licencing of such services. In 2017, Law no. 3/17 on Electronic Transactions established a legal framework for electronic transactions and partially addressed cybercrime.

Other laws relevant to cybercrime and media practice are: Law no. 25/19, the new Criminal Procedure (Penal) Code; Law no. 14/2013 on Preventing and Combating Money Laundering and Financing of Terrorism; Law no. 13/22 on the Prevention, Suppression and Countering of Terrorism and Proliferation of Weapons of Mass Destruction; and Law no. 19/91 on Crimes against State Security. Together, these laws criminalise defamation, publishing false news, hate speech, incitement, terrorism, child pornography, interference in privacy, computer fraud, data interference, systems interference, and misuse of devices. Only with judicial authorisation can surveillance (communication interception and wiretapping) be done legally. Nonetheless, some civil society activists have reported that government intelligence services and ruling party operatives have monitored telephone calls and emails, conducted surveillance of their offices, and followed members of opposition parties without warrants. Biometric SIM card registration is mandated and no information on take-down notifications was located.

Although the freedom of expression is constitutionally guaranteed to every citizen, the government does not respect this right. The President himself has waged a consistent verbal attack war against academics, civil society members, and journalists accusing them of spreading false information about Cabo Delgado (where some of the world's largest reserves of natural gas have been discovered and an outbreak of an Islamic insurgency reported) resulting in an atmosphere of fear and, hence, self-censorship. Journalists working in the region often risk police harassment, including arbitrary arrest and detention, revocation of accreditation, and deportation (for foreigners). At least one journalist was last heard from “surrounded by soldiers” and is suspected to have been forcibly ‘disappeared’.

Mozambique will hold general elections in October 2024. As there were notable election irregularities in 2019, the National Electoral Commission (CNE), supported by the Technical Secretariat for Electoral Administration, are under pressure to do a better job this time as by law established. Elections are held under the Elections Law (Law no. 8/13), which also protects the rights of freedom of expression of the media during election periods.





NAMIBIA

Namibia is the only SADC country without a dedicated cybercrime law or a set of cybercrime offences in a broader law. And even though subsidiary legislation make state surveillance for state security reasons possible, journalists and civil society organisations are relatively free of this threat unlike their counterparts in the SADC region. The enactment of the Draft Computer Security and Cybercrime Bill, 2019, would, however, drastically change all this.

Access the full country chapter [here](#)

The Newspaper and Imprint Registration Act 63, 1971, prohibits the printing and publishing of any newspaper that is not registered under the Act. Digital newspapers though are exempt. The Namibia Film Commission Act 6, 2000 has never been brought into force, although the Commission operates as though the law is active. Even though Namibia has no dedicated cybercrime law, the constitutional right to freedom of speech and expression explicitly includes freedom of the press and other media, which is sufficiently broad to include online expression. There are several grounds for restrictions including the national security, public order, decency and defamation. However, any such restriction must be reasonable, lawful and necessary.

The communications sector in Namibia (including telecommunications) is generally regulated by the Communications Act 8, 2009. The Act establishes the Communications Regulatory Authority of Namibia (CRAN) to regulate the communications industry, including electronic communications and the postal service. CRAN, which is hardly independent, is responsible for issuing broadcasting licences, telecommunications licences and postal service licences. The following state media outlets are also established and governed by legislation: The New Era newspaper, by the New Era Publication Corporation Act 1, 1992; the Namibian Press Agency (NAMPA) by the Namibian Press Agency Act 3, 1992; and the Namibian Broadcasting Corporation (NBC) by the Namibian Broadcasting Act 9, 1991.

Journalists in Namibia receive few verbal attacks from government functionaries and, even though several public officials have filed civil defamation suits against media practitioners in Namibia, there were few reports of rough or intimidating treatment of journalists during 2020-2022. Notably, in 2011, a decade-long State advertising boycott of The Namibian, the country's largest daily newspaper, finally came to an end.

Namibia is the only SADC country without a dedicated cybercrime law. However, it has the Draft Computer Security and Cybercrime Bill, 2019, which envisages a predictable list of technical and content-related offences, specifically

applying the existing search, seizure and forfeiture provisions in Namibia's Penal Code to the digital realm. Other relevant drafts are the Combating of Harassment Bill and the Combating of Sexual Exploitation Bill.

Namibia's Communications Act 8, 2009 creates criminal offences relating to communications including misuse of a communication device. It also has problematic provisions on data retention – which police can access without court authorisation in urgent situations – and state surveillance. Other laws that have potential to impede media work include the Namibian Central Intelligence Service Act 10, 1997; the Combating and Prevention of Terrorist and Proliferation Activities Act 4, 2014; and the the Electronic Transactions Act 4, 2019. The latter concerns itself with take-down notifications i.e. the liability of service providers for unlawful material.

A general election is scheduled in Namibia for late 2024. Under the supervision of the Electoral Commission of Namibia (ECN), which is set up by the Constitution as an independent body, and run under the Electoral Act 5, 2014, no significant irregularities or abuse of the law are anticipated.



SEYCHELLES

While journalists are generally free to do their work and are not subjected to arrests or violence, there are several aspects of the Penal Code that threaten freedom of expression and of the media. In addition, penalties under the cybercrime law seem inconsistent with respect to the severity of the offences based on international standards and common sense.

Access the full country chapter [here](#)

Article 22 of the Seychellois Constitution is admirable for its explicit inclusion of “the freedom to hold opinions and to seek, receive and impart ideas and information without interference”. Print newspapers are regulated by the Newspaper Act [Cap 147]. They are required to register with the government before they commence publication. Films are governed by the Film Classification Board (FCB) Act 2, 1994. Broadcasting and telecommunications are governed by the Broadcasting and Telecommunication Act 2, 2000, which is set to be replaced by the Communications Act 3, 2023, passed by Parliament but not yet in force. This Act is intended to be a comprehensive law for the regulation of the ICT and broadcasting services under a new independent regulator, the Seychelles Communications Regulatory Authority (SCRA).

There is also a state-run press agency, the National Information Services Agency (NISA) which publishes the Seychelles Nation newspaper and aims to contribute generally to the development of the mass media in Seychelles.

This body is governed by the National Information Services Agency Act, 2010, which was revised in 2017. There's also the Seychelles Media Commission (SMC), established under the Seychelles Media Commission Act, 2010 "to preserve the freedom of the media, improve and maintain high standards of journalism, require publishers of newspapers, radio and television broadcasters, news agencies and journalists to respect human dignity, freedom from discrimination on any grounds except as are necessary in a democratic society, and to maintain high standards of integrity and good taste".

Few specific incidents involving freedom of expression have been reported in Seychelles. Journalists are generally free to do their work, but there are complaints of harassment, intimidation and harsh criticism from authorities in respect of critical reporting. In the past, the media exercised self-censorship to protect advertising revenues and to avoid being charged with criminal defamation. However, self-censorship has declined since the repeal of the criminal defamation law in October 2021, the same year the country enacted the Cybercrimes and Other Related Crimes Act 59. The maximum terms of imprisonment under this Act seem inconsistent with respect to the severity of the offence – for instance, computer fraud or forgery being potentially punished far more heavily than making or distributing child pornography.

The law provides for traffic data and computer data subscriber information storage and retrieval for police use under the law. Any investigatory authority can issue a preservation order, against loss or modification, for computer data. Searches and seizures are warranted. Take-down orders (referred to as "deletion orders") are limited. In addition to the power given to investigatory authorities under the cybercrimes law, the Electronic Transactions Act 8, 2001 provides broad authority for the Supreme Court to issue an order allowing any agency of the government to intercept any information (data, text, images, sound, codes, and databases) transmitted through any computer resource. The justifications for such an interception order include the security of the Republic and the interests of public order. SIM card registration is mandatory under the Broadcasting and Telecommunication Act, 2, 2000.

Several aspects of the Penal Code are relevant to freedom of expression. These include provisions on prohibited publications, sedition, incitement, publishing false statements, and publishing statements that can hurt religious feelings.



SOUTH AFRICA

South Africa has arguably the most vibrant and robust media landscape in the SADC region, and probably on the continent. While South African courts have upheld the common law crime of defamation, the courts have also been robust defenders of freedom of expression and media freedom in the post-apartheid era. With regard to cybercrime legislation, the wording of the technical and content-based offences in the South African Cybercrimes Act is substantially different from the formulations used in other SADC member states demonstrating acute deliberateness in the crafting and application of this law.

Access the full country chapter [here](#)

Unlike other SADC countries, South Africa has no law requiring newspapers and other periodicals to register. The Imprint Act 43, 1993 only requires a commercial printer to identify themselves on printed matter. Films are regulated by the Films and Publication Act 65, 1996, which was amended in 2019 to encompass online content broadly. The Independent Communications Authority of South Africa (ICASA) Act 13, 2000 establishes ICASA to regulate electronic communications, broadcasting and postal services in South Africa. The Broadcasting Act 4, 1999 has been replaced for the most part by the Electronic Communications Act 35, 2005. Its remaining provisions relate primarily to the South African Broadcasting Corporation (SABC) and the South African Broadcast Production Advisory Body. The Electronic Communications Act 36, 2005 provides for the licencing of electronic communications services, electronic communications network services, and broadcasting services. There is also a statutory Media Development and Diversity Agency (MDDA) formed to promote development and diversity in the media throughout the country.

In terms of constitutional protection of free expression, the Constitution of South Africa does not illegalise forms of expression relating to propaganda for war; incitement to imminent violence; and advocacy of hatred based on race, ethnicity, gender or religion that constitutes incitement to cause harm; rather than illegalise these, it denies them constitutional protection.

Criminal defamation is recognised in South Africa as is the right to receive information, which is invoked to get official government information for journalistic purposes. Journalists are rarely arrested in South Africa but the police sometimes fail to protect them when they are exposed to violence.

Child pornography, grooming and the non-consensual publication of intimate images (revenge porn) – covering electronic communications as well as other channels of communication – are addressed in the Criminal Law (Sexual Offences and Related Matters) Amendment Act 32, 2007. Depictions of sexual assault and violence against children, are also addressed in the Films and Publications Act 65, 1966, along with revenge porn. Cyber harassment is covered, along with other forms of harassment, in the Protection from Harassment Act 17, 2011. The Cybercrimes Act 19, 2020 covers certain forms of hate speech, which is also covered by most laws cited here. In addition, hate speech is covered by the Promotion of Equality and Prevention of Discrimination Act 4, 2000. In future, the Prevention and Combating of Hate Crimes and Hate Speech Bill that has been under consideration for some time may be added to the list.

The Cybercrimes Act also authorises the interception of indirect communications and real-time communication-related information through procedures in the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002. The Act also places reporting obligations on electronic communications service providers and financial institutions to ensure that they promptly inform police of any suspicion of certain technical cybercrime offences involving their electronic communications system or network. It criminalises illegal access; unlawful interception of data; unlawful acts in respect of software or hardware tool; unlawful interference with data or computer program; unlawful interference with computer data storage medium or computer; unlawful acquisition, possession, provision, receipt or use of password, access code or similar data or device; cyber fraud; cyber forgery and uttering; cyber extortion; theft of incorporeal property; data message which incites damage to property or violence; data message which threatens persons with damage to property or violence; and disclosure of data message of intimate image. Attempting to commit any of these offences is also an offence, as is conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring another to commit any of these offences. The National Director of Public Prosecutions is required by the Act to keep statistics on all prosecutions for cybercrimes under the Act, and their outcomes.

The Electronic Communications and Transactions Act 25, 2002, which initially contained some provisions on cybercrimes, still covers some issues more typically found in cybercrime laws. It contains provisions on identification and protection of critical databases, registration of SIM cards, establishes a register of cryptography providers, and provides a take-down notification procedure.

Elections in South Africa are administered by the Independent Electoral Commission (IEC), which is largely considered independent, and the electoral framework fair. The Constitution sets out the basic framework for this body, which is further regulated by the Electoral Commission Act 51, 1996. Elections are governed by the Electoral Act 73, 1998, which contains several provisions pertaining to speech.



TANZANIA

The Cybercrimes Act, which has been described as a close copy of the SADC Model Law, and the Media Services Act have been used repeatedly to muzzle free expression and prosecute journalists over recent years. Police have the power to search and seize a computer system with no judicial involvement. They can also compel a person to disclose data relevant to the investigation of an offence. Disclosure of data includes obtaining subscriber information from service providers. Court involvement is required only where the data disclosure or preservation cannot be done without the use of force.

Access the full country chapter [here](#)

The United Republic of Tanzania consists of Mainland Tanzania and Zanzibar. While the Cybercrime Act, the Tanzania Communications Regulatory Authority Act (TCRA), 2003, the Electronic and Postal Communications Act, and the Tanzania Telecommunications Corporation Act 12, 2017 apply throughout the United Republic of Tanzania, there exist laws impacting freedom of expression and journalism practice applicable independently separately in the two jurisdictions – Mainland Tanzania and the semiautonomous Zanzibar.

TCRA regulates telecommunications, radio and television broadcasting, postal services, and electronic technologies including the internet and other ICT applications, and establishes the Tanzania Broadcasting Services (TBC). The Electronic and Postal Communications Act, 2022 provides a comprehensive regulatory regime for electronic communications service providers under the TCRA. The Tanzania Telecommunications Corporation Act, 2017 sets up a public telecommunications corporation aimed at enhancing the safety, security, economic and commercial viability of national telecommunications services and telecommunications infrastructure.

The Media Services Act, 2016, which applies only in Mainland Tanzania, provides for the licensing of print media and the accreditation of journalists through a Journalists Accreditation Board. The Act gives the government powers to ban or suspend publications on national security or public safety grounds, and this power has been applied in practice against various media outlets. The Act contains provisions on criminal defamation, sedition, and the publication of false news. It also sets up an Independent Media Council which is tasked to adopt a Code of Ethics for professional journalists, review the performance of the media sector, promote media accountability and handle complaints relating to print media only. All accredited journalists are members of the Council, which elects its own leadership. The Council is expected to adhere to “national unity, national security, sovereignty, integrity and public morality” in carrying out its functions. Other laws that contain provisions inimical to free expression are the Films and Stage Plays Regulations, 2020, and the National Arts Council Act 23, 1984.

In Zanzibar, the Registration of Newsagents, Newspapers and Books Act 5, 1988 requires the registration of all newspapers in Zanzibar. This Act empowers the government to suspend the publication of a newspaper if this is in the public interest. The registration of a journalist under this law can be suspended or revoked in the public interest. The Zanzibar Arts and Censorship Council Act 7, 2015 regulates the making and public screening of films in Zanzibar. Broadcasting in Zanzibar is regulated by the Zanzibar Broadcasting Commission Act 7, 1997. The Zanzibar Broadcasting Corporation (ZBC) is established as Zanzibar's national broadcaster by the Zanzibar Broadcasting Corporation Act, 2013.

The Constitution of the United Republic of Tanzania provides for freedom of speech but negates this with very wide grounds for limitations. The 1984 Zanzibar Constitution also protects freedom of expression, which too is subject to limitations.


Tanzania experienced a steep decline in press freedom during the rule of late president John Magufuli. The incumbent, Ms. Samia Suluhu Hassan, hasn't improved things significantly. Media monitors report serious restrictions on free expression and media, including wanton closures of media outlets and publications, unjustified arrests or prosecutions of journalists, censorship, enforcement of criminal libel laws, and serious restrictions on internet freedom.

Tanzania's Cybercrimes Act, 2015 has been described as a close copy of the SADC Model Law, including aspects that have been criticised as being problematic. In general, attempting, abetting, or conspiring to commit any offence under the Act is also an offence. Police have the power to search and seize a computer system and to order data preservation with no judicial involvement. They can also compel a person to disclose data relevant to the investigation of an offence. Disclosure of data includes obtaining subscriber information from service providers. Court involvement is required only where the data disclosure or preservation cannot be done without the use of force as might be the case in "forensics". The Act includes procedures for a take-down notifications.

The Electronic and Postal Communication Act, 2010, makes it an offence to use network facilities, network services, applications services or content services to knowingly make, create, solicit or initiate the transmission of any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person. It is also an offence to use any applications service to initiate a communication with intent to annoy, abuse, threaten or harass any person at any number or electronic address. Electronic and Postal Communications (Online Content) Regulations, 2020 restricts anonymity by requiring licensees to have in place mechanisms that can identify the source of all content.

In addition to these, the Penal Code criminalises hate speech; obscene, abusive or insulting language; deliberate intention of wounding the religious feelings of any person; making or sharing photos, pictures, videos or images of corpses, dead persons, victims of crimes or gruesome incidents; tending to corrupt morals; and criminal defamation. These provisions are also there in the Zanzibar Penal Act 6, 2018 which, in addition includes, degrading, reviling or exposing to hatred or contempt a foreign ambassador or dignitary. It also contains offences against intellectual property, destruction of computer equipment, interfering with data, interfering with a computer system, unlawful interception of data, production and sale of illegal devices and many others.

The Electronic and Postal Communications (SIM Card Registration) Regulations, 2020 requires all SIM cards to be biometrically registered. Take-down procedures are contained in both the Cybercrimes Act and the Electronic and Postal Communications (Online Content) Regulations, 2020.



ZAMBIA

Specific sections of Zambia's Penal Code have been used over recent years to arrest and charge journalists, while sections of the Cyber Security and Cyber Crimes Act have been used to intimidate the media, including online publications.

[Access the full country chapter here](#)

There's a new administration in Lusaka that has promised to be friendlier to the media and journalists. Before the installation of the new Hichilema Hakainde Administration, the government was so intolerant to criticism that in 2015, it shut down the Post newspaper, days before an election, it turns out for good, an action that was in 2022 declared illegal by the courts. Previously, journalists were arrested, questioned, assaulted and charged with obstruction, destroying evidence, sedition, and defaming the President amongst others.

This was been made possible by draconian laws the worst of which is the Penal Code, which, even though recently reviewed, criminalises prohibited publications; seditious practices; expressing or showing hatred, ridicule or contempt for persons because of race, tribe, place of origin or colour; obscene matters or things; libel; and alarming publications. In fact on libel, Zambia has a (civil) Defamation Act (1953) firmly in place.

The Prisons Act makes it an offence to publish any part of a letter or document if there is reasonable cause to believe that it was written by or on behalf of a prisoner but was not endorsed by the officer in charge to authorise its removal from the prison. The State Security Act bans espionage, which includes publishing any information which might be directly or indirectly useful to a foreign power or a disaffected person, even if there was no intention to have this effect. The Anti-Terrorism and Non-Proliferation Act makes it an offence to publish information that might be of use to a terrorist.

The Cyber Security and Cyber Crimes Act 2, 2021 covers cyber security, the licensing of cyber security service providers, cybercrimes, interception of communications and electronic evidence. It deals with issues such as extradition, admissibility of electronic evidence, search and seizure, collection of traffic data, interception of content data and mutual assistance and cooperation relating to the investigation and prosecution of offences under the Act – as well as intelligence gathering, investigation, prosecution and judicial processes in respect of cybercrimes, cyber terrorism and cyber warfare. Many aspects of this Act have the potential to infringe on internet freedoms and freedom of expression. As a matter of fact, it has been reported that the Zambian government uses an international surveillance tool to monitor the private communications of citizens, particularly protestors and opposition leaders. The surveillance platform in question allows access to telephone calls, text messages, and location services.

Through Statutory Instrument Number 65, 2011, biometric SIM card registration is mandated while take-down notifications are governed by the Electronic Communications and Transactions Act.

Print media publications are required to register under the Printed Publications Act while broadcasting in Zambia is regulated by the Independent Broadcasting Authority Act 17, 2002. The state broadcaster, the Zambia National Broadcasting Corporation (ZNBC), is regulated by the Zambia National Broadcasting Corporation Act. The Information and Communication Technologies Act 15, 2009, regulates ICTs.

The Constitution of Zambia protects the freedom of expression with some logical limitations except the curious one, on confidentiality grounds, banning civil servants, including those in the education sector, from publicly sharing official information.



ZIMBABWE

The Criminal Law (Codification and Reform) Act, as amended by the Cyber and Data Protection Act, has in recent times been the basis of arrests of journalists and numerous others for offences related to expression.

[Access the full country chapter here](#)

The key regulatory body for the media is the Zimbabwe Media Commission established by the Constitution and regulated by supplementary legislation, the Zimbabwe Media Commission Act, 2020. Broadcasting in Zimbabwe is regulated by the Broadcasting Services Act, 2001, which creates the Broadcasting Authority of Zimbabwe (BAZ) whose mandate is to issue licences for radio and television broadcasting as well as developing broadcasting codes of conduct.

State broadcaster, the Zimbabwean Broadcasting Corporation (ZBC), is governed by the Zimbabwe Broadcasting Corporation Act, 2001, which is set to be replaced by the Zimbabwe Broadcasting Corporation (Commercialisation) Act, 2001. The Postal and Telecommunications Act, 2000 establishes the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) which licenses and regulates postal and telecommunication services, including internet service licences.

Zimbabwe's constitutional provisions are strong, with a sound basis for limited restrictions on the right to freedom of expression that incorporates necessity and proportionality. The constitutional protections have been applied in

practice to invalidate specific legislative provisions. In 2014, the Constitutional Court of Zimbabwe relied on the constitutional protection for freedom of expression to declare the offence of criminal defamation unconstitutional. The Public Order and Security Act, 2002 has implications for how journalists can go about their business during charged and tense situations such as riots.

Although the levels of violence against journalists have declined since the exit of Robert Mugabe, they still remain alarmingly high, and self-censorship is widely practiced to avoid reprisals. Amnesty International reports that three journalists were the first people to be arrested under the Criminal Law Codification and Reform Act, as amended by the Cyber and Data Protection Act, in 2022. Journalists have been charged with transmitting false data intending to cause harm, cyberbullying, and using foul language to describe the Zimbabwean ambassador to Tanzania and his wife in a WhatsApp group. There have been internet shutdowns in Zimbabwe in recent years although it is not clear under what laws this was undertaken.

Criminal Law (Codification and Reform) Act as amended by the Cyber and Data Protection Act, 2021 seems to borrow heavily from the SADC Model Law and leans heavily towards the Tanzanian Cybercrime Act. The procedural issues relating to cybercrime are all contained in the Criminal Procedure and Evidence Act as amended by the Cyber and Data Protection Act and in the Interception of Communications Act as amended by the Cyber and Data Protection Act. The latter, subject to certain procedures, allows for search and seizure actions, data preservation orders, take-down provisions, interception of communications, and SIM card registration. Access to mandated electronic databases is available for several purposes including for assisting law enforcement agencies, for safeguarding national security, and for undertaking approved educational and research purposes.

Elections are administered by the Zimbabwe Electoral Commission (ZEC), which is covered in detail in the Constitution, and conducted in accordance with the Electoral Act. These – elections – were conducted in August 2023, and predictably, because of the skewed playing ground, the ruling party, ZANU-PF's candidate, Emmerson Mnangagwa, won.





KEY FINDINGS

This comprehensive review of laws affecting media practice and the freedom of expression, including cyber laws, penal codes, constitutions and acts of parliament, in the sixteen SADC countries makes the following key findings:

- 1) Despite the clear reliance on the Malabo Convention, the SADC Model Law and in some cases the Budapest Convention, there is still a great deal of variation across the region in both technical and content-based offences. While local adaption is not a bad thing, one question to consider is whether the variations in national laws will affect international cooperation on cybercrimes, which often involve multiple jurisdictions.
- 2) Content-based criminal offences are the ones most often employed to inhibit speech, and these are most often contained in laws other than cybercrime law, such as Penal Codes. Criminal defamation and outdated laws on sedition, public order and criticism of government officials are amongst the most common culprits. Some countries (such as Madagascar, Malawi, Tanzania and Zimbabwe) include ill-defined content-based crimes aimed at insult, harassment, disturbing the peace or publishing false information in their cybercrime legislation – which are in some cases so widely and vaguely drafted that they invite subjective application.
- 3) Cybercrime laws often have provisions prohibiting access to or use of materials originally obtained via illegal access to computer systems, which could affect journalists' use of materials from whistle blowers or caches of documents such as Wikileaks or the Panama Papers. We found no evidence of this concern playing out in practice yet, but many cybercrime laws are relatively new and perhaps not yet widely applied.
- 4) Take-down procedures which do not involve judicial decision-makers are of concern, although these do not seem to have inspired much discussion or debate in the region to date. This is an area which warrants more in-depth study, as such provisions can be used to remove online speech on the mere allegation of illegality without sufficient safeguards – and can be particularly dangerous when combined with vague content-based criminal provisions that provide a wide basis for alleging illegality. There is significant variation in the mechanics of such procedures across the region, which could be usefully compared and contrasted, with a view to developing detailed regional recommendations. It would also be useful to collect data on how widely used such provisions are, and in respect of what kinds of speech.
- 5) Prior restraints on speech tended to take the form of discretionary mechanisms for suspending media activity or revoking media licences.
- 6) There is a need for attention to the independence of regulatory bodies – particularly where they have significant degrees of discretion (such as the discretion to suspend or cancel media licences). There also appears to be scope for more exploration of relationships between government regulatory systems and self-regulatory media bodies – an area that is already under discussion and debate in some countries, such as South Africa and Lesotho. Procedures for appointment, accountability and representation of a wide spectrum of stakeholders warrant more detailed examination – along with the question of how the bodies that administer cybercrime regulations will fit into overarching schemes for media regulation.
- 7) Where there is political will to inhibit speech, legal tools will be found. Some SADC countries have used mechanisms as unexpected as aviation regulations, allegations of non-payment of utility accounts and bogus charges of illegal drug trafficking to harass journalists and shut down media businesses. Legal tactics to control speech that is critical of government are likely to become even more pronounced as many crucial elections take place in the SADC region in 2023-2024.

- 8) One area that could be further explored is the power of the government to close down internet access, either partially or completely. This power was not typically found in cybercrime laws, but in more general laws on electronic communications.
- 9) Cybercrime and related media laws are rapidly evolving across the region, with many new developments. This means that even recent research in this field quickly becomes outdated and must be frequently revised and refreshed.
- 10) While most SADC member states have since the early 2010s, and even earlier, introduced and implemented cyberspace, cybersecurity and/or cybercrime related laws, some – such as Namibia and Lesotho – are still in the process of finalising substantive laws and regulatory frameworks for enactment or implementation.
- 11) Aside from the democracy and human rights challenging aspects emerging from the latest regional trend to legislate for cyberspace, all SADC member states already had or have a range of problematic laws and regulatory frameworks, from colonial era laws or outdated post-colonial frameworks to more recent press laws or penal code amendments, on their statute books that can be or have been used for repressive purposes.
- 12) In this regard, over the years, the primary tools used to clampdown on the media, as well as civil society and political opposition in countries across the region, have been criminal defamation or insult provisions, as well as decency, national security or public order provisions, among others, in criminal procedures laws or penal codes, along with media registration and communications regulatory mechanisms and, of late, provisions related to the dissemination of what can broadly be labelled as fake news.
- 13) Concerningly, in many instances where repressive state practices have been recorded and reported, such practices have occurred as a result of law enforcement and/or state security actors having acted extrajudicially.
- 14) Similarly, media freedom and free expression violations have occurred where law enforcement and/or state security overreach have been enabled by poorly developed or under-developed law or regulatory provisions.
- 15) At the same time, across the region human rights safeguards, along with public oversight guardrails, and transparency and accountability mechanisms, where such exist, are generally also poorly developed or under-developed in law and regulation, and especially so in the context of cybersecurity or cybercrime law and regulation.
- 16) The enabling of state surveillance abuse and/or overreach – especially through mass surveillance enabling legislative and regulatory measures – has become a primary concern, particularly for media freedom advocates, in the context of cybersecurity and/or cybercrime law and regulatory crafting and drafting in the SADC region.



RECOMMENDATIONS

Taking into consideration the totality of this analysis, the following sectoral recommendations are proffered:

FOR JOURNALISTS AND THE MEDIA:

- Journalists and the media in countries across the region are encouraged to continuously and persistently focus the glare of public scrutiny on law and regulatory crafting and implementation that threaten freedom of expression and media freedom, both domestically and regionally.
- Specifically, journalists and the media in general are encouraged to proactively engage with law, policy and regulatory crafting and drafting processes – on such issues as promoting the repeal of criminal defamation provisions – that could impact media freedom and freedom of expression generally.
- In the same vein, journalists and the media in countries across the region are encouraged to continuously and persistently contribute to raising public awareness and knowledge of the content and potential impacts of state-driven actions in the realm of cyberspace law and regulation.
- Regionally, journalists and media organisations are encouraged to form effective information and advocacy sharing networks that engage at the highest levels with regional governments and international stakeholders on media freedom issues in the digital age.

FOR CIVIL SOCIETY:

- Donor programming and advocacy efforts should focus on bringing laws regulating freedom of expression and media freedom, and practice thereof, in line with best practice guidance and standards, making them compliant with international and continental instruments that speak to protecting and enhancing such freedoms.
- Domestic and regional civil society actors are encouraged to form alliances and collaborations with local and regional media actors to raising local and regional public awareness and knowledge of the content and potential impacts of state-driven actions in the realm of cyberspace law and regulation.
- Similarly, human rights and civil society actors, both domestically and regionally, are encouraged to continuously and persistently focus the glare of public interest advocacy on law and regulatory crafting and implementation that threaten freedom of expression and media freedom, both domestically and regionally.

FOR SADC GOVERNMENTS:

- Laws regulating freedom of expression and media freedom should be brought in line with best practice guidance and standards and reflective of compliance with international and continental instruments that speak to protecting and enhancing such freedoms.

- SADC member states are encouraged to look to international and continental best practice guidance and examples, such as the Malabo Convention, in the context of domestically legislating for cyber security and cybercrime, and to bring laws and regulatory frameworks in line with such guidance and examples.
- In this regard, states are also encouraged to look to the Declaration of Principles on Freedom of Expression and Access to Information in Africa as guidance in law, policy and regulatory crafting and drafting in the context of free expression and media freedom, as well as cyber security and cybercrime related matters.
- In line with the above, states are explicitly encouraged to build out, where necessary in cyber security and cybercrime laws and regulatory frameworks, meaningful and effective public and judicial oversight and transparency mechanisms as necessary guardrails against executive, law enforcement and state security abuse and overreach.
- Similarly, in the context of elections, states are encouraged to give life to the Guidelines on Access to Information and Elections in Africa, both legislatively and practically.
- SADC member states are encouraged to revisit and review criminal defamation and insult provisions, that generally adversely impact media freedom, in their criminal procedure and penal codes with a view to bringing such measures in line with best practice, either through repealing them or updating them, in line with domestic constitutional arrangements.



CONCLUSION

As this report illustrates, media freedom and journalism are under heightened threat and sharpened assault across the African continent, with developments across the Southern African Development Community (SADC) over recent years becoming especially troubling. International human rights and security NGOs, scholars and political observers have expressed concern over ongoing trends which include:

- i. Criminalisation of technical offences e.g. computer possession.
- ii. Criminalisation of content-based offences e.g. covering a report by a hacker.
- iii. Legalisation of state surveillance – allowing authorities to intercept, retain, and access people’s data.
- iv. Punitive take down provisions.
- v. Laws, especially election laws, that outright muzzle journalism practice – especially in the cyberspace.

Additionally, there are miscellaneous legal provisions that might be applied to restrict freedom of expression – such as the misuse of civil defamation to silence activists, or general laws on topics such as terrorism, national security, money laundering and “foreign agents”. These arsenal of repressive tools are unrelentingly being deployed to undermine media freedom and civic spaces within SADC. Against the backdrop of upcoming crucial national elections – nine of the 16 SADC member states are holding elections between August 2023 through to the end of 2024 – donors and other development partners should be concerned about this trend and make investments to protect the freedom of expression.



USAID
FROM THE AMERICAN PEOPLE



Internews
Local voices. Global change.



ADVANCING RIGHTS
IN SOUTHERN AFRICA
ARISA