

20
26

State of Internet
Freedom in Zambia
Report
6th Edition

Theme: Advancing Zambia's digital future,
bridging the digital divide while fighting for freedom

A Bloggers of Zambia In-country Digital Rights Initiative
for Promoting Digital Democracy



Bloggers of Zambia is an independent, not-for-profit organisation that was established in the year 2017. Our thematic areas of work are; Digital Rights, Press Freedom, Civic Tech and Media and Information Literacy.

CURRENT AND PAST PROJECTS

Some of the current and previous projects that Bloggers of Zambia has undertaken under our four thematic areas include;

a. **Digital Rights**

- Promoting Digital Rights and Democracy in Zambia, supported by German Development Corporation GIZ (2022 – 2024). The objective of the project is to influence and monitor enactment and implementation of cyber legislation in Zambia.
- Expanding the Space for Freedom of Expression and Digital Rights, supported by National Endowment for Democracy (2022 – 2024). The objective of this project is to expand protections and citizen awareness around digital rights, freedom of expression, and access to information in Zambia.

b. **Press Freedom**

- Strengthening Police and Media relations for the safety and security of journalists in Zambia supported by the German Federal Foreign Office through the German Embassy in Lusaka (2019 – 2022). This is a project focused on safety and security of journalist from police work/ violations.
- Bloggers of Zambia is also the secretariat for the National Organising Committee for World Press Freedom Day 2023 and 2024.
- With support from our partners, Bloggers of Zambia has trained members four press clubs in digital literacy and online safety and security.

c. **Civic Tech**

- Journalism X. This is a prototype online tool for newsroom collaboration on fact-checking and verification and artificial intelligence education supported by Duetsche Welle (2023 – March 2024).
- Safe City Project in collaboration with Red Dot Foundation. This is a crowd mapping tool for reporting online and offline gender based violence in Zambia. This project is on-going.

d. **Media and Information Literacy**

- Bloggers of leveraging internal tools and skills in addition to a cohort of young creative content producers to make and popularise various types of online content such as animations, short videos and skits, podcasts and illustrations covering topics such as digital literacy, online safety and security for different stakeholder groups for education and awareness purposes.

MISSION:

An open society where digital rights and the rights-based offline and online media platforms are guaranteed and protected

MOTTO:

Our motto is, 'Keeping Online Spaces Open'.
Hashtag #OpenSpaceZM

Contents

Acknowledgements | 4

Executive Summary | 5

Key Findings | 7

Purpose and Scope of the Report | 9

Introduction | 11

Freedom of Expression and Media Freedom | 13

Access to Information and Digital Civic Space | 14

Cyber Harassment | 17

Cyber Crime, Cybersecurity, Enforcement and Digital Safety | 18

Internet Access, Affordability and Digital Inclusion | 21

Misinformation and Information Integrity | 23

Digital Literacy and Skills Development | 24

Artificial Intelligence and Emerging Technologies | 26

Gender, Youth and Marginalised Groups | 27

Digital Ids | 29

Challenges and Concerns in the Protection of Internet Freedoms | 30

Recommendations | 33

Conclusion | 37

CONTACTS

Website: <https://bloggersofzambia.org/>

Facebook: www.facebook.com/zambloggers

Twitter: www.twitter.com/zambloggers

Telephone/ WhatsApp/ Signal: +260975174238

Acknowledgments

The development of the 2025 State of Digital Rights in Zambia Report was made possible by the British Foreign Commonwealth and Development Office through Diakonia Zambia and BBC Media Action, Deepening Democracy Facility project.

Gratitude goes to the Consultant who led the process. Congratulations to staff members from Bloggers of Zambia for their support and technical input to the development of the report. Without this support and dedication to duty, the development of this report would not have been possible. We would like to thank everyone who supported the development of this report and assisted the team to obtain the necessary information. We would like to thank everyone who helped with setting up appointments, reviewing and finalising this important report. We would like to thank the Board and Management of Bloggers of Zambia for playing an active supportive role in the entire process.

Executive Summary



The 2025 State of Internet Freedom in Zambia presents an analysis of the digital rights landscape in Zambia, highlighting the progress, challenges, and opportunities that have emerged over the past year in the midst of rapid digitalization.

This report is under the theme, 'Advancing Zambia's digital future, bridging the digital divide while fighting for freedom'. We are glad to present the 2025 State of

- Digital Rights in Zambia report.
- Zambia's internet landscape is characterized by expanding, yet lower-than-expected, user numbers compared to subscription-based reports. There were 7.29 million individuals using the internet in Zambia at the end of

2025, when online penetration stood at 33.0 percent.

The report objectives are focused on assessing the status of digital rights in Zambia during the period being covered. Particularly, this report analyses the impact of laws, policies, and regulatory practices on digital rights. The report also documents key incidents, patterns and case studies of digital rights violations and positive developments in Zambia's digitalisation agenda, which has been one of the fastest-paced on the continent. Additionally, the report examines access, affordability and digital inclusion across different demographics and regions and the patterns reveals development being made to bridge the digital gaps when it comes to connectivity, affordability and gender issues where women and girls remain among the marginalised and excluded demographics such as disability and rural-urban.

The implications of misinformation, elections, surveillance and emerging technologies such as AI, Internet of Things etc on human rights continue to be growing challenges although some investment by civil society, government and private are being made in digital literacy, fact-checking and verification for various groups.

In this report, freedom of expression and media freedom operating environment online have improved, but remain challenging because of digital literacy, harmful content and legislation, which is perceived to be targeting journalism activities. In addition to this, access to information and digital civic space have continued to escalate as more citizens have the desire to participate in public discourse especially on social and multimedia platforms such as WhatsApp.

Privacy, data protection and surveillance is also highlighted and particularly, the prominent CCTV Bill alongside the Cyber Security Act and Cybercrimes Act of 2025 for weak oversight and broad surveillance scope that could interfere with privacy and other online freedoms.

Regarding cybercrime, cybersecurity enforcement and digital safety, the report notes continued increases in investment in

cybersecurity infrastructure with notable improvements in the detection and prevention of cyber threats. Collaboration between the government, private sector and civil society has strengthened cybersecurity measures.

On Internet access, affordability and digital inclusion, this report highlights progress and also challenges to connectivity based on various reasons such as gender, affordability and safety. These challenges have escalated digital exclusion.

Misinformation, elections and information integrity is also highlighted as a key issue especially in view of the August 2026 general elections in which the internet and particularly social media are key tools for political discourse and participation.

Artificial Intelligence and emerging technologies present interesting findings, with an increase in the deployment and consumption in various sectors. For instance, AI literacy is essential in the adoption of emerging technologies.

Progress has been made on advancing digital rights issues for women and girls, youth and marginalised groups but the conversation around LGBTQI in the digital space is still a shunned narrative based on the treatment of the subject in the Zambian social context.

Legislation remains one of the most topical internet rights issues and its implementation is monitored in the new political environment where Internet consumers have various opinions regarding its implementation. This report remains a crucial resource for policymakers, Civil Society Organisation (CSOs), lawyers, journalists, academia, students, media associations, regulators, law enforcement, Parliamentarians, international development partners and all stakeholders in the internet governance and technology sector who are aiming to foster a more inclusive, affordable, secure and more equitable internet environment for all Zambians.

Key Findings

1: Legal and Regulatory Frameworks

Progress: The Zambian Parliament enacted two major pieces of legislation (the Cyber Security Act, 2025 and the Cyber Crimes Act, 2025) replacing the Cyber Security and Cybercrimes Act number of 2021. The government presents these as milestones in strengthening digital governance, offering clearer frameworks for handling cybercrime, aiding prosecution of online offences such as identity theft, phishing, and fraud, and enhancing national cybersecurity resilience. Additionally, the government introduced to parliament, the Closed-Circuit Television (CCVT) Bill to regulate CCTV systems in public and private spaces, aiming to enhance security, establish a National Public Security Command Centre, and define regulations for mobile and stationary cameras¹. Furthermore, the \$100 million [Digital Zambia Acceleration Project \(DZAP\)](#) is expanding and enabling internet access to facilitate digital, inclusive public services.

Challenges: Enforcement of this legislation remains inconsistent and gaps in legislation need to be addressed to keep pace with technological developments. Experts have also cited capacity issues and consistency in the adoption of best practices. Additionally, stakeholders have raised concerns on stakeholder consultations and involvement in the law and policy developments citing heavy bias towards state apparatus at the detriment of other groups.

2: Privacy, data protection and Surveillance

Progress: The Closed-Circuit Television (CCTV) Bill was introduced earlier in 2025 to regulate CCTV systems in public and private spaces, aiming to enhance security, establish a National Public Security Command Centre, and define regulations for mobile and stationary cameras. Cabinet approved plans to repeal the 2021 Data Protection Act to broaden Zambia's legal framework for data management, AI, analytics, and emerging digital technologies². Zambia's Office of the Data Protection Commissioner (ODPC) is now fully operational and actively enforcing the Data Protection Act 2021. A Code of Conduct for Data Controllers and Data Processors was developed in early 2025 under the authority of the Act. The online registration portal was launched, with a compliance deadline of 30 April 2025. Enforcement of the Act including penalties for non-registration, data breaches, and non-compliance officially started in March 2025³.

Challenges: Digital Rights Groups and Civil Society Organisations (CSOs) flagged the CCTV Bill for weak oversight and broad surveillance scope that could interfere with privacy and other freedoms. These laws are considered as intrusive and raise concerns about its potential impact on the private lives of citizens.

3: Freedom of Expression and Censorship

Progress: Despite regulatory concerns, internet penetration continues to rise, enhancing public engagement in online political discourse and information exchange. This broader connectivity gives more people tools to express opinions and access diverse viewpoints

Challenges: Censorship, content moderation and restrictions on online speech persist. Balancing the need for security and the protection of free expression is an ongoing challenge. The Cyber Security Act, 2025 and the Cyber Crimes Act, 2025 broad wording and surveillance powers could undermine privacy and freedom of expression.

4: Cyber Security

Progress: The Zambia Police Service deployed cybercrime officers to provincial headquarters nationwide, expanding the government's capacity to investigate, respond and prosecute digital offences outside of Lusaka. The Zambia Cyber Security Agency (ZCSA), ZICTA (the Zambia Information and Communications Technology Authority), the Police, and other entities now work more closely to harmonize enforcement, capacity building, reporting and incident response as part of the implementation of the cyber security Acts⁴.

Challenges: The sophistication and frequency of cyber-attacks and scams in financial technology, especially mobile money continue to rise, outpacing the current capacity to respond effectively. Enhancing cybersecurity resilience remains a critical priority.

Additionally, the overlapping and duplication of roles and mandates between ZICTA and ZCSA is a likely source of confusion and cyber security enforcement processes.

5: Digital Literacy

Progress: Investment in cybersecurity infrastructure has increased, with notable improvements in the detection and prevention of cyber threats. Collaboration between the government, private sector and civil society has strengthened cybersecurity measures.

Challenges: The sophistication and frequency of cyber-attacks and scams in financial and limited education and Awareness: Many Zambians are unaware of their digital rights and the risks associated with digital activities, leading to increased vulnerability to online fraud, data breaches and misinformation.

6: Internet Access

Progress: The government reports that over 92% of the population is now connected in some form, through fibre links, satellite and mobile networks, reflecting significant infrastructure build-out.

Challenges: Estimates of internet penetration vary widely—from about 33 % actual internet use to much higher subscription figures, pointing to a digital divide between urban and rural areas and differences between having a subscription versus regular usage. Additionally, the internet landscape is characterized by expanding, yet lower-than-expected, user numbers compared to subscription-based reports.

7: Gender, youth and marginalised Groups Equity

Progress: Efforts to promote gender equity in the digital space have shown positive results, with increased participation of women and marginalised groups in digital activities.

Challenges: Women and marginalized groups often face additional barriers, such as online harassment and limited access to digital tools, which hinder their ability to exercise their digital rights. The legal environment remains hostile to LGBTQI individuals, with same-sex sexual conduct remaining criminalized. Despite advocacy, the draft Constitution of Zambia (Amendment Bill No. 7 of 2025) contains no provision for the decriminalization of same-sex relationships.

Purpose and Scope of the Report

The 2025 State of Digital Rights in Zambia Report showcases the key developments and changes within the digital rights landscape, state of internet freedoms in Zambia, and updates to digital law and policy in Zambia. This is the sixth edition of the in-country report from the time the initiative was launched in 2019. This study provides a comprehensive assessment of the state of digital rights and internet governance aspects in Zambia, examining legal, policy, technological and socio-political developments that shaped the digital environment during the review period. The scope of the study is structured around three major components: desk research, field and stakeholder engagement, and thematic analysis, guided by a mixed-methods, human-rights-based research approach that are detailed below:

Desk research included

1. Review of national laws, regulations, policies and bills affecting digital rights in Zambia.
2. Analysis of regional and international human rights instruments relevant to Zambia.
3. Review of existing research, reports, court decisions, media articles and civil society documentation

Field and stakeholder engagement

Key informant interviews with, journalists and media practitioners, content creators, civil society organisations, lawyers, academia, ICT regulators and policymakers

The report covers the following thematic areas

1. Freedom of expression and media freedom online
2. Access to information and digital civic space
3. Privacy, data protection and surveillance
4. Cyber Harassment
5. Cybercrime, cybersecurity enforcement and digital safety
6. Internet access, affordability and digital inclusion
7. Digital Public Infrastructure
8. Misinformation, elections and information integrity
9. Digital literacy and digital skills development
10. Artificial Intelligence and emerging technologies
11. Gender, youth and marginalised groups including LGBTQI in the digital space
12. Digital Identity

The methodology uses a mixed-methods, human rights-based approach, incorporating

- Qualitative and quantitative research
- Legal and policy analysis
- Case studies and incident documentation
- Stakeholder consultations
- Comparative regional and international perspectives

Purpose and Scope of the Report

The report provides an in-depth analysis and comprehensive overview of the primary objectives of this report which are to;

1

Debate and dialogue

The report serves as a tool for identifying multistakeholder issues and a platform for debating and shaping laws, policies and regulatory frameworks.

2

Assess and evaluate

The report aims to assess the current status of digital rights standards in Zambia, including the examination of the legal, policy and regulatory frameworks in place, the implementation of digital laws and policies and the overall protection of Internet freedoms. The report seeks to evaluate the impact of digital rights on various sectors such as health, education, governance, the economy and social inclusion.

3

Awareness and Advocacy

The report is also a tool for education and awareness raising among various stakeholders, policymakers, civil society organizations, the private sector, and the general public about the importance of digital rights. The report is intended to serve as an advocacy tool, providing evidence-based recommendations for the enhancement and protection of digital rights in Zambia.

4

Monitoring and Accountability

The report functions as a monitoring tool to track progress and identify challenges in the realization of digital rights in Zambia. It aims to hold relevant authorities and institutions accountable for their roles in protecting and promoting digital rights and internet freedoms.

5

Capacity Building

By offering detailed insights and analyses, the report aims to build the capacity of stakeholders to understand, protect, and advocate for inclusive and progressive internet and digital rights. The report serves as an educational resource for training and awareness programs focused on digital rights issues.



Introduction

Press Freedom, Freedom of Expression, and Internet Rights are fundamental rights in any democratic society.

However, these fundamental rights remain constantly under threat due to several competing factors, including offline and digital authoritarianism, suppression of critical and oppositional voices and the misuse of national security as a means to trample internet freedoms. While the above reasons could be genuine with contextual justifications, there is the need to balance public security needs with the stated fundamental rights. Freedom of expression, privacy, media freedom, access to information and the broader digital rights are some of the fundamental rights that contribute to deepening democracy in Zambia. These rights that are guaranteed in the Constitution of Zambia create an atmosphere that promotes citizens' voices in public decision-making processes, including being able to hold public institutions accountable.



Traditional media and online platforms play a crucial role in promoting democracy in a democratic environment because they provide a platform for inclusion, participation and access to information. Particularly, these online and offline platforms facilitate for access to information, which is key for informed decision making and participation in a democracy⁵.

Internet freedom acts as an enabler for social, economic, and political development. It ensures equal access to knowledge, supports democratic processes, and enables safe communication, which is increasingly threatened by global surveillance, internet shutdowns, and censorship. Zambia is classified as "Partly Free" with an Internet Freedom Score of 62 out of 100. While the country does not actively block major social media platforms or restrict network access, it faces

- challenges regarding user arrests and a shrinking space for digital expression⁶.
- Internet freedom offers the protection of individual freedoms, promotes equality, and enables people to fully participate in the digital world. As technology continues to evolve, safeguarding these rights becomes ever more critical to ensure a fair, just, and inclusive digital future. The report therefore highlights the state of internet freedoms in critical areas of both progress and regression and provides recommendations for expanding the digital space in Zambia.

Freedom of Expression and Media Freedom Online

Article 19 of the International Covenant on Civil and Political Rights (ICCPR) firmly guarantees the right to freedom of opinion and expression, protecting every individual's ability to seek, receive, and impart information and ideas of all kinds, through any media and across all borders. This foundational human right applies equally in digital spaces, underpinning freedom of expression and media freedom online. Article 19(3) recognises that restrictions may be imposed, but only under strict conditions: they must be clearly provided by law, pursue a legitimate aim such as protecting the rights or reputations of others, safeguarding national security or public order, or promoting public health or morals, and must be necessary and proportionate. In the context of the modern digital environment—where online platforms, social media, and digital journalism are central to public discourse—Article 19 provides critical support for safeguarding online expression, ensuring that states uphold an open, free, and inclusive digital civic space while preventing unjustified censorship, surveillance, or suppression of independent media⁷.

Zambia is a party to the ICCPR, and its Constitution domestically recognises and applies these standards. ICCPR General Comment No. 34 interprets Article 19 extensively, clarifying that freedom of expression covers political discourse, criticism of government, journalism, and expression online. It emphasises that restrictions must be necessary and proportionate and must not be used to silence dissent⁸. The African Charter on Human and Peoples' Rights (ACHPR / Banjul Charter) Article 9 explicitly protects freedom of expression and information (including the right to receive and impart information). Restrictions are permitted only where necessary under law and for legitimate aims. The Charter obliges State Parties (like Zambia) to guarantee these rights and report periodically on compliance⁹.

The Constitution of Zambia guarantees freedom of expression under Article 20 (1)¹⁰. The Constitution also guarantees freedom of assembly and association regardless of frontier. In April 2025, the Zambian president signed into law the revised Cyber Security Act and the Cyber Crimes Act (the Acts), a legislative package intended to address rising cyber threats and promote digital safety, security and hygiene. These Acts were developed and deliberated upon with minimal transparency and public participation¹¹. While the Global Network Initiative (GNI) acknowledges Zambia's efforts to strengthen its digital infrastructure and tackle cybercrime, some provisions in these laws raise many concerns to freedom of expression, access to information and privacy. Prior to the enactment, efforts were made on stakeholder consultations and submissions to parliament. However, there was limited stakeholder input that was incorporated into the final bills. The limited stakeholder participation and obscured processes resulted in laws that contain several provisions that have purposely vague definitions. This process, which was rushed and was heavily biased towards state institutions, including the military contradicts President Hichilema's earlier promises to reform Zambia's digital laws through inclusive dialogue with civil society¹².

Zambia's online environment is relatively open dissemination of news, ideas and opinions, including political content, yet freedom of expression is shaped by legal and political considerations. Broadly framed provisions in the Cyber Security Act and Cyber Crimes Act and public order laws often create uncertainty about what constitutes permissible online commentary. Online self-censorship has become prevalent, especially when covering oppositional and politically related topics, corruption, governance, or social justice issues. Journalists report that fear of reprisals ranging from online harassment to potential legal consequences can constrain investigative reporting and opinion-based journalism. Smaller, independent digital outlets are particularly vulnerable, as they operate without institutional protection or legal resources to defend against harassment or content takedown¹³.

Findings in this report indicate an increase in defamation and hate speech arrests for posts and comments made online, where citizens have been arrested and charged under the Cyber Security and Cybercrimes Act 2021. For instance, three individuals were arrested and charged under the 2025 Cyber Crimes Act for allegedly spreading false statements about President Hakainde Hichilema's health on social media in January, 2025. The revised cyber legislation was promoted as enhanced tools for targeting citizen voices online, rather than laws for making the internet safe and secure and increasing access. Many citizens were constrained from engaging on politically sensitive topics and also criticising government officials, including those from the ruling party for fear of being arrested under provisions of the Cybercrimes Act¹⁴.

The conviction of Munir Zulu (May 2025), a former parliamentarian and his subsequent sentencing to 18 months imprisonment with hard labour for a 2023 social media post that was deemed seditious, following continued enforcement of online speech control is a case in point. On 15 March 2025, the Zambia Police Service denied clearance for nationwide protests planned by the opposition Tones Alliance, citing the Public Order Act. Authorities stated that the demonstrations posed a threat to public order. In contrast, the Citizen First party leader Harry Kalaba was able to hold a public rally in March without interference or obstruction from the police. These actions have created a tense and uncertain environment for civil society actors, opposition leaders, activists and human rights defenders, undermining their ability to express themselves, associate and assemble freely¹⁵.

Access to information and digital civic space



The reintroduction of laws like the Cyber Security Act No. 3 of 2025 and the Cyber Crimes Act No. 4 of 2025 (the “new cyber laws”) have the potential to further restrict fundamental freedoms and negatively impact the civic space in Zambia.

The Cyber Crimes and Cyber Security Acts were passed on 8 April 2025. Section 5 & Section 6 – Critical Information Data for criminalizes the unauthorised disclosure or possession of “critical information” or data related to “critical information infrastructure.” Critics say these definitions are overly broad and vague, covering anything linked to public safety, economic stability, health, international stability, or national security. This could make routine journalistic, academic, or whistleblowing activities unlawful without State approval. No clear public-interest exceptions or safeguards are included to protect legitimate disclosure. Section 19 – Deceptive Electronic Communications prohibits transmission of unsolicited or “deceptive” communications and, in particular, falsified headers in electronic messages with intent to mislead. Legal commentators warn that terms like “deceptive” or “misleading” are open-ended, meaning journalists or social commentators

- could be prosecuted for subjective editorial choices or satire. These laws have sparked widespread debate and backlash across various sectors of society, raising concerns about their true intent, particularly regarding the treatment of oppositional voices and critical citizens¹⁶.

- Although there are verbal policy pronouncements for press houses to operate freely, the freedom of information and media freedom in Zambia remain under threat, with isolated incidents of journalists being targeted and arrested for journalistic activities such as covering opposition activities, photographing or filming police in operations etc. For instance, on March 7, 2025, journalist Hope Chooma was arrested in Mazabuka under unclear circumstances linked to coverage ruling UPND members who were not in good standing with the party. The arrest drew condemnation from media rights advocates and media development organisations, who viewed it as a troubling act of repression against press freedom¹⁷.

Privacy, data protection and Surveillance



The Constitution of Zambia affirms the right to privacy in Article 17.

The Data Protection Act established the functions of the Data Protection Authority and provides for the protection of personal data and the rights of data subjects including the right to privacy. The law also regulates the use of personal data and regulates data collectors, processors and controllers. The Data Protection Act addresses the key principles

- of personal data protection and privacy like
- the right to access or obtain information on
- whether an entity is processing the
- individual's personal information and the
- right to erase or restrict processing of such
- data. In addition, the law sets out strong
- measures for data processors and
- controllers to notify the Data Protection
- Authority of any security breaches involving

personal information within 24 hours¹⁸.

Zambia's Office of the Data Protection Commissioner (ODPC) is now fully operational and actively enforcing the Data Protection Act 2021. This marks a shift from a dormant legislative framework to enforcement and compliance oversight. A Code of Conduct for Data Controllers and Data Processors was developed in early 2025 under the authority of the Act. This helps clarify practical obligations such as lawful data handling, security, and accountability. Under the Act, all entities that collect, use, process, or store personal data must register with the ODPC. The online registration portal was launched, with a compliance deadline of 30 April 2025. Enforcement of the Act including penalties for non-registration, data breaches, and non-compliance officially started in March 2025¹⁹.

The United States Embassy in Zambia has raised alarm over the country's newly enacted cybercrime law, which grants authorities sweeping powers to intercept and monitor electronic communications. The advisory issued by the United States Embassy notes that the revised cybercrime law enforces the monitoring of phone calls, emails, text messages, and streamed content, to determine whether they contain what the law describes as "critical information".

"As this new law introduces an intrusive surveillance ecosystem significantly different from privacy protection provisions that prevail in many countries, the embassy of the United States encourages Americans living in Zambia or considering visiting the country to carefully assess the implications of this law and adjust accordingly," the US statement said²⁰.

The Closed-Circuit Television Public Protection Bill, 2025 was published for public notice and introduced in the Zambian National Assembly in March 2025. It was

intended to provide a legal framework governing the licensing, installation, and operation of CCTV systems including public and private surveillance cameras through regulation, registration, and a national command structure²¹. Key features in the draft included:

- Establishing a National Public Security Command Centre to oversee CCTV systems and coordinate security functions.
- Licensing requirements for operating CCTV or mobile CCTV systems on both public and private premises.
- Rules on applications, renewals, suspensions, and revocations of CCTV licences.
- Provisions on prohibiting disclosure of information to unauthorised persons.

The CCTV Bill had previously passed through Parliament, paving the way for the expansion and regulation of surveillance systems in public spaces. However, concerns emerged regarding the scope of surveillance powers and the safeguards available to protect citizens' rights. There are strong concerns that the legislation could erode privacy rights and democratic freedoms, similar to criticisms levelled against the 2025 Cyber Security Act and Cybercrimes Act. Despite controversies and opposition concerns regarding surveillance overreach, the bill had successfully passed its third reading in Parliament in July 2025 and only awaited Presidential assent. Laws that touch on surveillance and personal privacy must be approached with caution, stressing the importance of balancing security objectives with constitutional protections. Legislation of such nature should not undermine civil liberties or create room for misabuse²².

Cyber Crime, Cybersecurity enforcement and digital safety



As Zambia increasingly embraces digital transformation, the importance of a robust cybersecurity framework becomes paramount.

This assessment of the cybersecurity landscape in Zambia highlights key areas such as legal, infrastructure, and regulatory frameworks, cybersecurity threats and the capacity of institutions to handle cybersecurity challenges. Zambia's digital environment has undergone notable changes in 2025, particularly following the enactment of the Cyber Security Act No. 3 of 2025 and the Cyber Crimes Act No. 4 of 2025 introducing new regulatory frameworks that may impact digital rights and civic engagement²⁴.

These laws grant the state and law enforcement extensive powers to monitor and control online activities if left unchecked, with minimal safeguards for genuine citizen actions. These laws are intended to safeguard users and secure online spaces.

- However, enforcement is inconsistent and lacks transparency. Broadly interpreted provisions create uncertainty regarding legitimate expression. Instances exist where
- journalists, bloggers, or citizens have faced intimidation, content removal requests, or legal threats for online commentary. The
- Zambia Police Service, in collaboration with the Zambia Information and Communication Technology Authority (ZICTA), has arrested three individuals for allegedly spreading
- inflammatory statements about President Hakainde Hichilema's health. The suspects Daniel Augustine Chitendwe (27), Abraham
- Kapya (34), and Mwale Siliya (27) were apprehended in Kitwe and Kalulushi following investigations. Police Public
- Relations Officer Rae Hamoonga confirmed that the trio has been charged under Section 69 of the Cyber Security and Cyber Crimes

Act (No. 2 of 2021) for Harassment Utilizing Means of Electronic Communication²⁵.

Authorities have warned the public against spreading unverified information online, emphasizing the legal consequences of cyber-related offenses.

- **Legal and Regulatory Frameworks:**

Zambia has enacted legislation to address cybersecurity and data protection issues. Key legislative instruments include the Cyber Security Act No. 3 of 2025 and the Cyber Crimes Act No. 4 of 2025 introducing new regulatory frameworks that may impact digital rights and online civic engagement. These laws grant the state and law enforcement extensive powers to monitor and control online activities if left unchecked, with minimal safeguards for genuine citizen actions. These provisions have raised concerns among CSOs and legal experts who warn that, if left unchecked, these provisions could infringe on citizens' rights to privacy and freedom of expression, peaceful assembly and association. For instance, the Law Association of Zambia (LAZ) called for reconsideration of several clauses, arguing that they could undermine democratic values by allowing mass data collection without adequate judicial oversight. LAZ further announced its intention to petition the enacted law in the high court for a review of the constitutionality of the “contentious” provisions that can potentially infringe the rights and civil liberties and freedoms of citizens²⁶.

- **Cybersecurity Threats:** The cybersecurity threat landscape in Zambia includes:

- i. AI-Powered Phishing & Social Engineering:* Attackers are using AI to

create highly personalized, convincing messages to trick individuals and employees, with scams focusing on fake, large cash prizes. In early 2025, fraudsters used AI-generated video technology to impersonate the Minister of Finance and National Planning, Dr. Situmbeko Musokotwane. These deepfake videos were used to promote fake investment products, such as "LightGameKg" and "CapitalInsight.Ink" deceptively showing the Minister endorsing fast-money schemes. Many Zambians receive SMSes claiming they've won cash, fake empowerment grants, or a promotion but must “verify details” first. Don't share anything. These fake prize scams are designed to steal your information²⁷.

- ii. Ransomware-as-a-Service (RaaS):* Criminal networks are selling ransomware kits, lowering the barrier for attacks on Zambian organizations, which often lead to data encryption and ransom demands. For instance, in November 2025, the Clop ransomware group claimed responsibility for a ransomware attack against Zambia National Commercial Bank Plc (ZANACO). According to reporting, attackers threatened to leak sensitive banking data unless their demands were met — a typical ransomware extortion scenario in which data is encrypted and/or threatened with public disclosure²⁸.

iii. *Online Impersonation & Financial Fraud:*

Impersonation cases have caused major losses, with fraudsters targeting the financial technology, particularly mobile money and bank wallets. In a joint statement, the Minister of [Home Affairs and Internal Security](#), Hon. Jack J. Mwiimbu, SC, MP, and the [Minister of Technology and Science](#), Hon. Felix Mutati, MP, highlighted the growing misuse of digital platforms by cybercriminals. Social media services such as Facebook and WhatsApp have become key channels for scammers impersonating MPs to defraud citizens through false job offers, phishing schemes, and malicious disinformation campaigns. According to the ministers, recent cases of impersonation have resulted in financial losses totaling approximately K111 million²⁹.

iv. *Data Breach and Theft:* High-value data from businesses and government agencies is being targeted for exfiltration, leading to reputational damage and service disruptions. In late 2025, a major data breach allegedly targeting Zambian government social protection systems was advertised on [BreachForums](#), exposing personal data of 15 million citizens. This incident aligns with 2025 trends where high-value, centralized databases are targeted for extortion, threatening significant reputation damage and

public service disruption. In another incident, Zambian Authorities raided a Chinese-run business in Lusaka, arresting 77 people involved in a fraudulent online platform known as "JIXW". The operation used "unsuspecting" Zambian youths to conduct deceptive conversations over WhatsApp and Telegram to scam citizens. Over 13,000 SIM cards, two firearms, and 78 rounds of ammunition were recovered³¹.

To counter cybercrimes, the Zambia Police Service deployed cybercrime officers to provincial headquarters nationwide, expanding the government's capacity to investigate, respond and prosecute digital offences outside of Lusaka. ZICTA (the Zambia Information and Communications Technology Authority), the Police, and other entities now work more closely to harmonize enforcement, capacity building, reporting and incident response as part of the implementation of these Acts. The 707# short code was fully activated in 2025, enabling citizens to *report suspicious mobile numbers or activity directly to authorities*. The code and related reporting infrastructure help capture real-time information about scams and potential threats circulating via mobile networks. Authorities deactivated *over 10,000 SIM cards* tied to suspected scams and fraud activities early in 2025, which helped prevent potential financial losses (estimated up to K16.1 million) and disrupted networks used for impersonation and fraud³².

Internet Access, Affordability and digital inclusion

Internet access in Zambia is increasingly competitive, with some of the lowest mobile data rates in the Southern African Development Community (SADC) region, yet remains expensive relative to local incomes, limiting widespread adoption.

While mobile data is relatively affordable, fixed broadband is costly, with high initial hardware fees for alternatives like Starlink. Internet affordability has decreased, with many workers requiring significant portions of their income for access. Internet connectivity is high in urban centers but limited in rural, remote regions. Additionally, the internet landscape is characterized by expanding, yet lower-than-expected, user numbers compared to subscription-based reports. A total of 23.5 million cellular mobile connections were active in Zambia in late 2025, with this figure equivalent to 106 percent of the total population. However, note that some of these connections may only include services such as voice and SMS, and some may not include access to the internet. There were 7.29 million individuals using the internet in Zambia at the end of 2025, when online penetration stood at 33.0 percent. Zambia was home to 4.10 million social media user identities in October 2025, equating to 18.6 percent of the total population. There were 3.70 million active social media users in January 2025, which is 17.1% of the total population. Zambia was home to 4.10 million social media user identities in October 2025, equating to 18.6 percent of the total population³³.

Kepios's analysis indicates that the number of internet users in Zambia increased by 199 thousand (+2.8 percent) between October

2024 and October 2025. And for added perspective, Zambia's internet adoption rate (i.e. the percentage of the total population that uses the internet) remained unchanged during the same period. But these user figures also suggest that 14.8 million people in Zambia did not use the internet at the end of 2025, suggesting that 67.0 percent of the population remained "offline" at the end of the year.. There were 19.9 million active cellular mobile connections in early 2025, with 90.8% of these considered "broadband" (3G, 4G, or 5G). A significant portion of the population (67%, or 14.5 million people) remained offline at the start of 2025³⁵.

Findings also emphasize that these disparities exacerbate inequalities, concentrating online discourse in urban, better-connected communities. Significant data service outages exist and they affect essential services like mobile data, voice services, and online transactions, causing widespread inconvenience and economic impact for users. The Zambia Information and Communications Technology Authority (ZICTA) aggressively fined mobile network providers and ordered compensation for affected users, particularly targeting Airtel Zambia over K6 million for major data outages experienced on one on 2 February and 10 June 2025. The regulator also penalised MTN Zambia and demanded, in addition to fines, significant investments in network quality³⁶.

Digital Public Infrastructure



The World Bank Group has approved the Digital Zambia Acceleration Project (DZAP) to support the Zambian government to increase access to, and inclusive use of, the internet and digitally enabled services.

With a strong emphasis on fostering digital inclusion, the project aims to empower women and girls, persons with disabilities (PwDs), and other vulnerable communities through the use of digital public services. Supported by a \$100 million International Development Association (IDA)* grant to Zambia, DZAP is part of the second phase of the regional Inclusive Digitalization in Eastern and Southern Africa (IDEA) program. Zambia joins Angola, Malawi, the Democratic Republic of Congo, and the Common Market for Eastern and Southern Africa (COMESA) in this regional effort to foster inclusive digital economies across the region³⁷.

“I am confident that DZAP will enhance digital access, including access to e-government services for faster, more transparent public service delivery,” said Achim Fock, World Bank Country Manager for Zambia.

- High data costs and poor network coverage in rural areas limit the ability of citizens to access information, engage with governance, or participate in online civic activities and also access to fintech. As part of the broader Government's efforts to bridge the digital divide, bringing fast and reliable internet connectivity to rural communities, the Electronic Government Division of the Smart Zambia Institute ([SZI](#)) installed Starlink satellite internet kits such as Moomba Chiefdom, one of the most remote areas within the Kazungula District's Game Management Area.

- A separate government project ("51-Tower Project") saw 43 towers for remote areas completed in 2025. Airtel made a significant US\$107 million investment towards upgrading over 400 network sites across the country, improving both 4G and 5G capabilities. Zamtel launched a nationwide network upgrade plan to mode³⁸.

Misinformation and Information Integrity

The Cyber Crimes Act, which was enacted in April 2025, criminalized certain forms of online speech including spreading false information, and contains broadly worded clauses that allow punishment of speech intended to harm someone's reputation. Political influence shapes online media freedom, particularly during elections.

If found guilty of these offences, internet users could face up to two years in prison, a steep fine, or both³⁹. In January 2025 for instance, three people were arrested and charged under the Cybercrimes Act after allegedly spreading false statements about President Hakainde Hichilema's health⁴⁰. The arrests came as some observers had expressed concern about growing intolerance of political dissent as the government prepares for general elections in 2026⁴¹. In May 2025, former parliamentarian Munir Zulu was sentenced to 18 months in prison with hard labour for a seditious social media post from 2023, in which he claimed that President Hichilema planned to dissolve the parliament and hold early elections⁴². The Cyber Security Act, another law enacted in April 2025, gave authorities disproportionate surveillance powers and required internet service providers to install software and hardware that can support the real-time interception of communications. For instance, Power to Inspect and Monitor (Section 9). This section authorises cyber inspectors appointed under the Act to:

- *Monitor and inspect a computer system or activity on an information system (even if not publicly accessible) with a warrant; and*

- *Enter and inspect premises of cyber service providers if there are "reasonable grounds" to believe the Act has been contravened. This can include deep packet inspection, traffic analysis, or real-time observation of online behaviour, and critics argue it enables extensive state monitoring of digital communications⁴³.*

Government portals and online platforms are recognized as essential channels for disseminating official information, public notices, and regulatory guidance. However, challenges remain where information is not regularly updated or is presented in formats that are difficult for the general public to understand. The findings indicate gaps in access to credible information often contribute to misinformation and online panic and anxiety, which can escalate into public disorder. Findings indicate heightened pressure, monitoring, and coordinated misinformation campaigns during electoral periods are common. Misinformation, particularly during fiscal reforms and election processes, poses a risk to public understanding and institutional trust. Therefore, effective measures to address misinformation must balance accuracy with freedom of expression.

Digital Literacy and digital skills development



The pace of innovation is accelerating at an unprecedented rate, driven by rapid technological advancements, vast access to data, and exponential growth in computing power.

Findings highlight uneven digital literacy among the population. While urban youth often demonstrate advanced skills, a significant portion of citizens lack the knowledge to navigate online platforms safely, identify false information, or engage constructively in civic debates. Technology platforms such as Meta's Facebook, X (formerly Twitter), Signal, Tiktok and WhatsApp provide moderation tools, but responsiveness to local safety concerns and cultural context is limited. There is the need to advocate for collaboration between digital platforms, regulators, and civil society to improve

- moderation effectiveness and user protection (third party responsibilities).

- Digital literacy in Zambia remains low and faces significant hurdles, characterized by a stark urban-rural divide, low foundational Information and Communication Technology (ICT) skills, and limited infrastructure, particularly in schools and rural areas especially for women, girls, youths and persons with disabilities. While the government, civil society, private sector/ service providers and partners like International Telecommunication Union (ITU) are driving initiatives such as the

ZamPortal training for women and youth to enhance digital inclusion, over 40 percent of users still possess only basic, rather than intermediate or advanced, skills. This situation needs urgent redress especially in this digital era. Literacy today is not only about knowing how to read and write on paper, but also about the ability to access, understand, and safely use digital content. To thrive in this digital era, Zambia must bridge the digital divide by ensuring equitable access to digital platforms, the internet, ICT devices, and skills for both rural and urban communities, especially women, young people and persons with disabilities. Literacy in the digital era is a lifeline. For women and girls in particular, internet literacy creates ripple effects, including improving family health, increasing school attendance for children, and strengthening communities⁴⁴. Findings show that digital illiteracy negatively affects women and learners with various forms of vulnerabilities (e.g. poverty, disabilities) more. In Zambia, for example, illiteracy is a hindrance to accessing empowerment initiatives such as Constituency Development Funds (CDF) in rural areas. Hence, knowing how to read and write and use digital platforms is therefore an economic imperative.

In 2025, SMART Zambia Institute has signed an agreement with the Library and Information Association of Zambia (LIAZ) to prioritise digital literacy training for citizens in underserved and unserved communities. The partnership aims to bridge the digital divide and enhance access to digital skills for all Zambians⁴⁵.

Additionally, SMART Zambia rolled out digital literacy training specifically for healthcare professionals, such as a one-day program at Mansa General Hospital. The training covered key aspects like cybersecurity, the Government Service Bus for data exchange, and the Smartcare Pro electronic medical records system, empowering medical staff to adopt digital tools in service delivery⁴⁶.

The SMART Zambia and pursued digital literacy at local government level. For instance, the SMART Zambia Luapula team led digital literacy sessions in Mwense District targeting non-technical local government officers. The training included cybersecurity awareness, troubleshooting, use of shared services, and understanding of national digital platforms, helping frontline officials better utilise digital systems in their work⁴⁷.

Artificial Intelligence and Emerging Technologies



There has been a steady increase in the uptake and deployment of Artificial Intelligence (AI) technologies in Zambia by different sectors, notably in media, mining, healthcare, transportation and logistics, and financial sectors.

The 2024-2026 National Artificial Intelligence Strategy seeks to position Zambia as a regional hub for “AI for development” that accelerates economic growth, improves public services, and drives social inclusion. It aligns AI initiatives with national development goals such as economic diversification, social progress, and public-sector transformation provides guidance on management on emerging technologies and the rapid automation of applications and platforms. Emerging technologies are profoundly reshaping digital rights in Zambia, acting as a catalyst for economic growth while simultaneously introducing significant challenges to privacy, free expression, and data protection.

IndabaX Zambia 2025 Conference was held in November 2025 in Lusaka, this two-day event brought together policymakers, researchers, innovators, and practitioners to

- showcase AI solutions tailored to national challenges. Discussions highlighted practical AI applications in healthcare (e.g., Dawa Health lowering maternal risk), mining exploration by AI-driven tools, and agriculture advisory systems boosting crop yields. The conference reinforced Zambia's intention to build an inclusive, ethical AI ecosystem anchored in local needs and national development goals⁴⁸. In late 2025, Zambia's Ministry of Technology and Science, in partnership with consultancy Pranary, convened a high-level executive briefing on artificial intelligence with business leaders and public sector representatives to accelerate enterprise-level AI deployment aligned with national digital transformation objectives . The session gathered 30 senior leaders to develop practical strategies for enterprise AI deployment, aligning with the country's digital transformation agenda⁴⁹.



Gender, youth and Marginalised Groups

Women, youth, persons with disabilities, and LGBTQI individuals are disproportionately affected by online harassment and exclusion.

These groups face barriers in participating in digital civic life, limiting their voices in public discourse. Organizations like Born Short Living Tall (BSLT) have called for urgent action to include young persons with disabilities, who face severe barriers due to inaccessible platforms and lack of assistive technologies. The Lesbian, Gay, Bisexual, Transgender, Queer/Questioning, and Intersex (LGBTQI) situation in the Zambian digital space problems of online harassment increased digital connectivity and a challenging legal/social landscape.

- While Zambia is expanding its digital infrastructure, the legal environment remains hostile to LGBTQI individuals, with same-sex sexual conduct remaining criminalized. Despite advocacy, the draft Constitution of Zambia (Amendment Bill No. 7 of 2025) contains no provision for the decriminalization of same-sex relationships.
- Broader regional data (e.g., GSMA reports on LMICs) consistently show that women in low- and middle-income countries like Zambia tend to have smaller gender gaps in mobile ownership than in other aspects of the digital divide, but digital skills and usage gaps remain large. Despite the relatively

small gap in smartphone ownership between men and women in Zambia (about 35% for women compared to 37% for men), there is a significant gender divide in digital literacy. Only 5.8% of women are computer literate, highlighting a major barrier to meaningful digital participation⁵⁰. Digital inclusiveness measures introduced include the "Girls in ICT" initiative and the GRZ-UN Joint Programme on GBV are providing digital skills training to bridge this gap. The government is also amending the Electronic Government Act (No. 41 of 2021) to enhance digital security and inclusion for women, aiming to overcome "digital shyness".

The Zambian government has heavily prioritized "digital safety" during the 16 Days of Activism (Nov-Dec 2025), but this focus is officially on protecting women, children, and reducing gender-based violence (GBV) but it does not have anything specifically addressing LGBTQI safety and inclusion. However, LGBTQI people are often not explicitly mentioned in such frameworks. That omission can matter significantly because:

- LGBTQI individuals frequently

experience **disproportionate online harassment, outing, blackmail, and hate speech.**

- Digital spaces may be one of the few avenues for community-building in restrictive environments.
- In Zambia, same-sex relations remain criminalized under the Penal Code, which creates additional safety risks for LGBTQI persons both online and offline.

Online Harassment: Activists, including those working on gender equality, face significant online harassment, cyberbullying, and gendered insults from groups opposing their work. Due to high risks of online surveillance, harassment, and discrimination, the digital space is not inherently safe for the LGBTQ+ community. Activists in Zambia often operate in a restricted environment regarding digital rights⁵¹.

Digital Ids



In October 2025, the Government of Zambia formally announced that the issuance of digital identification (ID) cards would be deferred until after the next general elections.

This postponement was framed by officials as a way to avoid politicisation of the process and ensure citizens would not allege unfair targeting of voters before the polls. The statement explicitly noted the decision to pause issuing digital IDs during the 2025–26 election cycle to avoid controversy and mistrust among the electorate. This reflects significant policy risk awareness, but also raises concerns about transparency and whether adequate public consultation has been conducted⁵².

a) System Deployment and Enrolment

- Zambia has been actively implementing its Integrated National Registration Information System (INRIS) — a national biometric registration infrastructure designed to support a future digital identity ecosystem⁵³.
- By late December 2025, about 1.3 million citizens had been enrolled onto the national registration system, signifying significant progress in capturing biometric and demographic data ahead of eventual rollout⁵⁴.

Challenges and Concerns in the Protection of Internet Freedoms

Addressing the challenges related to the protection of internet freedom requires a multi-stakeholder approach that balances security with fundamental human rights.

The period under review identified the following key challenges regarding internet freedom in Zambia;

1. **Legal and Enforcement Gaps:**
Restrictive Cyber Security & Cybercrimes Laws:

- Zambia's revised Cyber Security Act and Cyber Crimes Act (both enacted in 2025) are widely perceived as major threats to internet freedom. Civil society, digital rights groups, and rights bodies have raised several concerns. The laws give law enforcement agencies wide discretion and creates a chilling effect on public debate online. This is coupled with limited or no literacy and awareness on the provisions and extent of the laws. The majority of Zambians believe the Cyber Security and

Cybercrimes legislation when first enacted in 2021 was meant to target citizen online activities rather than provide a basis for fostering a safe digital environment. The additional challenge to cyber law enforcement and why it lacks wide public support is the perception that the laws target critical and oppositional voices (expression) as the majority of victims of these laws are offences centred on expression, opinions and utterances.

- Weak judicial safeguards and oversight mechanisms, which increase the risk of arbitrary enforcement. Enforcement remains inconsistent due to limited resources, lack of/ insufficient

trained personnel, and insufficient infrastructure. The laws also lack exemptions for whistle-blowers and journalistic work, which are criminalised, but this is not ideal for fostering a democratic environment.

2. **Censorship and Freedom of Expression:**

- The latest **MISA FOE Annual Report** underscores that the combined effect of ambiguous legal provisions, punitive cybercrime-related offences, weak protections for public-interest expression, and broad surveillance powers has significantly eroded Zambia's digital civic space. These pressures have led to a noticeable rise in **self-censorship**, with journalists, activists, content creators, and ordinary citizens increasingly avoiding sensitive political or governance-related issues online for fear of criminal liability, monitoring, or retaliation. As highlighted in the report, this environment undermines open democratic participation and contributes to a shrinking culture of free expression both online and offline⁵⁵.
- There is a growing tendency to self-censor political and critical commentary, worried about crossing legally undefined boundaries. The Freedom on the Net 2025 report noted arrests linked to social media posts, which further erodes confidence in safe online civic engagement.

3. **Privacy, data protection and Surveillance:**

- Cyber Security Act, No. 3 of 2025 gives government bodies, particularly the Central

Monitoring and Coordination Centre authority to conduct lawful interceptions of communications and to coordinate interception activity. The Centre is placed under government control, which critics say weakens independence and oversight. The Act mandates the telecommunications providers to install interception-capable hardware and software; support real-time and full-time monitoring capabilities; and transmit intercepted communications and related metadata to the monitoring centre when requested by authorities⁵⁶. This has triggered warnings from international networks and civil society that the law could be used to invasively surveil ordinary citizens, weakening privacy protections

4. **Cyber Crime, Cybersecurity enforcement and digital safety**

Growing Cyber Attacks: The Zambian Parliament reported growing cyber threats including online impersonation, hacking, identity theft and financial exploitation, with hundreds of cases recorded in the first half of 2025 and significant financial loss reported (~K111 million)⁵⁷.

Weak Security Measures: Many organizations, particularly small and medium-sized enterprises lack strong cybersecurity protocols, making them easy targets for cybercriminals.

5. **Digital Divide**

Access Inequality: Significant disparities exist in access to digital technologies and the internet, particularly between urban and rural areas. This limits

the ability of many Zambians to fully exercise their digital rights. Limited connectivity and uneven digital literacy remain barriers to inclusive participation.

Cost Barriers: The high cost of internet access and digital devices continues to be a barrier for many people, hindering their ability to participate in the digital space.

6. Digital Literacy

Limited education and Awareness: Many Zambians are unaware of their digital rights and the risks associated with digital activities, leading to increased vulnerability to online fraud, data breaches and misinformation. Digital literacy in Zambia is growing but faces significant hurdles, characterized by a stark urban-rural divide, low foundational Information and Communication Technology (ICT) skills, and limited infrastructure and connectivity, particularly in schools and rural areas. Low levels of digital literacy are identified as a major concern that highlights the need for consumer education on safe internet use, data protection, and accountable online behaviour.

7. Artificial Intelligence and emerging technologies

AI and Automation Risks: The Ministry of Technology and Science engaged with tech companies (e.g., Yango Zambia) to explore AI solutions to strengthen public services including revenue management,

transport systems, customs processes, healthcare, education, agricultural intelligence, and data-driven planning⁵⁸. The deployment of AI and automated systems raises concerns about bias, transparency, and accountability, potentially infringing on digital rights if not properly regulated. There is the need to explore how innovations such as artificial intelligence (AI), blockchain, and the Internet of Things (IoT) are impacting key aspects of digital rights, including privacy and freedom of expression, among others.

8. Gender, youth and marginalised Groups

Women, youth, persons with disabilities, LGBTQI and other marginalized groups are identified as particularly vulnerable to online abuse, cyberbullying, and exploitation. Stakeholders highlight the need for inclusive digital policies and accessible reporting mechanisms, while stigma and fear often discourage victims from reporting online violations. Marginalized communities, including LGBTQI individuals face disproportionate targeting in digital spaces. This stems from the legal environment which remains hostile to LGBTQI individuals, with same-sex sexual conduct remaining criminalized. Despite advocacy, the draft Constitution of Zambia (Amendment Bill No. 7 of 2025) contains no provision for the decriminalization of same-sex relationships. Ace additional barriers, such as online harassment and limited access to digital tools, which

Recommendations

The following recommendations and measures are proposed to broad based stakeholders to strengthen the protection and enjoyment of digital rights in Zambia

1. Government of Zambia

a. Strengthen Legal and Policy Safeguards

- i. Ensure implementation of the Data Protection Act prioritises independence of the Data Protection Commissioner and transparent oversight mechanisms.*
- ii. Embed human rights safeguards within new digital frameworks, including Digital Public Infrastructure (DPI), AI governance and the national Digital ID initiatives.*

b. Ensure Transparency in Surveillance Practices

- i. Publish annual transparency reports on interception requests, data access procedures, and cybersecurity operations.*
- ii. Introduce judicial oversight for all interception authorisations to prevent political misuse.*

c. Expand Internet Access and Affordability

- i. Reduce sector taxes (especially on devices and internet services) to support affordable access.*
- ii. Prioritise expansion of rural broadband and community network initiatives.*

- iii. The government should encourage or even increase investment in Internet Exchange Points (IXPs) across Zambia to improve the efficiency of local internet traffic and reduce the cost of internet access. Strengthening and expanding national and regional IXPs, internet service providers can exchange local data within Zambia rather than routing it through international networks, which often increases bandwidth costs and latency.*

2. ICT and Financial Services Regulators

a. Improve Accountability and Independence

- i. Increase transparency in licensing, content regulation, cybersecurity enforcement, and data protection oversight.*
- ii. Conduct periodic regulatory audits to ensure neutrality and non-interference from political actors.*

b. Strengthen Consumer Rights

- i. Enforce quality-of-service standards and publish regular internet performance reports.*
- ii. Mandate clear public notifications for major network disruptions.*

c. Engage Stakeholders in Policy Consultations

Hold open consultations before introducing regulations on digital platforms, cybersecurity, AI, or data protection.

d. Strengthen Consumer Protection and Dispute Resolution Mechanisms

- i. The Bank of Zambia should take interest and collaborate with ZICTA and ZCSA to enhance existing mechanisms that allow users to report fraud, service failures, or unauthorised transactions so that consumers can receive timely remedies. Establishing clear service standards for complaints handling, refunds and dispute resolution will increase trust in digital financial services and protect consumers from financial harm.

e. Support Interoperability and Fair Competition

- i. To promote a more inclusive and competitive digital financial ecosystem, the regulator should continue advancing interoperability among mobile money platforms, banks, and fintech providers. Improved interoperability will reduce transaction costs, prevent market concentration, and ensure that users can seamlessly transact across different financial service providers.

f. Promote Transparency in Digital Financial Service Fees

- i. The regulator should require mobile money operators and fintech companies to provide clear, accessible, and standardised disclosure of transaction fees, service charges and terms of use. Transparent pricing will empower consumers to make informed decisions and reduce the risk of hidden or confusing charges that

disproportionately affect low-income users who rely heavily on mobile money services.

g. Strengthen Consumer Data Protection in Digital Financial Services

- i. The financial services regulator should strengthen regulatory oversight to ensure that mobile money providers and other digital financial service operators comply fully with Zambia's data protection requirements. This includes enforcing clear standards on data collection, storage, sharing and consent to ensure that customer financial data is not misused, exploited or shared without the minimum standards.

3. Civil Society Organisations (CSOs)

a. Expand Digital Rights Advocacy

- i. Monitor emerging legislative proposals such as Digital ID, e-government systems, AI frameworks, and cybersecurity regulations. This includes monitoring implementation of the existing legislation and policies.
- ii. Advocate for stronger human rights protections in data governance and surveillance practices.

b. Strengthen Community Awareness

- i. Conduct public education and awareness raising campaigns on privacy rights, online safety, and responsible/ accountable digital citizenship.
- ii. Support marginalised groups (youth, women, LGBTQI communities) with tailored digital literacy interventions.

c. Enhance Multistakeholder Collaboration

- i. Strengthen coalitions and collaborations with regional and global digital rights networks digital rights and internet governance to ensure regional solidarity, including learning from successes such as Kenya's Huduma Namba and Nigeria's digital ID lessons.

4. Media Practitioners and Journalists

a. Promote Responsible Online Journalism

- i. Adopt fact-checking and verification tools and standards to counter harmful content and information disorders such as misinformation.
- ii. Strengthen investigative reporting on digital rights, surveillance, and technology governance and the broader internet governance architecture.

b. Prioritise Safety Online

- i. Use secure communication tools to protect sources and sensitive data especially during independent and investigative journalism.
- ii. Engage in digital safety training to enhance protection from cyber threats and foster data protection and privacy.

c. Advocate for Media Freedom Online

- i. Push for reforms to laws that criminalise legitimate journalism, especially those with overly broad cybercrime provisions that lack exemptions for

journalistic work.

5. Content Creators and Online Influencers

a. Promote Ethical Online Engagement

- i. Avoid amplifying misinformation or harmful content.
- ii. Adhere to responsible digital communication standards.

b. Build Digital Literacy in Communities

- i. Use platforms to spread awareness on data privacy, online safety, and responsible internet use.

6. Academia and Researchers

a. Strengthen Evidence-Based Policy Contributions

- i. Conduct research on digital rights, AI ethics, cybersecurity, misinformation, and DPI systems.
- ii. Provide independent assessments of government digital policies.
- iii. Host multi-stakeholder forums on internet freedoms, elections, and digital governance.

7. Private Sector (Telecoms, ISPs, Tech Companies)

a. Protect User Data

- i. Comply with data protection standards and adopt privacy-by-design practices.
- ii. Publish transparency reports on government data requests and network disruptions.

b. Promote Affordable Access

- i. Collaborate with the government to reduce the cost of devices and data.
- ii. Expand infrastructure in underserved rural communities.

c. Innovate Responsibly

- i. Build AI and digital products aligned with global best practices on transparency, fairness and safety.

8. Policymakers (Parliamentarians)

a. Enhance Parliamentary Oversight

- i. Demand accountability for surveillance mechanisms, cybersecurity operations, and digital ID systems.
- ii. Review the constitutionality of digital-rights-related laws.
- iii. Establish mandatory stakeholder consultation processes for all new digital-related legislation.
- iv. Address barriers faced by women, youth, persons with disabilities and marginalised groups in digital spaces.

CONCLUSION

Zambia's internet freedom remained partly free but under increasing strain, shaped by both structural improvements and emerging restrictions.

Internet access and mobile penetration continued to grow, with more Zambians having connectivity than in previous years. This expansion supports broader participation in online discourse and civic engagement, including increased blogging and use of digital platforms for informative and educational purposes. However, legal and regulatory developments in 2025 have eroded aspects of digital freedom. The enactment of the Cyber Crimes Act and Cyber Security Act broadened state surveillance powers, introduced criminal penalties for certain forms of online speech, and raised concerns about privacy and self-censorship. Issues of digital literacy are also still persisting amidst rapid digitalisation coupled with emerging technologies such as AI. Media freedom advocates report a decline in public internet freedom, incidences of harassment of journalists, and ongoing difficulty in accessing official information all indicating inconsistencies in a more restrictive environment for online expression.

- In 2025, Zambia's digital transformation is accelerating, shaped by expanding mobile connectivity, growth in digital public services, and early adoption of artificial intelligence (AI) across both public and private sectors. The government and key institutions are increasingly integrating digital tools into service delivery—in areas such as education, agriculture, health systems, and public administration—while fintech, e-commerce, and mobile-based platforms continue to drive innovation in the private sector. On one hand, AI-driven platforms, e-government systems, and mobile innovations have the potential to expand access to information, enhance public service delivery, and improve inclusion for underserved populations. On the other hand, these same technologies, if deployed without strong safeguards, risk amplifying existing inequalities, enabling expanded surveillance, deepening algorithmic bias, and widening gendered skills gaps.

Endnotes

- 1: Cyber Crimes Act, 2025, Act 4 of 2025, https://zambialii.org/akn/zm/act/2025/4/eng%402025-04-15?utm_source=chatgpt.com, (accessed 16 February 2026)
- 2: National Digital Transformation Strategy 2023-2027, <https://www.mots.gov.zm/wp-content/uploads/2023/10/National-Digital-Transformation-Strategy.pdf>, (accessed 15 February 2026)
- 3: Cabinet approves repeal of data protection Act to broaden legal framework for AI, analytics | Zambia Monitor
- 4: Cyber Acts now fully operational, ZP deploys cyber crimes officers to headquarters -
- 5: ZAMBIA Media Institute of Southern Africa (MISA Zambia) "A Perception of the Freedom of Expression, Media Freedom and Digital Rights in Zambia Report" (2025).
- 6: Zambia Freedom in the World 2025 Report, <https://freedomhouse.org/country/zambia/freedom-net/2025> (accessed 26 January 2026)
- 7: Freedom of Expression and the Digital Environment in Eastern Africa | Article 19
- 8: The State of Human Rights in Zambia, October 18, 2025, https://hrc.org.zm/wp-content/uploads/2025/06/2021_2022_State-of-Human-Rights-Report-1.pdf?utm_source=chatgpt.com, (accessed 14 February, 2026)
- 9: Zambia's Ratification of the ICCPR, UN Treaty Collection – Status of ICCPR (Zambia country profile). <https://treaties.un.org>
- 10: News Diggers, (2021) Zambia Using Israeli ICT Tools to spy on Citizens, <https://diggers.news/local/2021/02/26/zambia-using-israeli-ict-tools-to-spy-on-citizens-report> (accessed 26 January 2026)
- 11: "Why the rush? Civil societies urge withdrawal of cyber security, anti-terrorism bills, seek broader consultations | Zambia Monitor (accessed 26 January 2026)
- 12: 'GNI Statement on Zambias new Cyber Laws: A blow to freedom of expression and privacy - Global Network Initiative (accessed 25 January 2026)
- 13: New restrictive laws raise concerns - Civicus Monitor,
- 14: Freedom House — "Zambia: Freedom on the Net 2025 Country Report": <https://freedomhouse.org/country/zambia/freedom-net/2025>, (accessed 14 February, 2026)
- 15: Ibid 7
- 16: Enabling Environment Snapshot Report" (May 2025), Enabling Environment National Assessment, (accessed 14 February, 2026)
- 17: Zambian journalist attacked, facing criminal charges after covering ruling party supporters, Zambian journalist attacked, facing criminal charges after covering ruling party supporters (accessed 26 January 2026)
- 18: The Constitution of Zambia Act 18 of 2016, Art 17
- 19: Cabinet approves repeal of data protection Act to broaden legal framework for AI, analytics | Zambia Monitor
- 20: Privacy fears mount as U.S. Embassy warns over Zambia's restrictive cybercrime law, 18 April 2025 03:38 PM, 'Privacy fears mount as U.S. Embassy warns over Zambias restrictive cybercrime law | Business Insider Africa, (accessed 26 January 2026)
- 21: <https://www.parliament.gov.zm/sites/default/files/documents/bills/N.A.B%201%20of%202025.pdf>
- 22: Zambia : HH Declines to Sign CCTV Bill, Citing Privacy Concerns, (accessed 7 February 2026)
- 23: Zambia: Northern Province records decline in reportage of GBV
- 24: LAZ to Challenge New Cyber Laws in Court, Cites Threat to Democracy and Free Press, April 22, 2025, LAZ to Challenge New Cyber Laws in Court, Cites Threat to Democracy and Free Press - The Zambian Observer ((accessed 26 January 2026)
- 25: <https://x.com/diamondtvzambia/status/1885299174221967713>
- 26: LAZ to Challenge New Cyber Laws in Court, Cites Threat to Democracy and Free Press - The Zambian Observer ((accessed 26 January 2026)
- 27: "Many Zambians receive SMSes claiming theyve won cash, fake empowerment grants, or a promotion but must "verify details" first. Dont share anything. These fake prize scams are designed to steal your information. #KeepGrowing #FraudAwarenessWeek #CyberSecure
- 28: Clop Ransomware Strikes Zambia National Commercial Bank - DeXpose, (accessed 27 January 2026)

- 29: [Zambian Government Strengthens Cybersecurity After K111 Million Lost to Online Scams - TechAfrica News](#)
- 30: [Zambia Data Leak Exposed: 15M Citizens in Alleged Breach | DarknetSearch](#)
- 31: <https://www.facebook.com/zambiapolice/posts/april-23-2025-police-in-lusaka-have-arrested-a-32-year-old-chinese-national-iden/660554286612699/>
- 32: [Cyber Acts now fully operational, ZP deploys cyber crimes officers to headquarters -](#)
- 33: [Make Sense of Digital Trends, Digital 2025: Zambia https://datareportal.com/reports/digital-2025-zambia \(accessed 14 February, 2026\),](#)
- 34: [Kepios, \(accessed 26 January 2026\)](#)
- 35: [The "state of digital" in Zambia", 8 November 2025, —Digital 2026: Zambia DataReportal Global Digital Insights, \(accessed 27 January 2026\)](#)
- 36: [Press Statement on MTN Service Outage on March 3, 2025, https://www.zicta.zm/resources/press-releases, \(accessed 27 January 2026\)](#)
- 37: [New World Bank Program Helps Zambia Increase Jobs Through Inclusive Digital Access](#)
- 38: [Smart Zambia Brings Starlink Internet to Remote Moomba Chiefdom - TechAfrica News, \(accessed 27 January 2026\)](#)
- 39: [Zambian Parliament, "The Cyber Crimes Act No. 4 of 2025," 2025, https://www.parliament.gov.zm/sites/default/files/documents/acts/Acts%2...; Solomon Ekanem, "Privacy fears mount as U.S. Embassy warns over Zambia's restrictive cybercrime law," Business Insider Africa, April 18, 2025, https://africa.businessinsider.com/local/lifestyle/privacy-fears-mount-...; Global Network Initiative, "GNI Statement on Zambia's new Cyber Laws: A blow to freedom of expression and privacy," July 2, 2025, https://globalnetworkinitiative.org/gni-statement-on-zambias-new-cyber-....\(accessed 25 January 2026\)](#)
- 40: [@Diamond Media, "THREE \(3\) ARRESTED FOR SOCIAL MEDIA CLAIMS ON HH'S HEALTH," X, January 31, 2025, https://x.com/diamondtvzambia/status/1885299174221967713. \(accessed 26 January 2026\)](#)
- 41: [Zambia: Authorities must immediately end escalating crackdown on human rights - Amnesty International.\(accessed 26 January 2026\)](#)
- 42: ["Munir Zulu Sentenced to 18 Months with Hard Labour for Seditious Remarks Against President," LusakaTimes,May2, 2025, https://www.lusakatimes.com/2025/05/02/munir-zulu-sentenced-to-18-month-....\(accessed 26 January 2026\)](#)
- 43: ["How Zambia's Cyber Laws Rebrand Repression," Journal of Democracy, August 2025, https://www.journalofdemocracy.org/online-exclusive/how-zambias-cyber-l-.... \(accessed 26 January 2026\)](#)
- 44: [ZANEC Press Statement on 2025 International Literacy Day, \(accessed 29 January 2026\)](#)
- 45: [SMART Zambia, Library association partner to boost digital literacy in underserved areas \(Video\)](#)
- 46: [SMART Zambia Trains Government Officers in Digital Capacity Building - TechAfrica News, \(accessed 18 January 2026\)](#)
- 47: [SMART Zambia Advances Digital Literacy in Mwense as Part of National ICT Strategy - TechAfrica News](#)
- 48: [Zambia Advances AI Strategy with National Conference on Innovation and Development - TechAfrica News, \(accessed 1 March 2026\)](#)
- 49: [Zambia Convenes Executive Briefing to Accelerate National AI Adoption - African Gambit,](#)
- 50: [Progress closing the mobile internet gender gap stalls in LMICs: GSMA Mobile Gender Gap Report 2025 - Newsroom](#)
- 51: [MISSING CONTEXT : Old headline falsely links Zambias Chief Justice to 2025 Constitutional Amendments advocacy on gay rights. Center for Young Leaders In Africa](#)
- 52: [Thursday, 2nd October, 2025 | National Assembly of Zambia](#)
- 53: [THE INRIS PROJECT Ministry of Home Affairs and Internal Security](#)
- 54: [Over 1.3 Million Citizens Enrolled on INRIS - ZNBC](#)
- 55: [MISA Zambia report highlights decline in media freedom, raises digital rights concerns](#)
- 56: [Cyber Security Act, 2025 ZambiaLII](#)
- 57: [Wednesday, 9th July, 2025 | National Assembly of Zambia](#)
- 58: [Yango Zambia and Ministry of Technology and Science Explore AI for Public Service Delivery](#)

Call to Action for Stakeholders to Prioritise and Protect Digital Rights in Zambia

We urge stakeholders to prioritize and protect digital rights in Zambia to drive economic growth, enhance social inclusion, and strengthen democratic participation. By developing comprehensive policies, strengthening legal frameworks, and promoting digital literacy, we can create a safe and equitable digital environment for all citizens. Additionally, we call for enhanced collaboration among government, private sector, and civil society stakeholders, which is crucial to achieving Zambia's digitalisation goal. Together, let's ensure a thriving digital future for Zambia.

Specifically,

- Civil Society organizations are urged to continue to play an oversight role and provide the necessary checks and balances, including recommendations in the development and enforcement of human rights-based ICT policy and legal frameworks.
- Academia is urged to continue to study the area of digitalisation and how it may marginalise or affect people's rights, including studies on the impact of Artificial Intelligence and emerging technologies to help inform the development of various ICT-related strategies and policies.
- The private sector is encouraged to implement the appropriate cybersecurity and data protection measures, including raising awareness of risks among its customers. In addition, supporting the growth of the ICT sector through increased investments that ensure universal, equitable and meaningful access to ICTs.
- The government is encouraged to expedite the enactment and implementation of rights based legislation that should facilitate for enhanced digital literacy, safety and security and personal data protection