Implications of Zambia's Cyber Security and Cyber Crimes Act 2021 on Digital Rights

May **2021**

Introduction

In March 2021, Zambia adopted the Cyber Security and Cyber Crimes Act, 2021[1] following assent by President Edgar Lungu.[2] The Act was passed amidst criticism that it was primarily aimed at policing the cyber space and gagging freedom of expression and speech of government critics and opponents ahead of the general election slated for August 12, 2021.[3] Indeed, President Lungu's statement that the law was intended "to protect citizens from abuse by people who feel they can do or say whatever they want using the veil of cyberspace" cannot be underestimated, as it sounds warning bells to online dissenters and critics.[4]

The law was first introduced in April 2018 as the Cybersecurity and Cybercrimes Bill and approved for review by the Cabinet in August 2018.[5] Consequently, a number of concerns were raised by civil society organisations.[6] Echoing local civil society groups' concerns, the International Center for Not-for-Profit Law at the time noted that the bill addressed legitimate cybercrimes issues and offered some protections to freedom of expression and the right to privacy. However, it had numerous shortfalls, such as a chilling effect on freedom of expression, promoting censorship by the state and self-censorship, as well as unfettered intrusion on the right to privacy by the state through systematic monitoring, interception and surveillance. While proposals were made to revise the bill to address these concerns, the law was passed without addressing the concerns raised by civil society. As this analysis shows, the Act has negative ramifications for the enjoyment of digital rights in Zambia.

Purpose of the Cyber Security and Cyber Crimes Act, 2021

The aim of the law is to provide for cyber security, constitute the Zambia Computer Incidence Response Team and the National Cyber Security Advisory and Coordinating Council; and the continuation of the Central Monitoring and Coordination Centre. Others are to protect persons against cybercrime, promote child online protection, and to facilitate identification, declaration and protection of critical information infrastructure, the collection and preservation of evidence of computer and network related crime, admission in criminal matters of electronic evidence, and registration of cyber security service providers.

While the stated aims of the law are progressive and the law contains positive provisions that could potentially contribute to prevention of cybercrimes, enhance online access to criminal justice, and prevent online violence against children, there are several provisions that, if not addressed, could have a negative impact on the enjoyment of digital rights in Zambia.

The Positives

The interpretations provided for under **section 2** are elaborate and provide certainty as to the meaning of terms as used in the Act.

Part II on regulation of cyber security services presents an opportunity for collaboration between the Zambia Information and Communications Technology Authority (ZICTA), the Zambia Computer Incidence Response Team constituted under **section 6** and the National Cyber Security Advisory Coordinating Council constituted under **section 7**. Such collaboration could enhance detection and prevention of cybercrime.

The processes related to the office of the Inspectorate, including its appointment **(section 8)**, procedures requiring a warrant before exercise of powers **(sections 9, 11 and 75)**, and powers of the inspector to monitor and inspect computer systems or activity **(section 9)**, and appointment of a cyber-security technical expert **(section 13)** provide some confidence in the Inspectorate's execution of its duties. The provisions on protecting critical information and critical information infrastructure under **Part V (sections 16, 18—25)** have the potential to enhance national security if rightly applied.

The provision in **section 31** prohibiting disclosure of intercepted communication contrary to the provisions of the Act, if rightly implemented, could help prevent unlawful disclosure, use and dissemination of personal data. Prescribed penalties are a fine of 300,000 kwacha (USD 13,286), imprisonment not exceeding 10 years, or both.

1 *The Cyber Security and Cyber Crimes Act, 2021, https://www.zicta.zm/storage/posts/attachments/5B0E7uR3LSBIXVimAVsilYdIur2NwLnjT0TlScrl.pdf*
2 *Zambia Okays Tough Cyber Law Sparking Fears Over Misuse, https://www.barrons.com/articles/zambia-okays-tough-cyber-law-sparking-fears-over-misuse-01616785209?tesla=y*
3 *Electoral Commission of Zambia, 2021 General Election Calendar, https://www.elections.org.zm/2021/02/26/2021-general-election-calendar/*
4 *President Lungu has Signed the Cyber Security and Cyber Bill into Law, https://www.lusakatimes.com/2021/03/26/president-lungu-has-signed-the-cyber-security-and-cyber-bill-into-law/*
5 *Freedom of the Net 2018, https://www.refworld.org/docid/5be16ae910.html*
6 *CSOs demand for withdrawal of Cyber Security and Cybercrimes Bill, https://www.lusakatimes.com/2021/02/23/csos-demand-for-withdrawal-of-cyber-security-and-cybercrimes-bill/*

Section 26(1) prohibits unlawful interception of communications, while **section 34(1)** bars service providers from engaging in random monitoring of customers' communications except for mechanical or service quality control checks. This offense is punishable by a fine or imprisonment of up to five years or a fine not exceeding 150,000 kwacha (USD 6,643).

Under **part IX, sections 49 and 50**, the law criminalises unauthorised access to individuals' data. Section 49 specifically prohibits unauthorised access to, interception of or interference with computer systems data while section 50 prohibits the production, sale, procurement for use, importation, exportation or distribution of illegal devices and software. Furthermore, **section 50(1)** and **section 60** prohibit the use of illegal devices and software to compromise cyber security. **Section 62** also prohibits the transmission of unsolicited electronic messages.

The Act attempts to address a range of cybercrimes including cyber extortion through accusations, or threats to force a victim to perform or abstain from performing a particular task **(section 52)**, identity theft **(section 53)**, publication intended to compromise security and safety of any other person **(section 54)**, and hate speech **(section 65)**. Further, the law prohibits aiding and abetting or inciting online crime **(section 55)**, as well as production and transmission or dissemination of pornography **(section 56)**. Under **section 61**, the Act prohibits intentional activities aimed at rendering a computer system incapable of providing normal services to its legitimate owner.

The law is commendable for prohibiting child pornography under **section 57** and child solicitation under **section 58**, including through sexual activities arising from deception using computer systems or computer networks. Moreover, section 57 is buttressed by a harsh prison term for offenders, a minimum of 15 years. On the other hand, the offence of child solicitation may attract a prison sentence of up to 15 years.

Other crimes provided for in the Act include genocide and crimes against humanity **(section 66)**, cyber terrorism **(section 70)** and cyber attacks **(section 71)**.

The Appeal process laid down in **section 74**, if applied impartially, could yield desired justice for aggrieved parties. It provides that where a person is dissatisfied with a decision made by the Zambia Information and Communication Technology Authority (ZICTA), they may appeal to the Minister, and those aggrieved by the Minister's decision may appeal to the High Court. The utilisation of internal administrative structures for appeals before seeking court indulgence is commendable as it helps overcome delayed justice due to court case backlogs and prohibitive costs.

Areas of Concerns in the Act

Despite the aforementioned positives, the Act falls short on the protection of individual rights to privacy, anonymity and freedom of expression online. Below, we detail the troublesome provisions.

Limited Safeguards Over Interception of Communications

Section 27 of the Act provides for the establishment of the Central Monitoring and Co-ordination Centre as an authorised centre for interception of communications. Under **section 28**, the interception is conducted by a law enforcement officer when there are reasonable grounds to believe that an offence has been committed, is likely to be committed or is being committed, and for the purpose of obtaining evidence of the commission of an offence. Before intercepting communications, a law enforcement officer applies to a judge for an interception of communications order, after making a written application to the Attorney General for a written consent and such consent has been obtained. The interception order is valid for an initial period of three months, renewable by a judge for an unspecified period.

The failure to limit the period of validity of an interception order could subject individuals, especially government critics and political opponents, to continued surveillance. These fears are not far-fetched since a 2020 report by Citizen Lab, a global digital rights watchdog, identified Zambia as a possible customer of cyber espionage software.[7] This was the second time that Zambia, alongside other African governments, was featured in the report that unmasks clients of spyware vendors.[8]

Another concern is that, while section 27(3) provides for management, control and operation of the Central Monitoring and Co-ordination Centre by the department responsible for Government communications in liaison with ZICTA, the said department is not defined under the Act, as civil society in the country has pointed out.[9] The functions of ZICTA are listed in section 5 and those of the Zambia Computer Incidence Response Team are listed in section 6. Failure to specify this department could provide yet another avenue for abuse of the processes associated with the handling of personal data and state surveillance.

7 *Citizen Lab, Running in Circles:Uncovering the Clients of Cyberespionage Firm Circles, https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/*

8 *Africa in the Crosshairs of New Disinformation and Surveillance Schemes that Undermine Democracy, https://cipesa.org/2019/12/africa-in-the-crosshairs-of-new-disinformation-and-surveillance-schemes-that-undermine-democracy/*

9 *Joint CSO Press Statement Dated 18th February 2021 on The Proposed Cyber Security And Cyber Crimes Bill, http://acazambia.org/joint-cso-press-statement-dated-18th-february-2021-on-the-proposed-cyber-security-and-cyber-crimes-bill/*

Under **sections 29**, which is mirrored by section 30, an enforcement officer may intercept any communication and the request may be made orally to a service provider "on reasonable grounds to prevent possible or inflicted bodily harm, loss of life or threats to kill oneself, or damage to property or actual or possible cause of financial loss."

The various provisions with limited safeguards over interception of communications have the potential to violate privacy rights and are contrary to established principles of limitations to privacy under international law. These include legality, which requires that limitations be provided for by the law; the necessity principle which requires that the limitation should be necessary in a democratic society and should be necessary for achieving a legitimate aim; and proportionality, which aims to ensure that the intrusion on individuals' privacy is balanced with the intended public benefit and that this intrusion is therefore appropriate for attaining legitimate aims. These principles are laid down in, among others, the U.N. General Assembly Resolution on the Right to Privacy in the Digital Age of 2014,[10] the Report of the Office of the United Nations High Commissioner for Human Right to Privacy in the Digital Age, (June 30, 2014),[11] and the Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, 2014.[12]

Further, the African Commission on Human and Peoples' Rights (ACHPR) Declaration on Principles of Freedom of Expression and Access to Information in Africa,[13] in particular Principle 41(3), requires the prior authorisation of interception by an independent and impartial judicial authority. The Zambian law fails to institute due process safeguards, and gives law enforcement agents the leeway to conduct unsupervised surveillance. Given Zambia's mixed human rights record, the targets of that surveillance are likely to be journalists, government critics and political opponents, and the sum effect of these provisions would be to undermine citizens' access to information and their enjoyment of the right to free expression.

Heavy Demands on Service Providers

Section 38 requires electronic communication service providers to use electronic communication systems that are technically capable of supporting lawful interceptions, install hardware and software facilities and devices that enable interception, provide services capable of rendering real time and fulltime monitoring facilities for the interception of communications, and provide call-related information in real time or as soon as possible upon call termination. Further, service providers are required to provide interfaces for transmission of intercepted communication to the Central Monitoring and Coordination Centre. The penalty for non-compliance is a fine of 150,000 Kwacha (USD 6,643), imprisonment for up to five years, or both. This high penalty will compel service providers to render interception assistance even when they receive dubious oral orders that lack judicial backing or any evidence justifying the interception.

If Zambia does not repeal the new law, it is imperative that regulations are quickly made to provide guidance on how service providers will meet obligations under **sections 38 and 40** (on interception capability of service providers, including storage of call-related information) while at the same time providing safeguards for individuals' data and privacy. In their current form, these provisions present a threat to freedom of expression online and offline.

Restrictions of Anonymity

Section 39 of the Act requires electronic communication service providers to collect personal data from individuals including names, residential addresses and identity numbers contained in identity cards before entering into a contract for provision of any service. Moreover, under **subsection (1)(c)**, the service provider may collect any other information considered necessary. The service provider is further charged with keeping proper records and updating them frequently.

While collection of such information is important for tracking criminal elements, there is no guarantee of safety and protection of collected personal data despite the enactment of the Data Protection Act, 2021 that is yet to be operationalised.[14] Moreover, under the Data Protection Act, processing of personal data in the interest of national security, defence and public order (section 39), processing personal data for enforcing legal rights or claims, and advice in an impending legal processing (section41) are exempt from principles regulating processing of personal data. This could potentially lead to breach of individuals' privacy, particularly when viewed together with the other loopholes in the Cyber Security and Cyber Crimes Act.

10 *U.N. General Assembly Resolution on the Right to Privacy in the Digital Age of 2014, https://digitallibrary.un.org/record/788140?ln=en*

11 *Report of the Office of the United Nations High Commissioner for Human Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 30, 2014), https://www.ohchr.org/en/hrbodies/hrc/regularsessions/session27/documents/a-hrc-27-37_en.doc*

12 *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/69/397 (23 September 2014), https://www.ohchr.org/en/hrbodies/hrc/regularsessions/session31/documents/a.hrc.31.65_auv.docx*

13 *Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019, https://www.achpr.org/public/Document/file/English/draft_declaration_of_principles_on_freedom_of_expression_in_africa_eng.pdf*

14 *Data Protection Act, 2021, https://www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%203%20The%20Data%20Protection%20Act%202021_0.pdf*

Limitation on Freedom of Expression

Section 59 criminalises the production, possession, conveyance, importation, exportation or causing importation or exportation, advertising or exhibition of obscene drawings, paintings, pictures, images, posters, emblems, photographs, videos or any other object tending to corrupt morals. The offence attracts a penalty up to 3,000 Kwacha (USD 133) or imprisonment up to a maximum of 15 years.

The words "any other object tending to corrupt morals," in the provision make it ambiguous and so wide in scope that it has a chilling effect on freedom of expression and speech. The words "corrupt morals" are not defined in the Act and thereby present uncertainties in implementation. Moreover, this potentially inhibits artistic, journalistic, research and education works on the basis of undefined obscenity, and corruption of morals. Indeed, authorities could use the section to levy charges of choice to prosecute critics of the government.

Broad Definition of Hate Speech

Section 65 of the Act prohibits hate speech. Hate speech and conduct under section 2 is defined as "verbal or non verbal communication, action, material whether video, audio, streaming or written, that involves hostility or segregation directed towards an individual or particular social groups on grounds of race, ethnicity, antisemitism, tribalism, sex, age, disability, colour, marital status, pregnancy, health status and economic status, culture, religion, belief, conscience, origin."

Whereas fighting hate crime is a legitimate state responsibility the world over, this definition of hate speech is overly broad and vague and does not delineate legitimate expression which would not amount to hate crime. Accordingly, this provision could be abused to persecute critics through arbitrary arrests and detention. It could thus have a chilling effect on freedom of expression and information, promote self-censorship, and limit the exercise of the profession of journalism. The penalty for hate speech is a fine of up to Kwacha 150,000 (USD 6,643), imprisonment for up to two years, or both.

The Offence of Harassment

Section 69 introduces the offence of harassment yet there is no definition of the crime under the Act. Moreover, the provision that "A person who uses a computer system intentionally initiates any electronic communication, with the intent to coerce, intimidate, harass, or cause emotional distress to a person commits an offence" is ambiguous. Further, the penalty for the offence is high - a fine not exceeding 150,000 Kwacha (USD 6,643), imprisonment for up to five years, or both. This provision can form the basis for silencing critical voices.

Conclusion

While cyber security is critical in the highly evolving technological era, it is important that a rights-based approach is employed in the development of policies and laws to ensure that the adopted laws and policies do not wantonly limit individual rights and freedoms. The Cyber Security and Cyber Crimes Act, 2021 in its current state offers some solutions to emerging challenges in the digital space. However, it has wide negative impacts on the protection, promotion and enjoyment of digital rights and freedoms.

Under international human rights law, the rights to privacy, freedom of expression and information may only be restricted if prescribed by law, in pursuit of a legitimate aim, and if the restrictions are necessary and proportionate in pursuance of a legitimate aim. Many provisions in the law are vague and overly broad, in contravention of the principle of legality. The law extends the powers of state authorities to restrict and punish online expression, and gives law enforcement agents leverage to conduct unsupervised surveillance without the backing of a judicial order.

Indeed, the new law falls short of the established regional and international human rights standards on the right to privacy as laid down in the African Union Convention on Cyber Security and Personal Data Protection, Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and the African Commission on Human and Peoples' Rights (ACHPR) Declaration on Principles of Freedom of Expression and Access to Information. Hence parliament should consider repealing or amending the regressive provisions to ensure digital rights and freedoms are protected.

CIPESA

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Tel: +256 414 289 502
Email: programmes@cipesa.org
Twitter: @cipesaug
Facebook: facebook.com/cipesaug
www.cipesa.org