CHAPTER 18

ZIMBABWE

CHAPTER 18: ZIMBABWE

ZIMBABWE KEY INDICATORS
2023 WORLD PRESS FREEDOM RANKING: **126th globally; 39th out of 48 African countries** "The media situation in Zimbabwe has improved slightly since the dictator Robert Mugabe's ouster in 2017. Access to information has increased and self-censorship has declined."
MALABO CONVENTION: NOT signatory or party
BUDAPEST CONVENTION: NOT signatory or party

CONSTITUTIONAL PROTECTION FOR FREEDOM OF EXPRESSION:
Zimbabwe's 2013 Constitution, as amended through 2017
The Constitution of Zimbabwe Amendment Act No. 2 of 2021 does not affect the quoted provisions.

61. FREEDOM OF EXPRESSION AND FREEDOM OF THE MEDIA

1. Every person has the right to freedom of expression, which includes -
a. freedom to seek, receive and communicate ideas and other information;
b. freedom of artistic expression and scientific research and creativity; and
c. academic freedom.

2. Every person is entitled to freedom of the media, which freedom includes protection of the confidentiality of journalists' sources of information.
3. Broadcasting and other electronic media of communication have freedom of establishment, subject only to State licensing procedures that –
a. are necessary to regulate the airwaves and other forms of signal distribution; and
b. are independent of control by government or by political or commercial interests.

4. *All State-owned media of communication must –*
a. be free to determine independently the editorial content of their broadcasts or other communications;
b. be impartial; and
c. afford fair opportunity for the presentation of divergent views and dissenting opinions.

5. *Freedom of expression and freedom of the media exclude –*
a. incitement to violence;
b. advocacy of hatred or hate speech;
c. malicious injury to a person's reputation or dignity; or
d. malicious or unwarranted breach of a person's right to privacy.

86. LIMITATION OF RIGHTS AND FREEDOMS

1. **The fundamental rights and freedoms set out in this Chapter must be exercised reasonably and with due regard for the rights and freedoms of other persons.**

2. **The fundamental rights and freedoms set out in this Chapter may be limited only in terms of a law of general application and to the extent that the limitation is fair, reasonable, necessary and justifiable in a democratic society based on openness, justice, human dignity, equality and freedom, taking into account all relevant factors, including-**

a. the nature of the right or freedom concerned;
b. the purpose of the limitation, in particular whether it is necessary in the interests of defence, public safety, public order, public morality, public health, regional or town planning or the general public interest;
c. the nature and extent of the limitation;
d. the need to ensure that the enjoyment of rights and freedoms by any person does not prejudice the rights and freedoms of others;
e. the relationship between the limitation and its purpose, in particular whether it imposes greater restrictions on the right or freedom concerned than are necessary to achieve its purpose; and
f. whether there are any less restrictive means of achieving the purpose of the limitation.

KEY LAWS:

- Criminal Law (Codification and Reform) Act [*Chapter 9:23*]
  as amended by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*]
- Criminal Procedure and Evidence Act [*Chapter 9:07*]
  as amended by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*]
- Interception of Communications Act, 2007 [*Chapter 11:20*]
  as amended by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*]
- Criminal Law Codification and Reform Amendment Act, 2023 ("Patriots Act")

CRIMINAL DEFAMATION: No[1]

DATA PROTECTION: Zimbabwe has a combined cybercrimes and data protection law.[2]

ACCESS TO INFORMATION: Zimbabwe has a right of access to information in its Constitution[3]
as well as an access to information law.[4]

[1] Madanhire & Another v AG (CCZ 2/14 Const. Application No CCZ 78/12) [2014] ZWCC 2 (12 June 2014); MISA-Zimbabwe v Minister of Justice (Const. Application No CCZ 7/15) (order available here); see the summary of the case by Global Freedom of Expression here and the summary by Southern Africa Litigation Centre here.
[2] Data Protection Act, 2021 [Chapter 11:22] originally, now part of the Cyber and Data Protection Act, 2021 [Chapter 12:07].
[3] Zimbabwe's 2013 Constitution, as amended through 2017, section 62.
[4] Freedom of Information Act, 2020 [Chapter 10:33], which replaced the Access to Information and Protection of Privacy Act of 2003. See also Freedom of Information (General) Regulations, 2021 [Statutory Instrument 229 of 2021, CAP. 10:33].

18.1 CONTEXT

Journalists, news agencies and media services were previously required to be accredited or registered under the **Access to Information and Protection of Privacy Act, 2003**. In 2005, the African Commission on Human and People's Rights found that the onerous regime for the accreditation of journalists in terms of this law was inconsistent with the African Charter on Human and People's Rights. The Commission found that, while compulsory registration procedures are not in themselves a violation of the right to freedom of expression if they are merely administrative in nature, the Zimbabwean law - which contained an offence for "abusing journalistic privilege" which included the publication of false news - created considerable scope for politically motivated action by the authorities" and was aimed at control rather than regulation. It recommended specific changes to remove the offending sections of this law.[5] The entire law was repealed by the Freedom of Information Act, 2020 – although, confusingly, fees for accreditation are still being issued under the authority of the repealed Act.[6]

The key regulatory body for the media is **the Zimbabwe Media Commission established by section 248 of the Zimbabwe Constitution** and comprising a Chairperson appointed by the President and eight members appointed by the President from a list of not fewer than twelve nominees proposed by the Parliamentary Committee on Standing Rules and Orders.[7] Its core functions are set out in section 249 of the Zimbabwe Constitution as follows:

a) to uphold, promote and develop freedom of the media;
b) to promote and enforce good practices and ethics in the media;
c) to monitor broadcasting in the public interest and, in particular, to ensure fairness and diversity of views broadly representing Zimbabwean society;
d) to encourage the formulation of codes of conduct for persons employed in the media and, where no such code exists, to formulate and enforce one;
e) to receive and consider complaints from the public and, where appropriate, to take action against journalists and other persons employed in the media or broadcasting who are found to have breached any law or any code of conduct applicable to them;
f) to ensure that the people of Zimbabwe have fair and wide access to information;
g) to encourage the use and development of all the officially recognised languages of Zimbabwe;

[5] Scanlen & Holderness v Zimbabwe, Case No. 297/2005, decided 3 April 2009; the case is analysed by Global Freedom of Expression here.
[6] Section 41 of the Freedom of Information Act preserved regulations made under the repealed law the extent that they could have been made under the appropriate provisions of the new law – but the Freedom of Information Act makes no provision for accrediting journalists or registering media services and news agencies. "AIPPA Resurrected : New Media Accreditation & Registration Fees Gazetted", Commissions Watch: Zimbabwe Media Commission. 1 February 2021; "Zimbabwe: 2022 Media Accreditation Fees Gazetted", *The Herald*, 2 April 2022
[7] [7] Zimbabwe's 2013 Constitution, as amended through 2017, section 248.

h) to encourage the adoption of new technology in the media and in the dissemination of information;
i) to promote fair competition and diversity in the media; and
j) to conduct research into issues relating to freedom of the press and of expression, and in that regard to promote reforms in the law.[8]

The **Zimbabwe Media Commission Act, 2020 [*Chapter 10:35*]** gives the Commission these additional powers:

(a) to monitor and secure compliance with any –
(i) law which regulates media practitioners and media services including broadcasting, print and electronic media, in order to ensure respect for the rights protected by section 61 of the Constitution [on freedom of expression and freedom of the media];
(ii) international treaty to which Zimbabwe is a party with respect to the protection, promotion or advancing of people's rights in relation to the media in Zimbabwe;

(b) to collaborate and co-operate with other independent constitutional Commissions in supporting and entrenching human rights and democracy.[9]

The Commission is also empowered to consider complaints from any person alleging a violation of the right to freedom of expression, and "on its own motion, investigate or inquire into any action on the part of any person that constitutes, or is likely to result in, a violation of any of the rights protected under section 61 of the Constitution".[10] Where the Commission finds a violation of section 61 rights, it is empowered to order various forms of redress – including compensation to aggrieved persons, orders that decisions or practices resulting in the violation must be stopped, reversed or altered, and recommendations that any law on which the offending action was based should be reconsidered. It can also pursue an action in court to redress such a violation.[11]

Broadcasting in Zimbabwe is regulated by the **Broadcasting Services Act, 2001 [*Chapter 12:06*]**, which creates a Broadcasting Authority of Zimbabwe (BAZ) appointed by the relevant minister after consultation with the President,[12] and the minister has the power to give policy directions to the Board.[13] BAZ issues licences for radio and television broadcasting[14] and is tasked with developing broadcasting codes of conduct.[15] All licensees have a duty to "provide sufficient coverage of national events" - which means any "event or occasion which is declared to a national event by the minister by notice in the Government Gazette – and a duty, when providing an information service, to "provide a fair, balanced, accurate and

[8] Id, section 249.
[9] Zimbabwe Media Commission Act, 2020 [*Chapter 10:35*], section 4.
[10] Id, section 8.
[11] Id, sections 12 and 15.
[12] Broadcasting Services Act, 2001 [*Chapter 12:06*], section 4.
[13] Id, section 4B.
[14] Id, Part III.
[15] Id, section 24.

complete service".[16] No broadcaster may broadcast any matter that contains "false or misleading news";[17] it appears that violation of this condition could be a basis for suspension or cancellation of the broadcasting licence.[18]

The Zimbabwean Broadcasting Corporation (ZBC), which operates as a state broadcaster, is governed by a board appointed by a Minister, under the **Zimbabwe Broadcasting Corporation Act, 2001 [*Chapter 12:01*]**, which is set to be replaced by the **Zimbabwe Broadcasting Corporation (Commercialisation) Act, 2001**.[19]

The **Postal and Telecommunications Act, 2000 [*Chapter 12:05*]** establishes the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) which licenses and regulates postal and telecommunication services, including internet service licences.[20] The Board of POTRAZ is appointed by the relevant minister after consultation with the President,[21] and the minister has the power to give policy directions to the Board.[22] The minister is also empowered, after consultation with the President, to direct the Board to reverse, suspend or rescind its decisions or actions if the minister considers on reasonable grounds that a decision or action "is not in the national or public interest or the interests of consumers or licensees as a whole".[23]

According to Freedom House, "POTRAZ is expected to operate independently, but in practice its independence has been questioned over the years, as it has become increasingly subordinated to state security agencies". Freedom House also states that POTRAZ was largely seen as having supported and enabled the infamous Government directive to suspend Internet services in 2019 (discussed below).[24]

The Postal and Telecommunications Act has a few content-based offences. It is a criminal office to send by post any "indecent or obscene article", or any postal article containing any word or other content "of an indecent, obscene, seditious, scurrilous, threatening or grossly offensive character".[25] It is also an offence to use a telephone for any message that is "grossly offensive or is of an indecent, obscene or threatening character", or any message that the sender knows to be false "for the purpose of causing annoyance, inconvenience or needless anxiety to any other person". In addition, it is an offence to make any telephone call "without reasonable cause for the purpose of causing annoyance, inconvenience or needless anxiety".[26]

[16] Id, section 39.
[17] Id, Fifth Schedule (section 11(1)(b)), Standard Conditions of Licences, item 7. This provision is contained in a section on political matters and medicines. but it is worded generally.
[18] Id, sections 11(1) and 16(1)(b).
[19] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 16: Zimbabwe", Konrad Adenauer Stiftung, 2021, pages 229-ff.
[20] Postal and Telecommunications Act, 2000 [*Chapter 12:05*].
[21] Id, section 5.
[22] Id, section 25.
[23] Id, section 26.
[24] "Freedom on the Net 2022: Zimbabwe", Freedom House, section A5.
[25] Postal and Telecommunications Act, 2000 [*Chapter 12:05*] section 84.
[26] Id, section 88.

Zimbabwe's constitutional provisions are strong, with a sound basis for limited restrictions on the right to freedom of expression that incorporates necessity and proportionality.[27] The constitutional protections have been applied in practice to invalidate specific legislative provisions.

In 2014, the Constitutional Court of Zimbabwe relied on the constitutional protection for freedom of expression (under Zimbabwe's previous constitution) to declare the offence of criminal defamation unconstitutional in the *Madanhire* case. The case concerned charges of criminal defamation against a journalist and an editor after the publication of an article critical of a medical aid company. The relevant statute was section 96 of the Criminal Law Code, which made dissemination of false information with intent to cause harm to the reputation of another person punishable by a fine or a maximum of two years imprisonment. Although the Court found the law to be rationally related to the important objective of protecting the reputation, rights and freedoms of others, it found that the criminalization of defamatory statements lacked proportionality and was not a necessary means to protect reputation. The Court also noted that criminal sanctions for the publication of inaccurate or erroneous statements had the inherent effect of silencing the free flow of information on public matters. It viewed the monetary damages for of civil defamation as a more appropriate way to protect reputation.[28] In 2016, the Constitutional Court affirmed that section 96 of the Criminal Law Code is equally void under Zimbabwe's current Constitution, in the case of *MISA-Zimbabwe v Minister of Justice*.[29]

Section 50(2)(a) of the Law and Order (Maintenance) Act, 1960 (which is no longer in force) previously made it an offence to make, publish or reproduce any "false statement, rumour or report which (a) is likely to cause fear, alarm or despondency among the public or any section of the public or (b) is likely to disturb the public peace". In 2000, in the *Chavunfuka* case, the Supreme Court of Zimbabwe declared the provision unconstitutional (under the previous Zimbabwe Constitution). The case followed on the arrest of the author of a 1999 article describing a failed *coup d'etat* and the subsequent arrest of twenty-three soldiers. The article claimed that the insurrection was inspired by dissatisfaction with the mismanagement of the economy and Zimbabwe's involvement in war in the Democratic Republic of the Congo. The editor of the publication where the article appeared was also arrested. The Supreme Court found that the provision in questions did not constitute a justifiable limitation of the freedom of expression because it was too vague and arbitrary to be qualify as a restriction imposed under the authority of law. The following were relevant factors:

- the provision not only criminalised statements that *actually* caused fear, alarm or despondency, but also statements that were *likely* to do so; the law required no proof of any damage to the state or impact on the public;
- given that the relevant provision was concerned with *likelihood* rather than *reality,* it was too vague to give clear guidance and could thus discourage expression by persons wary of prosecution;

[27] Zimbabwe's 2013 Constitution, as amended through 2017, sections 61 and 86 (quoted in the table at the beginning of this chapter).
[28] Madanhire & Another v AG (Judgment No CCZ 2/14, Const. Application No CCZ 78/12) [2014] ZWCC 2 (12 June 2014); see the summary of case by Global Freedom of Expression here.
[29] MISA-Zimbabwe v Minister of Justice (Const. Application No CCZ 7/15) (order available here); see the summary of the case by Global Freedom of Expression here and the summary by Southern Africa Litigation Centre here.

- the expression "fear, alarm or despondency" was overbroad since anything that is newsworthy is likely to cause some of these emotions in some members of the public;

- the use of the word "false'" was too wide, because it covered inaccurate statements, rumours or reports as well as intentional lies, and the law does not require actual knowledge of the statement 's falsity to impose liability; thus, the law criminalises negligence.

The entire law was later replaced by the **Public Order and Security Act, 2002**, which includes no comparable provision.[30]

In 2021, the Constitutional Court ruled in the *Chimakure* case that **section 31(a)(iii) of the Criminal Law (Codification and Reform) Act** was invalid in terms of the previous Constitution. Two journalists were charged with violating this provision, which made the **reporting of false news that would undermine public confidence in the uniformed forces** punishable with a significant fine and a prison sentence of up to twenty years. Their publication had accused intelligence and police officials of involvement in the abduction of opposition and human rights activists in 2008. The Court issued an initial order stating that the provision restricted freedom of expression as protected under the previous Constitution, and the State failed to put forward reasons to show that the restriction was justifiable – with the effect being that the provision in question was declared void.[31] (The other prohibitions on false news in section 31 of this Act remain in force and are discussed below.)

In 2019, on the second day of a stay-away called by the Zimbabwe Congress of Trade Unions, the Minister of State in the President's Office for National Security issued **a directive under section 6 of the Interception of Communications Act ordering the suspension of all** *internet services – which effectively also shut down* email services and social media platforms. The directive was challenged by three individual journalists and MISA Zimbabwe, who asserted (amongst other things) that the Act did not give authority to the Minister of State to issue directives (since the President had reserved administration of the Act to himself under a statutory instrument issued in terms of the Act), that section 6 of the Act did not authorise a blanket suspension of Internet services and that section 6 violated the constitutional protection for freedom of expression, producing disproportionate disruption of services and loss of income to ordinary citizens and businesses. The government defended its actions on the basis of national security, asserting that the Internet shutdown was aimed at preventing violence and illegal activity. The Court invalidated the directive to suspend Internet services on the narrow basis that it had not been issued by the President, without reaching the broader constitutional issues.[32]

[30] Chavunfuka v Minister of Home Affairs 2000 JOL 6540 (ZS); see the summary of the case by Global Freedom of Expression here.
[31] Chimakure v Attorney-General of Zimbabwe (Judgment No. CCZ 6/201411, Const. Application No. CCZ 247/09), 22 July 2014; see the analysis of the case by Global Freedom of Expression here.
[32] Zimbabwe Lawyers for Human Rights v. Minister of State, National Security, HC 261/19, 21 January 2021. See Veritas, "Court Watch: Internet Shutdown Case – High Court's Ruling", as published in The Zimbabwean, 1 February 2019; "High Court sets aside internet shut down directives", MISA-Zimbabwe. 21 January 2019; "Freedom on the Net 2022: Zimbabwe", Freedom House, section B3; and case analysis by Global Freedom of Expression here.

It appears noteworthy that the Constitution specifically protects "the confidentiality of journalists' sources of information",[33] but Reporters Without Borders reports that the confidentiality of sources is not actually respected in practice.[34]

18.3 CASE STUDIES

The 2022 Bertelsmann Transformation Index provides this overview of shrinking civic space and violence and harassment against journalists in recent years:

> *In the past two years, the hope for positive change in Zimbabwe after the departure of former President Robert Mugabe has been effectively dashed. Under President Emmerson Mnangagwa's "new dispensation" many of the country's challenges remained unaddressed or even intensified. Zimbabwe's multi-faceted crisis was further exacerbated by this and the impact of COVID-19. Its continued economic decline was characterized by high prices, cash shortages and a huge debt overhang. The phased reintroduction of the Zimbabwe dollar led to record inflation, which peaked at over 700% in July 2020 and nearly eradicated the income of many Zimbabweans. The economic decline resulted in a severe humanitarian crisis, with over seven million Zimbabweans in need of food aid at the end of 2020, according to the U.N.*
>
> *Of particular concern in the past two years have been the further shrinking of democratic space and the failure to uphold constitutionalism. The January 2019 crackdown by the state security apparatus, which responded with disproportionate force to protests over poor living conditions, was followed by two years of increased repression against opposition members, activists, journalists and other actors. The most notable cases were the abduction, torture, sexual abuse and subsequent arrest of three female opposition leaders in 2020 and the repeated arrest and detention of prominent journalist Hopewell Chin'ono after he had exposed government corruption. The government's systematic repression made use of an increasingly partisan judiciary, which led to lengthy pretrial detentions of opposition members, activists and journalists. These arrests have led to further polarization of the political domain and to a continued stalemate between the ZANU-PF (Zimbabwe African National Union-Patriotic Front) and the MDC Alliance, which also negatively affected the prospects for a much-needed national dialogue process.*[35]

According to Reporters without Borders, "levels of violence against journalists have declined significantly under the Mnangagwa administration" but still remain alarmingly high, meaning that self-censorship is routinely practiced to avoid reprisals. It is also reported that police often use disproportionate force against journalists and confiscate their equipment. Intimidation, verbal attacks and threats (especially on social media) are also common practices. Cases of journalists being imprisoned and prosecuted are more rare than in the past, but journalists' phone communications are often subject to surveillance.[36]

[33] Id, section 61(2).
[34] "2023 World Press Freedom: Zimbabwe", Reporters Without Borders, "Legal Framework".
[35] "Zimbabwe Country Report 2022", BTI (Bertelsmann Transformation Index), Bertelsmann Stiftung, "Executive Summary".
[36] "2023 World Press Freedom: Zimbabwe", Reporters Without Borders. "Safety".

In 2022, Freedom House reported that "[b]oth journalists and ordinary users continued to face arrest and harassment for their online activities, particularly those that criticize President Emmerson Mnangagwa's government."[37]

Amnesty International reports that three journalists were the first persons to be arrested under the **Criminal Law Codification and Reform Act , as amended by the Cyber and Data Protection Act,** in 2022. The first two to be arrested were editor Wisdom Mdzungairi and senior reporter Desmond Chingarande. After publishing a news story on a private business enterprise allegedly operated by individuals with government connections, they were charged with **transmitting "false data intending to cause harm"**. Freelance sports journalist Hope Chizuzu was arrested on the same charge after board members of the Dynamos Football Club filed a complaint against him. Police reportedly confiscated his mobile phone and iPad for the purpose of further investigations.[38]

Other arrests have been based on **cyberbullying**. In May 2022, Raymond Chari was reportedly charged with cyberbullying in violation of **section 164B of the Criminal Law Codification and Reform Act, as amended in the Cyber and Data Protection Act** for allegedly using foul language to describe the Zimbabwean ambassador to Tanzania and his wife in a WhatsApp group. Also in May 2022, television actor David Kanduna was reportedly fined for cyberbullying after he posted a video to WhatsApp and Tik Tok which showed an incident at a local university where a police officer was heckled.[39]

The **Criminal Law (Codification and Reform) Act** has been the basis of numerous arrests for offences related to expression:

- In August 2022, editor Wisdom Mdzungairi and senior reporter Desmond Chingarande were charged with **publishing false data messages intending to cause harm in contravention of section 164C of the Criminal Law (Codification and Reform) Act, as amended by the Cyber and Data Protection Act**. The charge stemmed from a news story alleging that a local cemetery was being run without government approval.[40]
- In January 2021, Vongai Chiminya and Devine Panashe Maregere were charged with **communicating false statements prejudicial to the State in violation of section 31(a)(i) of the Criminal Law (Codification and Reform) Act** for sending an audio message to a WhatsApp group claiming that President Mnangagwa had died from COVID-19. Neither Chiminya nor Maregere were the original creators of the audio message, and there was reportedly no evidence that sharing the message cause any public harm.[41]
- In April 2020, an opposition politician, Chrispen Rambu, was charged under

[37] "Freedom on the Net 2022: Zimbabwe", Freedom House, "Overview".
[38] Amnesty International Report 2022/23, "Zimbabwe 2022"; "Zimbabwean journalist Hopewell Chin'ono denied bail", Reporters Without Borders, 12 November 2020.
[39] Freedom on the Net 2022: Zimbabwe", Freedom House, section C3; Otto Saki and Nompilo Simanje, "Affordable connectivity and privacy violations plague Zimbabwe", Association for Progressive Communications, 8 November 2022.
[40] "LEXOTA Country Analysis: Zimbabwe", last updated May 2023; "Journalists charged with publishing false data messages", African Freedom of Expression Exchange, 6 August 2022.
[41] "LEXOTA Country Analysis: Zimbabwe", last updated May 2023.

section 33 of the **Criminal Law (Codification and Reform) Act** for calling President Mnangagwa a fool in a WhatsApp message. Two other persons, Robert Zakeyo and Admire Mupemhi, were charged the **undermining the authority of the President in violation of section 33(2)(b) of the Criminal Law (Codification and Reform) Act** for sharing a video clip on which criticised President Mnangagwa's economic policies and referred to him as a frog. Another man, Goodman Musariri, was also arrested in April 2020 for **undermining the authority of the President in violation of this provision**, for a WhatsApp message saying that President Mnangagwa had nothing to offer the country and so should resign.[42]

- In April 2020, Lovemore Zvokusekwa was arrested and charged for **publishing or communicating false statements prejudicial to the state under section 31 of the Criminal Law (Codification and Reform) Act**. on the basis that he had instigated a rumour about a planned extension of the COVID-19 lockdown by 13 days, which the president later denied. State authorities claimed that the rumour was causing public distress and unrest, and that it posed a threat to public health. However, the rumour later proved to be true when the lockdown was in fact extended.[43]
- Prominent journalist Hopewell Chin'ono (winner of CNN's African Journalist of the Year award in 2008) was arrested in January 2021, for **publishing false information** for a statement on Twitter that a police officer had beaten a child to death while enforcing COVID-19 restrictions. He was granted bail, once again subject to limits on his Twitter usage. These charges were thrown out in April 2021, when **section 31(a)(iii) of the Criminal Law (Codification and Reform) Act was ruled unconstitutional.**[44]

There have been internet shutdowns in Zimbabwe in recent years. In January 2019, a total **internet shutdown** was ordered by a warrant issued pursuant to the Interception of Communications Act – which (as discussed in more detail below) provides for the interception of telecommunications to fight crime and protect national security. It defines interception as "to listen to, record, or copy" a communication. The law makes no reference to blocking or disrupting communication services. In 2016, the government disrupted Internet-based communications without referring to the Interception of Communications Act. On that occasion, there was a partial shutdown for about four hours that targeted social media websites.[45]

Problematic government attitudes are illustrated by some of the statements that have been reported in recent years. A presidential spokesperson stated that the 2017 creation of a new Ministry of Cyber Security, Threat Detection and Mitigation was

[42] Freedom on the Net 2022: Zimbabwe", Freedom House, section C3.
[43] "LEXOTA Country Analysis: Zimbabwe", last updated May 2023.
[44] Id. Chin'ono has been repeatedly arrested under various laws for his online reporting activities. for instance, in July 2020, he was charged with **incitement to violence** in connection with photos and videos anti-government protests posted on Twitter, with some speculating that his arrest could have been a consequence of series of Facebook posts alleging that the president's son was involved in corrupt business dealings related to government contracts for medical supplies. Chin'ono was released on bail in September 2020, but banned from using social media for his activism as part of his bail conditions. In November 2020, Chin'ono was arrested for violating his bail conditions with a Twitter post about the initial denial of bail in his case. He was granted bail again in November 2020, on the condition that he would not anything on Twitter that would "obstruct justice."
[45] "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 8.

aimed at catching mischievous elements using social media.[46] Freedom House reports that President Mnangagwa has referred to online campaigns against human rights abuses and corruption as "a cyber-war on our country in pursuit of a regime change agenda."[47] In November 2021, the Minister of Information, Publicity, and Broadcasting Services announced that the government had set up a "cyber-team" for the purpose of monitoring social media.[48] It is reported that, in April 2022, the Permanent Secretary for the Ministry of Information suggested enactment of a law that criminalizes "campaigning against one's own country," following an address by journalist Hopewell Chin'ono on the state of human rights in Zimbabwe at a summit in Geneva.[49] It all points to concerns that criticisms of government will not be tolerated.

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

A) CRIMINAL LAW (CODIFICATION AND REFORM) ACT [CHAPTER 9:23] AS AMENDED BY THE CYBER AND DATA PROTECTION ACT, 2021 [CHAPTER 12:07]

The Cyber and Data Protection Act was previously called the Data Protection Act. Its title was changed when the law was amended in February 2022.[50] One analysis notes that this law "borrows extensively from the SADC Model Law; and "also leans heavily towards the Tanzanian Cybercrime Act".[51]

The wisdom of combining cybersecurity and data protection in one law, under one consolidated regulatory authority has been questioned.[52] However, in fact, the substantive provisions on cybercrimes are all actually contained in the **Criminal Law (Codification and Reform) Act *as amended by* the Cyber and Data Protection Act,**[53] with the Cyber and Data Protection Act itself being exclusively a data protection law. (The Criminal Law (Codification and Reform) Act is the current version of Zimbabwe's general penal code.)

The procedural issues relating to cybercrime are all contained in the **Criminal**

[46] Malvern Mkudu, "Policy Brief: Zimbabwe's Cyber Crime and Cyber Security Bill 2017", 2018.
[47] Id, section B8, citing "Zimbabweans unfazed by cyber attacks", *The Herald*, 28 August 2020.
[48] "Freedom on the Net 2022: Zimbabwe", Freedom House, section B4; Otto Saki and Nompilo Simanje, "Affordable connectivity and privacy violations plague Zimbabwe", Association for Progressive Communications, 8 November 2022.
[49] "Freedom on the Net 2022: Zimbabwe", Freedom House, section B4.
[50] This law replaced sections 163-166 of the Criminal Law (Codification and Reform) Act [Chapter 9:23] with new provisions, added new provisions to the Criminal Procedure and Evidence Act [Chapter 9:07] and amended the Interception of Communications Act [Chapter 11:20].
[51] "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights", MISA-Zimbabwe/Konrad Adenauer Stiftung, [2021], page 32.
[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 35; "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights", MISA-Zimbabwe/Konrad Adenauer Stiftung, [2021], page 33.
[53] Criminal Law (Codification and Reform) Act [*Chapter 9:23*] as amended by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*]. section 35.

Procedure and Evidence Act *as amended by* the Cyber and Data Protection Act[54] and in the **Interception of Communications Act *as amended by* the Cyber and Data Protection Act.**[55] Some of these laws also have provisions pre-dating the Cyber and Data Protection Act that could compromise freedom of expression.

The computer-dependent offences are listed in the following table. One shortcoming with almost all of these offences (with the exception of section 165E) is that they fail to make provision for lawful justification, such as acting in good faith in the public interest or testing for security vulnerabilities.

CRIMINAL LAW (CODIFICATION AND REFORM) ACT AS AMENDED BY THE CYBER AND DATA PROTECTION ACT, 2021 - TECHNICAL OFFENCES	
Section 163: Hacking	It is an offence for a person who knows or suspects that he or she must obtain prior authority to access data, a computer programme, a computer data storage medium, or the whole or any part of a computer system, to secure such access intentionally, unlawfully and without such authority. o To "secure access" "includes - (a) to obtain, to make use of, gain entry into, view, display, instruct or communicate with, or store data in or retrieve data from; (b) to copy, move, add, change or remove data, critical data or a critical database, or otherwise to make use of, configure or reconfigure any resources of a computer device, a computer network, a database, a critical database, an electronic communications network, a critical information infrastructure, whether in whole or in part, including their logical, arithmetical, memory, access codes, transmission, data storage, processor or memory function, whether physical, virtual, by direct or indirect means or by electronic, magnetic, audio, optical or any other means." (section 163(2)) o This description helpfully narrows the offence beyond just logging onto a computer or computer system without authorisation.
Section 163A: Unlawful acquisition of data	It is an offence to unlawfully and intentionally - • intercept by technical or any other means any private transmission of computer data to, from or within a computer network, computer device, database or information system or electromagnetic emissions from a computer or information system carrying such computer data; • overcome or circumvent any protective security measure intended to prevent access to data; • acquire data within a computer system or data which is transmitted to or from a computer system. o For the purposes of this offence, "acquire" includes "to use, examine, capture, copy, move to a different location or divert data to a destination other than its intended location".

[54] Criminal Procedure and Evidence Act [*Chapter 9:07*], as amended by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*], section 36.
[55] Interception of Communications Act, 2007 [*Chapter 11:20*], as amended by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*], section 37.

	○ The offence does *not* appear to apply to the use of data unlawfully acquired from a computer system by another person (as in the case of journalistic use of Wikileaks material).
Section 163B: Unlawful interference with data or data storage medium	It is an offence to unlawfully and intentionally interfere with computer data or a data storage medium by - • damaging, corrupting, impairing or deteriorating computer data; • deleting computer data; • altering computer data; • rendering computer data meaningless, useless or ineffective; • obstructing, interrupting or interfering with the lawful use of computer data; • obstructing, interrupting or interfering with any person in the lawful use of computer data; • denying, hindering, blocking access to computer data to any person authorised to access it; or • maliciously creating, altering or manipulating any data, programme or system in whole or in part which is intended for installation in a computer.
Section 163C: Unlawful interference with computer system	It is an offence to unlawfully and intentionally interfere with the use of a computer or information system, a computer device, an electronic communications system or critical information infrastructure by blocking, hindering, impeding, interrupting, altering or impairing access to it, or its functioning or integrity.
Section 163D: Unlawful disclosure of data code	It is an offence to unlawfully and intentionally - • communicate, disclose or transmit any computer data, programme, access code or command or any other means of gaining access to any programme or data held in a computer or information system to any person not authorised to access the computer data, programme, code or command for any purpose; • activate, install or download a programme that is designed to create, destroy, mutilate, remove or modify any data, programme or other form of information existing within or outside a computer or computer system; • creates alter or destroy a password, personal identification number, code or any method used to access a computer or computer network. The offence applies regardless of whether the intended effect of the illegal interference is permanent or temporary. There is provision for an enhanced penalty where this offence is committed in relation to data that forms part of a database, or involves national security or the provision of an essential service. There is an exception for actions "authorised under the law" or "pursuant to measures that can be taken in terms of section 39". ○ It is unclear what is covered by the exception that references "section 39". Section 39 of the Criminal Law Code concerns dealing in or possession of prohibited knives, and there is no section 39 in the Cyber and Data Protection Act. Thus, the import of this exception cannot be assessed.

Section 163E: Unlawful use of data or devices	It is an offence to unlawfully and intentionally acquire, possess, produce, sell, procure for use, import, distribute, supply, use or make available an access code, password, a computer programme designed or adapted for the purpose of committing an offence, or any similar data or device by which the whole or any part of a computer or information system is capable of being accessed, for purposes of the commission or attempted commission of an offence in terms of this Act. It is also an offence to unlawfully and intentionally assemble, obtain, sell, purchase, possess, make available, advertise or use malicious software, programmes or devices for purposes of causing damage to data, computer or information systems and networks, electronic communications networks, critical information infrastructure or computer devices. o The title of this offence is somewhat misleading since it does not cover data in the simplest sense of the term, but only applies to access codes, passwords, computer programmes and malicious software. o The criteria that the items covered must be for the purpose of committing an offence, or for causing damage, keeps the offence appropriately narrow.
Section 163F: Aggravating circumstances	The aggravating circumstance listed in this section warrant enhanced penalties for all of the offences listed here except for section 163D which lists its own basis for enhanced penalties. It is an aggravating circumstance where the offence - • was committed in connection with a crime against the State specified in Part III of the Criminal Law (Codification and Reform) Act; • was intended for or results in damaging, destroying or prejudicing the safe operation of an aircraft; • was intended to conceal or disguise the proceeds of unlawful dealing in or partaking of dangerous drugs • results in defeating or obstructing the course of justice; • seriously prejudices the enforcement of the law by any law enforcement agencies; • involved any computer, computer network, information communications network data, programme or system owned by the State, a law enforcement agency, the Defence Forces, the Prison Service, a statutory corporation or a local authority; • results in considerable material prejudice or economic loss to the owner of the computer, computer network, data, programme or system; • seriously interferes with or disrupts an essential service; • was committed in furtherance of organised crime or the perpetrator was part of an organised criminal gang. o The enhancement of penalties where cybercrimes are committed in connection with crimes against the State listed in Part III of the Criminal Law (Codification and Reform) Act covers a number of offences that unreasonably compromise freedom of expression (sections 30, 31 and 33, all discussed below).

As in other SADC countries, it is the content-based offences which are the most problematic for freedom of expression. The offences described in the table below were introduced into the law by the Cyber and Data Protection Act.

CRIMINAL LAW (CODIFICATION AND REFORM) ACT AS AMENDED BY THE CYBER AND DATA PROTECTION ACT, 2021 - CONTENT-BASED OFFENCES	
Section 164: Transmission of data message inciting violence or damage to property	It is an offence to unlawfully by means of a computer or information system make available, transmit, broadcast or distribute a data message to any person, group of persons or the public with intent to incite such persons to commit acts of violence against any person or persons or to cause damage to any property. o According to MISA-Zimbabwe: "Provisions such as these are at risk of being relied on to inhibit constructive criticism which is important for promoting transparency and accountability especially from the government. There is therefore a danger that such provisions will be used as political tools and mechanisms by the state to prevent the expression of dissenting opinions. This will potentially stifle citizen engagement and open debate, both of which are necessary elements to promote democracy."[56] o Another assessment states that this provision "can easily be used to inhibit constructive criticism, which is important for promoting transparency and accountability especially from the government. In a context of polarized politics and retribution, such provisions can be used as political tools and mechanisms by the state to prevent the expression of dissenting opinions. In the end, such a provision can contribute immensely towards stifling citizen engagement and open debate, which are essential building blocks for electoral and constitutional democracy."[57]
Section 164A: Sending threatening data message	It is an offence to unlawfully and intentionally by means of a computer or information system send any data message to another person threatening "harm" to the person or the person's family or friends or damage to the property of such persons. This section includes an additional offence that appears to be misplaced. It is an offence for any person to "up skirt" and record nude images or videos of a citizen, or a foreigner who is resident in Zimbabwe, without consent. o Note that the formulation of the first offence covers messages sent via social media. o The first offence should be limited to threats of "physical harm", so as not to be confused with reputational harm. It otherwise amounts to a reintroduction of criminal defamation, which has been declared unconstitutional.[58]

[56] "Cybersecurity and Data Protection Bill entrenches surveillance: MISA Zimbabwe analysis of the Cybersecurity and Data Protection Bill, 2019". MISA-Zimbabwe, undated (accessed 26 June 2023)
[57] "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights", MISA-Zimbabwe/Konrad Adenauer Stiftung, [2021], page 34.
[58] See section 13.2 above.

	○ Although not the subject of this paper, it is curious that the second offence provides no protection for the invasion of the privacy of non-residents.
Section 164B: Cyber-bullying and harassment	This offence has been used to inhibit freedom of expression in practice and so is quoted in full. Any person who unlawfully and intentionally by means of a computer or information system generates and sends any data message to another person, or posts on any material whatsoever on any electronic medium accessible by any person, with the intent to coerce, intimidate, harass, threaten, bully or cause substantial emotional distress, or to degrade, humiliate or demean the person of another or to encourage a person to harm himself or herself, shall be guilty of an offence and liable to a fine not exceeding level 10 or to imprisonment for a period not exceeding ten years or to both such fine and such imprisonment. ○ MISA Zimbabwe notes that this offence criminalises not only the generation but also the communication of such offensive messages through any electronic medium, which includes social media. [59] ○ The intentionality required for this offence is low and vague, with key terms such as "harass", "bully" and "substantial emotional distress" left undefined. ○ The potential term of imprisonment is extremely disproportionate, given that any imprisonment for an offence based entirely on expression is widely considered to be inappropriate.
Section 164C: Transmission of false data message intending to cause harm	This is another overbroad offence that has been used to inhibit freedom of expression in practice, quoted here in full. Any person who unlawfully and intentionally by means of a computer or information system makes available, broadcasts or distributes data to any other person concerning an identified or identifiable person knowing it to be false with intend [sic] to cause psychological or economic harm shall be guilty of an offence and liable to a fine not exceeding level 10 or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment. ○ The fact that this offence is committed if there is an intent to cause either "psychological or economic harm" makes it very likely to inhibit reports of wrongdoing, since allegations of corruption or abuse of government power may not be known to be fully "true" until adjudicated. ○ It appears that this offence might be committed even if a report is substantially true, and there is no exception for fair comment in the public interest. ○ This offence also appears to reintroduce of criminal defamation, which has been declared unconstitutional.[60] ○ As in the case of offence above, the potential term of imprisonment is extremely disproportionate, given that any imprisonment for an

[59] "Cybersecurity and Data Protection Bill entrenches surveillance: MISA Zimbabwe analysis of the Cybersecurity and Data Protection Bill, 2019". MISA-Zimbabwe, undated (accessed 26 June 2023).
[60] See section 13.2 above.

	offence based entirely on expression is widely considered to be inappropriate. o According to one analysis: "It is not clear how it would be determined whether a message was "false" or the scope of "psychological or economic harm". Additional guidance is also needed on whether this provision applies to legal or natural persons. Section 164C therefore fails to provide clear guidance for individuals and provides an overly wide degree of discretion to those charged with the enforcement of this law.[61] o Another analysis also highlights the complexities of distinguishing truth from falsehood in this context: "This clause ignores the fact that there are multiple truths and various regimes of truth and non-truth. Even more important it ignores the fact that on the internet and social media platforms it difficult to determine the origin and authenticity of a message. In such an environment, individuals are exposed to communication messages voluntarily or involuntarily. In a context, where a culture of citizen journalism and blogging has taken route, this provision can be abused to implicate thousands of ordinary citizens who would have 'received' and communicated such messages."[62]
Section 164D: Spam	It is an offence to "intentionally and without lawful excuse" – • to use a protected computer system to relay or retransmit multiple electronic mail messages, with the intent to deceive or mislead recipients or any electronic mail or internet service provider as to the origin of such messages; • to materially falsifies header information in multiple electronic mail messages and initiate the transmission of such messages.
Section 164E: Transmission of intimate images without consent	It is an offence to unlawfully and intentionally by means of a computer or information system make available, broadcast or distribute a data message containing any intimate image or video of an identifiable person without the consent of the person concerned or with recklessness as to the lack of consent of the person concerned, with the aim of causing the humiliation or embarrassment of such person. An 'intimate image" for this purpose is a "visual depiction of a person made by any means in which the person is nude, the genitalia or naked female breasts are exposed or sexual acts are displayed". o The fact that the offence requires an aim of causing humiliation or embarrassment should protect persons who send such images for legitimate purposes, such as in genuine artistic material.
Section 164F: Production and dissemination of racist and xenophobic material	It is an offence "unlawfully and intentionally through a computer or information system - • to produce racist or xenophobic material for the purpose of its distribution (or to cause this to happen); • to offer, make available or broadcast racist or xenophobic material (or to cause this to happen); • to distribute or transmit racist or xenophobic material (or to cause this to happen);

[61] "LEXOTA Country Analysis: Zimbabwe", last updated May 2023.
[62] "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights", MISA-Zimbabwe/Konrad Adenauer Stiftung, [2021], page 34.

	• to use language that tends to lower the reputation or feelings of persons for the reason that they belong to a group of persons distinguished on the grounds set out in section 56(3) of the Constitution or any other grounds whatsoever, if used as a pretext for any of these factors. o Racist or xenophobic material" is not defined. The final point appears very broad and vague, since it appears to cover hurt feelings. However, it appears consistent with the provisions on hate speech in the Malabo Convention and the SDC Model Law on cybercrime which both cover "insult". Some laws criminalise hate speech only where it incites hatred, discrimination or violence on the prohibited grounds.
Section 164G: Identity-related offence	There seems to be an error in the law as this offence is almost identical to section 164B on cyberbullying and cyber harassment. (Several online versions were accessed, and all had the same version of section 164G.) The only substantive difference is that this provision states that special consideration must be given to a child who is found guilty of this offence, who must not be sentenced to imprisonment or acquire a criminal record as a result.
The amendments to the Criminal Law (Codification and Reform) Act also contain offences relating to - • the non-consensual recording of the genitalia and buttocks beneath clothing, or the sharing of such images by means of a data message (section 165) • child sexual abuse material [i.e., child pornography] and grooming of a child (section 165A) • exposing children to pornography for the purpose of grooming (section 165B). These offences do not appear to pose any problems, as they appear to limit freedom of expression in justifiable ways.	

Amnesty International has warned that the new offences have been used to intimidate and harass journalists for doing their work and threaten to further curtail media freedom in Zimbabwe.[63]

According to Dr. Allen Munoriyarwa, a senior media studies lecturer at the University of Botswana, the insertion of some of the content-based 'new offences' was "deliberate to try and balance public demands with the political survival" of the ruling party.[64] Munoriyarwa stated that on the one hand the politicians realise that they have to legislate on issues in the public interest, such as dealing with online harms, but on the other they then also exploit these law making processes to create laws that can be used for repressive purposes because such laws "give them ways of deploying surveillance capabilities".

[63] "East and Southern Africa: Attacks on journalists on the rise as authorities seek to suppress press freedom", Amnesty International, 3 May 2023.
[64] Dr Allen Munoriyarwa was interviewed via Zoom on 25 July 2023.

Some worrying content-based offences in Part III of the Criminal Law (Codification and Reform) Act ("Crimes against the State") pre-date the Cyber and Data Protection Act and remain in force. One small safeguard is that prosecution for any of the offences listed in the table below requires authorisation from the Attorney General,[65] but this is not sufficient to overcome the freedom-of-expression concerns and does nothing to prevent the existence of the crimes from inhibiting robust political discussion and debate.

CRIMINAL LAW (CODIFICATION AND REFORM) ACT - CONTENT-BASED OFFENCES	
Section 30: Causing disaffection among Police Force or Defence Forces	If any person who, whether inside Zimbabwe induces, or attempts to induce, or does any act with the intention or realising that there is a real risk or possibility of inducing or causing any member of the Police Force or Defence Forces to withhold his or her services, loyalty or allegiance or to commit breaches of discipline, he or she shall be guilty of causing disaffection among the Police Force or Defence Forces and liable to a fine not exceeding level seven or imprisonment for a period not exceeding two years or both. o Due to the reference to "real risk or possibility" in connection with intent, it is conceivable that this offence could capture the publication of allegations of corruption or mismanagement in the armed forces, even if (and perhaps particularly if) the allegations were true.
Section 31: Publishing or communicating false statements prejudicial to the State	Any person or outside Zimbabwe - (a) publishes or communicates to any other person a statement which is wholly or materially false with the intention or realising that there is a real risk or possibility of- (i) inciting or promoting public disorder or public violence or endangering public safety; or (ii)adversely affecting the defence or economic interests of Zimbabwe; or (iv) interfering with, disrupting or interrupting any essential service; shall, whether or not the publication or communication results in a consequence referred to in subparagraph (i), (ii), (iii) or (iv); or (b)with or without the intention or realisation referred to in paragraph (a), publishes or communicates to any other person a statement which is wholly or materially false and which - (i) he or she knows to be false; or (ii) he or she does not have reasonable grounds for believing to be true; shall, if the publication or communication of the statement- A. promotes public disorder or public violence or endangers public safety; or B. adversely affects the defence or economic interests of Zimbabwe; or C. undermines public confidence in a law enforcement agency, the Prison Service or the Defence Forces of Zimbabwe; or D. interferes with, disrupts or interrupts any essential service;

[65] Criminal Law (Codification and Reform) Act [*Chapter 9:23*], section 34.

	be guilty of publishing or communicating a false statement prejudicial to the State and liable to a fine up to or exceeding level fourteen or imprisonment for a period not exceeding twenty years or both. o This provision has been frequently applied in practice to restrict freedom of speech, including online speech. o Paragraph (a)(iii) was found to be an unconstitutional restriction on freedom of expression, with the reasoning in the case suggesting that other aspects of the law which have not yet been challenged might also raise constitutional problems. o The intention in subsection (a) is very broad since it covers "realising that there is a real risk or possibility" of the indicated harms and does not require that any of the listed consequences actually resulted. Subsection (b) is conversely based on a result without requiring intention (or even recklessness) to produce that result. o One analysis state: "It is not clear how a statement would be determined 'wholly or materially false' or what the threshold is for deciding whether there is a 'real risk' of 'adversely affecting the defence or economic interests of Zimbabwe. Section 31 thus fails to provide clear guidance for individuals to conform their behaviour and provides an overly wide degree of discretion to those charged with the enforcement of this law."[66]
Section 33: Undermining authority of or insulting President	(1) In this section - "publicly", in relation to making a statement, means - (a) making the statement in a public place or any place to which the public or any section of the public have access; (b) publishing it in any printed or electronic medium for reception by the public; "statement" includes any act or gesture. (2) Any person who publicly, unlawfully and intentionally - (a) makes any statement about or concerning the President or an acting President with the knowledge or realising that there is a real risk or possibility that the statement is false and that it may - (i) engender feelings of hostility towards; or (ii) cause hatred, contempt or ridicule of; the President or an acting President, whether in person or in respect of the President's office; or (b) makes any abusive, indecent or obscene statement about or concerning the President or an acting President, whether in respect of the President personally or the President's office; shall be guilty of undermining the authority of or insulting the President and liable to a fine not exceeding level six or imprisonment for a period not exceeding one year or both. o MISA Zimbabwe notes that this offence criminalises not only the generation but also the communication of such offensive messages through any electronic medium, which includes social media. [67]

[66] "LEXOTA Country Analysis: Zimbabwe", last updated May 2023.
[67] "Cybersecurity and Data Protection Bill entrenches surveillance: MISA Zimbabwe analysis of the Cybersecurity and Data Protection Bill, 2019". MISA-Zimbabwe, undated (accessed 26 June 2023)

	○ The intentionality required for this offence is low and vague, with key terms such as "harass", "bully" and "substantial emotional distress" left undefined. The potential term of imprisonment is extremely disproportionate, given that any imprisonment for an offence based entirely on expression is widely considered to be inappropriate.
Another problematically broad content-related provision, contained in another chapter of the Criminal Law (Codification and Reform) Act, makes it an offence **to use threatening, abusive or insulting words at a public gathering** (amongst other acts) with the intention of preventing the transaction of the business for which the gathering was called, or realising that there is a real risk or possibility of this result (section 44). We have not found any examples of this provision being used in practice purely against speech. Section 95 of the Criminal Law (Codification and Reform) Act contains the offence of **criminal insult** which applies to words or conduct that seriously impairs the dignity or invades the privacy of another person, punishable by a fine not exceeding level six or imprisonment for a period not exceeding one year or both. Many of the same problems that apply to criminal defamation - which has been ruled unconstitutional – would also be relevant to criminal insult.	

In July 2023, a new offence of **wilfully injuring the sovereignty and national interest of Zimbabwe** was added to the Criminal Law (Codification and Reform) Act, by the Criminal Law Codification and Reform Amendment Act – referred to by the Government during its discussion as the "Patriots Bill" or the "Patriotic Bill". This new offence prohibits actively taking part in a meeting, inside or outside Zimbabwe, that considers armed intervention in Zimbabwe by a foreign government, "subverting, upsetting, overthrowing or overturning the constitutional government in Zimbabwe", sanctions or a trade boycott. The penalty for some manifestations of this offence is the same as for treason, which can be punished by life imprisonment.[68] This would constitute a wildly disproportionate sentence. The bill was widely criticised, domestically and internationally. For instance, the Southern Africa Litigation Centre comments: "The criminalisation of any communication constitutes an immediate threat to the constitutional right to freedom of expression. The vague and broad wording of the suggested provision is further appalling as it constitutes a high potential of abuse and misuse by state authorities to silence any dissent or criticism of state authorities."[69]

Echoing these sentiments, Dr Munoriyarwa stated that the "Patriotic Bill" was "basically tailored against the people who speak up against the ruling party, it is basically an attempt to stifle opposition" and that it was also "tailored against activists, tailored against the journalists. You don't know what to write and you don't know what not to write" as "anything can be damaging of the national interest". Munoriyarwa was of

[68] Criminal Law Codification and Reform Amendment Bill [H.B. 15, 2022], clause 2 which would insert a new section 22A into the Criminal Law (Codification and Reform) Act [*Chapter 9:23*]. See section 20 of this law for the penalty for treason. Section 20 refers to the death penalty, but section 48 of the 2013 Constitution states that the death penalty may be imposed only for murder committed in aggravating circumstances. The Act was published as a bill 23 December 2022. The Bill was passed by the lower house of the National Assembly on 31 May 2023 and by the Senate on 7 May 2023. It was signed by the President on 14 July 2023. "Zimbabwe: President's signing of 'Patriotic Bill' a brutal assault on civic space", Amnesty International, 15 July 2023.

[69] "'Patriotic Bill' is a threat to democracy and the future of Zimbabwe", Southern Africa Litigation Centre, 8 June 2023. See also, for example, Columbus Mavhunga, "Amnesty International to Zimbabwe Leader: Don't Sign 'Patriotic Act' Into Law", *VOA News*, 9 June 2023; Columbus Mavhunga, "Zimbabwe Opposition, Rights Groups Bemoan Passing of 'Patriotic Bill'", *VOA News*, 9 June 2023.

the opinion that the "Patriotic Bill" was timed to be in place for deployment ahead of the August 2023 elections.

As can be seen, Zimbabwean law provides a host of broad, vague and overlapping offences that criminalise freedom of expression. It is highly doubtful that all of these provisions satisfy the international criteria for legitimate restrictions on freedom of expression.

B) INVESTIGATION TOOLS AND STATE SURVEILLANCE

The **Cyber and Data Protection Act** introduces new procedural provisions in the form of amendments to the Criminal Procedure and Evidence Act.[70]

Search and seizure of computer-related items require judicial authority (from a magistrate) and must involve the investigation of a specific offence. A police officer who has a warrant can direct a service provider to **preserve relevant data** [71] There is also provision for a **preservation** order in respect of traffic data, on judicial authority (from a magistrate).[72]

There are also new **take-down provisions**. In terms of section 379C(3), a service provider is not criminally liable for information stored at the request of a user of the service if the hosting provider promptly removes or disables access to the information *after receiving an order from any court of law* to this effect, Alternatively, if the service provider becomes aware of any illegal information in any other manner, that service provider can avoid criminal liability *by promptly informing "the appropriate authority" which can evaluate the nature of the information and if necessary, issue an order for its removal*.[73] This provision is a positive one in that it does not place the decision-making power in the hands of the service provider. Presumably no final order would be issued by a court or any other authority without providing the person who posted the data a chance to state his or her case. Section 379C(9), relating to internet service providers who enable access to information provided by a third person by providing an electronic hyperlink, takes a similar approach.[74] There are criminal penalties for service providers who fail to comply with orders issued under these two subsections.

However, these provisions appear to be undermined by section 379C(11), which places an even heavier penalty on any service provider who "knowingly enables access to, stores, transmits or provides an electronic hyperlink to, any information with knowledge of the unlawfulness of the content of any such information";[75] it is not clear whether the service provider is expected to make its own assessment on unlawfulness for the purpose of this section or if this relates to material determined to be unlawful by a court or another appropriate authority.[76]

[70] Criminal Procedure and Evidence Act [*Chapter 9:07*].
[71] Id, section 379A, as inserted by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*].
[72] Id, section 379B, as inserted by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*].
[73] Id, subsection 379C(3), as inserted by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*].
[74] Id, subsection 379C(9), as inserted by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*].
[75] Id, subsection 397C(11) as inserted by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*].
[76] "Freedom on the Net 2022: Zimbabwe", Freedom House, section B2 assume that these provisions impose penalties providers that fail to remove illegal content when ordered by a court or other public authority or *upon discovery by the service provider*.

In terms of evidence-gathering and policy on cybercrime, the Cyber and Data Protection Act amends the **Interception of Communications Act *[Chapter 11:20]*** to create a **Cyber Security and Monitoring of Interception of Communications Centre** located in the Office of the President. This is described as a "monitoring facility through which all the intercepted communications and call-related information of a particular interception target are forwarded to an authorised person". In addition to being the channel for effecting "authorised interceptions", its functions include advising Government on cybercrime and cyber security, operating a "protection-assured whistle-blower system", and promoting cyber security in the public and private sectors; (amongst other things). The Centre is advised by a Cyber Security Committee appointed by the relevant minister.

Disturbingly, in terms of the amended Interception of Communications Act, a warrant for the **interception of communications** (by post, telecommunications or radio communications) can be issued by the Minister on the advice of the Cyber Security Committee – with no judicial involvement. Applications for such interceptions can be made by or on behalf of the Chief of Defence Intelligence, the Director-General of the President's department responsible for national security, the Commissioner of the Zimbabwe Republic Police or the Commissioner General of the Zimbabwe Revenue Authority.[77] The criteria for the issue of such warrants include reasonable suspicion of a serious offence by an organised criminal group, one of a list of serious criminal offences (which do not at this stage include cybercrime offences),[78] an "actual threat to national security" or any "compelling national economic interest", or "a potential threat to public safety or national security"[79] - which are for the most part broad, general and subjective standards. Similarly, the same officials who can apply for a warrant under hits law can demand a decryption key, in the interests of national security, to prevent or detect a serious criminal offence, or to ensure the country's economic well-being.[80]

C) SIM CARD REGISTRATION

Another part of the surveillance picture is **SIM card registration**. In terms of the regulations issued under the Postal and Telecommunications Act, mobile phone subscribers are required to provide identification details to service providers, including full name, permanent residential address, nationality, gender, subscriber identification number, and national identification or passport number. Service providers are required to retain this information for five years after the subscription has been discontinued. They are also obliged to transmit all of this data to POTRAZ on a monthly basis. POTRAZ is to maintain a Central Subscriber Information Database, where all subscriber information will be stored. Access to the database will be available for several purposes including for assisting law enforcement agencies, for "safeguarding

[77] Interception of Communications Act, 2007 [*Chapter 11:20*], section 5, as amended by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*].
[78] The offences are listed in the Third Schedule and in paragraphs 1-8 of the Ninth Schedule to the Criminal Procedure and Evidence Act [*Chapter 9:07*].
[79] Interception of Communications Act, 2007 [*Chapter 11:20*], section 6.
[80] Id, section 11.

national security", and for "undertaking approved educational and research purposes."

Access to this data for law enforcement purposes initially required a written request from an official of a senior rank, with no requirement for any judicial authority. This was altered when 2014 regulations replaced the 2013 set, with the updated regulations requiring a warrant or a court order for access to subscribed data by law enforcement agencies.[81] However, Zimbabwe's Parliamentary Legal Committee noted that the amended regulations are still inadequate to ensure independent judicial oversight since a warrant can be issued by police officers who have been designated as justices of the peace.[82]

It has been noted that this scheme "clearly shows a disregard for the rights to privacy and free expression protected by the new Zimbabwean constitution" as well as eradicating the potential for anonymous communications, enabling location-tracking, and simplifying communications surveillance and interception.[83]

It has been reported that the privacy of mobile subscribers was violated during the July 2018 elections, when subscribers received unsolicited campaign messages from ZANU-PF (the ruling party). These campaign messages reportedly referred to the recipients by name, even though many were not party members, raising suspicions on this score.[84]

In 2020, an official from the Criminal Investigation Department Asset Forfeiture Unit obtained a warrant from a magistrate for a list of *all* the customers of the country's leading mobile network service provider during a specified six-month period, along with a summary of e-money or airtime credit services on the platform during the same period, for a money laundering investigation. However, the High Court cancelled the warrant on the found that it was excessively wide, speculative and liable to abuse. Observers noted that this search warrant, if allowed to stand, "would have gravely compromised the privacy of over 11 million people, who did not break the law", constituting an acute breach of the right to privacy. [85]

[81] Postal and Telecommunications (Subscriber Registration) Regulations, 2013 (Statutory Instrument 142 of 2013), replaced by Postal and Telecommunications (Subscriber Registration) Regulations, 2014 (Statutory Instrument 95 of 2014).
[82] Freedom on the Net 2022: Zimbabwe", Freedom House, section C6.
[83] "Zimbabwe: New SIM registration database law represses twin rights to privacy and expression", Association for Progressive Communications, 3 October 2012; "Freedom on the Net 2022: Zimbabwe", Freedom House, section C4.
[84] Freedom on the Net 2022: Zimbabwe", Freedom House, section C4.
[85] "Econet judgement guarantees privacy", *The Standard*, 13 September 2020.

18.5 ELECTION LAW AND FREEDOM OF EXPRESSION

Elections for the President, Members of Parliament and local councillors will be held in Zimbabwe in August 2023, with current President Emmerson Mnangagwa seeking a second term.[86]

Elections are administered by the **Zimbabwe Electoral Commission (ZEC)**, which is covered in detail in the Constitution, and conducted in accordance with the **Electoral Act**.[87]

ZIMBABWE CONSTITUTION

ZIMBABWE ELECTORAL COMMISSION

238. ESTABLISHMENT AND COMPOSITION OF ZIMBABWE ELECTORAL COMMISSION

1. There is a commission to be known as Zimbabwe Electoral Commission consisting of –

a. a chairperson appointed by the President after consultation with the Judicial Service Commission and the Committee on Standing Rules and Orders; and

b. eight other members appointed by the President from a list of not fewer than twelve nominees submitted by the Committee on Standing Rules and Orders.

2. The chairperson of the Zimbabwe Electoral Commission must be a judge or former judge, or a person qualified for appointment as a judge.

3. If the appointment of a chairperson to the Zimbabwe Electoral Commission is not consistent with a recommendation of the Judicial Service Commission, the President must cause the Committee on Standing Rules and Orders to be informed as soon as practicable.

4. Members of the Zimbabwe Electoral Commission must be Zimbabwean citizens and chosen for their integrity and experience and for their competence in the conduct of affairs in the public or private sector.

5. Members of the Zimbabwe Electoral Commission are appointed for a six-year term and may be re-appointed for one such further term, but no person may be appointed to or serve on the Commission after he or she has been a member for one or more periods, whether continuous or not, that amount to twelve years.

239. FUNCTIONS OF ZIMBABWE ELECTORAL COMMISSION

The Zimbabwe Electoral Commission has the following functions –

a. to prepare for, conduct and supervise –

[86] "Zimbabwe holds harmonized elections (presidential, parliamentary and local government elections) every five years." "Zimbabwe Country Report 2022", BTI (Bertelsmann Transformation Index), Bertelsmann Stiftung, "Political Participation".
[87] Electoral Act [*Chapter 2:13*].

i. elections to the office of President and to Parliament;
ii. elections to provincial and metropolitan councils and the governing bodies of local authorities;
iii. elections of members of the National Council of Chiefs established by section 285; and
iv. referendums;
and to ensure that those elections and referendums are conducted efficiently, freely, fairly, transparently and in accordance with the law;

b. to supervise elections of the President of the Senate and the Speaker and to ensure that those elections are conducted efficiently and in accordance with the law;
c. to register voters;
d. to compile voters' rolls and registers;
e. to ensure the proper custody and maintenance of voters' rolls and registers;
f. to delimit constituencies, wards and other electoral boundaries;
g. to design, print and distribute ballot papers, approve the form of and procure ballot boxes, and establish and operate polling centres;
h. to conduct and supervise voter education;
i. to accredit observers of elections and referendums;
j. to give instructions to persons in the employment of the State or of a local authority for the purpose of ensuring the efficient, free, fair, proper and transparent conduct of any election or referendum; and
k. to receive and consider complaints from the public and to take such action in regard to the complaints as it considers appropriate.

240. DISQUALIFICATIONS FOR APPOINTMENT TO ZIMBABWE ELECTORAL COMMISSION

In addition to the persons mentioned in section 320(3) [Members of Parliament and members of provincial or metropolitan councils, local authorities and Government-controlled entities], the following persons are ineligible for appointment to the Zimbabwe Electoral Commission –

a. public officers, other than judges;
b. employees of provincial and metropolitan councils and local authorities; and
c. members and employees of statutory bodies and government-controlled entities.

241. ZIMBABWE ELECTORAL COMMISSION TO REPORT ON ELECTIONS AND REFERENDUMS

In addition to the report it is required to submit in terms of section 323 [which requires every Commission to submit to Parliament, through the responsible Minister, an annual report describing fully its operations and activities], the Zimbabwe Electoral Commission must without delay, and through the appropriate Minister, submit a report to Parliament on the conduct of every election and every referendum.

The forthcoming elections should be viewed in historical context:

When Zimbabwe gained Independence in 1980, the abolition of the Rhodesian system of apartheid awakened hopes for political transformation. However, in the years afterward, Zimbabwe effectively transformed into a one-party state led by President Robert Mugabe and his Zimbabwe African National Union – Patriotic Front (ZANU-PF). One of the first, and most severe, glimpses of the violent nature of the new regime were the Gukurahundi massacres in Matabeleland, which resulted in around 20,000, mostly from the Ndebele minority, dead. However, Zimbabwe's economy continued to perform well in the first decade after independence, and Zimbabwe remained the "breadbasket" of southern Africa.

The formation of the Movement for Democratic Change (MDC) in 1999, by a wide range of civic movements, led to the first opposition party that posed a serious threat to ZANU-PF rule. Not only did the MDC win a significant number of parliament seats in 2000, but it also managed to successfully mobilize a "no" vote during a referendum around proposed constitutional amendments earlier that year.
The fast-track land reform program, which ZANU-PF initiated shortly after its defeat in the constitutional referendum in 2000, exacerbated an economic crisis that had started in the 1990s and was aggravated by Zimbabwe's adoption of the Economic Structural Adjustment Programs (ESAP). Combined with economic mismanagement and other factors, this led to a 40% decline in GDP between 1998 and 2009, and the notorious hyperinflation and shortages of almost all commodities in 2008.

After the 2008 elections, the Zimbabwe Electoral Commission (ZEC) took five weeks to announce the results, which many believed was an indication Morgan Tsvangirai's MDC-T had won. ZEC did indeed announce an MDC-T win but stated that Tsvangirai had received only 47.9% of the vote (against Mugabe's 43.2%), not enough to secure an outright, first-round victory. The resulting run-off was marred by violence, as opposition leaders and supporters were beaten, tortured, kidnapped and killed. To avoid further violence, Tsvangirai decided to withdraw from the run-off.

Following the international community's refusal to accept ZANU-PF's blocking of an apparent MDC-T victory, a Government of National Unity (GNU) was formed with South Africa acting as mediator. This forced political parties to jointly govern the country and form the first coalition government since independence. The GNU managed to ensure political and economic stability, halting inflation and ensuring economic growth. One of the other major gains in this period was the formulation of a new constitution, which was overwhelmingly approved in a referendum after years of negotiations.

The GNU ended with the 2013 elections, which resulted in a contested ZANU-PF win. It was the scale of their victory that shocked most observers, as Mugabe won 61% of the vote, while Tsvangirai only managed to secure 33%. Moreover, the ZANU-PF went from being a parliamentary minority to a holding resounding majority (from 99 to 160 out of 210 seats). In the years that followed, the political landscape was dominated by intense factionalism within ZANU-PF, continued political and economic paralysis and a lack of substantial reforms. The factionalism ultimately culminated in the coup presented as a military intervention, called Operation Restore Legacy, in November 2017, which led to the forced departure of President Mugabe.

The 2018 elections were historic, as they were the first ones in which Mugabe did not participate. ZANU-PF's Mnangagwa, who took over from Mugabe in 2017, beat the young MDC-A leader, Nelson Chamisa, who became the leader of the opposition after

Tsvangirai's death earlier that year.[88]

As noted by local and international election observers, the run-up to the 2018 elections was characterized by a largely peaceful environment. They further indicated the opening of democratic space and the ability of the opposition to campaign freely, including in areas it previously could not access. The fact that the EU was invited to send an Election Observation Mission (EOM) for the first time in 16 years further testified to this change. However, despite some positive developments, most international EOMs concluded the elections were not in accordance with international standards. They indicated there was no level playing field and highlighted the partisan role of the Zimbabwe Electoral Commission (ZEC), the biased state media, the use of state resources by ZANU-PF and subtle forms of intimidation.[89]

The departure of Mugabe after his 37-year rule led to renewed hope for political and economic transformation, which was further fueled by Mnangagwa's public remarks that his "new dispensation" was "open for business" and willing to implement democratic reforms. However, Mnangagwa's initial years were marked by increasing repression, a lack of reform, severe corruption and a worsening economic crisis.[90]

According to the Africa Centre for Strategic Studies, the Zimbabwean elections "are shaping up to be the bloodiest on the continent" in 2023, as the ruling Zimbabwe African National Union-Patriotic Front (ZANU-PF) ramps up its use of violence and intimidation in the attempt to retain its 43-year grip on power":[91]

The latest cycle of violence against opposition candidates has, in fact, already begun. In June 2022, opposition activist Moreblessing Ali was abducted on the outskirts of Harare. Her dismembered body was later found in a well nearby. Witnesses identified a ZANU-PF activist as the assailant. Over a dozen opposition politicians who attended her funeral were arrested for "inciting violence." Many remain incarcerated even though they have yet to be charged.

This is but one illustration of the pattern of intimidation and suppression of political opposition, including arrests and extrajudicial killings, that Zimbabwe faces as it heads toward elections. […]
What is noteworthy in the 2023 cycle is how early the violence against the opposition has started. The faction now in control of the ZANU-PF is also increasingly dropping any pretence that violence is not part and parcel of the party campaign playbook.
[…]

With this climate of violence and intimidation, it is a given that the elections will not be free and fair.
This perspective is reinforced by widely held perceptions that the Zimbabwe Electoral Commission (ZEC) is biased, with leading ZANU-PF family members serving as commissioners. ZEC's reputation also suffers from the outsized role of the military, where 15 percent of ZEC staff are former service personnel, including the chief elections

[88] "Zimbabwe Country Report 2022", BTI (Bertelsmann Transformation Index), Bertelsmann Stiftung, "Executive Summary".
[89] Id, "Political Participation".
[90] Id, "Executive Summary"
[91] Joseph Siegle and Candace Cook, "Africa's 2023 Elections: Democratic Resiliency in the Face of Trials", Africa Centre for Strategic Studies, 31 January 2023 (updated on 10 July 2023).

officer, who is a retired army major. Contrary to electoral best practice, ZEC has refused to publish an electronic copy of the electoral register to foster transparency. This pattern of institutional bias builds on a long history of election engineering in Zimbabwe including: limiting the number of polling stations in opposition strongholds, challenging the credentials of opposition candidates, and filing criminal charges against others—all with the aim of preventing them from standing for office.

An illustration of the latter is the imprisonment of Fadzayi Mahere, a 36-year-old lawyer and opposition member of Parliament with half a million Twitter followers. She was charged with "communicating false statements prejudicial to the state".[92]

Looking more specifically at freedom of expression, Zimbabwe's **Electoral Act** contains some specific provisions relating to media and media coverage.

Public broadcasters are required to afford all political parties and independent candidates such free access to their broadcasting services as may be prescribed by regulations which are aimed at providing at a fair and balanced allocation of time between each political party and independent candidate, by regulating the total time to be allocated to each political party and candidate, the duration of each broadcast by or on behalf of a party or candidate, and the times and areas in which these broadcasts are to be transmitted.[93]

Broadcaster or print media which publish any advertisement by or on behalf of a political party or candidate contesting an election must offer the same terms and conditions of publication to all the political parties and candidates contesting the election, without discrimination. All political advertisements must be clearly identified as such.[94]

The Zimbabwe Electoral Commission can require broadcasters and print publishers to publish statements issued by the Commission for the purpose of informing voters about the electoral process, upon payment by the Commission of a reasonable amount for such publication.[95]

During the election period (which will be identified by the Commission), broadcasters and print publishers must follow certain principles:

- All political parties and candidates must be treated equitably in their news media, in regard to the extent, timing and prominence of the coverage accorded to them.
- News reports on the election must be factually accurate, complete and fair,
- There must be a clear distinction between factual reporting and editorial comment.
- Inaccuracies in reports on the election must be rectified without delay and with due prominence.
- Political parties and candidates must be afforded a reasonable right of reply

[92] Id.
[93] Electoral Act [*Chapter 2:13*], as amended through 2018, section 160G.
[94] Id, section 160H.
[95] Id, section 160I.

to allegations by others.
- News media must not promote political parties or candidates that encourage violence or hatred against any class of persons in Zimbabwe.
- News media must avoid language that encourages racial, ethnic or religious prejudice or hatred, incites violence, or is likely to lead to "undue public contempt" towards any political party, candidate or class of person in Zimbabwe.[96]

The general rules appear to be fair and reasonable for the most part - although the duty to avoid producing "contempt" in news reporting about a candidate could inhibit justified criticism or reports of wrongdoing on the part of a candidate.

The media requirements in the Electoral Act overlap with those in the **Broadcasting Services Act**, which require broadcasters to give "reasonable and equal opportunities for the broadcasting of election matter to all political parties contesting the election" during an election period and forbids the broadcasting of election advertisements by broadcast licensees during the period from four days before the first polling day until the closing of the polls on the last polling day.[97]

The **Electoral Act** imposes certain restrictions on speech on **polling day**. It is an offence to do any of the following within three hundred metres of a polling station on a polling day:

- convoke or take part in any gathering of more than twelve persons: or
- canvass for votes; or
- utter slogans; or
- distribute leaflets or pamphlets for or on behalf of any candidate or political party; or
- organise or engage in public singing or dancing; or
- use bands or music or loudspeaker vans or apparatus.[98]

These seem to be reasonable restrictions to avoid voter intimidation.

The **Zimbabwe Electoral Commission, assisted by the Zimbabwe Media Commission**, will monitor the Zimbabwean news media during the election period to ensure that the rules in the Electoral Act are followed. although it is not clear what remedies or sanction will be applied in the case of violations.[99]

In the run-up to the August 2023 elections, there has already been a **collision between the Electoral Act and the Cyber and Data Protection Act**. The Zimbabwe Electoral Commission has indicated that the electronic version of the voters' roll cannot be released on the grounds that this would compromise the security of the personal data in the database and possibly lead to identity theft. Civil society groups counter-argue that section 11(5)(h) of the Cyber and Data Protection Act allows processing of sensitive personal data where this is authorised by a law or regulation for any reason

[96] Id, section 160J.
[97] Broadcasting Services Act, 2001 [*Chapter 12:06*], sections 2-3 read with the definitions in section 1.
[98] Electoral Act [*Chapter 2:13*], as amended through 2018, section 147.
[99] Id, section 160K. Penalties can be provided n statutory instruments issued by the Commission in terms of the Act. See section 192.

constituting substantial public interest, with some alleging that the reluctance to release the digital voters' roll is intended to provide leeway to manipulate it with a view to swaying the electoral outcome. In March 2023, the High Court refused to order the Commission to release an electronic copy of the voters' roll, on the grounds that this could compromise the security of the database. The case is on appeal to the Supreme Court.[100]

As noted above, **concerns about voters' data privacy** were raised after mobile phone users received personalised messages from the ruling party soliciting their votes. Following on a complaint about this by MISA-Zimbabwe, POTRAZ in its role as the Data Protection Authority undertook to investigate the matter.[101]

Another election issue that has already arisen concerns **media coverage of the voter registration process**. The Zimbabwe Electoral Commission denied journalists access to voter registration statistics and voter registration centres on the basis that they had not been accredited by the Zimbabwe Electoral Commission ZEC, even though they are already accredited as journalists by the Zimbabwe Media Commission.[102]

Disputes may well heat up even further as the 2023 election grows closer.

[100] "Zimbabwe's uneven electoral field: Data protection laws used to deny digital voter roll inspection", Advox, 13 June 2023; "ZEC wins voters' roll case… Releasing electronic format compromises security, court rules", *The Herald*, 8 March 2023.
[101] Wallace Mawire, "MISA-Zimbabwe pleased by POTRAZ bid to investigate violations of the Cyber and Data Protection Act", April 2023.
[102] "ZEC denies journalists access to voter registration stats", *The Zimbabwean*, 12 March 2023.