Cybersecurity and Data Protection Bill entrenches surveillance: MISA Zimbabwe analysis of the Cybersecurity and Data Protection Bill, 2019

Introduction

The advent of the Internet and related technological developments have been celebrated for providing platforms for widespread and 'unrestricted' exercise of freedom of expression and access to information rights and conducting of transactions online among other aspects.

Indeed, Africa in general, and in Zimbabwe in particular, has witnessed growth in internet penetration.

With the Covid-19 pandemic and implementation of national lockdowns, businesses, education and day to day work in general, is generally now being conducted online thus indicating the importance of digital platforms and tools.

These developments should thus be an awakening for Zimbabwe to have in place a democratic legal framework to regulate online activity. This comes at a time when the continued existence of colonial and unconstitutional laws and flawed democratic practices continue to hinder enjoyment of digital rights.

MISA Zimbabwe therefore notes the long awaited gazetting of the Cybersecurity and Data Protection Bill whose objective is to increase cyber security in order to build confidence and trust in the secure use of information and communication technologies by data controllers, their representatives and data subjects.[1]

In February 2019, following the approval for the repeal of AIPPA by Cabinet , the Data Protection Bill was one of the Bills that was proposed to address data protection and privacy issues in alignment with the Constitution. The gazetted Bill sets out to merge the two aspects: being cybersecurity and data protection.

Shortly before the ouster of former President Robert Mugabe, a Ministry of Cybersecurity, Threat Detection and Mitigation, was set up. Subsequent to reshuffles in government, this ministry morphed into a department under the existing Ministry of Information Communication Technologies.

It is therefore poignant to note that, and according to the then Presidential spokesperson at the material time, the ministry had been established to catch "mischievous rats" that abused social media.

More recently in March 2020, Zimbabwe National Army (ZNA) Commander, Lieutenant-General Edzai Chimonyo, addressing senior military commissioned officers at the Zimbabwe

[1]Section 2 of the Bill

Military Academy in Gweru, highlighted that the military would soon start snooping into private communications between private citizens to "guard against subversion," as social media has become a threat to national security.

MISA Zimbabwe therefore hopes that the crafting and enforcement of this legislation will not be blinkered or narrowed to entirely prioritise the protection of 'national interests' and the prevention of 'social media abuse' at the expense of digital security and protection of the privacy of internet users in Zimbabwe.

Analysis of the Bill

To begin with, Section 5 and 7 of the Bill seek to establish the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), as the Cybersecurity Centre and Data Protection Authority, respectively. This essentially gives POTRAZ the roles of potentially three bodies, being the regulator of the telecommunications industry, the cybersecurity centre and the data protection authority.

As rightly laid out in the Bill, POTRAZ is created in terms of the Postal and Telecommunications Act [Chapter 12:05] and likewise its roles should be limited to those laid out in [Chapter 12:05]. It is inappropriate to also allocate the functions of the Cybersecurity Centre and Data Protection Authority in their entirety to POTRAZ. There is no justifiable basis to promote such monopoly by POTRAZ as this frowns upon the basic principles of efficiency, before even delving into the nitty-gritties of the independence of this body.

It is MISA Zimbabwe's submission that a separate and independent body be set up to handle all cyber security issues, comprising stakeholders who advocate for internet freedom and protection of digital rights.

The Bill makes provision for the processing of data, which includes the organization and alterations among others. More recently, the Finance Minister, Mthuli Ncube, at a post-cabinet briefing on the economic relief for Covid-19, said government had used 'a sophisticated algorithm'[2] which used bank accounts and also relied on mobile numbers to access the locations of individuals.

In this regard, there was need to notify the data subjects prior to the collection of this information as well as clear information on how the data was processed.

Meanwhile, the processing of sensitive information, genetic data, biometric data and health data is prohibited under this Bill, except in specified circumstances which include where the processing is necessary to comply with national security laws and also for the prevention of imminent danger or the mitigation of a specific criminal offence.

It should be noted that Zimbabwe has a history of surveillance through its laws that seek to promote national security like the Official Secrets Act and the Interceptions of

[2] https://www.financialgazette.co.zw/mthuli-ncube-his-sophisticated-algorithms-for-corona-relief-funds-another-privacy-disaster-looming/

Communications Act. These laws are not aligned to the Constitution and have provisions that continue to violate the exercise of rights.

There is therefore need to ensure that all national security laws are reviewed in line with the human rights framework in the Constitution. In circumstances where information relates to national security, more often than not, there is no disclosure of sufficient information under the auspices of national interests.

This poses the danger of such provisions being abused and exposing citizens to over surveillance by government and state security agents, thus, violating their right to privacy.

In the event of any security breach, the Bill provides in Section 19, that the data controller shall notify the Authority, without any undue delay of any security breach affecting data that he or she processes. It is imperative that the law should provide a specific timeline under which the security breach shall be communicated rather than leaving the provision open to interpretation on what entails undue delay.

In addition, the Bill provides an obligation to data controllers, except for those in specified circumstances to notify the Data Protection Authority prior to any wholly or partly automated operation or set of operations intended to serve a single purpose or several related purposes.

The notification is not required where the data controller has appointed a data protection officer. It is also important for the law to make it obligatory for every data controller to appoint a data protection officer. A data protection officer in terms of the Bill, refers to any individual appointed by the data controller and is charged with ensuring, in an independent manner, compliance with the obligations provided for in this Bill.

However, the question that therefore arises is who polices the data protection officer and ensures that they are independent and exercise due diligence?

The Bill also amends the provisions in Sections 163-166 of the Criminal Law (Codification and Reform) Act, which speaks on offences relating to computer systems, computer data, data storage mediums, data codes and devices.

However, it is commendable that the law seeks to put in place provisions relating to hacking, unlawful interference and interception of data and computer systems. By nature, these crimes are usually premeditated (planned in advance) and threaten the online security of Internet users.

It is therefore important to question whether or not, the prosecuting authorities will have the know-how and the technical capacity to prosecute such offences. It should also be noted that the Internet has created a global village and such hacking or unlawful interferences can be perpetrated by persons outside Zimbabwe and thus outside the jurisdiction of our law enforcement authorities.

The provisions on offences relating to electronic communications and materials needs to be highlighted as well. It has been noted that online spaces have become unsafe due to instances

of brigading e.g. *Varakashi versus Nerr*orists[3], cyber bullying and harassment[4], revenge and child pornography, the production of racist and xenophobic material[5]among other incidences.

It is therefore commendable that the law takes note of these developments and seeks through the proposed law to regulate them.

There are, however, other provisions that have the potential to infringe on the exercise of media freedom, freedom of expression and access to information.

Section 164 states:

> *"Any person who unlawfully by means of a computer or information system makes available, transmits, broadcasts or distributes a data message to any person, group of persons or to the public with intend to incite such persons to commit acts of violence against any person or persons or to cause damage to any property shall be guilty of an offence and liable to a fine not exceeding level ten or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment."*

Provisions such as these are at risk of being relied on to inhibit constructive criticism which is important for promoting transparency and accountability especially from the government.

There is therefore a danger that such provisions will be used as political tools and mechanisms by the state to prevent the expression of dissenting opinions. This will potentially stifle citizen engagement and open debate, both of which are necessary elements to promote democracy.

Regarding the prohibition of cyberbullying and harassment in Section 164B, it should be noted that the proposed law criminalises not only the generation but also the communication of such offensive messages from '*any electronic medium accessible by any person'* which in essence also *includes* social media.

Section 164C of the Bill which also criminalises the use of a computer or information system to avail, broadcast, distribute data knowing it to be false and intending to cause psychological or economic harm to someone, also seems to be targeted against the spread of false information on social media.

In the prosecution of this offence, the law needs to be clear on who the arbiter of truth will be. It will also need to be proven that the perpetrator knew that the information was false and also that he or she had an intention to cause harm.

Assumptions should not be made of the fact that the accused person had knowledge of the falsity of the statement. This is particularly taking note of the magnitude of the use of Internet, which can make it difficult to determine the origin and authenticity of a message. This means that individuals will receive messages voluntarily or involuntarily.

---

[3] https://theconversation.com/a-vicious-online-propaganda-war-that-includes-fake-news-is-being-waged-in-zimbabwe-99402

[4]https://www.thestandard.co.zw/2020/04/19/cyber-bullying-surges-zim-lockdown/amp/?__twitter_impression=true

[5]https://twitter.com/Athi83496498/status/1261761432774946816?s=08

And, with the rise of citizen journalism through the use of the Internet, these provisions have the potential of implicating thousands of ordinary citizens who would have 'received' and communicated such messages.

MISA Zimbabwe therefore advocates for clear procedures and elements to establish intention to commit the offences so as to ensure that a balance will be struck between regulation of the Internet space and exercise of fundamental rights.

MISA Zimbabwe therefore calls for the equal prioritisation and balancing of the functions of the Cybersecurity Centre and Data Protection Authority to ensure that significance is not placed only on cybersecurity while data protection, privacy and the interrelated fundamental rights are neglected. The conflation of these three institutions poses a dual crisis, with POTRAZ, on one hand, becoming the surveillance arm of the state while also having access to the large volumes of data collected by the Mobile Network Operators (MNOs) and Internet Service Providers (ISPs). This therefore compromises data protection and the right to privacy.

It is therefore important to ensure that the proposed law is in conformity with the Constitution and international legal frameworks such as the African Declaration on Internet Rights and Freedoms.

Democratic law making processes places high significance and consideration on the views of key stakeholders and the general public.

MISA Zimbabwe therefore hopes that the law-making authorities will be open to submissions and suggestions that can refine this law in line with international policy guidelines on cybersecurity and data protection.

End