Understanding the Cyber Security and Data Protection Bill

Kubatana.net
30 June 2020

What do I need to know about the Bill?

The Cyber Security and Data Protection Bill was gazetted on 15 May 2020. It has been discussed before a parliamentary committee and the public was invited to submit their comments on the Bill in writing to the Clerk of Parliament by 26 June 2020. Public hearings about the bill are scheduled for 6 - 10 July 2020.

What is this Bill referring to when it talks of Data Protection and Cyber-security?

The "data" referred to here includes all electronically transmitted and stored communications and information data. Any unauthorised access, tampering or sharing of that data constitutes a violation of cyber security.

On the one hand, government needs to ensure its own sensitive information pertaining to national security is safeguarded from online attacks (e.g. information pertaining to military operations or sensitive financial documents).

On the other hand, government is obligated (mainly by the Constitution) to protect Zimbabweans from abuse of data collected about them through government, commercial, medical and other channels – particularly online.

Collection of data and use of data collected affects the following rights: right to dignity; personal security, privacy, freedom of expression; administrative justice; fair hearing; rights of accused persons and the rights of children protecting them against sexual exploitation.

What legislation currently manages our Cyber-Security and Data Protection laws?

- *Postal and Telecommunications Act* – creation of POTRAZ – regulatory body for all telecommunications.
- *Official Secrets Act* – prohibits the sharing of information about state buildings, people and classified information which could be deemed to threaten State security.
- *Interceptions of Communications Act* – provides for the lawful interception and monitoring of certain communications in the course of their transmission through a telecommunication, postal or any other related service or system in Zimbabwe. It also provides guidelines for monitoring and managing communications.
- *Criminal Law (Codification and Reform) Act* – offences related to computers, related technologies and electronic information sharing.

What is the purpose of the new Bill?

According to the Bill's memorandum, the purpose of this Bill is "to consolidate cyber related offences and provide for data protection with due regard to the Declaration of Rights under the Constitution and the public and national interest, to establish a Cyber Security Centre and a Data Protection Authority, to provide for their functions, provide for investigation and collection of evidence of cyber crime and unauthorised data collection and breaches, and to provide for admissibility of electronic evidence for such offences. It will create a technology driven business environment and encourage technological development and the lawful use of technology."

Does the Bill matter?

Yes. Every time you use an electronic device to communicate, search for information or make a transaction, it leaves a digital footprint which creates data that can be stored, collected and potentially used by others. The Bill is supposed to align Cybersecurity and Data Protection laws with Zimbabwe's Constitution and 'consolidate cyber related offences'. Every person living in Zimbabwe will be affected by this legislation.

The internet holds information about you which includes your contact details, your behaviours (including things like interest preferences as well as location information on where you go and how frequently), your medical records, financial records and so on. Who you talk to and what you say to those people is also part of this data bank. All of this data needs to be protected from damage, attack and unauthorised access. Some of your data is not considered sensitive and will be automatically processed and used for statistical analysis (e.g. how much time you spend online). Other data is considered sensitive (e.g. personal details and financial information) which should never be shared without your express consent.

The Bill is important as it creates new regulatory bodies: the Data Protection Authority and Cyber Security Centre. It also sets out the guidelines for data processing by a data controller, regulates protection of data subjects and sets out acts that constitute offences.

What are the key aspects of the Bill?

Creation of Cyber Security Centre and designation of POTRAZ as Data Protection Authority

Part II of the Bill explains the creation of a Cyber Security Centre within POTRAZ which will "advise Government and implement Government Policy on cybercrime and cyber security. The Cyber Security Centre shall also promote and coordinate activities focused on improving cyber security and prevention of cybercrime."

Part III explains that POTRAZ will be designated as the Data Protection Authority. The DPA will regulate the processing of data. It will also work closely with the Minister of Information Publicity and Broadcasting Services in a consultative and advisory capacity regarding policy and legal matters, both locally and internationally.

Data Processing Standards and Rules for Data Controllers

According to article 5 of the European Union General Data Protection Regulation (GDPR) the principles of data processing are:

- Lawfulness
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

Parts IV and V outline the quality of data and principles of data protection standard operating guidelines for data controllers (any person who business who acquires and uses data e.g. any company that holds employee information e.g. employee contact information and banking details. On a larger scale, a data controller might be Econet or TelOne) and data processors (any person or entity who does something with the data held by a controller for and behalf of them – e.g. a payroll company or Google Analytics). The guidance governs when and how to use non-sensitive (generally non-personal data that might be used for statistical analysis, such as how much traffic passes through a toll gate) and sensitive data (any piece of data that could link that data to a specific individual or organisation, such as contact details, banking information, biometric and health information etc).

Duties and Obligations of Data Controllers and Processors

The Bill outlines the duties and obligations of data controllers regarding data collection and these include:

- Ensuring the data subject is aware of the purpose of the processing,
- The right of the data subject to object
- The right of the data subject to access the information and rectify it
-

The Bill places an obligation on the data controller to ensure security of data and ensure that there is no negligent unauthorized destruction, negligent loss unauthorized alteration or access. Should there be any breach the data controller must notify the Authority without delay. However the Bill does not provide for notification of security breach to the subject: ie. if one's information has been breached they have a right to know. The Bill provides for openness of processing and accountability by the data controller of security breaches, and accountability. It places the duty of ensuring the security, integrity and confidentiality of data on the data controller.

Protection and Rights of Data Subjects

Part VII speaks directly to the rights of Data Subjects (ie. The people whose data has been collected for whatever reason). This section specifically talks about the right of subjects not to have their automatically processed data used to make decisions about them (for example being

disqualified from a loan or job based on information obtained without the subject's knowledge). The section also gives permits the guardians of children and legally incapacitated adults to exercise subjects' rights on their behalf.

The Bill also refers to subjects' rights elsewhere and includes the right to refuse consent; to rectify their data; the right to erasure and to access their data.

Management of data and accountability structures

Part VIII includes guidelines on the transfer of data outside of Zimbabwe. Data is shared beyond a country's borders through the use of online data storage services (iCloud, Dropbox etc), as well as through deliberate sharing of information between governments or organisations. The Bill does not go into much detail on the specifics of cross border data regulation.

Part IX instructs the Authority (i.e. POTRAZ) to provide guidelines on the drafting of codes of conduct for Data Controllers and Processors, and to authorise the same. It does not provide any further detail on what should be contained in these policies.

Part X makes provision for the establishment of a whistleblowing system which would expose misuse of data. The provision stops short of explicitly providing for the protection of whistleblowers. It also does not explicitly speak to the need for the system to be managed independently of the Data Protection Authority and the Cyber Security Centre.

Part XI gives the Minister of Information, Publicity and Broadcasting Services power to make regulations with regard to cyber security and data protection in consultation with the DPA. It also outlines the penalties for violating the provisions of the Bill.

Amendments to the Criminal Code in respect of cybercrime

Part XII outlines proposed amendments to the Criminal Law Act (Chapter VIII) in respect to existing cybercrime law.

Offences related to computer use to be re-examined include: hacking, unlawful acquisition of data, unlawful interference with data or data storage medium, unlawful interference with a computer system, unlawful disclosure of data code, unlawful use of data or devices.

Offences linked to electronic communication and materials include: transmission of data message inciting violence or damage to property, sending threatening data message, cyber-bullying and harassment, transmission of false data message intending to cause harm, spam, transmission of intimate images without consent, production and dissemination of racist and xenophobic material, identity-related offence.

Offences against children include: child pornography, and exposing children to pornography. This section also outlines when and how computers and data storage systems may be seized and searched and where data traffic may be collected, recorded or preserved.

While some of the amendments are certainly necessary, the wording in the Bill may suggest that there is room for interpretation which could facilitate a clamping down on critical political commentary and freedom of speech.

Key Questions to Ask

1. Is the Bill drafted in language that is clear and unambiguous for the benefit of ordinary citizens and policy implementers?
2. Why have the two separate issues of Cyber Security and Data Protection been bundled together when globally, the issues are regulated separately?
3. What is the relationship between POTRAZ, the Cyber Security Centre and the Data Protection Authority? Are the roles of each defined clearly enough to avoid duplication of duty and to ensure efficiency within and between the different bodies?
4. What checks and balances are in place to ensure the independence and efficacy of each body and to keep each body accountable to the public? What parliamentary oversight has been provided over the activities of each body?
5. Do the data protection principles in the Bill meet regional and international standards?
6. What structures are in place to ensure that data controllers and processors are kept accountable to the public? (i.e. where and how may the public access a register of approved data controllers and processors?)
7. What measures are in place to ensure the independence of the CSC and DPA from the Executive, through the Ministry of Information Publicity and Broadcasting Services?
8. Are the rights of data subjects explicit and comprehensive enough?
9. Does the guidance on regulation and the creation of codes of conduct go far enough in specifying absolute standards of practice?
10. Do exemptions to general codes of practice for the sake of “national security” or “public order” pose a threat to citizens’ constitutionally enshrined rights and freedoms, particularly when it comes to the criticism of authorities?
11. What measures will be in place to ensure the protection of whistleblowers?
12. Are the proposed amendments to the Criminal Code aligned to the Constitution? What provisions are explicitly in place to guarantee citizens’ rights and freedoms, particularly in respect to the right to privacy, the right to access and share information, freedom of speech, freedom of the media, and freedom of association?

Get more information

To find out more, read the Bill on the Veritas website, and read MISA Zimbabwe’s commentary on the Bill