CHAPTER 10

MALAWI

CHAPTER 10: MALAWI

MALAWI KEY INDICATORS
2023 WORLD PRESS FREEDOM RANKING: **82nd globally; 19th out of 48 African countries** "Political influence over the media restricts journalistic freedom in Malawi. Reporters are still subjected to threats and cyber-harassment."
MALABO CONVENTION: NOT signatory or party
BUDAPEST CONVENTION: NOT signatory or party
CONSTITUTIONAL PROTECTION FOR FREEDOM OF EXPRESSION: Malawi's 1994 Constitution, as amended through 2020 **34. FREEDOM OF OPINION** Every person shall have the right to freedom of opinion, including the right to hold, receive and impart opinions without interference. **35. FREEDOM OF EXPRESSION** Every person shall have the right to freedom of expression. **36. FREEDOM OF THE PRESS** The press shall have the right to report and publish freely, within Malawi and abroad, and to be accorded the fullest possible facilities for access to public information. **37. ACCESS TO INFORMATION** Every person shall have the right of access to all information held by the State or any of its organs at any level of Government in so far as such information is required for the exercise of his or her rights. **38. FREEDOM OF ASSEMBLY** Every person shall have the right to assemble and demonstrate with others peacefully and unarmed. **44. LIMITATIONS ON RIGHTS** 1. No restrictions or limitations may be placed on the exercise of any rights and freedoms provided for in this Constitution other than those prescribed by law, which are reasonable, recognized by international human rights standards and necessary in an open and democratic society.

2. Laws prescribing restrictions or limitations shall not negate the essential content of the right or freedom in question and shall be of general application.
KEY LAWS: • Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*] • Penal Code [*Chapter 7:01*] (selected provisions) • as amended by the Penal Code (Amendment) Act 8 of 2023
CRIMINAL DEFAMATION: constitutionality of "criminal libel" being challenged in court as of mid-2023[1]
DATA PROTECTION: Malawi does not have a data protection law, but a draft is being reviewed by the Ministry of Justice.[2]
ACCESS TO INFORMATION: Malawi has access to information law.[3]

10.1 CONTEXT

Newspapers (and any periodical published at least monthly) must be registered under the **Printed Publications Act 18 of 1947**.[4]

Under the **Censorship and Control of Entertainments Act 11 of 1968**, no one may direct or even take part in the making of any film in Malawi without a film permit; violation of this rule is a criminal offence.[5] The showing of films requires a theatre permit, even where this does not take place on a commercial basis. as well as a certificate of approval for the film (which may set age ratings or impose conditions on the exhibition of the film).[6] Plays, concerts, art exhibitions and other public entertainments require an entertainment permit, which can similarly be issued subject to conditions.[7] Failure to obtain the necessary permits, which are issued by a board appointed by the relevant minister, constitutes a criminal offence.[8]

The Communications Act 34 of 2016, which repealed the Communications Act 41 of 1998, regulates broadcasting, telecommunications and postal services in Malawi.[9] The key regulatory body is the Malawi Communications Regulatory Authority (MACRA). The Board of this body is made up of *ex officio* government officials alongside other members appointed by the President, subject to confirmation by the Public

[1] *Mbele v R* (Misc. Criminal Case No. 04 of 2022) 2022 MWHC 74 (20 June 2022) (issue of unconstitutionality referred to Chief Justice for certification as a constitutional matter to be heard by a three-judge panel); "Supreme Court rebuffs State on Army General Nundwe's defamation case against Chisa Mbele", *Nyasa Times*, 18 September 2022.
[2] Data Protection Bill, 2021. There are some provisions pertaining to data protection in the Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*].
[3] Access to Information Act 13 of 2016.
[4] Printed Publications Act 18 of 1947 [*Chapter 19:01*].
[5] Censorship and Control of Entertainments Act 11 of 1968 [*Chapter 21:01*], sections 19-ff.
[6] Id, sections 9-ff.
[7] Id. sections 14-ff.
[8] Id, section3 (appointment of Board of Censors); on offences, see the sections on each type of permit read with section 32.
[9] Communications Act 34 of 2016 [*Chapter 68:01*], section 2; definition of "communications service" in section 3.

Appointments Committee of Parliament.[10] Although, the Communications Act states that MACRA "shall be independent in the performance of its functions",[11] its independence is compromised by the absence of a public nomination process for Board members and by the fact that a third of its members are *ex officio* representatives of the executive.[12] The Act contains regulations for content services that cover topics such as the right of reply, fair comment, the duty to present news truthfully, accurately and objectively, and the duty to provide balance in respect of "controversial issues of public importance".[13] Broadcasting licensees must are also required to ensure equitable treatment of all political parties, election candidates and electoral issues during an election. It should be noted that this regulation says that content licensees must not "broadcast any material that is indecent or obscene or offensive to public morals, including abusive or insulting language, or offensive to religious beliefs of any section of the population, or likely to prejudice the safety of the Republic or public order and tranquillity".

Failure to comply with the Act can lead to suspension or revocation of a licence.[14]

The state broadcaster, the Malawi Broadcasting Corporation (MBC), is also regulated by the **Communications Act 34 of 2016**.[15] It is governed by a Board composed of four *ex officio* government officials, and five other members appointed by the President subject to confirmation by the Public Appointments Committee of Parliament.[16]

Online content is regulated by the **Electronic Transactions and Cybersecurity Act 33 of 2016**, discussed below.

The media has a self-regulatory body called the **Media Council of Malawi (MCM**). It is reported that the MCM, which was initially established in 1995, was dormant from 2010 until its re-launch on 31 December 2019. The MCM has a Code of Ethics and Professional Conduct (the Code) which governs the conduct and practice of journalists in Malawi which date from the period before its dormancy.[17]

10.2 CONSTITUTION

The sections of the Malawi Constitution most relevant to this discussion are reproduced in the table on the first page of this chapter.

Unlike many other constitutions in the SADC regions, the grounds for limiting the freedom of expression and other fundamental rights are not specified with reference

[10] Id, sections 5 and 8.
[11] Id, section 5(3).
[12] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 8: Malawi", Konrad Adenauer Stiftung, 2021, pages 370-371.
[13] Communications Act 34 of 2016 [*Chapter 68:01*], Second Schedule.
[14] Id, section 43(1)(a).
[15] Id, Part XIV.
[16] Id, sections 111-112.
[17] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 8: Malawi", Konrad Adenauer Stiftung, 2021, pages 406-ff. The Media Council of Malawi Code of Ethics and Professional Conduct is available here. The MCM's own website could not be accessed in mid-2023 as it was infected with a computer virus.

to concerns such as national security or public morals. Section 44 requires only that restrictions or limitations on rights and freedoms must be -

- prescribed by laws which are of general application and do not negate the essential content of the right or freedom in question;
- reasonable;
- recognized by international human rights standards; and
- necessary in an open and democratic society.

Section 36 of Malawi's Constitution is notable for explicitly guaranteeing to the press "the right to report and publish freely, within Malawi and abroad". It has been observed that this provision is important because it explicitly protects both the reporting and publishing rights of the press, and extends those rights to national and international media reporting on Malawi both inside and outside the country. It also recognises the political role of the press in providing information to the public, by stating that the press must be provided with access to public information.[18]

It is also unusual that Section 37 of the constitution on the right of assembly specifically protects the right to "demonstrate with others peacefully and unarmed", given that demonstrations are an important form of political expression.

In 2002 the President of Malawi issued an **oral directive at a political rally banning all forms of demonstrations against a proposed constitutional amendment** which would remove the limitations on the terms of office of the President and Vice-President. The Law Society and other concerned civil society groups approached the High Court seeking an order that the directive violated their constitutional rights to freedom of association, assembly and demonstration, expression, conscience and opinion. In *Malawi Law Society v The President*, the Court found the oral directive unconstitutional on the grounds that it did not amount to "law", and that the ban was also unreasonably wide and incapable of enforcement. Thus, it did satisfy the criteria in section 44 for restrictions on constitutional rights and freedom.[19]

The right to demonstrate peacefully was considered by the Supreme Court of Appeal (Malawi's highest court) in the 2019 case of *Attorney General v Trapence*. In the aftermath of Malawi's disputed 2019 Presidential election, the election results were challenged by opposition leaders who alleged vote-counting irregularities. The Malawi Human Rights Defenders Coalition organized a series of demonstrations calling for the dismissal of the chairperson of the Electoral Commission. A first round of protests was marred by violence. The Attorney General then sought an **injunction preventing future demonstrations on the election result until the issue of violence had been resolved** and the opposition leaders' court challenge had been finalized. The issue concerning demonstrations about a matter that was *sub judice* was moot by the time the Supreme Court ruled on the injunction, but it held that the concerns about possible violence did not warrant the requested injunction. While demonstrators, individually and collectively, have a duty to ensure that protesters are unarmed and that there is no violence during demonstrations, this is not their sole responsibility; police also have a duty to act to address violence and criminality, and their assertion

[18] Id, page 347.
[19] *Malawi Law Society v The President* (2002) AHRLR 110 (MwHC 2002); see the case summary by Global Freedom of Expression here.

that they lacked the resources to do this was not persuasive to the Court.[20]

In the aftermath of the disputed 2019 election, there was intense public debate on many platforms, including radio and television. Live call-in radio shows where listeners aired their opinions on the electoral process proved to be particularly popular. In June 2019, the Director-General of MACRA issued a **public announcement banning call-in radio shows** on the basis that these shows were a platform for callers to incite the public to violence. The relevant minister then issued the **Communications (Broadcasting) Regulations, 2019**, which **banned all live radio phone-in programmes unless the broadcasters utilised a delay machine to allow sufficient time to remove any prohibited content**. Both measures were challenged by the National Media Institution of Southern Africa (NAMISA) and two affected radio stations.

The High Court found that the Director-General's "ban" had no proper legal basis. It also found that the regulations were issued without following the statutory requirements for stakeholder consultations. The Court stated: "Whereas the intentions of ensuring that a potentially volatile political climate does not degenerate into social disorder through unwholesome radio content cannot be gainsaid, such measures have to be both proportionate and appropriate promulgated".[21] It went on to say that "the broad extent of the proposed measures amounted to illegal censorship of publication of legitimate opinions and the communication of diverse points of view. Freedom of expression and its corresponding right to hold and share opinions need to be jealously guarded especially within the context of a contest electoral process […]."[22] However, the Court also indicated that requiring a few seconds delay by broadcasters might be an acceptable way to avoid the publication of "unsavoury and even inflammatory opinions" if proper procedures for issuing such regulations were followed – while finding it unnecessary to decide in this case whether a properly-promulgated regulation to this effect would be a justifiable limitation of the constitutional rights that were implicated.[23]

In the 2022 *Mbele* case, the High Court found merit in the contention that the offence of **criminal libel** is unconstitutional. Section 200 of the Penal Code provides: "Any person who, by print, writing, painting, effigy, or, by any means otherwise than solely by gestures, spoken words, or other sounds, unlawfully publishes any defamatory matter concerning another person, with intent to defame that other person, shall be guilty of the misdemeanour termed 'libel'."[24] The penalty for libel is an unspecified fine or imprisonment for up to two years. The High Court found that a *prima facie* "discordance" between this offence and the constitutional right to freedom of expression. It considered jurisprudence on criminal defamation and freedom of expression under the African Charter on Human and People's Rights and the International Covenant on Civil and Political Rights, and concluded that there was merit in a consideration of whether the Malawi law on criminal libel constituted a

[20] *Attorney General v Trapence*, Supreme Court of Appeal, MSCA Civil Appeal No. 55 of 2019, 30 September 2019l see the case summary by Global Freedom of Expression here.
[21] *S v MACRA; Ex Parte The Registered Trustees of National Media Institute of Southern Africa & 2 Others* (Constitutional Reference 3 of 2019) [2020] MWHC 193 (29 May 2020), paragraph 26.
[22] Id, paragraph 27.
[23] Id, paragraphs 33-35.
[24] Penal Code [*Chapter 7:01*], section 200. The Penal Code was recently further amended by the Penal Code (Amendment) Act 8 of 2023, which does not affect this section, but (as discussed below) did repeal some other provisions of the Penal Code relevant to expression.

limitation on the right to freedom of expression that met the requirements of reasonableness, recognition by international human rights standards and necessity in an open and democratic society. The High Court thus referred the case to the Chief Justice for certification as a constitutional matter to be heard by a three-judge panel.[25] As of mid-2023, the Supreme Court had not yet issued a ruling on this case.

10.3 CASE STUDIES

According to Reporters Without Borders:

> *The disputed elections of 2019 had a negative impact on press freedom. Several TV channels were vandalised, and radio phone-in programmes were banned when the results were being announced. Malawi has not yet adopted a whistleblower protection law, and journalists are sometimes subjected to threats and online intimidation. Several cases of physical attacks on journalists, especially by political party activists or police, have been reported in recent years. Journalists are still sometimes arrested arbitrarily […].*[26]

Freedom House gave this overview of internet freedom in Malawi in 2022:

> *Internet freedom in Malawi declined during the coverage period, as state authorities retaliated against journalists who published corruption allegations against the government. The arrests and detentions of journalists who cover political leaders or discuss corruption in their online content has [sic] resulted in increased self-censorship. Online news outlets have been subject to government manipulation via unofficial directives in recent years, though there were no reported cases of censorship or forced removal of content during the coverage period.*27

The International Press Institute noted in 2021 that the current Malawi government, which has been in office since June 2020, has made several efforts to position itself in a good light in terms of media freedom – citing as one example the inclusion of journalists among the priority group of people to be first in line for the Covid-19 vaccine; yet, on the other hand, journalists are still often the target of attacks, both by the police and the public.[28]

In 2023, *Maravi Post* journalist Dorica Mtenje was charged with **criminal libel** and **offensive communication under the cybercrime law** following a complaint by the Director of the National Intelligence Service about an article concerning his suspension for alleged gross incompetence and misappropriation of funds**.** She was detained for about 12 hours. Police reportedly confiscated her phone but returned it

[25] *Mbele v R*, Misc. Criminal Case No. 04 of 2022, High Court of Malawi, 20 June 2022.
[26] "2023 World Press Freedom: Malawi", Reporters Without Borders, "Safety".
[27] "Freedom on the Net 2022: Malawi". Freedom House, "Overview". See also section B4.
[28] Antonio Prokscha. "Malawi: Recent detentions of journalists overshadow positive press freedom image", **International Press Institute, 12 April 2021.**

upon her release. The article in question did not carry a byline, and Mtenje asserted that she did not write or publish it.[29]

In 2022, the privately owned news website *Platform for Investigative Journalism* published an article alleging police corruption in connection with a contract for the procurement of water cannons. A few days later, Gregory Gondwe, the managing director of this news site, was detained for about six hours while police questioned him, in the presence of his lawyer, about the sources for that article. Police also searched the news office under a warrant issued in connection with the alleged offence of **spamming, pertaining to the illegal transmission of information online, under section 91 of the Electronic Transaction and Cyber Security Act, 2016.** Police confiscated Gondwe's cell phone and laptop and forced him to disclose his passwords. The devices were returned the next day. Gondwe was not formally charged, but police indicated that they were still investigating the case. The Attorney-General apologised for Gondwe's detention and questioning, stating that he had no knowledge that police would take this route, and committing to a government review of archaic laws that restricted media freedom. A police spokesperson said that Gondwe had not been arrested but merely "interviewed" in connection to an ongoing investigation into the news article and related issues.[30] Not long after this incident, the *Platform for Investigative Journalism* reported that its website had been hacked and compromised; the Media Institute of Southern Africa (MISA) in Malawi claimed that the hacking was an intentional act committed by state authorities.[31]

In 2022, Chidawawa Mainje was arrested and charged with the offence of **cyber harassment under section 86 of the Electronic Transactions and Cyber Security Act, 2016** for allegedly insulting the President in a WhatsApp conversation. This arrest raised concerns that authorities were monitoring private electronic communications despite their encryption, without appropriate legal authority and without any notice to those being monitored.[32]

In 2022, a man was arrested for posting a message on Facebook saying that a Member of Parliament had siphoned maize meant for his constituency. He was charged with **cyberstalking under the Electronic Transactions and Cyber Security Act** before being released at the request of the MP in question.[33]

In 2022, social media influencer Joshua Chisa Mbele was charged with **criminal libel** and **publication of offensive communication in violation of section 87 of the Electronic Transactions and Cyber Security Act**. According to one account, this was in connection with posts alleging that a Malawi Defence Force commander had accepted bribes from a corruption suspect.[34] According to another source, the arrest

[29] "Malawi police detain, charge journalist Dorica Mtenje over story she did not write", Committee to Protect Journalists, 22 February 2023.
[30] "Malawi journalist Gregory Gondwe detained, questioned about sources for article on alleged corruption", Committee to Protect Journalists, 8 April 2022.
[31] Freedom on the Net 2022: Malawi", Freedom House, section C8; Lameck Messina, "Malawi Police Accused of Hacking Website of Investigative Media Group", *VOA*, 17 April 2022; "East and Southern Africa: Attacks on journalists on the rise as authorities seek to suppress press freedom", Amnesty International, 3 May 2023.
[32] "2022 Country Reports on Human Rights Practices: Malawi", US State Department, section 1F; "Malawi 2022", Amnesty International, "Freedom of expression".
[33] "Freedom on the Net 2022: Malawi", Freedom House, section C3.
[34] "2022 Country Reports on Human Rights Practices: Malawi", US State Department, section 2A. See also Duncan Mlanjira, "Law Professor Accuses Army General of Abusing his Power in Social Media Activist Arrest", *Nyasa Times*, 2022.

related to a Facebook post where he shared a list of government officials who allegedly had offshore bank accounts, although he deleted the post after realising that he had fallen for misinformation.[35] Mbele's case led to the challenge to the constitutionality of criminal libel, discussed in the section above.

In 2021, Ignatius Kamwanje plead guilty to a charge of **spamming in violation of the Electronic Transactions and Cyber Security Act** in connection with a Facebook post in which he alleged that money was being stolen from customers at the National Bank of Malawi. Bank employees filed a complaint with the police, contesting this allegation.[36]

It was also reported in 2021 that police in the capital city Lilongwe interrogated Watipaso Mzungu, chief reporter of the privately-owned news website *Nyasa Times*, about an article quoting a local activist who referred to the President as "a joker" and a "time waster" in relation to a proposed Cabinet reshuffle. Mzungu was asked by police to come to police headquarters for questioning, where he was told that the article constituted a **criminal insult of the President and an attempt to undermine the authority of the head of state.** The interrogation lasted about two hours, with Mzungu being asked about his motivations for writing the report and whether he had manipulated the activist's statements to attract public attention. Police also demanded the unedited draft of the news story, as well as the activist's original statement. Mzungu was released without charge after this questioning. The police later stated that Mzungu had merely been "invited for an interview" in connection with an ongoing investigation, and that he had cooperated with the police.[37]

In another 2021 incident, police detained Enock Balakasi, a reporter for the privately owned broadcaster *Joy Radio*, for more than two hours after he photographed police who had responded to an attempted suicide in a suburb of Lilongwe. Police allegedly accused him of photographing them without permission, and deleted photos from his phone. He was initially charged with **conduct likely to cause a breach of peace**, **obstructing police officers on duty**, and **working without permission from the police**, but the charges were dropped after police questioning.[38]

In 2021, Irene Chisulo Majiga was arrested for publishing a voice note on WhatsApp, which later went viral, alleging that a person detained on rape charges was released under questionable circumstances. She plead guilty to a charge of disseminating false information in violation of **section 60(1) of the Penal Code** and paid a fine. The State Prosecutor argued that the post had created public unrest, but it is not clear that there was any clear, objective public harm. [39]

Raymond Siyaya, a journalist from *Chanco Community Radio*, was also arrested in 2021 for allegedly reporting "fake news" on his Facebook page in violation of **section 60(1) of the Penal Code**, by claiming that government officials had mismanaged

[35] "Freedom on the Net 2022: Malawi", Freedom House, section C3. See also "Malawi Police arrest social media activist", *Malawi24*, 11 January 2022/
[36] "Freedom on the Net 2022: Malawi", Freedom House, section C3.
[37] "Malawi police question journalist Watipaso Mzungu over article calling president 'a joker'", Committee to Protect Journalists, 14 April 2021.
[38] Id.
[39] "LEXOTA Country Analysis: Malawi", last updated December 2022.

COVID-19 emergency relief funds. He was later released the charges against him were dropped.[40]

Also in 2021, **police officers beat and briefly detained** Oliver Malibisa, a reporter with *Likoma Community Radio*, as he tried to cover a student demonstration. Malibisa alleged that a police officer hit him in the chest with a gun and told him to stop filming the demonstration. When the journalist continued to film the event, police used pepper spray on him and detained him. He was held at the Likoma Police Station for about two hours before being released without charge. His phone was taken but returned upon his release. [41]

It was reported in 2020 that Tumpale Mwakibinga was arrested and charged with **offensive communication under the Electronic Transactions and Cyber Security Act** for a Facebook post in which he mocked the former First Lady. He was released on bail pending trial, subject to a bail condition prohibiting him from posting anything on social media related to the former First Lady.[42]

In 2020, three journalists were detained for two hours at Kamuzu International Airport in Lilongwe, after attempting to cover the arrival of an EU delegation due to present their final report on the disputed election. Their equipment was confiscated and their footage deleted, and they were locked in a police cell in the airport. Police first charged the three with "**conduct likely to cause breach of the peace**," but the charge was changed to **disorderly conduct under the Aviation (Airport Security) Regulations issued in terms of the Aviation Act**. A police spokesperson stated that the journalists were arrested because they had not sought the necessary permission to "cover airport activities", which requires a permit in terms of the aviation regulations.[43]

These incidents indicate that the application of cybercrime offences against journalists and persons who post on social media is taking place in practice. This could be in part due to the fact that Malawi's cybercrime law has been in force longer than those in some other jurisdictions, or it could be due to overbroad drafting of some of the offences covered by the law or targeted application of the laws to dampen criticisms of public figures.

There is some indication that the Malawian government considered an internet shutdown in connection with its 2019 elections, although in the end there was only some temporary disruption of debatable origin:

[40] Id.
[41] "Malawi police beat, detain radio reporter Oliver Malibisa", Committee to Protect Journalists, 21 July 2021.
[42] "Statement by Michael Kaiyatsa, Acting Executive Director for the Centre for Human Rights and Rehabilitation" [2020].
[43] "Malawi detains, charges 3 journalists seeking to cover EU delegation's return", Committee to Protect Journalists, 10 January 2020.

Leading up to the election on 21 May 2019, there were rumours swirling that the government of Malawi was considering shutting down the internet on the day of the election. Several meetings between the government, the Malawi Communications Regulatory Authority (MACRA), and civil society occurred during the weekend before the election. Lawyers from MACRA resisted efforts by the government to shut down the internet and stated that while they believed Malawian law gave them the authority to shut off internet access, they did not think that it was necessary. There were also reports that the government was directly pressuring individual ISPs within the country to shut off access.

On the day of elections, there were reports that several of the major internet arteries between Blantyre and Lilongwe were cut. NetBlocks reported a 20% decrease in internet activity in the three hours following the closure of the polls. The government stated both that there was no internet shutdown, and that vandals had cut lines that caused some services to be down temporarily.[44]

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

A) ELECTRONIC TRANSACTIONS AND CYBER SECURITY ACT 33 OF 2016

Malawi's **Electronic Transactions and Cyber Security Act 33 of 2016** is an omnibus piece of legislation that covers electronic transactions, e-commerce, certain data protection issues, management of domain names and e-government as well as cyber security and cybercrime.[45] The Act has three key objectives:

- to set up a responsive information and communication technology (ICT) legal framework to facilitate competition and development in the sector and "the participation of Malawi in the information age and economy";
- to protect ICT users from undesirable impacts, including the spread of pornographic material, cybercrime and digital fraud;
- to put in place mechanisms that safeguard ICT users from fraud, breach of privacy, misuse of information and immoral behaviour brought by the use of ICT.[46]

The Act is administered by the **Malawi Computer Emergency Response Team** (Malawi CERT, or MCERT) which is set up as a unit within MACRA.[47] MACRA also has the power to appoint cyber inspectors with certain monitoring and investigative powers.[48]

The Act's reach is very broad, as many of its provisions apply to "online public communication" which means "any transmission of digital data, signs, signals, texts, images, sounds or messages, of whatever nature, that are not private

[44] "Navigating Litigation during Internet Shutdowns in Southern Africa", Southern Africa Litigation Centre, June 2019, page 8 (footnote omitted).
[45] Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*].
[46] Id, section 2
[47] Id, sections 5-6.
[48] Id, sections 69-70.

correspondence, by electronic communication means that enable a reciprocal exchange of information between an issuer and a receiver".[49]

In general, the Act states that online public communication may be restricted in order to –

- prohibit child pornography;
- prohibit incitement of racial hatred, xenophobia or violence;
- prohibit justification for crimes against humanity;
- promote human dignity and pluralism in the expression of thoughts and opinions;
- protect public order and national security;
- facilitate technical restriction to conditional access to online communication; and
- enhance compliance with the requirements of any other written law.[50]

Freedom House notes concerns about the approval of restrictions to "protect public order and national security", on the grounds that this is a broad provision that is open to abuse. It also expresses concerns about restrictions to "facilitate technical restriction to conditional access to online communication", on the basis that this is "an unclear statement that could be interpreted to enable network shutdowns or blocks on social media platforms".[51]
The cybercrime offences in the law are as indicated in the tables below. They "are informed by the **SADC framework** and other international principles".[52]

ELECTRONIC TRANSACTIONS AND CYBER SECURITY ACT, 2016 - TECHNICAL OFFENCES	
Section 84: Unauthorized access, interception or interference with data	It is an offence – • to intentionally **access** or **intercept** any data without authority or permission to do so, or to exceed the authorized access (subsection (3)); • to intentionally and without authority to do so, **interfere** with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective (subsection (4)). The Minister shall, by regulations, come up with specific cases where unauthorized access to, interception of, or interference with, data may be permitted in specific conditions set out in the regulations (subsection (2)). It is an offence - • to unlawfully produce, sell, offer to sell, procure for use, design, adapt for use, distribute or possess any **device**, including a computer program, a component or a phone, which is designed primarily to overcome security measures for the protection of data, or to perform any of these acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilize such item (subsection (5)); • to utilise any device or computer program referred to above in order to **unlawfully overcome security measures** designed to protect "such data or access thereto" (subsection (6));

[49] Id, section 3 (definition of "online public communication").
[50] Id, section 24(2).
[51] "Freedom on the Net 2022: Malawi", Freedom House, section A3.
[52] "An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, page 26.

	• to commit any act described in this section with the intent to interfere with access to an information system so as to constitute a **denial, including a partial denial, of service** to legitimate users (subsection (7)); • to **communicate, disclose or transmit any data, information, program, access code or command** to any person not entitled or authorized to access it (subsection (8)(a)); • to knowingly **introduce or spread a software code that damages** a computer, computer system or network (subsection (8)(b)); • **to access or destroy any files, information, computer system or device** without authorization, or for the purposes of concealing information necessary for an investigation into an offence (subsection (8)(c)); or • to **damage, delete, alter or suppress any communication or data without authorization** (subsection (8)(d)). It is also an offence for a person to **knowingly receive data** which that person is not authorized to receive (subsection (9)). There is an **enhanced penalty** where an offence is committed in relation to data concerned with "national security" (which is not defined) or the provision of an "essential service" (not defined) (subsection (10)). o "Access" is not defined. o While some assert that criminalisation of "mere access" without more is justified given that it compromises data confidentiality, there is no universal consensus on whether criminalization of mere access to non-protected systems is warranted, or whether this crime should be narrowed by additional conditions.[53] The *SADC Model Law on Computer Crime and Cybercrime* qualifies the offence of illegal access by requiring that it take place "intentionally, without lawful excuse *or justification* or in excess of a lawful excuse or justification".[54] o There are overlaps between the offences of unauthorised access in section 87(3), overcoming computer security measures designed to protect the security of data in section 87(6) and hacking in section 89. o Regarding the statute's reference to illegal interception of data (section 84(3)), one analysis comments: "Malawi's definition is unnecessarily skeletal and basic. The definition would have been improved by merely looking at how other countries both regionally and internationally have drafted their own offences on data interference. Moreover, the requirement that the interception must be to non-public transmission of data has not been included, and omission that renders the offence overly broad."[55] o Interfering with data is covered generally in section 84(4), but this overlaps with other provisions that talk about destroying damaging, deleting, altering or suppressing data (sections 86(8)(b)-(c)). o Section 84(6) is unclear because it references section 86(5) which uses the word "data in two different senses (once to refer generally to information that is protected, and once to refer to "a password, access

[53] *Comprehensive Study on Cybercrime*, United Nations Office on Drugs and Crime (UNODC), draft dated February 2013. page 82.
[54] SADC Model Law on Computer Crime and Cybercrime, section 4.
[55] Lewis C Bande, "Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities", *International Journal of Cyber Criminology*, Vol 12 Issue 1, Jan-June 2018, page 17. Note that some of the section numbers referred to by Bande in respect of the Malawi law are incorrect.

	code or any other similar kind of data" - and then ambiguously refers to "such data". o Regarding the offences relating to devices covered by sections 86(5) and (6), It has been noted that limiting these offences to devices *designed to overcome security measures for the protection of data* means that the offence does not apply to devices that can be used to commit other cybercrimes.[56] o The offence of communicating or disclosing data or information to any person not entitled or authorized to access it in section 86(8)(a) could impede whistleblowers. o Making it an offence to knowingly receive data which one is not authorized to receive (section 86(9)) could affect public access to information acquired by a whistleblower or placed in a cache such as Wikileaks. There is no exception for lawful excuse or acting in the public interest. o The conditions which lead to an enhanced penalty are unclear since the key terms ("national security" and "essential service") are general and undefined.
Section 89: Prohibition of hacking, cracking and introduction of viruses	It is an offence to hack into any computer system, or knowingly introduce or spread a virus into a computer system or network. o "Hacking" and "cracking" are not defined, and the term "cracking" appears only in the heading of the provision and not in the text. This makes the prohibited conduct unclear. It has also been noted that the use of the technical term "hack" in the definition "violates one of the best practices in the drafting of cybercrime legislations, viz., that as much as possible, and whilst not compromising on the clarity of the law, 'technology–neutral language' must be preferred when defining cybercrime offences. This is necessary to ensure that the criminalization covers both existing and future technologies."[57] o This offence appears to overlap with section 87(3) on unauthorized access, and section 87(6) which makes it an offence to utilise a device or computer program to unlawfully overcome security measures designed to protect computer data or access to it.[58] o Note that no malicious intention is specified for any of the acts listed, and that hacking is not specifically required even to take place knowingly – although this may be implied by the generally-understood meaning of the term "hack". The general principles of criminal liability would require some degree of *men's rea* (criminal intent).
Section 90: Unlawfully disabling a computer system	It is an offence to wilfully or maliciously render a computer system incapable of providing normal services to its legitimate users. o "Anything that renders a computer system incapable of providing normal services to legitimate users is covered. A literal reading of the provision would include both technical and non-technical activities. In practice, however, most activities that would hinder a computer system from providing normal services would be technical in nature."[59]

[56] Id, page 22.
[57] Id, page 15 (reference omitted).
[58] Id, page 24.
[59] Id, page 19.

	○ This offence overlaps with section 87(8)(b), which makes it a crime to introduce or spread a software code that damages a computer, computer system or network. One commentary suggests that these two offences should have been combined into one because "they target various modes of interfering with a computer's system", while it would have been better to enact "a single offence of system interference, which would capture the various ways of committing that offence."[60]
Section 91: Prohibition of spamming	It is an offence to transmit any unsolicited electronic information to another person for the purposes of illegal trade or commerce, or other illegal activity. ○ Note that the use of spam is not criminalised unless it relates to some illegal activity; spamming by legitimate businesses is not covered here. ○ As the case studies in section 103 of this chapter indicate, this offence has been applied in practice to inhibit freedom of expression. Since this offence has to be underpinned by some other "illegal activity," these applications of it must have been supported by the offence of criminal libel – which is currently the subject of a constitutional challenge.
Section 92: Prohibition of illegal trade and commerce	It is an offence to use the internet as a medium for any illegal activity or trade, fraudulent transaction or as a means of procuring any internet-related fraud.

The cybercrime law includes only four content-based offences, as summarised in the table below.

Unusually, **the law does not include any offences relating to the publication of racist or xenophobic material or material relating to genocide and other crimes against humanity**, via electronic means or otherwise. This seems odd, given that the Act explicitly states that online public communication may be restricted in order to prohibit incitement of racial hatred, xenophobia or violence and justification for crimes against humanity (amongst other things).[61] No other laws covering publication of materials about these topics were located, other than a provision in the Penal Code prohibiting commission of the crime of genocide.[62]

ELECTRONIC TRANSACTIONS AND CYBER SECURITY ACT, 2016 - CONTENT-BASED OFFENCES	
Section 85: Child pornography	There is a range of offences relating to "child pornography in an electronic form". For the sake of protecting children from pornography, establishments serving the public, and places open to the public proposing access to the Internet, are required to use adequate pornography filtering software as defined by subsidiary legislation made under the Act.

[60] Id, page 20.
[61] Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*], section 24(2)(b) and (c).
[62] Penal Code [*Chapter 7:01*], section 217A.

	○ "Child pornography" is defined in section 2 to mean "visual and pornographic material that depicts, presents or represents a person under the age of eighteen engaged in sexually explicit conduct or an image representing a person under the age of eighteen engaged in sexually explicit conduct". "Pornography" is defined in section 2 as "visual material that depicts images of a person engaged in sexually suggestive or explicit conduct". Thus, the reference to "pornographic material" in the definition of "child pornography" seems circular. ○ There is no defence for materials with a genuine artistic, educational, legal, medical, scientific or public benefit purpose. ○ The provision requiring filters in places where the Internet can be accessed by the public is fairly uncommon in the SADC region.
Section 86: Prohibition of cyber harassment	It is an offence to use any computer system and continue - • making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent; or • threatening to inflict injury or physical harm to the person or property of any person; or • knowingly permitting any electronic communications device to be used for any of the abovementioned purposes. ○ Many of the key terms in this offence are not defined ("obscene, lewd, lascivious or indecent"). ○ The reference to continued acts indicates that cyber harassment requires repeated acts of the kind described. However, if this is correct, it should be made more clear. ○ The acts that constitute cyber harassment are narrower than in many other SADC cyberlaws, as there is no mention of insult or annoyance. Here, the harassment requires either suggestions of a sexual nature or threats of harm. The reference to "injury or physical harm" indicates that psychological or emotional injury is covered by the word 'injury" - a point which should be clarified.
Section 87: Prohibition of offensive communication	It is an offence wilfully and repeatedly to use electronic communication to disturb or attempt to disturb the peace, quietness or right of privacy of any person with no purpose of legitimate communication. "Any person who wilfully and repeatedly uses electronic communication to disturb or attempts to disturb the peace, quietness or right of privacy of any person with no purpose of legitimate communication whether or not a conversation ensues, commits a misdemeanour and shall, upon conviction, be liable to a fine of K1,000,000 and to imprisonment for twelve months." ○ This has been identified as a provision "that public officials could exploit to punish critical speech by online journalists or internet users" [63], or put another way. "To clamp down on dissenting voices."[64] This provision has in fact been used against journalists in Malawi.[65]

[63] "Freedom on the Net 2022: Malawi". Freedom House, section C2.
[64] "An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, page 29.
[65] See, for example, "Statement by Michael Kaiyatsa, Acting Executive Director for the Centre for Human Rights and Rehabilitation" [2020] and the case studies in section 10.3 of this chapter.

Section 88: Prohibition of cyber stalking	It is an offence to wilfully, maliciously, and repeatedly use electronic communication to harass another person *and* to make a threat with the intent to instil reasonable fear in that person for his or her safety or that of a member of his or her immediate family.[66] o It is a limiting factor that this offence requires, not just vague "harassment" but also the making of threats with an intent to instil reasonable fear for personal safety. It is also a limiting factor that this form of harassment must take place repeatedly and maliciously.

While some of these offences might be used to restrict speech, it has also been reported that cyberbullying is being increasingly used as a tool to silence critics of the government, with online trolls using pseudonyms targeting columnists and journalists who are deemed to be too critical of the current government.[67]

In general, **attempting, aiding or abetting any of the offences in the Act** – both technical and content-based – is also an offence.[68]
The law's provisions on **encryption** have given rise to come concern. It requires providers of cryptography services or products to register with MACRA and to provide the regulator with "the technical characteristics of the encryption means as well as the source code of the software used".[69] Freedom House notes that this provision potentially affects services with end-to-end encryption, such as WhatsApp.[70] The result could be to compromise the privacy of those who engage in online communication, which in turn may inhibit freedom of expression.

ELECTRONIC TRANSACTIONS AND CYBER SECURITY ACT, 2016

52. Encryption

(1) A person shall not provide cryptograph services or products in Malawi without registration under this Part.

(2) Registration for provision of cryptograph services or products shall be made -
(a) to the Authority.
(b) in the prescribed manner and form; and
(c) upon payment of applicable fees.

(3) The Minister in consultation with the Authority shall issue regulations -
(a) in respect of use, importation and exportation of encryption programmes and encryption products; and

[66] The wording on this point a somewhat ambiguous: "…makes a threat with the intent to instil reasonable fear in that person for his safety or *to a member of that person's immediate family*". It is not entirely clear if this refers to making *a similar threat to an immediate member of the family*, or making *a threat to a person that instils fear in that person for the safety of immediate family members*.
[67] Teresa Temweka Chirwa-Ndanga, "New Access to Information Law Brings Hope" in "The State of Press Freedom in Southern Africa 2020-2021", Media Institute of Southern Africa (MISA), page 39.
[68] Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*], section 93.
[69] Id, sections 52 and 67 (quoted on the box in the text).
[70] "Freedom on the Net 2022: Malawi". Freedom House, section C4.

(b) prohibiting the exportation of encryption programmes or other encryption products from Malawi generally or subject to such restrictions as may be prescribed.

(4) For the avoidance of doubt, subject to any regulations made under sub regulation (1), it is lawful for any person to use encryption programme or product provided that it has lawfully come into possession of that person.

67. Provision of encryption services

(1) A person who provides encryption services shall declare to the Authority the technical characteristics of the encryption means as well as the source code of the software used.

(2) Regulations made under this Act shall define the conditions for making declarations referred to in subsection (1), and may define encryption services whose technical characteristics or conditions of supply are such that, with regard to national defence or internal security interests, their provision shall not require any prior formality.

(3) An encryption services provider shall be bound by professional secrecy.

(4) Unless it is proved that no intentional wrongful conduct or negligence was involved, a provider of encryption services for confidentiality purposes shall be liable, notwithstanding any contractual provision to the contrary, for the damage suffered by the persons that entrusted the management of their confidential conventions to them in case of violation of the integrity, confidentiality or availability of the data object of such convention.

Privacy is also implicated in the requirement that **online content providers must display on their website the full name, domicile, telephone number, and email address of the editor**. Legal entities that provide online content must display their corporate name, postal and physical address of their registered office, telephone number, email address, authorized share capital, and registration number, of the editor. [71] Failure to display the required information is a criminal offence.[72] This provision has been called "unworkable" since many platforms are operated by global entities that Malawi cannot regulate – such as, for example, a Facebook page that is not required under the Facebook platform rules to list the actual legal name of an individual or a corporate entity; "This kind of regulation of the internet is typical of authoritarian governments which hope to encourage self-censorship by creating an atmosphere that discourages freedom of expression."[73] According to Freedom House, "[e]ven though the government does not actively enforce this provision, its presence in legislation undermines citizens' rights to privacy and anonymity and may encourage self-censorship".[74]

[71] Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*], section 31(1).
[72] Id, section 95.
[73] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 8: Malawi", Konrad Adenauer Stiftung, 2021, page 376.
[74] "Freedom on the Net 2022: Malawi". Freedom House, section C4.

Regarding enforcement of the Act, as noted above, MCERT has the power to appoint **cyber inspectors** whose powers include the following:

- to monitor and inspect any website database with critical data or activity on an information system in the public domain and report any unlawful activity to the Authority;
- to investigate the activities of suppliers of encryption and of encryption service providers
- to search premises and information systems under the authority of a search warrant
- the information system;
- to access and inspect the operation of any computer or equipment forming part of an information system and any associated apparatus or material which the cyber inspector has reasonable cause to believe is, or has been used in, connexion with the commission of any offence.

A cyber inspector may be accompanied by a police officer when carrying out these functions.[75] **Search warrants** may be issued by a court on the application of a cyber inspector.[76]

The Act includes a provision for **take-down notifications**. Any complainant may notify a service provider of "any content which is unlawful or infringes, or may infringe, on such person's rights". It is an offence to make a false notification, punishable by a fine of K1,000,000 and imprisonment for twelve months. The service provider is not liable for hosting or caching material that is promptly removed in response to such a notification – nor is the service provider liable for a takedown in response to a wrongful or false notification. As in most such systems, this approach mitigates in favour of removal. However, the Malawi framework offers some helpful elements that are not commonly seen in the region:

- A service provider offering access to online public communication services must inform its subscribers of the existence of any technical means which permit restriction of access to certain services – ie filtering mechanisms.
- A service provider must set up "an easily accessible and visible system" for reporting content which is unlawful or infringes on a person's rights.
- A service provider must promptly inform MACRA of any illegal content reported to it by a member of the public and "make public the means taken to fight against the dissemination of such illegal content" – a requirement which would, in theory, enable MACRA to play a monitoring role.[77]

[75] Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*], section 70.
[76] Id, section 83.
[77] Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*], section 30 read with sections 27-28. These requirements technically apply to the "intermediary service provider". which is the person or entity "that provides electronic communications services consisting of the provision of access to communications networks, storage, hosting or transmission of information through communication networks" (definition in section 2).

B) OTHER LAWS THAT MAY IMPACT FREEDOM OF EXPRESSION

In 2023, the **Penal Code** was amended to repeal some crimes that previously impacted freedom of expression. This amendment removed the provisions of the Penal Code on **sedition** – which had previously criminalised speech and publications intended to incite hatred, contempt or disaffection against the President, the Government or the administration of justice; to inspire the public to try to alter any matter by unlawful means; to raise discontent or disaffection amongst citizens; or to promote feelings of ill-will and hostility between different classes of the population.[78]

However, some provisions that remain are still problematic in respect of freedom of expression.

- Section 60 of the Penal Code criminalises **the publication of false information that is likely to cause fear and alarm to the public or to disturb public peace.**[79] It has been observed that this provision is vague and fails to provide clear guidance, which gives an overly wide degree of discretion to those charged with the enforcement of this law.[80] This crime has been used against individuals in practice in respect of online publications.[81]
- Section 61 of the Penal Code makes the **defamation of foreign dignitaries** a misdemeanour, where this takes place with intent to disturb the peace and friendship between Malawi and the Republic and the country in question.
- Section 88 of the Penal Code on the offence of **intimidation** covers, in addition to threats of personal harm or property damage, words that threaten another with any injury to his reputation or to the reputation of any other person where this is done with intent to cause alarm or to influence a person's actions. The offence applies to the publisher, editor or printer of any newspaper, pamphlet or other document containing any such threat. This offence is related to criminal libel.

PENAL CODE

60. PUBLICATION OF FALSE NEWS LIKELY TO CAUSE FEAR AND ALARM TO THE PUBLIC

(1) Any person who publishes any false statement, rumour or report which is likely to cause fear and alarm to the public or to disturb the public peace shall be guilty of a misdemeanour.

(2) It shall be a defence to a charge under subsection (1) if the accused proves that, prior to publication, he took such measures to verify the accuracy of such statement, rumour or report as to lead him reasonably to believe that it was true.

[78] The Penal Code (Amendment) Act 8 of 2023 repealed sections 50-53 of the Penal Code [*Chapter 7:01*]. Note that sections 46-49 of the Penal Code, which previously prohibited the importation or re-publication of publications which the minister believed to be contrary to the public interest, were repealed by Act 24 of 2012. Penal Code [*Chapter 7:01*].

[79] Penal Code [*Chapter 7:01*], section 60.

[80] "LEXOTA Country Analysis: Malawi", last updated December 2022.

[81] See section 10.3 of this chapter.

- Section 130 of the Penal Code makes it an offence **to speak or write words with the intention of wounding religious feelings**. This offence also applies to sounds and gestures. However, it has been reported that this provision is not enforced.[82]
- Section 181 of the Penal Code makes it an offence to publicly conduct oneself in a manner likely to cause a **breach of the peace**. This offence is so broad and vague that it could capture many forms of freedom of expression.
- Section 182 of the Penal Code makes it an offence to use **insulting, abusive, indecent or threatening language** or otherwise conduct oneself in a manner likely to provoke any person to breach the peace. This offence's overbroad formulation makes it vulnerable to selection enforcement.
- Section 200 of the Penal Code concerns **criminal libel**. As has been discussed above, this provision is currently the subject of a constitutional challenge.[83]

PENAL CODE

200. DEFINITION OF LIBEL
Any person who, by print, writing, painting, effigy, or by any means otherwise than solely by gestures, spoken words, or other sounds, unlawfully publishes any defamatory matter concerning another person, with intent to defame that other person, shall be guilty of the misdemeanour termed "libel".

Section 3 of the **Preservation of Public Security Act 11 of 1960** empowers the minister to make regulations that prohibit the publication and dissemination of any matter that appears to the minister to be "prejudicial to public security".[84] **The Public Security Regulations** issued under this Act prohibit any person from publishing anything likely to prejudice public security, undermine public confidence in the Government, promote a feeling of ill-will or hostility between any sections or classes or races of people in Malawi, or promote industrial unrest.[85] One commentary states that the "vague construction of this law fails to provide sufficient guidance to individuals and gives an overly wide degree of discretion to those charged with the enforcement of this law."[86] Another analysis states that the criteria for this prohibition given are based on opinion rather than being objective, making this provision inconsistent with international best practice.[87]

Section 4 of the **Protected Flag, Emblems and Names Act** makes it an offence to do any act, utter any words or publish any writing "calculated to or liable to insult, ridicule or to show disrespect to" the President, the National Flag or other specified national emblems.[88]

Section 83 of the **Prisons Act** makes it an offence to publish in whole or in part a letter or document written by a prisoner which has not been endorsed by a prison officer.[89] This could obviously inhibit the exposure of abuse of prisoners or prison conditions.

[82] "2022 Country Reports on Human Rights Practices: Malawi", US State Department, section 2A.
[83] See section 10.2 of this chapter.
[84] Preservation of Public Security Act 11 of 1960 section 3(2)(a).
[85] The Public Security Regulations (reproduced below the text of the act on this website), regulation 4 read with regulation 14.
[86] "LEXOTA Country Analysis: Malawi", last updated December 2022.
[87] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 8: Malawi", Konrad Adenauer Stiftung, 2021, pages 284-285.
[88] Protected Flag, Emblems and Names Act [*Chapter 18:03*], section 4.
[89] Prisons Act [Chapter 9:02], section 83(3)-(4).

C) SIM CARD REGISTRATION

The **Communications Act 34 of 2016** requires registration of "generic numbers" and SIM cards. Individual subscribers must provide their full names, identity card (or other document proving identity), and residential or business address. Legal entities must provide a certificate of registration or incorporation; a business licence; and, where applicable, a taxpayer identification certificate number.[90] In terms of the Communications (SIM Card Registration) Regulations, 2023, the service provider must confirm the subscriber's identity by means of fingerprint verification with the National Registration Bureau, and must keep subscribers' records based on the details electronically retrieved from the National Registration Bureau. Registrations by companies and institutions are verified against the fingerprint of a representative of the entity.[91] This removes the ability to communicate anonymously via mobile phones.[92]

D) STATE SURVEILLANCE

No legal authority for interception of communications by government or law enforcement officers was located, nor any authority for the retention of traffic data by service providers for access by government authorities – but there are indications that state monitoring of communications takes place in practice, as evidenced by arrests related to online activities.[93]

Freedom House reports:

> *Government surveillance of ICT activities is strongly suspected in Malawi, particularly in light of the regulatory authority's January 2018 implementation of the Consolidated ICT Regulatory Management System (CIRMS), which is known locally as the "spy machine". […] MACRA described the system as a tool for monitoring the performance of mobile phone companies and improving the quality of service. However, news reports said that the system would also allow MACRA—without judicial oversight—to obtain data from telephone operators, including the time, duration, and location of calls; short-message service (SMS) messages sent and received; the type of handset used; and other subscriber details.*[94]

In one 2011 commercial court case,[95] a telecommunications subscriber complained about a violation of privacy after MACRA issued a directive to four telecommunication providers to provide it with information about who called which

[90] Communications Act 34 of 2016 [*Chapter 68:01*], section 92.
[91] Communications (SIM Card Registration) Regulations, 2023, regulation 5.There are additional details for other categories of registrations, including minors, foreigners, refugees and diplomatic institutions.
[92] Freedom on the Net 2022: Malawi". Freedom House, section C4.
[93] Personal communications, July 2023.
[94] Id, section C5 (references omitted).
[95] *Kimu v Access Malawi Limited and Others* (Commercial Case No. 54 of 2011) [2012] MWComm C1 (02 May 2012).This judgment could not be located online.

number; details of calls received; time and duration of calls; the location where the call was made or received; SMSs sent and received; type of handset used and other detailed subscriber information. The telecommunication companies (Access Malawi Limited, Airtel Malawi Limited, Telekom Networks Malawi Limited and Malawi Telecommunications Limited) initially raised concerns that this directive violated the constitutional right to privacy, but eventually acquiesced to the request. The Court found that providing the information did indeed violate the right to privacy, which can only be limited by law where the limitation is reasonable, recognized by international human rights standards and necessary in a democratic society. The Court also emphasised that "a limitation does not become legal merely because it comes from MACRA or any other regulatory body.[96]

E) TAKE-DOWN NOTIFICATION

This is discussed above since it is contained in the combined **Electronic Transactions and Cyber Security Act 33 of 2016**.

[96] Case description and quotes as reported in Jimmy Kainja, "Mapping Digital Surveillance and Privacy Concerns in Malawi", Media Policy and Democracy Project, November 2021, pages 9-10; "Navigating Litigation During Internet Shutdowns In Southern Africa", Southern Africa Litigation Centre, June 2019, pages 47-49.