

Digital Rights in Zimbabwe Stakeholder Submission to The Fourth Cycle Universal Periodic Review

54th Session of the UPR Working Group

July, 2026



Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

CIPESA is one of two centres established under the Catalysing Access to Information and Communications Technologies in Africa (CATIA) initiative, which was funded by the UK's Department for International Development (DfID). CIPESA focuses on decision-making that facilitates the use of ICT in support of good governance, human rights, and livelihoods.

CIPESA's establishment in 2004 was in response to the findings of the Louder Voices Report for DFID, which cited the lack of easy, affordable, and timely access to information about ICT-related issues and processes as a key barrier to effective and inclusive ICT policy-making in Africa. As such, our work responds to the shortage of information, resources, and actors consistently working at the nexus of technology, human rights, and society.

Plot 10B Katalima Crescent, Naguru. | P.O.Box 122311, Kampala (U)
+256 414 289 502 | programmes@cipesa.org | [@cipesaug](https://www.cipesa.org)

Zimbabwe Lawyers for Human Rights (ZLHR)

ZLHR is a not-for-profit law-based human rights organisation, established in 1996, whose core objective is to foster a culture of human rights, equality, and respect for the rule of law in Zimbabwe. ZLHR's secretariat and member lawyers provide legal defence support to human rights defenders and conduct strategic impact litigation, training, research, and advocacy in all areas of human rights law.

Kodzero-Amalungelo House, 103 Sam Nujoma Street, Harare, Zimbabwe
+263 242 705370 | bellinda.chinowawa@zlhrr.org | <https://www.zlhrr.org.zw>

The University of Birmingham

It is a leading public research university in the United Kingdom, recognised for its high-quality teaching, interdisciplinary research, and global engagement. Founded in 1900, the University brings together students and scholars from around the world to address major social, economic, scientific, and cultural challenges. University of Birmingham, Edgbaston, Birmingham B15 2TT, United Kingdom, email: m.regnitz@bham.ac.uk, Website: <https://www.birmingham.ac.uk/>,

The Pan-African Lawyers Union

The Pan-African Lawyers Union (PALU) was founded on 9th September 2002. PALU's network includes over 60 regional and national lawyers' associations and over 1,000 lawyers spread across Africa and in the Diaspora. PALU works to advance the legal profession, rule of law, good governance, human and peoples' rights, and the socio-economic development of the African continent. To realise a united, just and prosperous Africa, built on the rule of law and good governance, PALU has adopted three core areas of thematic focus, namely institutional development, development of the legal profession, and the rule of law and good governance.

Plot 1 Kaunda Road, off Haile Selassie Road, P.O. Box 6065, Arusha, Tanzania. +255 (68) 507-8794 (mobile)
Email: secretariat@lawyersofafrica.org, Website: <https://www.lawyersofafrica.org/>

The Digital Rights Alliance Africa (DRAA)

The Digital Rights Alliance Africa (DRAA) is a pan-African, diverse coalition of formal civil society organisations (CSOs), human rights defenders (HRDs), media practitioners, lawyers, and technology specialists in Africa that seek to champion digital civic space and counter threats to digital rights on the continent. The Alliance was jointly established in 2023 by the International Center for Not-for-Profit Law (ICNL) and the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) to strengthen expertise and action by civil society in Africa to shape rights-based, enabling digital policies and counter threats to digital rights and internet freedoms across the continent. DRAA currently has members from 15 countries across Africa.

Members undertake research, legal advocacy, and share experiences to navigate digital restrictions and promote digital policy reforms in line with international norms.

Introduction

1. Digital rights and freedoms should be accorded the same protection as rights exercised offline. Zimbabwe is bound by constitutional, regional, and international obligations to protect freedom of expression, access to information, privacy, equality, and participation in public affairs, including in digital spaces.¹ The 2021 joint UPR submission on digital rights in Zimbabwe identified restrictions on online expression, internet access, access to information, data protection, and privacy as key human rights concerns.²
2. Zimbabwe's third-cycle UPR review was conducted on 26 January 2022.³ Its fourth-cycle review is scheduled under the 54th session of the UPR Working Group, with stakeholder submissions due by 17 July 2026.⁴ Zimbabwe received 264 recommendations during its 2022 review, of which it supported 168 and noted 96. While digital rights were addressed primarily through recommendations on internet access, freedom of expression, privacy, access to information, and civic space, significant legislative and policy developments have since shaped Zimbabwe's digital landscape.
3. Since the previous review, Zimbabwe has made some legal and infrastructural progress, including the enactment of the Cyber and Data Protection Act, the operationalisation of the Freedom of Information Act through implementing regulations, the expansion of internet and broadband access, and the licensing of additional satellite internet services.⁵ However, these developments have been accompanied by persistent challenges, including restrictions on online expression, vaguely defined criminal offences, inadequate oversight of surveillance powers, barriers to affordable internet access, election-period network disruptions, and the rise of technology-facilitated gender-based violence.⁶
4. This report assesses the state of protection and promotion of digital rights in Zimbabwe during the review period, taking stock of progress made and persistent challenges in implementing recommendations received during the Third Cycle UPR in 2022. It evaluates these developments against Zimbabwe's constitutional, regional, and international human rights obligations, highlighting both progress and continuing challenges affecting the enjoyment of rights in the digital environment.

¹ Constitution of Zimbabwe Amendment (No 20) Act 2013, ss 57, 58, 61 and 62; International Covenant on Civil and Political Rights, arts 17 and 19; African Charter on Human and Peoples' Rights, arts 9 and 18.

² Media Institute of Southern Africa Zimbabwe Chapter, *Small Media and Collaboration on International ICT Policy for East and Southern Africa, Digital Rights in Zimbabwe*, UPR Submission, Session 40 (2021); https://cipesa.org/wp-content/files/briefs/Digital-Rights-in-Zimbabwe_2021-UPR-submission.pdf

³ Office of the United Nations High Commissioner for Human Rights, 'Universal Periodic Review: Zimbabwe' <https://www.ohchr.org/en/hr-bodies/upr/zw-index>

⁴ Office of the United Nations High Commissioner for Human Rights, '4th UPR Cycle: Contributions and Participation of "Other Stakeholders" in the UPR' [https://www.ohchr.org/en/hr-bodies/upr/ngos-nhris, OHCHR UPR Documentation, 'UPR 54 Submission Window'](https://www.ohchr.org/en/hr-bodies/upr/ngos-nhris/OHCHR%20UPR%20Documentation,%20UPR%2054%20Submission%20Window) <https://uprdoc.ohchr.org/>

⁵ Data Protection Act [Chapter 11:22] No 5 of 2021; Freedom of Information (General) Regulations 2021, SI 229 of 2021; Reuters, 'Zimbabwe approves licensing of Musk's Starlink internet service' (25 May 2024) <https://www.reuters.com/world/africa/zimbabwe-approves-licensing-musks-starlink-internet-service-2024-05-25/>

⁶ MISA Zimbabwe, 'Internet degrade on the eve of elections' (22 August 2023) <https://zimbabwe.misa.org/2023/08/22/internet-degrade-on-the-eve-of-elections/> accessed 2 July 2026; Amnesty International, 'Zimbabwe: President's signing of "Patriotic Bill" a brutal assault on civic space' (15 July 2023) <https://www.amnesty.org/en/latest/news/2023/07/zimbabwe-presidents-signing-of-patriotic-bill-a-brutal-assault-on-civic-space/> accessed 2 July 2026; United Nations Zimbabwe, 'Turning the Tide, Zimbabwe's Push to End Gender-Based Violence in a Digital Age' (24 November 2025) <https://zimbabwe.un.org/en/305894-turning-tide-zimbabwe%E2%80%99s-push-end-gender-based-violence-digital-age>

Updates since the previous review

5. Zimbabwe's digital environment has expanded significantly since the 2021 submission. According to the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), internet penetration increased to 84.55% in the fourth quarter of 2025, active internet and data subscriptions rose from 12.99 million to 13.25 million, and broadband penetration rose to 82.63%.⁷ While these figures reflect continued growth in the sector, subscription-based indicators may overstate meaningful individual access, as many users maintain multiple ownership of SIM cards and access remains constrained by affordability, device costs, electricity shortages, and the quality of service.
6. The approval of Starlink's licensing in 2024 created opportunities for improved connectivity, particularly in rural and underserved areas.⁸ POTRAZ's 2025 sector reporting also showed growth in VSAT connections, largely attributed to Starlink's rollout and adoption.⁹ While this is a positive development, satellite connectivity remains dependent on affordability, competition safeguards, consumer protection, equitable licensing, and service availability beyond higher-income users.
7. Zimbabwe enacted the Cyber and Data Protection Act in 2021. The Act established a Data Protection Authority, designated POTRAZ as that Authority, created data protection obligations, and amended criminal law provisions to introduce cyber-related offences.¹⁰ This law introduced offences relating to cyber-bullying and harassment, threatening data messages, transmission of false data messages intending to cause harm, non-consensual transmission of intimate images, and cyber-related child protection offences.¹¹ While these provisions respond to real online harms, several remain broad and carry heavy criminal penalties, creating risks for protected expression, journalism, political debate, and whistleblowing.¹²
8. In 2024, Zimbabwe adopted the Cyber and Data Protection (Licensing of Data Controllers and Appointment of Data Protection Officers) Regulations.¹³ These regulations require data controllers to apply for licences and appoint data protection officers, and introduce compliance obligations for organisations processing personal data.¹⁴ These measures strengthen the data protection framework, but the independence of the supervisory authority remains a concern because POTRAZ is both the communications regulator and the designated Data Protection Authority.¹⁵
9. The Freedom of Information Act, enacted in 2020, was operationalised through the Freedom of Information (General) Regulations, 2021.¹⁶ These regulations require entities to publish institutional information within six months from the date of establishment of the entity, and provide procedures relating to information officers, registers of requests, and appeals.¹⁷ However, implementation remains uneven, and public bodies still require stronger systems for proactive disclosure, timely responses, accessible formats, independent appeals, and public reporting.

⁷ Gamuchirai Mapako, 'Zimbabwe's Internet Data Penetration Surges to 84.55% in Q4 2025' *TechnoMag* (29 April 2026) <https://technomag.co.zw/zimbabwes-internet-data-penetration-surges-to-84-55-in-q4-2025/>

⁸ Reuters, 'Zimbabwe approves licensing of Musk's Starlink internet service' (25 May 2024) <https://www.reuters.com/world/africa/zimbabwe-approves-licensing-musks-starlink-internet-service-2024-05-25/>

⁹ Mapako (n 7) 15.

¹⁰ Data Protection Act [Chapter 11:22] No 5 of 2021, ss 2, 5 and 6.

¹¹ Data Protection Act [Chapter 11:22] No 5 of 2021, ss 164, 164A, 164B, 1, 64C and 164E.

¹² Section 164C of the Cyber and Data Protection Act [Chapter 17:12]; see also <https://www.newsday.co.zw/southerneye/news/article/4735/zimbabwes-new-cyber-law-brought-outlawed-criminal-defamation-provisions-back-say-experts>.

¹³ Cyber and Data Protection (Licensing of Data Controllers and Appointment of Data Protection Officers) Regulations 2024, SI 155 of 2024.

¹⁴ *ibid* regs 3–6.

¹⁵ Data Protection Act [Chapter 11:22] No 5 of 2021, s 5; DLA Piper, 'Data Protection Laws of the World: Zimbabwe' (20 March 2026) <https://www.dlapiperdataprotection.com/?c=ZW&t=law>.

¹⁶ Freedom of Information (General) Regulations 2021, SI 229 of 2021.

¹⁷ MISA Zimbabwe, 'Unpacking the Freedom of Information Regulations' (20 October 2021) <https://zimbabwe.misa.org/2021/10/20/unpacking-the-freedom-of-information-regulations/>.

1. Freedom of Expression and Opinion

10. The 2023 general elections exposed continuing digital rights concerns. MISA Zimbabwe reported internet degradation on the eve of elections, affecting NetOne, Econet, TelOne, and Liquid Telecoms.¹⁸ Election-period throttling, degradation, or shutdown fears undermine access to information, expression, media freedom, election observation, and public participation.
 11. Zimbabwe also enacted section 23A of the Criminal Law Codification and Reform Amendment Act, commonly referred to as the “Patriotic Act”, in 2023.¹⁹ Human rights organisations warned that its provisions on “wilfully injuring the sovereignty and national interest of Zimbabwe” risk criminalising legitimate engagement with foreign actors, advocacy, criticism, and civic participation.²⁰ In June 2025, Zimbabwe’s High Court reportedly struck down parts of the Act, including section 22A(3), but broader concerns remain regarding the chilling effect of national-interest offences on civic space.²¹ These concerns were validated in February 2026, when government officials issued threats of arrest against Blessed Mhlanga, a journalist who addressed the Geneva Summit for Human Rights and Democracy.²²
-
12. Section 61 of the Constitution of Zimbabwe protects freedom of expression and freedom of the media, including the right to seek, receive, and communicate ideas and other information.²³ Despite this protection, Zimbabwe continues to maintain and apply laws that unduly restrict expression online and offline.
 13. The concerns raised in the 2021 submission remain relevant. Sections 31 and 33 of the Criminal Law (Codification and Reform) Act criminalise publication or communication of false statements prejudicial to the State and undermining the authority of or insulting the President.²⁴ These offences remain incompatible with international standards where they impose criminal penalties for protected speech, criticism of public officials, satire, political commentary, or public-interest reporting.²⁵ For example, in March 2025, a 34-year-old man from Makoni District was prosecuted under section 33 of the Criminal Law (Codification and Reform) Act after allegedly shouting slogans critical of President Emmerson Mnangagwa and expressing support for Blessed Geza during a verbal altercation at a local bottle store. He was charged with undermining the authority of or insulting the President and remained in detention for several weeks pending trial.²⁶

¹⁸ MISA Zimbabwe, ‘Internet degrade on the eve of elections’ (22 August 2023) <https://zimbabwe.misa.org/2023/08/22/Internet-degrade-on-the-eve-of-elections/>.

¹⁹ Criminal Law (Codification and Reform) Amendment Act 2023.

²⁰ Amnesty International, ‘Zimbabwe: President’s signing of “Patriotic Bill” a brutal assault on civic space’ (15 July 2023) <https://www.amnesty.org/en/latest/news/2023/07/zimbabwe-presidents-signing-of-patriotic-bill-a-brutal-assault-on-civic-space/>.

²¹ Zimbabwe Lawyers for Human Rights, ‘ZLHR Welcomes High Court Judgment Impugning Unpatriotic Provisions of Patriotic Act’, available at <https://www.zlhr.org.zw/zlhr-welcomes-high-court-judgment-impugning-unpatriotic-provisions-of-patriotic-act/>.

²² <https://genevasummit.org/geneva-summit-coalition-condemns-zimbabwe-threats-against-un-speaker/>

²³ Constitution of Zimbabwe Amendment (No 20) Act 2013, s 61

²⁴ Criminal Law (Codification and Reform) Act [Chapter 9:23], ss 31 and 33; Media Institute of Southern Africa Zimbabwe Chapter, *Small Media and CIPESA* (n 2)

²⁵ Human Rights Committee, General Comment No 34: Article 19: Freedoms of Opinion and Expression UN Doc CCPR/C/GC/34 (12 September 2011) paras 38 and 47

²⁶ ZLHR, ‘Man Charged with Insulting Mnangagwa after Praising Geza’, <https://www.zlhr.org.zw/man-charged-with-insulting-mnangagwa-after-praising-geza/>

14. The Cyber and Data Protection Act introduced additional speech-related offences. Section 164 criminalises transmission of data messages inciting violence or damage to property; section 164B criminalises cyber-bullying and harassment; and section 164C criminalises transmission of false data messages intending to cause psychological or economic harm.²⁷ Notably, in February 2025, journalist Blessed Mhlanga was arrested after voluntarily presenting himself to the police and charged under section 164 of the Cyber and Data Protection Act with transmitting data messages alleged to incite violence or cause damage to property.²⁸ While states may regulate genuine threats, incitement, and serious online harms, such offences must be narrowly framed and should not be used against journalists, human rights defenders, opposition actors, and citizens engaging in legitimate political expression.
15. The “Patriotic Act” has deepened this concern by introducing broad national-interest and sovereignty-related offences.²⁹ Furthermore, the Private Voluntary Organisations (PVO) Amendment Act 2025 in as far as it imposes mandatory registration and broad state oversight on non-governmental bodies. Such provisions deter civil society organisations, journalists, opposition actors, and human rights defenders from engaging regional and international mechanisms, including the African Commission on Human and Peoples’ Rights, the United Nations, and diplomatic missions.³⁰
16. Arrests, prosecution, and intimidation of journalists and commentators remain a serious concern. In 2025, Freedom House reported that Zimbabwe continues to record arrests, threats, and harassment of users and journalists for online activity.³¹ Such cases contribute to self-censorship, especially among journalists, women in public life, activists, artists, opposition supporters, and ordinary citizens using social media to discuss governance, elections, corruption, public services, and human rights.
17. The Human Rights Committee’s 2025 concluding observations on Zimbabwe raised concerns relevant to civic space and the exercise of civil and political rights.³² The African Commission on Human and Peoples’ Rights also reviewed Zimbabwe’s 16th periodic report in 2025 and issued recommendations on strengthening human rights protections under the African Charter.³³ These regional and international reviews reinforce the need to align domestic speech offences with legality, legitimate aim, necessity, and proportionality.

²⁷ Data Protection Act [Chapter 11:22] No 5 of 2021, ss 164, 164B and 164C

²⁸ Human Rights Watch, “Zimbabwe: Journalist Held on Baseless Charges - Detention of Blessed Mhlanga Highlights Threats to Free Expression, Media Freedom”, <https://www.hrw.org/news/2025/03/26/zimbabwe-journalist-held-baseless-charges>.

²⁹ Criminal Law (Codification and Reform) Amendment Act 2023

³⁰ Amnesty International, ‘Zimbabwe: President’s signing of “Patriotic Bill” a brutal assault on civic space’ (15 July 2023) <https://www.amnesty.org/en/latest/news/2023/07/zimbabwe-presidents-signing-of-patriotic-bill-a-brutal-assault-on-civic-space/>

³¹ Blessed Mhlanga, ‘Silenced for Reporting: Zimbabwe’s War on the Press’ (Geneva Summit for Human Rights and Democracy, 18 February 2026) <https://genevasummit.org/speech/silenced-for-reporting-zimbabwes-war-on-the-press/>

³² Human Rights Committee, Concluding Observations on the Second Periodic Report of Zimbabwe UN Doc CCPR/C/ZWE/CO/2 (6 May 2025)

³³ African Commission on Human and Peoples’ Rights, Concluding Observations and Recommendations on the 16th Periodic Report of the Republic of Zimbabwe, 2019–2023 (30 July 2025) <https://achpr.au.int/sites/default/files/files/2025-09/concluding-observations-zimbabwe-16th-periodic-report-2019-2023eng.pdf>

2. Freedom of Information and Censorship of Content

18. Section 62 of the Constitution guarantees the right of access to information held by the State and, where necessary for the exercise or protection of a right, information held by any person.³⁴ The enactment of the Freedom of Information Act and its regulations was a positive step following the repeal of the Access to Information and Protection of Privacy Act.³⁵
19. However, the effective enjoyment of access to information remains constrained by implementation gaps. Public bodies should proactively publish information, appoint and train information officers, respond to requests within lawful timelines, provide accessible formats, and ensure affordable appeals.³⁶ The right of access to information is particularly important during elections, public health emergencies, public procurement, digital identity programmes, surveillance procurement, telecommunications regulation, and public finance management.
20. The African Commission on Human and Peoples' Rights has urged Zimbabwe to strengthen human rights implementation and oversight following its review of Zimbabwe's 16th periodic report.³⁷ Access to information is central to public accountability and democratic participation, particularly where public authorities regulate digital infrastructure, communications services, media licensing, data protection, and surveillance powers.
21. Censorship and content regulation remain a concern. Sections 13 and 14 of the Censorship and Entertainments Control Act prohibit and empower examination of "undesirable" publications, pictures, statues, and records.³⁸ These provisions use broad morality-based standards that may enable arbitrary restriction of artistic expression, journalism, public-interest commentary, political content, and minority viewpoints.
22. In 2025, Zimbabwe adopted the Broadcasting Services Amendment Act.³⁹ MISA Zimbabwe and the Media Alliance of Zimbabwe warned that the reform process failed to adequately address independence of the broadcasting regulator, public participation in licensing, parliamentary oversight, media diversity, and the realities of convergence and artificial intelligence.⁴⁰ Regulation of broadcasting should not become a licensing system for online expression, citizen journalism, podcasts, social media live streams, independent commentary, or civic education.
23. Election-related access to information remains a major concern. Network degradation or interference during elections undermines voters' access to information, media reporting, election observation, incident verification, and public debate.⁴¹ Zimbabwe should guarantee open, secure, and reliable internet access during elections and other periods of public interest.

³⁴ Constitution of Zimbabwe Amendment (No 20) Act 2013, s 62

³⁵ Freedom of Information Act 2020; Freedom of Information (General) Regulations 2021, SI 229 of 2021.

³⁶ MISA Zimbabwe (n 16).

³⁷ African Commission on Human and Peoples' Rights (n 29).

³⁸ Censorship and Entertainments Control Act [Chapter 10:04], ss 13 and 14; Refworld, 'Zimbabwe: Censorship and Entertainments Control Act' <https://www.refworld.org/legal/legislation/natlegbod/1967/74513> accessed 2 July 2026.

³⁹ Broadcasting Services Amendment Act 2025

⁴⁰ MISA Zimbabwe and Media Alliance of Zimbabwe, 'Statement on passage of the Broadcasting Services Amendment Bill in the National Assembly' (5 March 2025) <https://zimbabwe.misa.org/2025/03/05/misa-zimbabwe-maz-statement-on-passage-of-the-broadcasting-services-amendment-bill-in-the-national-assembly/>.

⁴¹ MISA Zimbabwe, 'Internet degrade on the eve of elections' (22 August 2023) <https://zimbabwe.misa.org/2023/08/22/internet-degrade-on-the-eve-of-elections/>

3. Digital Connectivity and Inclusion

24. Zimbabwe has recorded growth in mobile, broadband, and internet subscriptions. POTRAZ's fourth-quarter 2025 figures show an increase in active internet and data subscriptions, internet penetration, broadband penetration, mobile internet use, and fixed internet traffic.⁴² These developments reflect growing reliance on digital platforms for communication, livelihoods, education, financial services, public information and civic participation.
25. However, connectivity gains have not translated into universal, affordable and meaningful access. Official penetration figures are subscription-based and may overstate individual access, especially where users hold multiple SIM cards or rely on intermittent connectivity. Meaningful connectivity requires reliable service, affordable data and devices, stable electricity, relevant local content, digital literacy, accessible services and safe participation.⁴³
26. Rural communities continue to face weaker infrastructure, higher service gaps and fewer public access points. The approval of Starlink and the growth of VSAT services may improve connectivity in underserved areas, but affordability remains central to whether rural and low-income communities benefit.⁴⁴ Satellite and high-speed broadband policy should therefore prioritise inclusive access, transparent licensing, infrastructure competition, consumer protection, and non-discrimination.
27. Women and girls face intersecting barriers to meaningful digital access, including affordability, digital skills gaps, social norms, online abuse, and limited access to devices.⁴⁵ These barriers restrict access to education, livelihoods, public participation, health information, and digital financial services, and may deepen existing gender inequalities.
28. Persons with disabilities continue to face exclusion where devices, platforms, public services, and government information are not designed or delivered in accessible formats. Zimbabwe's digital inclusion policies should therefore mainstream accessibility standards, assistive technologies, accessible public websites, affordable devices, and disaggregated data on disability inclusion.
29. Zimbabwe's Universal Service Fund should be deployed transparently to expand affordable broadband, community networks, school connectivity, public access centres, assistive technologies, and last-mile infrastructure in rural and marginalised communities. The previous UPR submission noted that Zimbabwe's universal access framework is intended to support underserved communities and is financed through operator levies.⁴⁶ Regular publication of fund collections, expenditure, project locations, beneficiaries, and impact would strengthen accountability.

⁴² Gamuchirai Mapako, 'Zimbabwe's Internet Data Penetration Surges to 84.55% in Q4 2025' TechnoMag (29 April 2026) <https://technomag.co.zw/zimbabwes-internet-data-penetration-surges-to-84-55-in-q4-2025/>

⁴³ Alliance for Affordable Internet, *Meaningful Connectivity: A New Target to Raise the Bar for Internet Access*(A4AI, 2020).

⁴⁴ Reuters (n 8); Mapako (n 7).

⁴⁵ United Nations Zimbabwe (n 6); Media Institute of Southern Africa Zimbabwe Chapter, *Small Media and CIPESA* (n 2).

⁴⁶ Postal and Telecommunications Act [Chapter 12:05], Part X; Media Institute of Southern Africa Zimbabwe Chapter, *Small Media and CIPESA* (n 2).

4. Data Protection and Privacy

30. Section 57 of the Constitution protects the right to privacy, including the privacy of communications and personal information.⁴⁷ The enactment of the Cyber and Data Protection Act was a significant legal development since the 2021 submission because Zimbabwe previously lacked a comprehensive data protection framework.⁴⁸
31. The Act establishes data protection obligations and designates POTRAZ as the Data Protection Authority.⁴⁹ It regulates the collection, control, and processing of personal information. It establishes standards for lawful and fair processing, recognises sensitive data, provides for data subject rights, regulates cross-border transfers, and provides for accountability obligations.⁵⁰ These protections are important for safeguarding individuals against unlawful collection, processing, storage, disclosure, and transfer of personal information.
32. The independence of the Data Protection Authority remains a central concern. POTRAZ is designated as the Data Protection Authority, while also regulating the communications sector.⁵¹ Effective data protection requires an independent, adequately resourced and rights-based supervisory authority with clear investigative, corrective and sanctioning powers, as well as safeguards against political or commercial influence.
33. The Act contains broad exceptions relating to national security, public interest, and law enforcement.⁵² These exceptions should be narrowly defined and subject to independent oversight, necessity and proportionality tests, transparency obligations, and effective remedies for affected individuals. Without such safeguards, data protection law may be weakened by broad state discretion.
34. Zimbabwe's surveillance framework remains inadequate. The Interception of Communications Act permits lawful interception, and the Cyber and Data Protection Act amended that framework by establishing a Cyber Security and Monitoring of Interceptions of Communications Centre in the Office of the President.⁵³ This raises serious concerns regarding executive control, insufficient judicial oversight, limited transparency, and weak remedies.
35. Surveillance powers should be subject to prior independent judicial authorisation, clear legal thresholds, notification where appropriate, public reporting, and parliamentary oversight.⁵⁴ The previous UPR submission already identified unlawful surveillance concerns, including facial recognition, biometric data transfers, and reported use of surveillance technologies.⁵⁵ These concerns remain relevant in light of the expansion of biometric systems, digital identity tools, and cybersecurity powers.
36. Biometric and digital identity systems require stronger safeguards. The Act recognises biometric, genetic, and health data as sensitive categories and prohibits processing unless written consent is given, subject to several exceptions.⁵⁶ The law should be strengthened to require human rights and data protection impact assessments, transparency in procurement, independent audits, data minimisation, retention limits, and effective remedies before deployment of facial recognition, biometric databases, digital identity systems, and surveillance tools.
37. Public and private actors should be required to conduct human rights and data

⁴⁷ Constitution of Zimbabwe Amendment (No 20) Act 2013, s 57.

⁴⁸ Media Institute of Southern Africa Zimbabwe Chapter, *Small Media and CIPESA* (n 2).

⁴⁹ Data Protection Act [Chapter 11:22] No 5 of 2021, ss 5 and 6.

⁵⁰ Data Protection Act [Chapter 11:22] No 5 of 2021, ss 7–29.

⁵¹ Data Protection Act [Chapter 11:22] No 5 of 2021, s 5; DLA Piper (n 14).

⁵² Data Protection Act [Chapter 11:22] No 5 of 2021, ss 10–12 and – 29.

⁵³ Data Protection Act [Chapter 11:22] No 5 of 2021, s 37.

⁵⁴ Human Rights Committee, General Comment No 16: Article 17: Right to Privacy (8 April 1988); Human Rights Committee, General Comment No 34 (n 23); https://cipesa.org/wp-content/files/briefs/Digital-Rights-in-Zimbabwe_2021-UPR-submission.pdf

⁵⁵ Media Institute of Southern Africa Zimbabwe Chapter, *Small Media and Collaboration on International ICT Policy for East and Southern Africa, Digital Rights in Zimbabwe, UPR Submission, Session 40* (2021). https://cipesa.org/wp-content/files/briefs/Digital-Rights-in-Zimbabwe_2021-UPR-submission.pdf

⁵⁶ Data Protection Act [Chapter 11:22] No 5 of 2021, s 12.

5. Technology-Facilitated Gender-Based Violence

protection impact assessments before deploying high-risk technologies, including facial recognition, predictive analytics, digital identity systems, biometric databases, algorithmic decision-making tools, and surveillance technologies. The Act recognises a right not to be subject to decisions based solely on automated processing where such decisions produce legal or similarly significant effects.⁵⁷ This right should be made practical through enforceable safeguards, transparency, and access to remedy.

38. Technology-facilitated gender-based (TFGBV) violence has become an increasingly serious barrier to equality, expression, political participation, media freedom, and safety online. Women journalists, women human rights defenders, women politicians, activists, and girls face cyber-bullying, coordinated harassment, non-consensual sharing of intimate images, sexualised disinformation, doxing, impersonation, threats, and blackmail.⁵⁸
39. Zimbabwe's Cyber and Data Protection Act includes offences relating to cyber-bullying and harassment, transmission of intimate images without consent, and offences involving electronic communications and harmful materials.⁵⁹ These provisions are important, but implementation must be survivor-centred, gender-responsive, and consistent with freedom of expression, privacy, and due process.
40. Recent evidence indicates that TFGBV is widespread. A 2025 UN-supported national symposium reported that a UNESCO/MISA study found 63% of women journalists in Zimbabwe had experienced TFGBV, while a national survey by Emthonjei Women's Forum found that 75% of respondents had faced digital abuse in the previous year.⁶⁰ Women in politics were particularly affected during the 2023 electoral cycle, with online abuse frequently taking the form of gendered insults, body shaming, misogynistic attacks, and threats intended to intimidate and discourage their political participation.⁶¹ Politicians such as Fadzayi Mahere and Linda Masarira were among those subjected to sustained gender-based online harassment, despite representing different political parties.⁶² These findings show that online abuse is not isolated, but a systemic barrier to women's equal participation in media, civic space, and public life.
41. TFGBV has a chilling effect on women's participation in journalism, politics, human rights work, and civic debate. It pushes women out of public digital spaces, limits professional opportunities, causes psychological harm, and weakens democratic participation.⁶³ Zimbabwe should therefore strengthen prevention, response, and remedy mechanisms, including trained police and prosecutors, confidential reporting channels, preservation of digital evidence, psychosocial support, legal aid, platform cooperation, data collection, and public education on online safety and equality.

⁵⁷ Data Protection Act [Chapter 11:22] No 5 of 2021, s 25.

⁵⁸ United Nations Zimbabwe (n 6); UNESCO, 'International Day to End Impunity for Crimes against Journalists 2025' (2 November 2025) <https://www.unesco.org/en/articles/international-day-end-impunity-crimes-against-journalists-2025> accessed 2 July 2026.

⁵⁹ Data Protection Act [Chapter 11:22] No 5 of 2021, ss 164B and 164E.

⁶⁰ United Nations Zimbabwe (n 6).

⁶¹ AIJS, 'African feminist activism and democracy: Social media publics and Zimbabwean women in politics Online', <https://www.si-ajis.org/wp-content/uploads/2023/12/African-feminist-activism-and-democracy-Social-media-publics-and-Zimbabwean-women-in-politics-online.pdf>.

⁶² Dube N, 'Cyberbullying Against Women in Power: The Dark Reality Facing Female Politicians in Zimbabwe and Beyond', <https://www.berthaslegacy.org/post/cyberbullying-against-women-in-power-the-dark-reality-facing-female-politicians-in-zimbabwe-and-bey>.

⁶³ UNESCO (n 57); United Nations Zimbabwe (n 6).

Recommendations

In light of the foregoing, the aforementioned organisations recommend that the Government of Zimbabwe;

With regard to the Freedom of Expression and Opinion:

1. Review and repeal sections 31 and 33 of the Criminal Law (Codification and Reform) Act to decriminalise protected expression, including criticism of public officials, satire, political commentary, journalism, and public-interest reporting.⁶⁴
2. Review and amend the Criminal Law Codification and Reform Amendment Act, 2023, including provisions on “sovereignty” and “national interest”, to ensure that civic engagement, international advocacy, human rights reporting, and participation in regional and international mechanisms are not criminalised.⁶⁵
3. Revise or reform speech-related provisions of the Cyber and Data Protection Act, including sections 164, 164B, and 164C, to ensure that they are narrowly defined and comply with legality, legitimate aim, necessity, and proportionality.⁶⁶
4. End arrests, harassment, intimidation, and prosecution of journalists, activists, artists, opposition supporters, human rights defenders, and citizens for lawful online and offline expression.⁶⁷

Freedom of Information and Censorship of Content:

5. Fully implement the Freedom of Information Act and its regulations by appointing trained information officers, publishing proactive disclosure policies, ensuring accessible request procedures, and publishing annual compliance data.⁶⁸
6. Guarantee timely access to election-related, public health, procurement, telecommunications, digital identity, surveillance, and public finance information.⁶⁹
7. Review and amend sections 13 and 14 of the Censorship and Entertainments Control Act to remove vague and overbroad content restrictions that enable arbitrary censorship.⁷⁰
8. Review the Broadcasting Services Act and the 2025 amendments to ensure that online content, podcasts, streaming, social media live broadcasts, citizen journalism, and public-interest commentary are not subjected to disproportionate licensing or censorship.⁷¹
9. Strengthen the independence, transparency, and resourcing of media and information regulators, including the Zimbabwe Media Commission and the Broadcasting Authority of Zimbabwe.⁷²

⁶⁴ Criminal Law (Codification and Reform) Act [Chapter 9:23], ss 31 and 33; Human Rights Committee, General Comment No 34 (n 23).

⁶⁵ Criminal Law (Codification and Reform) Amendment Act 2023; Amnesty International (n 19).

⁶⁶ Data Protection Act [Chapter 11:22] No 5 of 2021, ss 164, 164B and 164C.

⁶⁷ Freedom House (n 27); Human Rights Committee, Concluding Observations on the Second Periodic Report of Zimbabwe (n 28).

⁶⁸ Freedom of Information Act 2020; Freedom of Information (General) Regulations 2021, SI 229 of 2021; MISA Zimbabwe (n 16)

⁶⁹ Constitution of Zimbabwe Amendment (No 20) Act 2013, s 62; African Commission on Human and Peoples' Rights (n 29).

⁷⁰ Censorship and Entertainments Control Act [Chapter 10:04], ss 13 and 14.

⁷¹ Broadcasting Services Amendment Act 2025; MISA Zimbabwe and Media Alliance of Zimbabwe (n 36).

⁷² Constitution of Zimbabwe Amendment (No 20) Act 2013, s 61(3); MISA Zimbabwe and Media Alliance of Zimbabwe (n 36).

Digital Connectivity and Inclusion:

10. Guarantee open, secure, and uninterrupted internet access during elections, protests, public emergencies, and periods of political contestation.⁷³
11. Prohibit internet shutdowns, throttling, and arbitrary platform blocking, and require public disclosure of any network restriction orders, including their legal basis, scope, duration, and responsible authority.⁷⁴
12. Use the Universal Service Fund transparently to support rural broadband, community networks, school connectivity, public access centres, assistive technologies, and affordable devices.⁷⁵
13. Publish disaggregated connectivity data by gender, disability, age, income level, and rural-urban location to guide inclusive digital policy.⁷⁶
14. Promote affordable connectivity by reducing the cost of data, encouraging competition, supporting infrastructure sharing, and ensuring that new satellite and broadband services benefit underserved communities.⁷⁷

Data Protection and Privacy

15. Strengthen the independence, capacity, and accountability of the Data Protection Authority, including through institutional safeguards that separate data protection oversight from telecommunications sector regulation.⁷⁸
16. Amend broad national security, law enforcement, and public-interest exemptions in data protection law to ensure they are necessary, proportionate, time-bound, and subject to independent oversight.⁷⁹
17. Amend the Interception of Communications Act to require prior independent judicial authorisation for surveillance, clear thresholds for interception, transparency reporting, parliamentary oversight, and effective remedies.⁸⁰
18. Adopt specific safeguards for biometric data, facial recognition, digital identity systems, artificial intelligence, public-sector databases, and surveillance technologies, including mandatory human rights and data protection impact assessments.⁸¹
19. Require public transparency in the procurement, deployment, and auditing of surveillance and biometric technologies.⁸²

⁷³ MISA Zimbabwe, 'Internet degrade on the eve of elections' (22 August 2023) <https://zimbabwe.misa.org/2023/08/22/internet-degrade-on-the-eve-of-elections/>

⁷⁴ Human Rights Council, *The Promotion, Protection and Enjoyment of Human Rights on the Internet* UN Doc A/HRC/RES/32/13 (18 July 2016).

⁷⁵ Postal and Telecommunications Act [Chapter 12:05], Part X; Media Institute of Southern Africa Zimbabwe Chapter, *Small Media and CIPESA* (n 2).

⁷⁶ Mapako (n 7); Alliance for Affordable Internet (n 39).

⁷⁷ Reuters (n 8); Mapako (n 7).

⁷⁸ Data Protection Act [Chapter 11:22] No 5 of 2021, s 5; DLA Piper (n 14).

⁷⁹ Data Protection Act [Chapter 11:22] No 5 of 2021, ss 10–12 and 28–29.

⁸⁰ Interception of Communications Act [Chapter 11:20]; Data Protection Act [Chapter 11:22] No 5 of 2021, s 37.

⁸¹ Data Protection Act [Chapter 11:22] No 5 of 2021, ss 12 and 25.

⁸² Media Institute of Southern Africa Zimbabwe Chapter, *Small Media and CIPESA* (n 2).

Technology-Facilitated Gender-Based Violence

20. Implement a survivor-centred and gender-responsive framework for preventing and responding to TFGBV, including cyberstalking, doxing, coordinated harassment, sextortion, non-consensual intimate image abuse, online grooming, misogynistic disinformation, and deepfake sexual abuse.⁸³
21. Train police, prosecutors, judicial officers, teachers, and social workers on digital evidence, survivor-centred response, confidentiality, trauma-informed practice, and freedom of expression safeguards.⁸⁴
22. Establish accessible reporting channels, legal aid, psychosocial support, and referral pathways for survivors of online abuse.⁸⁵
23. Require digital platforms and service providers to cooperate with lawful, rights-respecting processes for reporting, evidence preservation, and takedown of unlawful, abusive content.⁸⁶
24. Collect and publish disaggregated data on TFGBV while protecting survivor privacy and safety.⁸⁷

⁸³ Data Protection Act [Chapter 11:22] No 5 of 2021, ss 164B and 164E; United Nations Zimbabwe (n 6).

⁸⁴ MISA Zimbabwe, 'Internet degrade on the eve of elections' (22 August 2023) <https://zimbabwe.misa.org/2023/08/22/internet-degrade-on-the-eve-of-elections/> accessed 2 July 2026; Amnesty International, 'Zimbabwe: President's signing of "Patriotic Bill" a brutal assault on civic space' (15 July 2023) <https://www.amnesty.org/en/latest/news/2023/07/zimbabwe-presidents-signing-of-patriotic-bill-a-brutal-assault-on-civic-space/> accessed 2 July 2026; United Nations Zimbabwe, 'Turning the Tide, Zimbabwe's Push to End Gender-Based Violence in a Digital Age' (24 November 2025) <https://zimbabwe.un.org/en/305894-turning-tide-zimbabwe%E2%80%99s-push-end-gender-based-violence-digital-age>

⁸⁵ Data Protection Act [Chapter 11:22] No 5 of 2021, ss 164B and 164E.

⁸⁶ Data Protection Act [Chapter 11:22] No 5 of 2021, ss 164B and 164E.

⁸⁷ United Nations Zimbabwe (n 6).



Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

☎ +256 414 289 502

✉ programmes@cipesa.org

✕ @cipesaug 📘 facebook.com/cipesaug 🔗 [Linkedin/cipesa](https://linkedin/cipesa)

🌐 www.cipesa.org