CHAPTER 7

ESWATINI

CHAPTER 7: ESWATINI

ESWATINI KEY INDICATORS
2023 WORLD PRESS FREEDOM RANKING: **111th globally; 29th out of 48 African countries** "Renamed eSwatini by royal decree in 2018, the former Swaziland is an absolute monarchy that prevents journalists from working freely and independently."
MALABO CONVENTION: NOT signatory or party
BUDAPEST CONVENTION: NOT signatory or party
CONSTITUTIONAL PROTECTION FOR FREEDOM OF EXPRESSION: eSwatini's 2005 Constitution **24. PROTECTION OF FREEDOM OF EXPRESSION** 1. A person has a right of freedom of expression and opinion. 2. A person shall not except with the free consent of that person be hindered in the enjoyment of the freedom of expression, which includes the freedom of the press and other media, that is to say – a. freedom to hold opinions without interference; b. freedom to receive ideas and information without interference; c. freedom to communicate ideas and information without interference (whether the communication be to the public generally or to any person or class of persons); and d. freedom from interference with the correspondence of that person. 3. Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision – a. that is reasonably required in the interests of defence, public safety, public order, public morality or public health; b. that is reasonably required for the purpose of – i. protecting the reputations, rights and freedoms of other persons or the private lives of persons concerned in legal proceedings; ii. preventing the disclosure of information received in confidence; iii. maintaining the authority and independence of the courts; or iv. regulating the technical administration or the technical operation of telephony, telegraphy, posts, wireless broadcasting or television or any other medium of communication; or c. that imposes reasonable restrictions upon public officers, except so far as that provision or, as the case may be, the thing done under the authority of that law is shown not to be reasonably justifiable in a democratic society.
KEY LAWS: • Computer Crime & Cybercrime Act 6 of 2022 • **Sedition and Subversive Activities Act 46 of 1938** (certain provisions)

• Suppression of Terrorism Act 3 of 2008 (certain provisions)
CRIMINAL DEFAMATION: Yes
DATA PROTECTION: eSwatini has a data protection law.[1]
ACCESS TO INFORMATION: eSwatini has no access to information law.

7.1 CONTEXT

The eSwatini media and civil society landscapes, as well as the general human rights climate, are characterised by continuous and ongoing repression.

The publication of newspapers requires registration under the **Books and Newspapers Act 20 of 1963.** Newspaper editors must be resident in eSwatini.[2]

The **Swaziland Communications Commission Act 10 of 2013** establishes a body that regulates all communications services in the country, including postal services, broadcast media and the internet. This body, now known as **eSwatini Communications Commission (the SCC)**, resorts under the Ministry of Information, Communication and Technology. The Board is appointed by the minister in consultation with the relevant Cabinet standing committee, and many of its functions require ministerial approval.[3] The SCC is thus not an independent authority. although it is charged with acting in "an objective, transparent, proportionate and non-discriminatory manner".[4] The creation of this Commission was reportedly the catalyst for the enactment of a trio of related laws in 2022: Computer Crime and Cyber Crime Act, 2022, the Data Protection Act, 2022, and the Electronic Communications and Transactions Act, 2022.[5]

The state broadcaster, the eSwatini Television Authority (STA), is established by **The Swaziland Television Authority Act, 1983.** It operates under the direction of a Board of Control, appointed by the minister, which monitors "the content of programmes and other transmissions to ensure that they conform with acceptable moral standards".[6]

Regulation of the broadcasting sector is in the process of being updated by the **eSwatini Broadcasting Bill 20 of 2019**, which has been repeatedly revised and delayed for years and is, as of mid-2023, awaiting Royal Assent.[7] According to press reports, this Bill will create a Broadcasting Corporation that merges the eSwatini Television Authority and the eSwatini Broadcasting and Information Services (the State radio

[1] Data Protection Act 5 of 2022.
[2] Books and Newspapers Act 20 of 1963, section 4. A "newspaper" is defined in section 2 to include "any printed matter containing news, or intelligence, or reports of occurrences of interest to the public or any section thereof, or any views, comments or observations thereon printed for sale or distribution and published periodically or in parts or numbers at intervals not exceeding one month but does not include a visiting or business card, billhead, letter-head, price list, annual report, trade circular, trade advertisement or other legal or trade or business document".
[3] The Swaziland Communications Commission Act 10 of 2013, read with section 6 of The Public Enterprises (Control And Monitoring) Act 8 of 1989.
[4] The Swaziland Communications Commission Act 10 of 2013, section 6.
[5] Ndimphiwe Shabangu,"eSwatini passes cyber laws under dark clouds", Association for Progressive Communications, 23 August 2022.
[6] The Swaziland Television Authority Act, 1983, sections 9-10 in particular.
[7] Personal communication with local expert, July 2023.

service). It would also create a three-tier broadcasting system for public, commercial and community broadcasting, transform state-owned media houses into independently controlled entities, and regulate the broadcasting sector in a way that will improve accountability and professionalism.[8]

The media has a self-regulating body in the form of the **Media Complaints Commission**, which was registered in 2011.[9] It has been reported that this body is underfunded, and its independence has been questioned.[10] The Commission's role is to ensure the implementation of the Swaziland Journalists Code of Ethics and to provide aggrieved persons with an opportunity for redress outside the courts in respect of the print media. However, as of 2018, it was reported that only two publications, the *Times* and the *Observer*, were participating in this body. The broadcasting sector is not engaged in the Commission and has no complaints body of its own.[11]

In general, according to one journalist, there is "not much freedom to report as most of the media houses are state owned and even the independent media outlets use self-censorship so that their licences wouldn't get revoked".[12]

7.2 CONSTITUTION

Section 24 of the Constitution is quoted in the table on the first page of this chapter. With regard to the grounds for justifiable limitation of the right which it enumerates, it has been observed that:

> *These limitations are generally not out of step with international norms for limitations on freedom of expression, except in one respect, namely, the restriction imposed on public officers. Obviously, many public officials do have secrecy obligations, particularly in defence, intelligence and police posts. Nevertheless, the general ability of whistleblowers in the public service to bring illegal conduct, including corruption, to the attention of the media in the public interest is a critical part of a functioning democracy. Consequently, such limitations provisions could have a chilling effect on public servants, unduly preventing the disclosure of official misconduct.*[13]

In the 2014 *Swaziland Independent Publishers* case, the Supreme Court was asked to consider whether the conviction for contempt of court of editor and journalist Bheki Makhubu, along with the publisher of his articles, constituted an unjustifiable infringement of the right to freedom of expression. The case concerned two articles

[8] Sifiso Nhlabatsi, "Parliament Passes Broadcasting Bill", *Eswatini Observer*, 16 October 2020; "Eswatini Broadcasting Bill heralds new hope", *Inhlase*, 31 October 2020; "African Media Barometer: Eswatini 2018", Media Institute of Southern Africa (MISA) and Friedrich-Ebert-Stiftung (FES), section 3.
[9] "Eswatini: Misa Applauds Registration of Media Complaints Commission", Media Institute of Southern Africa (Windhoek) press release, 15 June 2011.
[10] "Freedom of the Press 2016 – Swaziland", Freedom House, "Legal Environment".
[11] "African Media Barometer: Eswatini 2018", Media Institute of Southern Africa (MISA) and Friedrich-Ebert-Stiftung (FES), page 47.
[12] Journalist quoted anonymously in Ronja Koskinen and Helsingin Sanomat, "Crackdown on press freedom in Eswatini", International Press Institute, 7 July 2021.
[13] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 5: eSwatini", Konrad Adenauer Stiftung, 2021, page 246.

published in *The Nation* magazine. One article criticized the Swazi judiciary on the basis that they "could not be bothered to interpret the Constitution". Even though this article used words such as "criminal" and "treasonous" with reference to the judges, the Court found that this was merely the opinion of the author and overturned the conviction in respect of this article, saying that its criticisms of the judiciary were "bland and eminently permissible within the context of Swaziland's constitutional freedom of the press guarantees". The second article the second article compared the Chief Justice to Tarzan, a "high school punk" and a "street punk". The Court found that this article, in contrast to the other one, "mounted a scurrilous and unwarranted attack upon the judiciary as a whole, and upon the administration of justice in this Kingdom" and that the conviction of contempt of court for "scandalising the judiciary" was warranted in this instance but reduced the sentence imposed by the lower court.[14]

In 2015, the case of *Maseko v R* again considered convictions for contempt of court. Journalists Bheki Makhubu and Thulani Maseko wrote articles in *The Nation* magazine again criticizing the judiciary system for partiality and lack of independence. Both were arrested, charged, and convicted for two counts of contempt of court, and sentenced to two years in prison, with a fine being imposed on the publisher of the magazine. In the Supreme Court, the State Prosecutor conceded the appeal, The judge found that the case had constituted "a travesty of justice," noting that the High Court did not properly balance the right to freedom of expression with the authority of the courts. The Supreme Court judgment stated that the "importance of freedom of expression in promoting democracy and good governance cannot be over emphasized." The Supreme Court overturned the convictions and ordered the immediate release of the two journalists.[15]

In 2016, in the case of *Maseko v The Prime Minister of Swaziland*, the High Court struck down certain sections of the Sedition and Subversive Activities Act No. 46 of 1938 and the Suppression of Terrorism Act 3 of 2008 on the grounds that they infringed the fundamental rights to freedom of expression and association in a manner that was not reasonably required and proportionate. Thulani Maseko and Maxwell Dlamini were both charged with sedition, subversion, and contravention of the Terrorism Act on the basis of speeches at a May Day celebration in 2014. Dlamini along with two other political activists had been charged with seditious intention in 2013 for participating in a rally while carrying a banner calling for the boycott of the 2013 national elections. Maseko had previously been charged with "uttering words with a seditious intention" after speaking at a May Day Celebration in 2009. With respect to the Sedition and Subversive Activities Act, the High Court found that the challenged provisions of this law (sections 3(1), 4(a) and (e), and 5) were unconstitutional since it was unlawful to limit free speech for the sole purpose of shielding the government from criticism or discontent, which did not lie within the permissible constitutional grounds for limitation. Regarding the Suppression of Terrorism Act, the Court found that the State did not offer sufficient justification to save the impugned provisions (portions

[14] *Swaziland Independent Publishers v The King* [2014] SZSC 25, 30 May 2014; see the case summary by Global Freedom of Expression here.
[15] *Maseko v R* [2015] SZSC 03, 29 July 2015; see the case summary by Global Freedom of Expression here.

of section 2(1) and sections 11(1)(a) -(b), 11(2), 28 and 29(4)).[16] However, the State is now appalling this judgment. In 2022, the Supreme Court condoned the delays that should have caused the appeal to lapse, holding that the State's appeal can proceed, on the grounds that the constitutional issues at stake are too important to be decided by default.[17]

It should be noted that human rights lawyer Thulani Maseko, who was involved in two of the cases discussed here, was tragically shot dead by unknown assailants at his home in eSwatini on 21 January 2023 – the same day on which the King of eSwatini made a veiled threat against members of the country's pro-democracy movement.[18]

7.3 CASE STUDIES

Reporters without Borders observes that any criticism of the monarchy "is liable to lead to a trial and heavy penalties", noting further that "dozens of draconian laws muzzle freedom of expression and information, and the judicial system is often used to undermine journalism.[19] It also states that journalists are often arrested and subjected to violence.[20]

The US State Department's 2022 report on human rights practices in eSwatini contains the following overview:

> *Civil society tension remained high since 2021 unrest, resulting in reports of citizens, businesses, and even government officials and parliamentarians not exercising their right to free speech in fear of direct and indirect retaliation by the government, and fear of targeting by unidentified opposition elements that claimed responsibility for violent actions. [ ] Although journalists have spoken out against the government in recent years, criticism of the king was discouraged by government and traditional leaders. According to an October report by the Campaign for Free Expression and the Inhlase Center for Investigative Journalism, a widespread culture of self-censorship existed among journalists, especially regarding reporting related to the king and the royal family. Most journalists and broadcast media avoided criticizing the palace due to fear of reprisals such as being professionally ostracized or losing paid government advertising in their outlets. One independent monthly magazine that covered sociopolitical topics reportedly lost advertising revenue from a parastatal after it published criticism of the royal family. Self-censorship only applied to matters regarding the palace and was virtually non-existent in relation to the government, which media frequently criticized. Daily independent newspapers routinely criticized government corruption and inefficiency but avoided criticizing the royal family. […]*[21]

[16] *Maseko v The Prime Minister of Swaziland* [2016] SZHC 180, 16 September 2016; see the case summary by Global Freedom of Expression here. See also Angelo Dube and Sibusiso Nhlabatsi, "The (Mis)application of the Limitation Analysis in *Maseko and others v Prime Minister of Swaziland and others*" [referring to the dissenting judgment], *Law, Democracy and Development*, Vol 22, 2018.
[17] Peter Fabricius, "Historic Swazi court judgment striking down parts of sedition and terrorism laws is under threat", *Daily Maverick*, 29 September 2022,
[18] "eSwatini: Experts condemn killing of human rights defender Thulani Maseko, demand accountability", UN Office of the High Commissioner on Human Rights, 26 January 2023; Pavan Kulkarni, "Assassination of Thulani Maseko has killed prospects of peaceful struggle in Swaziland", *People's Dispatch*, 27 January 2-23.
[19] "2023 World Press Freedom: eSwatini", Reporters Without Borders, "Legal framework".
[20] Id, "Safety".
[21] "2022 Country Reports on Human Rights Practices: eSwatini", US State Department, section 2A.

A representative of the Media Institute of Southern Africa (MISA) stated: "The government is uneasy with the free flow of information. Every time a journalist reports something critical about the government, they and their families are hunted. The government and the King do not want press freedom in the country, because this would expose the underlying corruption and problems in the country".[22] In October 2022, the Inhlase Centre for Investigative Journalism described a "deeply concerning political and economic environment in Eswatini, where, following the June 2021 unrest, citizens are afraid to speak out to express their political views or to demand service delivery; journalists' work is being compromised by threats to their lives; and the right to protest is under attack."[23]

In 2022, a group of about 20 correctional officers reportedly **assaulted** Nomthandazo Maseko, a reporter for the news website *Swati Newsweek, after she* livestreamed a protest outside a prison where the local prison where two pro-democracy members of Parliament were detained. She stated that the correctional officers hauled her out of her care, slapped her, kicked her and beat her with sticks. She also stated that one officer pointed a gun at her and threatened to shoot her.[24]

In 2021, two South African reporters for the South African news website *New Frame,* Magnificent Mndebele and Cebelihle Mbuyisa, were **arrested** after attending the funeral of a police shooting victim. Soldiers reportedly threatened the journalists at gunpoint, seized their cameras, and forced them to delete footage of the funeral. They were then taken to a police station for interrogation, where they were tortured; amongst other assaults, police held plastic bags over their heads to suffocate them. They were released several hours later, and both received medical treatment at a local hospital. They both returned to South Africa the next day.[25]

In 2021, two Members of Parliament representing an opposition party, Mduduzi Bacede Mabuza and Mthandeni Dube, were charged under **section 5(1) of the Suppression of Terrorism Act, 2008** for "terrorist acts" in respect of three events: a gathering on 5 June 2021 where one of the MPs allegedly suggested that there be a democratically elected Prime Minister, rather than one appointed by the King; a meeting at a restaurant, where one of the MPs allegedly encouraged sending petitions to Tinkhundla centres (local government constituencies); and a speech in which one MP allegedly said "*Akuklalwa Namuhla*" (roughly translated to "not sleeping today") – in other words, the "terrorist acts" constituted the voicing of political opinions that made no reference to violence.[26]

In 2020, Zweli Martin Dlamini, editor of the website *Swaziland News*, was arrested in connection with **sedition** after publishing two articles critical of the King. Police seized his laptops, cell phones, hard drives, and other electronic devices and took him into custody. There, police officers reportedly handcuffed him to a bench and tried to

[22] Ronja Koskinen and Helsingin Sanomat, "Crackdown on press freedom in Eswatini", International Press Institute, 7 July 2021, quoting Nqaba Matshazi, MISA's fundraising and regional campaigns coordinator.
[23] Hanifa Manda, "Eswatini Freedom Of Expression Summit", Inhlase Centre for Investigative Journalism, October 2022, page 3.
[24] "eSwatini prison officers assault, threaten to shoot reporter covering pro-democracy protest", Committee to Protect Journalists, 16 February 2022.
[25] "eSwatini police detain, abuse 2 reporters from South African outlet New Frame", Committee to Protect Journalists, 8 July 2021.
[26] "More delays as Eswatini MPs languish in jail", Southern Africa Litigation Centre, 22 September 2021.

suffocate him by putting a plastic bag over his head. He was released without charge after some six hours, but police did not return the confiscated devices. Dlamini fled to South Africa the next day, where he received medical attention. His lawyers filed a complaint with eSwatini's Commission on Human Rights and Public Administration, accusing the police of "torture and humiliation" and violation of Dlamini's right of expression. The next day, *Swaziland News* published a report questioning the state of the King's health during the Covid pandemic. Police again raided Dlamini's home and confiscated some material, without producing a search warrant. They took Dlamini's wife into custody, leaving the couple's two young children alone in their home. She reported that she was questioned about Dlamini's whereabouts, slapped and verbally abused. She also alleged that police officers handcuffed her and covered her head with a plastic bag to suffocate her. She was released without charge after about three hours. The government denied that Dlamini's arrest related to his criticism of the King, stating that he had allegedly violated Covid regulations that criminalised the spreading of false news about the virus.[27]

In 2020, an assistant weekend editor of the privately owned newspaper *The Times of eSwatini*, Welcome Dlamini, received **threatening text messages** from a person who claimed to be a member of a banned opposition party after the newspaper published a column *supporting* eSwatini's system of government. He received another death threat via text after he opened a case with the police.[28]

In another 2020 incident, police officers reportedly raided the home of Eugene Dube, the editor and publisher of the privately owned news website *Swati Newsweek*, seizing three mobile phones, a laptop, and work documents. Dube was taken into custody and interrogated for about seven hours about two articles critical of the King. He was then brought before a magistrate to record a statement. before being released without charge. The police retained his devices and documents on the grounds that they were required for further investigation. According to Dube, police told him that the King was immune from criticism and warned him that he could face charges of **high treason**. Police then went to the home of journalist Mfomfo Nkhambule, who wrote one of the two articles published by Dube. Nkhambule was also taken to a police station and interrogated about the articles, where he was also threatened with charges of **treason**. Nkhambule said that he had also been interrogated by police in connection with articles about the King written the previous year for another online publication, *Swaziland News*. On that occasion, a police officer allegedly threatened to throw him out of a second floor window, explaining that they would cover it up by claiming that he had tried to escape.[29] A report in the weekly publication *Independent News quoted p*olice commissioner William Tsintsibala Dlamini as saying that authorities would come down hard on journalists who wrote negatively about King Mswati III and that the law would take its course. Government spokesperson

[27] "Swazi editor flees to South Africa, wanted in false news investigation", Committee to Protect Journalists, 15 May 2020. Dlamini had previously received death threats from a local businessman, in 2017, in connection with an article about the King's involvement in a corruption case. He fled to South Africa at that stage, and his newspaper, ,*Swaziland Shopping,* was shut down by the government. He returned to Swaziland in 2018 after the businessman who had threatened him passed away. "2023 World Press Freedom: eSwatini", Reporters Without Borders, "Safety.

[28] "eSwatini editor receives death threats over pro-government article", Committee to Protect Journalists, 13 July 2020. The opposition party in question denied that the person who sent the threats was their member.

[29] "Swaziland journalists harassed, threatened with treason charges over reporting on king", Committee to Protect Journalists, 30 April 2020. Police apparently searched for Mthobisi Ntjangase, the reporter who wrote the other article, but could not find him.

Sabelo Dlamini said that Dube was under investigation for operating an unregistered media outlet, not for criticizing the King.[30]

In addition to government arrests and intimidation, it was reported in 2020 that there is an increasing trend of **civil defamation cases against the media** particularly by rich and powerful individuals, couples with concerns that courts do not always apply the principle of "fair comment" about matters of public interest as a defence against defamation claims. Bheki Makhubu, editor of *The Nation* magazine, was quoted as saying that the judiciary and prominent figures are turning the media into an "industry of compensation", as huge awards encourage people to become litigious. He worries that the judiciary "has moved beyond being an arbiter of justice and taken on a seeming censor's role. Fearful journalists then self-censor, shying away from reporting any story that might get them into trouble with the law. The media is now expected to do the bidding of the powerful people and government." [31] Some civil society groups have maintained that the hefty awards in defamation actions mean that "the justice delivery system is being used to create a climate of fear in the media that undermines reportage of issues of public interest and national development".[32] The managing editor of *Times of eSwatini,* Martin Dlamini, was quoted as stating said that hefty damages in civil defamation claims are sending a strong message to the media that they should not write stories critical of powerful people, noting that there are other avenues that aggrieved people can use to get redress from media houses, such as the Media Complaints Commission with an Ombud as well as some in-house ombuds at individual media outlets, but the courts do not encourage complainants to use them." [33]

The eSwatini Communications Commission **shut down Internet access** throughout the country on 29 June 2021 as protests against King Mswati III spread nationwide. This shutdown also prevented two print newspapers, the state-owned *eSwatini Observer* and the privately owned *Times of eSwatini*, from being able to publish on two consecutive days. General website traffic resumed on July 4, but social media platforms remained blocked until 8 July.[34] A MISA representative stated: "Without the access to internet the Eswatini government is able to control the narrative. Lack of internet access is making it difficult for the journalists to report about the crackdown to the international audience and put pressure on the government. Eswatini media and citizens are now isolated and left on their own without access to information. As long as the internet is shut down, Eswatini is a dark spot, and nobody knows exactly what's going on there and what the real scale of the violence towards citizens and journalists is." [35] A second internet blackout was imposed for a brief period in October 2021.[36]

[30] "Id. The *Independent News report referred to appears to be no longer available online.*
[31] Vuyisile Hlatshwayo, "'Climate of fear' in eSwatini media", *Mail & Guardian*, 11 November 2020.
[32] Joint submission by the Women and Law in Southern Africa Research and Educational Trust Eswatini (WLSA) and the Advancing Rights in Southern Africa (ARISA) Program on Eswatini to the 39th Session of the Working Group on the Universal Periodic Review (undated), page 10.
[33] Vuyisile Hlatshwayo, "'Climate of fear' in eSwatini media", *Mail & Guardian*, 11 November 2020,
[34] "eSwatini police detain, abuse 2 reporters from South African outlet New Frame", Committee to Protect Journalists, 8 July 2021.
[35] Ronja Koskinen and Helsingin Sanomat, "Crackdown on press freedom in Eswatini", International Press Institute, 7 July 2021.
[36] "Freedom in the World 2022: Eswatini", Freedom House, section D1.

7.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION

A) THE COMPUTER CRIME AND CYBER CRIME ACT, 2022

The Computer Crime and Cyber Crime Act, 2022 came into force on 4 March 2022.[37] The Association for Progressive Communications provides this overview:

> *The Computer Crime and Cyber Crime Act, 2022 criminalises offences committed against and through the use of computer systems and electronic communications networks. Whilst mechanisms to protect citizens against criminal and terrorist elements that emanate from the use of the internet are necessary, there is a danger and risk that this can be misused by governments to curtail freedom of expression on the internet, which has implications such as the shrinking of online civil society spaces. Among the concerns expressed is that the law has the potential to be interpreted in a way that targets vocal human rights defenders, media practitioners and activists. The regulations of the law are yet to be developed.*[38]

In early discussions around the Bill, the government proposed to include heavy fines and jail sentences for "Facebook abusers" and persons who posted "fake news" on the Internet.[39] This inspired a flurry of criticism.[40] No such provisions were included in the final law.

The Act is administered by the **Eswatini Communications Commission** established under the Eswatini Communications Commission Act, 2013, which has the power "to regulate and coordinate matters of cybersecurity and enforce standards applicable to the security of the critical information infrastructures".[41] The Act also authorizes the Prime Minister to establish a **National Cybersecurity Advisory Council** with a maximum of 15 members from a cross section of stakeholders, including the ICT, legal, finance, education, business, civil society, defence, police, international cooperation and national security sectors.[42]

The Act creates the technical offences listed in the table below. Most of these offences are actionable only if committed "intentionally, without lawful excuse or justification", which helps to narrow them and avoid capturing good faith conduct in the public interest – such as testing a computer system's vulnerabilities.

[37] Computer Crime & Cybercrime Act 6 of 2022, section 1.
[38] Ndimphiwe Shabangu,"eSwatini passes cyber laws under dark clouds", Association for Progressive Communications, 23 August 2022.
[39] The Bill originally included a prohibition on the publication of "any statement or fake news through any medium, including social media with the intention to deceive any other person or group of persons" (section 19). "LEXOTA Country Analysis: Eswatini", last updated July 2022.
[40] Ndimphiwe Shabangu,"eSwatini passes cyber laws under dark clouds", Association for Progressive Communications, 23 August 2022; "Fears that cybercrime bill will hit eSwatini's media freedom", The Economist Intelligence Unit, 14 September 2020.
[41] Computer Crime & Cybercrime Act 6 of 2022, section 2 (definition of "Commission") and section 52.
[42] Id, section 53.

THE COMPUTER CRIME AND CYBER CRIME ACT - TECHNICAL OFFENCES	
Section 3: Illegal access	It is an offence to intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, access the whole or any part of a computer system. There is an enhanced penalty where such access infringes security measures with the intention of obtaining computer data. o "Access" for purposes of this section means "logging into a computer system" (section 2). o It has been asserted that this crime carries an excessive maximum penalty – a E500 000 fine or imprisonment for five years (as the enhanced penalty) – which is out of line with that imposed for similar offences in other SADC countries. [43]
Section 4: Illegally remaining logged onto a computer	It is an offence to intentionally, without lawful excuse or justification, infringe security measures or with the intention of obtaining computer data or with other dishonest intent, remain logged in a computer system or part of a computer system or continues to use a computer system. o The requirement of having "the intention of obtaining computer data" or "other dishonest intent" helps to prevent this offence from being overbroad. o It has been asserted that "illegal-remaining" offences are unnecessary because they are covered by the offence of unauthorized access.[44]
Section 5: Illegal interception	It is an offence "intentionally without lawful excuse or justification, or in excess of a lawful excuse or justification", to intercept, by electronic means any non-public transmission to, from or within a computer system or any electromagnetic emissions from a computer system.
Section 6: Illegal data interference	All of the actions described in this section are offences only if done "intentionally without lawful excuse or justification, or in excess of a lawful excuse or justification". It is an offence to do any of the following: • damage or deteriorate computer data; • delete computer data; • alter computer data; • render computer data meaningless, useless or ineffective; • obstruct, interrupt or interfere with the lawful use of computer data; • obstruct, interrupt or interfere with any person in the lawful use of computer data; or • deny access to computer data to any person authorized to access it. It is also an offence to commit any of the acts described in this section in order to deny access, including a partial denial of service, to any person authorized to such access or service.

[43] "Computer, Cybercrime act: a necessary evil", *Times of Eswatini*, 31 October 2022. This article cites the Botswana Cybercrime and Computer Related Crimes Act 18 of 2018 as a point of comparison, where a similar offence attracts a maximum fine of P20 000 (equivalent to E27 200) or imprisonment for a maximum of one year, or both. In Botswana, the related offence of unauthorised access to a computer service *with the intent to intercept data* attracts a doubled maximum penalty – which is still significantly less than the eSwatini penalty.

[44] *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 14.

	It is an offence - • to communicate, disclose or transmit any computer data, program, access code or command to any person not authorized to access it; • to access or destroy any computer data for purposes of concealing information necessary for an investigation into an offence; or • to receive computer data that the person in question is not authorized to receive. It is an offence to destroy or alter computer data that is required by law to be kept or maintained, or data that is evidence in relation to any proceeding under the Act by – • creating, destroying, mutilating, removing or modifying data or a program or any other form of information within or outside a computer or computer network; • activating, installing or downloading a program that is designed to create, destroy, mutilate, remove or modify data, a program or any other form of information within or outside a computer or computer network; or • creating, altering, or destroying a password, personal identification number, code or method used to access a computer or computer network, There is an enhanced penalty for data in "a critical database", and data concerned with "national security" or "the provision of an essential service". For purposes of these offences, it is immaterial whether an illegal interference or its intended effect is permanent or temporary. o The most concerning part of the list of offence is to receive computer data without authorization (subsection (3)(c)), which could affect data acquired by a whistleblower or placed in a cache such as Wikileaks. It is not clear if the exception of "justification" would apply to exposing such information in the public interest – and doubts about the application of this exception could result in self-censorship. o Regarding the enhanced penalties, "critical database" is not defined, but "critical infrastructure" is broadly defined in section 2 as "computer systems, devices, networks, computer programs, computer data, vital to the country [such] that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on, national or economic security, national public health and safety, national elections or any combination of those matters; or physical infrastructure, assets or systems declared as such by Government". There is no definition of "national security or "essential service". o Best practice avoids potential risks arising from an overly broad definition of "critical infrastructure".[45] o The Southern Africa Litigation Centre has asserted that subsection (6) (enhanced penalties in respect of data in a critical database, or data concerned with national security or the provision of an essential service, and subsection (7) (making it immaterial whether the interference or its effect is temporary or permanent) are "so overly broad that they cannot possibly pass constitutional muster".[46]

[45] *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 15.
[46] "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020.

Section 7: Data espionage	It is an offence "intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification" to obtain for oneself or another person computer data which is not meant for that person and which is "specially protected against unauthorized access". o Without knowing that would be covered by "justification", it is possible that this offence could inhibit some instances of investigative journalism. o This formulation of the offence raises the question of how a person would know if data is "specially protected", as opposed to merely "protected". o Without more specificity, "unauthorized access" could be interpreted broadly to include data which is not legally protected, but has only been arbitrarily declared to be prohibited from access by a government official. [47] o It has been asserted that "data espionage" offences are unnecessary because they are covered by the general offence of unauthorized access.[48]

Section 8: Illegal system interference	All of the actions described in this section are offences only if done "intentionally without lawful excuse or justification, or in excess of a lawful excuse or justification".
	
	It is an offence to hinder or interfere with the functioning of a computer system or with a person who is lawfully using or operating a computer system.
	It is an offence to seize or destroy any computer storage medium.
	
	It is an offence to hinder or interfere with a computer system that is exclusively for the use of critical infrastructure operations, or one that is used in critical infrastructure operations, where that conduct affects that use or impacts the operations of the critical infrastructure. This offence attracts a harsher penalty than the other offences in the section: a fine of up to one million Emalangeni or imprisonment for up to ten years, or both.
	
	o "Critical infrastructure" is broadly defined in section 2 as "computer systems, devices, networks, computer programs, computer data, vital to the country [such] that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on, national or economic security, national public health and safety, national elections or any combination of those matters; or physical infrastructure, assets or systems declared as such by Government".
	o "Hinder" in relation to a computer system includes but is not limited to –
	  o cutting the electricity supply to a computer system;
	  o causing electromagnetic interference to a computer system;
	  o corrupting a computer system by any means; and
	  o inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data (section 2).
	o The offence of seizing or destroying any computer storage medium is " overly broad and can easily lead to abuse".[49] Note that this offence is punishable by a maximum penalty of E500 000 or 4 years' imprisonment.

Section 9:	It is an offence "intentionally without lawful excuse or justification or in excess of a lawful excuse or justification" to produce, sell, introduce, spread, procure

[47] Id.
[48] *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 14.
[49] "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020.

Illegal devices	for use, use, import, export, distribute or otherwise make available any of the following: • a device, including a computer program, that is designed or adapted for the purpose of committing an offence under Part II of the Act • a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed • a software code that damages a computer or computer system. It is an offence even to possess any of the described items, with the exception of the software code. However, this offence requires the intent that the item in question is to be used by any person for committing an offence described in Part II of the Act. o Section 2 includes a wide and yet non-exhaustive definition of "device". o The aspect of this section on *using* an illegal device essentially makes the means of committing the underlying offence into an additional offence – thus imposing double criminalization on a single act.[50]
Section 10: Computer related forgery and uttering	It is an offence "intentionally without lawful excuse or justification or in excess of a lawful excuse or justification" to input, alter, delete, or suppress computer data, resulting in inauthentic data, with the intention that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible. There is an enhanced penalty if this offence is committed by sending out multiple electronic mail messages from or through a computer system. o Section 2 defines "multiple electronic mail messages" as a mail message including e-mail and instant messaging sent to more than one recipient. The Southern Africa Litigation Centre suggested that this definition should require a message sent to more than 1000 recipients, to avoid overbreadth.[51]
Section 11: Computer related fraud	It is an offence "intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification" to cause loss of property to another person by any input, alteration, deletion or suppression of computer data, or any interference with the functioning of a computer system, with a fraudulent or dishonest intention of procuring, without permission, an economic benefit for oneself or someone else. o The required intent helps to ensure that this offence is properly targeted.
Section 12: Phishing	It is an offence "without a lawful excuse or justification" to use email, spoofed email, a website, social media or a text message to lure, deceive or threaten another person to give money or other value, or to reveal sensitive information, account login details, bank account or credit card information "or the like".

[50] Id. SALC believes that this offence was incorrectly transcribed from the SADC Model Law.
[51] Id.

	○ With regard to a "spoofed email", "spoofing" means "hiding the actual source address or identity behind another identity to appear as if the email or information is from the legitimate address (section 2). ○ The catch-all phrase "or the like" is arguably insufficiently clear to define a criminal offence.
Section 13: Cyber terrorism	It is an offence "intentionally without legal justification or legal excuse" to use a computer system - • to launch an attack on telecommunications or computer networks "through conventional methods"; • to launch attacks using physical devices, computer programs or other electronic means to - ○ render the financial or banking system of the country or city unusable; ○ compromise the defence system of the country; ○ seriously disrupt or interfere with the operations of the electricity grid, aviation control system, tax management systems, population register, government payroll and cabinet system; • to fund or raise funds with the purpose of financing or carrying out the listed acts. This offence carries a maximum penalty of a five hundred thousand Emalangeni fine or ten years' imprisonment or both. ○ The phrase used in other sections is "without lawful excuse or justification"; here it is "without legal justification or legal excuse". It is unknown if a different meaning was intended here. ○ Earlier versions of the bill had a much broader definition of this crime, but were evidently revised.[52] ○ It seems odd that a fine is a potential penalty for such a serious offence. ○ The Southern Africa Litigation Centre submits that cyberterrorism is already sufficiently covered by eSwatini's Suppression of Terrorism Act, as amended in 2017 and interpreted by the High Court. [53]
Section 16: Identity related crimes	It is an offence "intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification" to make use of a computer system to utilize someone else's identity for any unlawful activity.
Section 18: Extortion	This offence extends the crime of extortion to situations where the act of extortion takes place through the internet, email or any computer system platform – on other words, to situations where a computer is the tool. ○ Section 2 defines "extortion" as "an act of demanding favour or benefit from a person through coercion, or arising from an advantage one holds over the victim, by threatening to inflict harm to his person, family members, reputation or property by unleashing the advantage he holds over the victim".
Section 19: Website defacement	It is an offence "intentionally or without lawful excuse" to commit or participate in the website defacement of another entity's website. ○ "Website defacement" is defined in section 2 "as the act of attacking a

[52] Id.
[53] Id.

	website by changing the visual appearance, adding, changing, deleting or replacing content by a party or parties not authorized by the website owner". o This offence uses the phrase "intentionally *or* without lawful excuse" as opposed to the phrase "intentionally *and* without lawful excuse or justification: that appears in most of the other provisions in the Act. It is unclear what distinction was intended.
Section 24: Spam or Spamming	It is an offence "intentionally and without lawful excuse or justification" - • to initiate the transmission of spam messages from or through a computer system; • to use a hidden or disguised computer system to relay or retransmit multiple electronic mail messages, with the intention to deceive or mislead users, or any electronic mail or internet service provider, as to the origin of such messages; or • to materially falsify header information in multiple electronic mail messages and intentionally initiate the transmission of such messages. There are exceptions for transmission of multiple electronic mail messages within a customer or business relationship, where the recipient has not opted out of the relationship. o Section 2 defines "spamming" or "spam" as "the use of messaging systems to send unsolicited mail messages, text messages or adverts, usually for marketing or promotional purposes to customers, former or potential customers or other recipients". o Section 2 defines "multiple electronic mail messages" as messages including e-mail and instant messaging sent to more than one recipient.
Section 25: Denial of service and botnets	It is an offence to take "illegal control" of a computer system in a network, or an entire network of computer systems or network components, partially or fully and "remotely or otherwise". It is an offence "intentionally, without justification" to cause or launch an attack with data traffic on a computer system or network so as to overwhelm the network resources, resulting in slowed or denied service.
Section 49: General provision on cybercrimes	Any offence under any Act which is committed in whole or in part through the use of a computer, electronic device or in electronic form is deemed to have been committed under that Act and the provisions of that Act shall apply with the necessary modification. o This provision appears to be aimed at ensuring that any crime committed with computer tools can be prosecuted under the relevant law for that crime.

The Act creates ten content-related offences, covering a broad array of topics.

THE COMPUTER CRIME AND CYBER CRIME ACT – CONTENT-BASED OFFENCES	
Section 14: Child pornography	There is an extensive set of offences relating to "child pornography". The production of child pornography is an offence regardless of the medium used, but the other acts relating to children pornography are offences only if they involve a computer system or information and communication technologies. It is a defence in most cases if the conduct in question was for "a genuine artistic, educational, legal, medical, scientific or public benefit purpose, including Eswatini cultural events". It is also an offence to expose children to pornography, to engage in cybersex with a child or someone who lacks capacity to give legal consent to sex, or to subject such a person to sexual grooming. o "Child pornography" is defined in section 2 to mean "any material that depicts, presents or represents a child engaged in sexual conduct, or in the nude without a justifiable cause, or images representing a child engaged in sexual conduct", It includes, but is not limited to, audio, visual or textual material. o "Cybersex" means "sexual activity or fantasy which may lead to sexual arousal or pleasure gained through communication, for that purpose, by computer system with another person" (section 2). This definition seems somewhat unclear. o "Sexual grooming" means intentionally befriending or establishing an emotional connection with a child or an adult who is legally not able to consent to sex, to train them to agree to participate in acts of sexual abuse or exploitation or to , or lower their inhibitions in respect of such acts (section 2). The Southern Africa Litigation Centre finds this definition problematically cursory.[54] o It has been noted that the cybercrime version of this offence does not align well with the overlapping provision on pornography in eSwatini's Sexual Offences and Domestic Violence Act, 2018., which could lead to difficulties in implementation.[55]
Section 15: Prohibition of distribution or publication of pornography	It is an offence - • to distribute, publish, advertise or expose material, which is pornographic *to a child, or to non-consenting adults*; • to publish or exhibit any pornographic material without printing in such his or her name and the prescribed particulars of his or her address or without indicating the age restriction or consumer advice; or • to broadcast a pornographic film whether publicly or privately *to children or non-consenting adults.* There is a separate reference to commission of this offence by someone with parental power or control over the child in question, but the penalty prescribed is the same in this instance as in any other. o Note this offence is actually much narrower than its title suggests.

[54] Id.
[55] "Computer, Cybercrime act: a necessary evil", *Times of Eswatini*, 31 October 2022.

	○ The definition of pornography is reasonably specific. "Pornography" means a visual, text or audio presentation, simulated or real of – ○ a person who is, or is depicted as, participating in or assisting another person to engage in a sexual act or sexual violations, or a lewd display of nudity which is intended for sexual gratification; ○ explicit sexual conduct which degrades a person, or which constitutes incitement to cause harm; or ○ a sexual act between a person and an animal (section 2). ○ This offence replicates a provision of the Sexual Offences and Domestic Violence Act, with the exception of the penalties imposed, which is likely to lead to confusion.[56]
Section 17: Cyberbullying and cyberstalking	It is an offence to engage in cyberbullying or cyberstalking, or to aid or abet another person in these acts. ○ "Cyberbullying" is defined in section 2 as "the use of electronic communication to bully a person typically by sending messages of an intimidating or threatening nature". This definition is unclear, particularly with regard to what might be considered "intimidating". ○ "Cyberstalking" is defined in section 2 as "the use of the Internet or other electronic means to inflict repeated unwarranted actions on a natural or juristic person(s). Such actions may include false accusations, defamation, slander, libel, monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten, embarrass or harass; which may result in mental or corporate abuse." ○ The cybercrime law does not provide for restraining orders in cases where the cyberbullying or cyberstalking do not warrant imprisonment. The offence of cyberstalking is already provided for under the Sexual Offences and Domestic Violence Act, which defines unlawful stalking to include stalking by electronic means and is not limited to acts of a sexual nature; the Sexual Offences and Domestic Violence Act provides a remedy of a restraining order.[57]
Section 20: Racist, hate speech or xenophobic material	It is an offence "intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification" - • to produce racist, hate speech or xenophobic material with the intention of distributing it through a computer system; • to offer or make available racist, hate speech or xenophobic material through a computer system; or • to distribute or transmit racist, hate speech or xenophobic material through a computer system. ○ Section 2 defines "racist, xenophobic and hate speech [material]" as "any material, including but not limited to any image, video, audio recording or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals; which may be based on race, colour, descent, national or ethnic origin, religion, creed or social or economic standing, political opinion or disability". ○ This definition goes beyond the Malabo Convention requirements by including "creed or social or economic standing, political opinion or

[56] "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020.
[57] Id.

	disability". The Southern Africa Litigation Centre suggested that it could also have included sex, gender, sexual orientation, and gender identity.[58]
Section 21: Racist, hate speech and xenophobic motivated insult	It is an offence "intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification", through a computer system to "publicly" use language that "harms the reputation or feelings" of a person or a group of persons on the basis of race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors. o Although this is based on the Malabo Convention, criminalising "insult" - described here more widely than in the Convention as being harm to a person's reputation or feelings – seems extremely overbroad, even if based on one of the prohibited grounds. o The Southern Africa Litigation Centre suggested that this provision could also have included sex, gender, sexual orientation, and gender identity.[59] o One local journalism lecturer worries that this provision could result in "political opinion being classified as hate speech if one makes comments against certain political elements".[60]
Section 22: Genocide and crimes against humanity	It is an offence "intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification" to distribute or otherwise make available through a computer system to the public or to another person "material that - • denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity. • aids, induces or incites others to commit such acts, or • incites, instigates, commands, or procures any other person to commit such acts. o There is no definition of "genocide" or "crimes against humanity". o The Malabo Convention makes it an offence only to deny, approve or justify acts constituting genocide or crimes against humanity. This offence, in contrast, criminalises these acts as well as the encouragement of others to commit future genocide or crimes against humanity. o Note that this offence would capture even a private message from one individual to another denying or minimising genocide or crimes against humanity if sent through a computer system. Communication with even a single individual *inciting* genocide or crimes against humanity is clearly justifiable, but merely expressing an opinion about historical events in a private communication raises harder questions about privacy and freedom of expression. The Malabo Convention does not specify whether or not the communication must be public; it merely calls on States to make it a criminal offence to "deliberately deny, approve or justify acts constituting genocide or crimes against humanity through a computer system".

[58] Id.
[59] Id.
[60] Hanifa Manda, "Eswatini Freedom Of Expression Summit", Inhlase Centre for Investigative Journalism, October 2022, page 19, citing Nqobile Ndzinisa.

Section 23: Trafficking in humans, endangered species or illegal merchandise	It is an offence "without justification or lawful excuse" to use electronic or online methods to participate in the trafficking of humans, endangered animals, protected plants or any goods that he is not authorized to traffic in. o "Trafficking" is defined in section 2 as "initiating, carrying out, or being party to, actively or passively, an act of moving or facilitating the illegal movement or illegal transportation of people, animals, plants, money or goods within a country or across international borders for trade purposes to fulfil personal goals through the use of a computer system". o This offence uses the phrase "intentionally *or* without lawful excuse" as opposed to the phrase "intentionally *and* without lawful excuse or justification" that appears in most of the other provisions in the Act. It is unclear what distinction was intended.
Section 28: Harassment utilising means of electronic communication	It is an offence "intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification" to "initiate any electronic communication, with the intention to coerce, intimidate, insult, harass, or cause emotional distress to a person, using a computer system, to support hostile behaviour". o The drafting of this offence is somewhat confusing as it is not clear how the reference to supporting hostile behaviour fits in, even though this wording is similar to that used in the SADC Model Law on harassment.[61] o The Southern Africa Litigation Centre notes: "The offence of harassment is much broader than what is proposed in the SADC Model law. The Model law does not include "insult" under this offence and limits the offence to instances which are "severe, repeated *and* hostile", not simply "hostile". We submit that the approach of the SADC Model law is much clearer and preferred. We are concerned that the offence could be used to persecute human rights defenders."[62] o Insulting, harassing and causing emotional distress are all vague and subjective behaviours. None of these terms are defined, or applied with reference to an objective reasonable person. "Hostile behaviour" is similarly undefined. For example, legitimate criticism of improper behaviour by a government official might be seen as "hostile" and being insulting or causing emotional distress. This offence seems too broad and vague to constitute a justifiable restriction on freedom of expression.
Section 29: Violation of intellectual property rights.	It is an offence to use any computer or electronic device to violate any intellectual property rights protected under any law or treaty applicable to intellectual property rights in the Kingdom of Eswatini.

[61] *SADC Model Law on Computer Crime and Cyber Crime, 2012*, section 22: "A person, who initiates any electronic communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, *using a computer system to support severe, repeated, and hostile behaviour*, commits an offence…".
[62] "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020.

In general, **attempting, abetting or conspiring to commit any offence under the Act** – whether technical or content based – is also an offence.[63] This general prohibition overlaps with the references to aiding and abetting in some of the individual provisions.

Some assert that the **fines and prison sentences** imposed by the law are excessive, and higher than those in similar legislation in other SADC countries.[64] The Southern Africa Litigation Centre also finds the penalties "incredibly high" and worries that they might result in arbitrary and disproportionate sentences in specific cases. It also submits that the reasons for the differences in penalties for different offences are often unclear.[65]
Commenting on the issue of excessive fines and prison sentences, Ndimphiwe Shabangu, advocacy and communications officer at the Coordinating Assembly of NGOs (CANGO) in eSwatini, indicated that these penalties were even higher in initial drafts of the law, but through intervention from civil society and other stakeholders these fines and sentences were reduced, even though they were still considered excessive as contained in the law.[66]

The Act has also been criticised for **failing to cover the non-consensual sharing of intimate images**.[67]

Turning to procedural aspects of the law, **searches and seizures** require a warrant from a magistrate's court or the High Court based on an affidavit from a law enforcement agent that there are reasonable grounds to suspect that there may be a thing or computer data in a certain place that is either material evidence in proving an offence, or that has been acquired by a person as a result of an offence.[68] A "law enforcement agent" includes personnel from Royal Eswatini Police, the Anti-Corruption Commission, the Eswatini Revenue Authority and the Eswatini Communications Commission. [69] Where a Court has issued a warrant, a person who is not a suspect, but who has knowledge about the functioning of the computer system or measures applied to protect the computer data in the computer system, has a duty to assist law enforcement agents.[70]

A Court can also authorise the **general collection of traffic data by law enforcement agents** for the purposes of a specific criminal investigation; this must apply to a specified communication during a specified period, but the length of the period that

[63] Computer Crime & Cybercrime Act 6 of 2022, section 30. Section 2 defines "abetting" as "to encourage or assist someone to commit a crime or other offence".
[64] "Computer, Cybercrime Act: a necessary evil", *Times of Eswatini*, 31 October 2022.
[65] "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020. It cites these examples: "Using an illegal device to commit an offence can lead to a fine of E100m or 25 years' imprisonment or both (section 9), even though the offence being committed might be quite benign. In contrast, committing computer related forgery or computer related fraud can result in a lesser sentence of E10m or 10 years' imprisonment or both (section 10 and 11 respectively), but using a botnet to disrupt a service can attach E100m or 20 years' imprisonment." The SALC also noted that there is a lack of congruence between the fine and the number of years in imprisonment in respect of the various offences in the bill, but the examples it cites do not match the final law indicating that this issue was addressed.
[66] Ndimphiwe Shabangu was interviewed via Zoom on 19 July 2023.
[67] "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020.
[68] Computer Crime & Cybercrime Act 6 of 2022, section 33. There is a wide and non-exhaustive definition of "thing" in section 2.
[69] Id, section 2 (definition of "law enforcement agent").
[70] Id, section 34.

can be covered by the authority is not specified .[71] It can also authorise the **interception of content data**, again only in respect of specified communications for a specific criminal investigation. There is no time limit on such an authorisation. [72]

Furthermore, a Court may issue authority for the **use of a remote forensic tool for monitoring purposes**, including the installation of a forensic tool on the suspect's computer system. However, this power is limited to criminal investigations relating to a list of serious offences. Such an authority is limited to 3 months, but can be renewed.[73]

A Court also has the power to issue **production orders** to service providers or other persons in control of computer systems.[74]

However, **expedited preservation notices** in respect of traffic data and notices directing the **partial disclosure of traffic data**, to identify the service provider or the path through which a communication was transmitted, can be issued by a law enforcement agent, without court involvement.[75] A preservation notice issued in this way can require that the data specified in the notice be preserved for a period of up to 28 days – which far exceeds the SADC Model Law's recommendation that data can be preserved for 7 days subject to such a notice, and on court order for a further 7 days at a maximum.[76]

Given the complexity of the procedural matters, the Southern Africa Litigation Centre recommended that they should be handled only by the High Court,[77] but this recommendation was not taken up. They also expressed concern about the avenues for evidence collection issued by law enforcement agents without court involvement, on the basis that this departs from acceptable criminal procedure.[78]

The Act contains a provision allowing a court to order **forfeiture of assets** for persons convicted of any offence under the Act. This can apply to any asset, money or property constituting or traceable to the proceeds of the offence, as well as any computer, equipment, software or other technology used or intended to be used to commit or facilitate the offence. The Act also requires in every case that persons convicted of an offence under the Act must forfeit their passport or international travelling document to the State until they have paid any fines or served any sentence imposed. A court may release a person's travel document upon application if travel is required for medical treatment or in the interest of the public.[79]

[71] Id section 38. Section 2 defines "traffic data" as "computer data that relates to a communication by means of a computer system and generated by a computer system that is part of the chain of electronic communication; and may show one or more of the following, the communication's origin, destination, route, time, date, size, duration or the type of underlying services".
[72] Id, section 39.
[73] Id, section 40. Section 2 defines a "remote forensic tool" as "an investigative tool including software or hardware installed on or in relation to a computer system or part of a computer system and used to perform tasks that include but are not limited to keystroke logging or transmission of an IP-address".
[74] Id, section 35.
[75] Id, sections 36-37.
[76] *SADC Computer Crime and Cybercrime Model Law, 2012*, section 28; "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020.
[77] "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020.
[78] Id.
[79] Computer Crime & Cybercrime Act 6 of 2022, section 48.

B) OTHER LAWS THAT MAY INHIBIT FREEDOM OF EXPRESSION

Concerns about legislation that restricts freedom of expression was a strong theme in eSwatini's most recent Universal Period Review, with the following laws in particular being cited: the **Suppression of Sedition and Subversive Activities Act, 1938**; the **Suppression of Terrorism Act, 2008 as amended in 2017**; and the **Public Order Act, 2017**.[80] For example, the US Government recommended that the government should repeal the Sedition and Subversive Activities Act, 1938 "which has been used to silence journalists, human rights defenders, and political activists".[81] According to the Southern Africa Litigation Centre, the Suppression of Terrorism Act, 2008 and the Sedition and Subversive Activities Act, 1938 "have frequently been used to suppress any speech that is critical of the Government and the Monarch".[82]

The **Sedition and Subversive Activities Act 46 of 1938** contains several provisions affecting freedom of expression. As discussed above, some of these have been struck down on constitutional grounds (sections 3(1), 4(a) and (e), and 5), but the State is making a belated appeal of this holding. The full text of this Act could not be located online, but the key provisions of concern are reproduced in the box below, as quoted in the court judgment.[83] Note the breadth of "seditious intentions", and the narrow margin between what is seditions and what falls into the exceptions in the quoted provisions – which is bound to lead to self-censorship. Note also the deeming provision in section 3(3) which (in the words of the High Court) is "plainly contrary to the constitutionally entrenched right of being presumed innocent until proven otherwise".[84]

SEDITION AND SUBVERSIVE ACTIVITIES ACT 46 OF 1938

KEY PROVISIONS ON EXPRESSION

The provisions indicated in boldface type have been struck down on constitutional grounds, with this decision currently on appeal by the State.

3.

(1) A "seditious intention" is an intention to -

(a) bring into hatred or contempt or to excite disaffection against the person of His Majesty the King, His Heirs or successors, or the Government of Swaziland as by law established; or

(b) excite His Majesty's subjects or inhabitants of Swaziland to attempt to procure the alteration, otherwise than by lawful means, of any matter in Swaziland as by law established; or

(c) bring into hatred or contempt or to excite disaffection against the administration of justice in Swaziland; or

[80] "Report of the Working Group on the Universal Periodic Review: Eswatini", A/HRC/49/14, 7 January 2022.
[81] "U.S. Statement at the Universal Periodic Review of eSwatini", U.S. Mission Geneva, 8 November 2021.
[82] "Statement: Concern as states continue to use terrorism laws to inhibit freedom of expression and access to information", Southern Africa Litigation Centre, 27 September 2021.
[83] *Maseko v The Prime Minister of Swaziland* [2016] SZHC 180, 16 September 2016, paragraph 18.
[84] Id, paragraph 21.

(d) raise discontent or disaffection amongst His Majesty's subjects or the inhabitants of Swaziland; or
(e) promote feelings or ill-will and hostility between classes of the population of Swaziland.

(2) Notwithstanding subsection (1), an act, speech or publication shall not be seditious by reason only that it intends to -
(a) show that His Majesty has been misled or mistaken in any of His measures; or
(b) point out errors or defects in the government or constitution of Swaziland as by law established or in legislation or in the administration of justice with a view to the remedying of such errors or defects; or
(c) persuade His Majesty's subjects or the inhabitants of Swaziland to attempt to procure by lawful means the alteration of any matter in Swaziland as by law established; or
(d) point out, with a view to their removal, any matters which are producing or have a tendency to produce feelings of ill-will and enmity between different classes of the population of Swaziland.
(3) In determining whether the intention with which any act was done, any words were spoken, or any document was published, was or was not seditious, every person shall be deemed to intend the consequences which would naturally follow from his conduct at the time and under the circumstances in which he so conducted himself.

4. Any person who -
(a) does or attempts to do, or makes any preparation to do, or conspires with any person to do, any act with a seditious intention;
(b) utters any seditious words;
(c) prints, publishes, sells, offers for sale, distributes or reproduces any seditious publication; or,
(d) imports any seditious publication, unless he has no reason to believe that it is seditious;
(e) without lawful excuse has in his possession any seditious publication;
shall be guilty of an offence and liable on conviction to imprisonment not exceeding 15 years or a fine not exceeding E20, 000 and any seditious publication relating to an offence under this section shall be forfeited to the Government.

5.
(1) A person who does or attempts to do or makes any preparation to do an act with a subversive intention or who utters any words with a subversive intention shall be guilty of an offence and liable, on conviction, to imprisonment for a term not exceeding twenty years without the option of a fine.

(2) For the purposes of this section, "subversive" means -
(a) supporting, propagating or advocating any act or thing prejudicial to -
(i) public order;
(ii) the security of Swaziland; or
(iii) the administration of justice:

Provided that this paragraph shall not extend to any act or thing done in good faith with intent only to point out errors or defects in the government or constitution of Swaziland as by law established or in legislation or in the administration of justice with a view to remedying such errors or defects;

(b) inciting to violence or other disorder or crime, or counselling defiance of or disobedience to any law or lawful authority;
(c) intended or likely to support or assist or benefit, in or in relation to such act or intended acts as are hereinafter describe, persons who act, intend or act or have acted in a manner prejudicial to public order, the security of Swaziland or the administration of justice, or who incite, intend to incite, or have invited to violence or other disorder or crime, or who counsel, intend to counsel or have counselled defiance of or disobedience to any law or lawful authority;
(d) indicating, expressly or by implication, any connection, associated or affiliation with or support for an unlawful society;
(e) intended or likely to promote feelings or hatred or enmity between different races or communities in Swaziland: Provided that this paragraph shall not extend to comments or criticisms made In good faith and with a view to the removal of any causes of hatred or enmity between races or communities;
(f) intended or likely to bring into hatred or contempt or to excite disaffection against any public officer or any class of public officers in the execution of his or their duties, or any of His Majesty's armed forces, or any officer or other member of such a force in the execution of his duties: Provided that this paragraph shall not extend to comments or criticisms made in good faith and with a view to remedying or correcting errors, defects or misconduct on the part of such public officer, force or office or other member thereof and without attempting to bring into hatred or contempt or to excite disaffection against such a person or force;
(g) intended or likely to seduce from his allegiance or duty any public officer or any officer or other member of any of His Majesty's armed forces.

The **Suppression of Terrorism Act 3 of 2008, as amended in 2017,** has several problematic provisions, including these:

- Section 5(3)(e) makes it an offence to intentionally publish or communicate in any manner false information about the existence of any danger, dangerous thing, explosive or harmful or hazardous substance when that person does not believe in the existence of that thing or the truthfulness of that publication or communication.[85] This could, for instance, inhibit reports of threats that are doubtful but nonetheless newsworthy.

- Section 11(1)(a)-(b) makes it an offence to knowingly, and in any manner solicit support for, or give support to, any terrorist group or the commission of a terrorist act.[86] This provision was used to charge members of the Peoples United Democratic Movement (PUDEMO) because they were found wearing T-shirts

[85] Suppression of Terrorism Act 3 of 2008, as amended by the Suppression of Terrorism (Amendment) Act 11 of 2017, section 5(3)(e).
[86] Id, section 11(1)(a)-(b).

> and berets identifying this organization and chanting its slogans and demands.[87]

As discussed above, these provisions along with some other related ones have been struck down on constitutional grounds, but the State is making a belated appeal of this holding. Amnesty International and the Human Rights Institute of the International Bar Association called for the repeal of this law shortly after its enactment, on the grounds that it was inherently repressive, violated human rights standards, and was leading to violations of the rights of freedom of expression, association and assembly.[88]

Section 3 of the **Official Secrets Act 30 of 1968**, which could not be located online, makes it an offence, amongst other things, to publish any information that is likely to be even indirectly useful to an enemy. Section 4(2) makes it an offence to publish or communicate any information that relates to munitions of war or any other military or police matter in any manner or for a purpose prejudicial to the safety or interests of eSwatini. Section 9(b) essentially creates a presumption of guilt, by providing where a person is charged with publishing or communicating information for a purpose prejudicial to the safety or interests of eSwatini, without lawful authority, it is presumed that the purpose was prejudicial to the safety or interests of eSwatini.[89] This law has been cited as an impediment to whistleblowers and investigative journalists.[90]

Public gatherings are regulated by the **Public Order Act 12 of 2017**, which requires a minimum of 48 hours advance notice to the relevant local authority of any gathering of more than 50 people. A local authority may prohibit an intended gathering if it believes that the gathering will "endanger the maintenance of public order and public safety".[91] As one positive point, the law explicitly requires police and local authorities to respect the rights of media and independent monitors to observe public gatherings and report on them., including the right to make video or audio recordings of public gatherings. It also states that a police officer "may not prevent or obstruct the lawful activities of journalists or independent monitors during gatherings".[92] Whether or not these safeguards are always observed in practice is a different issue.) Amongst the offences that apply to public gatherings is a prohibition on the use of "threatening, abusive or insulting words" or any act or display which is likely to result in

---

[87] *Maseko v The Prime Minister of Swaziland* [2016] SZHC 180, 16 September 2016, paragraph 28.

[88] "Suppression of Terrorism Act undermines Human Rights in Swaziland", Amnesty International and International Bar Association, 2009. Amnesty International made the following comments after the 2017 amendment:

> Although Eswatini amended the 2008 Suppression of Terrorism Act in 2017, the Act continues to be used to silence and punish dissent. The Act's amendments limit the definitions of what constitutes a terrorist act although the wording is overly broad and vague in relation to terrorism related acts. The law also contained provisions that undermined the rights to freedom of expression, association and peaceful assembly. The STA (Amendment) Act 2017 remains inconsistent with Eswatini's obligations under international and regional human rights law as well as Eswatini's Constitution.

"Eswatini: Broken Promises" Amnesty International Submission for the UN Universal Periodic Review, 39th Session of the UPR Working Group, 1 – 12 November 2021, "Restrictions to Fundamental Freedoms".

[89] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 5: eSwatini", Konrad Adenauer Stiftung, 2021, page 270.

[90] Hanifa Manda, "Eswatini Freedom Of Expression Summit", Inhlase Centre for Investigative Journalism, October 2022, page 19, citing Nqobile Ndzinisa.

[91] Public Order Act 12 of 2017, sections 6 9 and 15(1), read with definition of "gathering" in section 2. See also section 16 on police power to prohibit any public event where "public disorder" is likely to arise.

[92] Id, section 14.

"a breach of public order",[93] or doing anything "to incite hatred or contempt against the cultural and traditional heritage of the Swazi Nation".[94] The Act also contains a broadly-formulated offence of "intimidation or harassment" which includes the use of threats to reputation to influence persons to assume or abandon a particular standpoint.[95]

The **Obscene Publications Act 20 of 1927**, which could not be located online, makes it an offence to import, produce, sell or distribute any indecent or obscene publication, which is defined to include a newspaper or a magazine. Since the key terms "indecent" or" obscene" are not defined, this offence could be arbitrarily applied.[96]

Section 3 of the **Proscribed Publications Act 17 of 1968** empowers the Minister for Public Service and Information to declare any publication or series of publications to be a proscribed publication if it is prejudicial or potentially prejudicial to the interests of defence, public safety, public order, public morality or public health. This is done by notice in the *Government Gazette*, with no judicial involvement. It is an offence for any person, amongst other things, to distribute, print, publish or even possess a proscribed publication without the authority of the minister.[97] A 2001 notice which declared the *Guardian* newspaper and *The Nation* magazine to be proscribed publications was set aside by the High Court, on the grounds that the minister did not give any reasons for declaring the publications to be proscribed in the notice or in the papers filed with the court in response to the challenge to the notice. The Court accordingly declared the notice invalid.[98]

The **Cinematograph Act 31 of 1920** gives the minister discretion to require that any film intended for public showing must first be inspected by a state official.[99] No one may make a film (or take photographs for a film) that portrays gatherings of Africans or scenes of African life without the prior written consent of the Minister for Public Service and Information.[100] State authority is also required to make a film, or to take a photograph, of specified events that are observed in certain specified locations: Incwala Day (a cultural event), the King's Birthday, the Reed Dance (a cultural tradition that celebrates women's chastity and virginity) and Independence Day.[101] Violation of these requirement is a criminal offence.[102]

[93] Id, section 15(3)(b).
[94] Id, section 15(3)(h).
[95] Id, section 19.
[96] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 5: eSwatini", Konrad Adenauer Stiftung, 2021, page 272.
[97] Proscribed Publications Act 17 of 1968, sections 3-4.
[98] *Swaziland Independent Publishers (Pty) Ltd T/A The Nation Magazine v the Minister of Public Service and Information* (Case 1155/01), as summarised in Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 5: eSwatini", Konrad Adenauer Stiftung, 2021, page 282.
[99] Cinematograph Act 31 of 1920, sections 4-5.
[100] Id. section 3(1).
[101] Id, section 3(1bis).
[102] Id, section 3(4).

This Act also makes it an offence to exhibit an "objectionable picture", which includes films. A picture is objectionable if it represents any of the following in an offensive manner:

- impersonation of the king;
- scenes holding any member of the naval, military or air forces up to ridicule and contempt;
- scenes tending to "disparage public characters";
- scenes calculated to affect the religious convictions of any section of the public;
- scenes suggestive of immorality or indecency;
- executions, murders or other "revolting scenes";
- scenes of debauchery, drunkenness, brawling or any other habit of life not in accordance with good morals or decency;
- successful crime or violence;
- scenes that are in any way "prejudicial to the peace, order or good government" of the country.

The Minister also has complete discretion to declare any other picture to be objectionable. Notice of the declaration that a picture is objectionable must be given to the proprietor of any theatre which exhibits cinematograph films, and the exhibition of any prohibited picture is an offence punishable by a fine or imprisonment. [103] According to one local journalism lecturer: "The law is problematic because one cannot show an objectionable picture without getting permission from the Minister. The Minister's powers are not restricted, and he can determine what is objectionable. This impacts how the story of Eswatini is told."[104]

C) SIM CARD REGISTRATION (REGISTRATION OF ELECTRONIC COMMUNICATIONS AND MOBILE CUSTOMERS)

The **Swaziland Communications Commission (Subscriber Registration) Regulations, 2016** require service providers of electronic communications and mobile services to collect the full names, surnames and identity numbers of all their customers. Customers without identification documents must verify their identity with tax documents from Swaziland Revenue Authority, a bank statement, a municipal rates and taxes invoice, a recent telephone or cell phone account, a utility bill, a recent account from a retailer, a lease, a rental or credit sale agreement, an insurance policy, a television licence or a motor vehicle licence document. This requirement applies to both residents and foreign visitors. The identification information must be stored for five years after the end of the contract or service.[105] This removes the possibility of anonymous electronic communications.

[103] Id, section 6.
[104] Hanifa Manda, "Eswatini Freedom Of Expression Summit", Inhlase Centre for Investigative Journalism, October 2022, page 19, citing Nqobile Ndzinisa.
[105] Swaziland Communications Commission (Subscriber Registration) Regulations, 2016. Legal Notice No. 126 of 2016, issued in terms of section 54 of The Swaziland Communications Commission Act 10 of 2013 (which merely provides for regulations for the better carrying out of the Act).

D) TAKE-DOWN NOTIFICATIONS

A provision on take-down notifications is contained in the **Electronic Communications and Transactions Act, 2022**. Anyone can lodge a notification in electronic form with a service provider (a person or party that makes information services available) identifying material that is claimed to be unlawful and stating the remedial action required by the service provider. The service provider is not liable for taking down material in a *bona fide* response to a take-down notification but avoids civil liability for caching or hosting or linking to the material in question if it is removed, or if access to it is disabled, in response to a take-down notification. There is no involvement of a judicial authority, and no requirement that the person who posted the material be notified.[106] This scheme obviously militates in the direction of erring on the side of removing material on the basis of a mere allegation that it is infringing the rights of any person. A person who lodges a take-down notification knowing that it materially misrepresents the facts may be held liable for damages for wrongful take-down.[107]

7.5 ELECTION LAW AND FREEDOM OF EXPRESSION

Eswatini will hold parliamentary elections in September 2023. By way of background, one article provides this very brief overview:

> *Eswatini - the last absolute monarchy in Africa where political parties are banned and lawmakers are sidelined by the king -- will hold parliamentary elections on September 29 […] The vote is unlikely to change the political scenery in the southern African nation of 1.2 million people that has been ruled by King Mswati III since 1986. The king wields absolute power. […] Elections in the country take place in a convoluted system that ensures Mswati faces no meaningful dissent. The vote comes two years after dozens of people were killed as police violently quashed demonstrations calling for democratic reforms. Winners in the 59 constituency ballots will take seats in parliament's lower house, along with 10 lawmakers that the king appoints directly. Mswati can veto any legislation, appoints the prime minister and cabinet, and is constitutionally above the law. He also selects 20 of the 30 senators in the upper house. The rest are elected by the lower house. Candidates cannot be affiliated to any political group under the constitution which emphasises "individual merit" as the basis for selecting members of parliament and public officials. […]*[108]

Another recent article gives a bit more detail about the election process:

[106] Electronic Communications and Transactions Act 3 of 2022, section 40 read with the definition of "service provider" in section 2 and with sections 37-39.
[107] Id, section 40(3).
[108] "Eswatini to hold parliamentary elections in September", *Agence France-Presse*, 6 May 2023.

Eswatini is an absolute monarchy, but does have a unique electoral system, known as the *Tinkhundla* system, to conduct elections. The House of Assembly is made up of 66 seats, where 55 are elected via elections, 10 are appointed by the King and the remaining seat is given to the speaker of parliament who is chosen from outside of Parliament.

The Senate on the other hand is made up of 31 members, 10 of whom are selected by the House of Assembly and 20 of whom are selected by the King. Under the *Tinkhundla* system, Eswatini is divided up into constituencies known as *inkhudla (Tinkhundla* in plural). The *Tinkhundla* are then divided up into smaller chiefdoms, where the first phase of elections takes place. Nominations for candidates to the legislature is done at the community level and in the open, where a person's name is called out and by a show of hands the community indicates if they nominate that person or not. The nominee then either accepts or rejects the nomination. A chiefdom must have at least three nominees, but no more than 20.

Following the nomination process, primary elections take place in the chiefdom via secret ballot. The primary elections must produce one candidate to contest the secondary elections. Between the primary and secondary elections, the candidates have an opportunity to campaign for votes. However, since political parties are banned in Eswatini, candidates must campaign on a non-partisan basis. The secondary elections take place at the *Inkhudla* level to decide on the candidates who will represent the *Inkundla* at the national level.

These scheduled elections are a key event in Eswatini. Elections have the potential in any country to heighten tensions and Eswatini may prove to be no different, especially as tensions are already raised. Elections are also proving to be a point of contention amongst pro-democracy parties, as opinions are divided on whether or not to compete in the elections. Elections do provide an opportunity to get pro-democracy candidates into the national legislature, but an argument against competing in elections is that participation may be interpreted as condoning the current system of elections.[109]

Elections are supervised by the **Elections and Boundaries Commission (EBC)**, which is established by the Constitution. Article 90(9) of the Constitution requires that the Commission must act independently. However, in practice, the EBC is not considered impartial. "It is financially and administratively dependent on the executive, and its members are appointed by the king on the advice of the Judicial Service Commission, whose members are also royal appointees."[110]

[109] Katharine Bebington, "Eswatini: the year ahead", ACCORD, 24 February 2023.
[110] "Freedom in the World 2022: Eswatini", Freedom House, section A3.

ESWATINI CONSTITUTION

90. Elections and Boundaries Commission

i. There shall be an independent authority styled the Elections and Boundaries Commission ("the Commission") for Swaziland consisting of a chairperson, deputy chairperson and three other members.

i. The members of the Commission shall be appointed by the King on the advice of the Judicial Service Commission.
A person shall not be appointed member of the Commission where that person –

a. is a member of Parliament;
b. is or has been in the last five years actively engaged in politics;
c. is a public officer other than judge of a superior court or magistrate;
d. is an unrehabilitated insolvent;
e. has been convicted of an offence involving dishonesty in any country during the last ten years.

4. A person shall be deemed to be "actively engaged in politics" or to have been so engaged during the relevant period or any part of that period where that person –

a. is or was at any time during that period a member of the House or a Senator;
b. is or was at any time during that period, nominated as a candidate for election to the House or Bucopho Committee; or
c. is or was at any time during that period the holder of an office in any organization that sponsors or supports or has at any time sponsored or supported a candidate for election as a member of the House or Bucopho committee.

5. The members of the Commission shall be appointed for a period not exceeding twelve years without the option for renewal.

6. The chairperson, deputy chairperson and the other members of the Commission shall possess the qualifications of a Judge of the superior courts or be persons of high moral character, proven integrity, relevant experience and demonstrable competence in the conduct of public affairs.

7. The functions of the Commission shall be to –

a. oversee and supervise the registration of voters and ensure fair and free elections at primary, secondary or other level;
b. facilitate civic or voter education as may be necessary in between elections;
c. review and determine the boundaries of tinkhundla areas for purposes of elections;
d. perform such other functions in connection with elections or boundaries as may be prescribed;
e. produce periodic reports in respect of work done.

8. Three members of the Commission including either the chairman or deputy chairman shall constitute a quorum.

9. A member of the Commission shall not enter upon the duties of that Commission until that member has taken and subscribed the oath of allegiance and oath for the due execution of office that are set out in the Second Schedule.

10. The provision of this Constitution relating to the removal of judges of the superior courts from office shall, subject to any necessary modifications, qualifications or adaptations, apply to the removal from office of the chairperson and other members of the Commission.
11. The office of any member of the Commission shall become vacant where that member resigns or circumstances arise that would disqualify that member for appointment as such.
12. If before the Commission has submitted its report under section 92 the office of chairperson or any other member of the Commission falls vacant or the holder of that office becomes unable for any reason to discharge the functions as chairperson or member of the Commission the King shall appoint another person to be chairperson or member as provided under subsection (2).
13. In the exercise of its functions under this Constitution, the Commission shall not be subject to the direction or control of any other person or authority.
14. There shall be a secretariat of the Commission provided by the Ministry responsible for elections.

There are several provisions of the **Election Act 6 of 2013** which are worded with sufficient open-endedness to raise concerns about how they might be applied. [111]

The Election Act contains a part that specifically covers election campaigns (quoted in full in the box below). Section 42 of this Part **prohibiting the use of "foul language"** is much wider than this heading suggests. The prohibition covers incitement to "public [dis]order, insurrection or violence"; statements that are "defamatory or insulting", statements that constitute "incitement to hatred" and statements that "excite or promote disharmony, enmity or hatred against any person".[112] These are very broad prohibitions that invite subjective application. Some have also expressed doubts that the restriction on campaigning during primary elections in section 39(1)) is enforced even-handedly.[113]

ELECTION ACT, 2013

PART VI ELECTION CAMPAIGN

39. CANVASSING FOR VOTES

(1) Canvassing for votes during primary elections is prohibited.
(2) A candidate contesting an election at secondary elections has the right to conduct campaigns freely in accordance with this Act.
(3) A candidate may, during an electoral campaign, publish campaign materials of such a nature and in a manner that may be approved by the Commission.

[111] Elections Act 6 of 2013. Note that this Act is variously referred to as Act 6 of 2013 and Act 10 of 2013, with these differing references even appearing on material on the website of The Elections And Boundaries Commission.
[112] Elections Act 6 of 2013, section 42.
[113] See, for example, Nomfanelo Maziya, "Some current MPs perceived as campaigning in disguise", *Swazi Observer*, 4 July 2023; Delisa Thwala, "EBC half way through their weekend target", *Eswatini Positive News*, 31 May 2023.

40. GENERAL CAMPAIGN

(1) The Commission shall prescribe a code of conduct to be complied with by all candidates during an election campaign.

(2) Subject to the provisions of this section and section 39, every candidate has the right to conduct that candidate's campaign freely.

(3) A public officer or public entity shall give and be seen to give equal treatment to all candidates to enable each candidate to conduct that candidate's campaign freely.

41. ORGANISED CAMPAIGN

(1) The Commission may determine the manner in which campaigns shall take place.

(2) In furtherance of subsection (1), the Commission shall give equal treatment to all candidates and enable each candidate to conduct that candidate's campaign freely, and each candidate shall be given an opportunity to address the meeting on matters of national interest and socio-economic development.

(3) The Commission shall ensure that adequate security is provided at campaign meetings organized by the Commission.

42. USE OF FOUL LANGUAGE PROHIBITED

(1) A person shall not, whether in a general or organized campaign, use any language –

(a) which constitutes incitement to public [dis]order, insurrection or violence;

(b) which is defamatory or insulting or which contains incitement to hatred; or

(c) which seeks to excite or promote disharmony, enmity or hatred against any person.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding five thousand Emalangeni or to imprisonment for a period not exceeding one year or to both.

43. CLOSE OF CAMPAIGN

A campaign meeting shall not be held within twenty-four hours before the polling day.

Section 78 of the Act concerns **undue influence**. While there is no problem with prohibiting the use of threats of force, violence or restraint to influence another person during an election period, the broader prohibition on threats of any "physical, psychological, mental or spiritual injury, damage, harm or loss" or threats of doing "anything to the disadvantage of any person" could be broadly applied.[114] This provision has been identified by at least one local journalist as being potentially problematic, although the article quoted a differing opinion from a member of the Swaziland Multi-Stakeholder Forum who felt that is legal provision would not prevent attempts to influence people through campaigns such as road-shows, public statements, banners, speeches and other forums, as opposed to influencing people

[114] Id, section 78(1). There is a similar provision on undue influence in the Voters Registration Act 4 of 2013, section 36.

by waylay them and hitting them with a knobkerrie or other use of violence.[115]

ELECTION ACT, 2013, SECTION 78(1)

78. UNDUE INFLUENCE

(1) A person shall not directly or indirectly, by oneself or by any other person –
(a) make use of or threaten to make use of any force, violence or restraint upon any other person;
(b) inflict or threaten to inflict by oneself or by any other person, or by any supernatural or non-natural means, or pretended supernatural or non-natural means, any physical, psychological, mental or spiritual injury, damage, harm or loss upon or against any person; and
(c) do or threaten to do anything to the disadvantage of any person; in order to induce or compel any person –
(i) to register or not to register as a voter;
(iii) to vote or not to vote;
(iv) to vote or not to vote for any candidate;
(v) to support or not to support any candidate; or
(vi) to attend and participate in, or not to attend and participate in, any election meeting, march, demonstration or other election event;
(d) interfere with the independence or impartiality of the Commission, any member, employee or officer of the Commission;
(e) prejudice any person because of any past, present or anticipated performance of a function under this Act;
(f) advantage, or promise to advantage, a person in exchange for that person not performing a function under this Act; or
(g) unlawfully prevent the holding of any election meeting.

ELECTION ACT, 2013, SECTION 79(2)

A person who, before or during an election, publishes any false statement of fact in relation to the personal character or conduct of a candidate in that election, shall be guilty of an illegal practice, unless that person can show that that person had reasonable grounds for believing, and did believe, the statement to be true.

Section 79 on the "**Illegal practice of publishing false statements in respect of candidates**" also contains some problematic aspects. The prohibitions on false claims of a candidate's illness, death or withdrawal from the election are not particularly worrying. However, this section also prohibits publication of "any false statement of fact in relation to the personal character or conduct of a candidate in that election", unless the publisher of the statement can show reasonable grounds for believing, and actual belief, that the statement was true. The maximum penalty for violation of the prohibition is a E20 000 fine or three years' imprisonment, or both.[116] It would be difficult to draw the line between fact and opinion in discussion of a candidate's character and conduct, and there is no defence of fair comment. The only defence articulated

[115] Mfanukhona Nkambule. "2-yr imprisonment for telling people not to vote", *Times of Swaziland*, 14 May 2023, which also quotes the contrary opinion of Sikelela Dlamini, the Secretary General of the Swaziland Multi-Stakeholder Forum.
[116] Id, section 79.

requires proof of actual belief of the truth of the statement, which would be difficult to establish in court beyond providing testimony of the accused's state of mind. Thus, this prohibition is likely to inhibit robust discussion of the merits and faults of the various candidates.

Section 81 on "**Illegal practices in respect of public meetings**" makes it illegal during the election period to act or incite others to act "in a disorderly manner for the purpose of preventing the transaction of the business for which the meeting is called". This formulation is also arguably overbroad.

There are **restrictions on certain acts in the vicinity of a polling place on election day**, similar to those found elsewhere. It is illegal to do the following acts within 400 meters of a polling station: canvass for votes, solicit the vote of a specific voter, induce any person not to vote or induce any person not to vote for a particular candidate, It is also prohibited to exhibit any notice or sign within 100 hundred metres of the entrance to any polling station on a poling day (other than official notices relating to the election authorised by an election officer in terms of the Act).[117] These do not seem unreasonable.

No rules were located on fairness in broadcasting or other media coverage during election periods.[118] The **Broadcasting Code 2020** states only that election-related programmes including campaign reports and polling night results must not be sponsored by advertisers.[119]

[117] Id, section 83(1)(d)-(e).
[118] The Broadcasting Code 2020 issued by the Eswatini Communications Commission does not cover this topic.
[119] Broadcasting Code 2020, item 5.10.1.3.