The CYBER SECURITY and DATA PROTECTION Bill [H.B. 18, 2019.]

Commentary by Chris Mhike, for **VERITAS**

28 September 2020

A. Introduction

1. The Cyber Security and Data Protection Bill [H.B. 18, 2019] was published in the Zimbabwean Government Gazette of Friday 15 May 2020[1] after numerous false starts,[2] and this is an analysis of the Bill with particular attention to the Bill's alignment with:

   1.1. The Constitution of Zimbabwe (2013), and
   1.2. International Standards, and
   1.3. Comparable statutes from other jurisdictions.

2. The introduction of this Bill to the legislative process is part of Government's declared media law reform agenda. On 12 February 2019, Information, Publicity and Broadcasting Services Minister Monica Mutsvangwa announced that as part of its media law reform and alignment of laws with the Constitution processes, Government had resolved to repeal the Access to Information and Protection of Privacy Act (AIPPA).

[1] Vol. Vol. XCVIII, No. 46.

[2] The initial draft dates as far back as 2016, when the proposed law was identified as "***The Cybercrime, Cybersecurity Bill***," which was approved by the Zimbabwean Cabinet in February 2019. In October 2019, Cabinet approved an updated version known as "***The Cyber Crime, Security and Data Protection Bill***." The version, under review in this commentary, is the Cyber Security and Data Protection Bill (of 15 May 2020).

3. The honourable Minister indicated that the repeal of AIPPA would give rise to at least three (3) new statutes, that is:

3.1. the Access to Information Bill, and

3.2. the Zimbabwe Media Commission Bill, and

3.3. the Protection of Personal Information/Data Protection Bill.[3]

4. What was then termed "the Access to Information Bill" was eventually published in the Government Gazette as the Freedom of Information Bill,[4] which is now law after the promulgation of the Freedom of Information Act [Chapter 10:33] on 1 July 2020.[5]

5. What the Minister referred to back in February 2019 as the Protection of Personal Information/Data Protection Bill, is now identified at the ***Cyber Security and Data Protection Bill***. There is chance there might still be a Protection of Personal Information Bill in the pipeline.[6]

6. It is clear from the content of the Bill under review (i.e H.B. 18, 2019), is more than a draft media law. The Cyber Security and Data Protection Bill affects everyone who relies of modern information communication technologies. That refers to, almost everyone.

7. The Bill, once finalized and promulgated into legislation, shall become part of Zimbabwe's **Cyber Law**, or **Law of the Internet**. This branch of the law has been

[3] https://www.herald.co.zw/cabinet-approves-aippa-repeal/
[4] on 5 July 2019 as [H.B. 6 of 2019.]
[5] Act No.1 of 2020.
[6] Clause 4 of H.B. 6 of 2019 refers to a statute by this name.

rather antiquated in Zimbabwe, and the introduction of new laws to update our legislation in this field has been long overdue for several years now.

8. Regrettably, when one reviews H.B. 18, 2019, it becomes clear that the Executive and Legislative arms of the Zimbabwean State have started on the wrong footing in updating this country's cyber laws.

B. Analysis

9. The most glaring shortcoming of the Bill lies in the failure of the drafters to recognize the importance of categorization of laws. The classification of laws is central to the attainment of justice, fairness and efficiency of laws.

10. The conceptual framework of the Bill is therefore significantly flawed, and needs to be urgently reviewed. Various improvements are needed in order for the Bill to inspire technological development, jurisprudential advancement, facilitation of enhanced modern transactions, business growth, or other noble cyber law related objectives that are recognizable in other jurisdictions.

i) <u>Categorization of Laws</u>

11. The two broad categories of law across numerous jurisdictions, including ours, are: **Criminal Law**, and **Civil Law**. This binary categorization means our legal system is essentially made up of both: criminal justice, and civil justice, systems – operating simultaneously. These two systems exist to deal with two different types of laws that have different purposes and that lead to very different consequences, if and when broken.

12. There are numerous other types of classifications of law, including *inter-alia*:

12.1. Public and Private Law, and

12.2. Civil Law and Criminal Law, and
12.3. Substantive and Procedural Law, and
12.4. Common Law and Equity.

13. However, the most relevant categorization for purposes of this analysis, in the criminal and civil laws distinction. One of the greatest weaknesses of the Cyber Security and Data Protection Bill is in that it attempts to solve criminal law and civil law questions in one statute. This significantly compromises the lucidity and precision of the proposed law in ways that are illustrated in latter parts of this analysis.

14. One of the major criticisms of AIPPA was that it consolidated two vastly different aspects of law, that is: a) **access to information** on the one hand, and b) **protection of privacy** on the other.

15. The attempt to mix regulatory considerations with the exercise of fundamental rights led to undue limitations on the legislature's stated objective of giving meaning to the individual's fundamental right to access information; and the media's entitlement of press freedom. That mistake, of apparently mixing components of the law that are enormously different, is being repeated in the Cyber Security and Data Protection Bill.

16. A more effective way in establishing a coherent and smart cyber law system would be the enactment of specialized laws and regulations that are tailor-made for online activities. For instance, in the United States, cyber security is managed at Federal level mainly through three sets of statutes that focus on industry-specific cybersecurity themes. The three laws are:

16.1. the 1996 Health Insurance Portability and Accountability Act (HIPAA), and
16.2. the 1999 Gramm-Leach-Bliley Act, and
16.3. the 2002 Homeland Security Act, which at the time of its promulgation, incorporated the Federal Information Security Management Act (FISMA).

17. In the American context, these three sets of regulations mandate in very clear and unambiguous terms, healthcare organizations, financial institutions and federal agencies to put in place adequate safeguards for their information and computer-based systems.

18. The conceptual weakness of the Zimbabwean Bill is also laid bare when one interrogates the stated Object of this proposed consolidated law. That Object is spelt out in Clause 2 of the Bill. The Purpose of the proposed law is specified in the Memorandum to the Bill, and the Preamble of the substantive draft law.

ii) **Purpose of the Bill** [H.B. 18, 2019]

19. The Memorandum to the Cyber Security and Data Protection Bill spells out the various purposes of the Bill to include:

    19.1. Consolidation of cyber related offences, and
    19.2. To provide for data protection with due regard to the Declaration of Rights under the Constitution and the public and national interest, and
    19.3. to establish a Cyber Security Centre and a Data Protection Authority, and to provide for their functions, and
    19.4. to provide for investigation and collection of evidence of cybercrime and unauthorised data collection and breaches, and to provide for admissibility of electronic evidence for such offences, and
    19.5. to create a technology driven business environment, and
    19.6. to encourage technological development and the lawful use of technology.

20. In order to assess the adequacy of the explicit Purpose of the Bill, it helps to briefly consider the definition of cyber law, and the purpose thereof. **Cyber Law** may be defined as any law that applies to the internet and internet-related technologies.

21. **Black's Law Dictionary** defines Cyber Law as:

> "***The field of law dealing with the Internet; encompassing cases, statutes, regulations, and disputes that affect people and business interacting through computers. Cyber Law addresses issues of online speech and business that arise***

because of the nature of the medium, including intellectual property rights, free speech, privacy, e-commerce, and safety, as well as questions of jurisdiction."

22. From that definition, it is clear that cyber law is more than just Cyber Security and Data Protection, hence the importance of assembling a battery of cyber-related laws, organized according to the various known classifications of laws; as opposed to consolidating issues into one composite statute.

23. The Bill's objective of consolidating cyber related crimes, and lumping numerous of the selected crimes with matters that could be resolved through civil procedure, or even non-legal remedies (e.g the processing of non-sensitive personal information, or creation of a technology-driven business environment), is clearly problematic.

24. In addition to arranging distinct cyber law issues into separate and issue-specific statutes, the lawmaker could make further progress in attaining clarity by sharpening the objectives of the proposed law, from the current one sentence objective, to a more descriptive identification of the law's objectives.

25. The Nigerian law is a good example of a law that is clearer as to the objects of a cybercrime statute. The stated objectives of the Nigerian Cybercrimes (Prohibition, Prevention, Etc) Act of 2015 are to:

> "(a) provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria;
>
> (b) ensure the protection of critical national information infrastructure; and
>
> (c) promote cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights."

26. **RECOMMENDATION**: The criminal elements of the Bill should be separated from the civil dimensions with two or more distinct cyber laws emerging from this Bill.

iii) <u>The Bill of Rights, Regional & International Instruments</u>

27. While the Bill explicitly recognizes the importance of fundamental rights in its Preamble, the content of the draft law does not go far enough in exhibiting the law-maker's respect for human rights. The rights specifically threatened by this Bill include provisions in the Bill of Rights the Constitution of Zimbabwe, as follows:

    27.1. Right to human dignity - **Section 51**, and

27.2. Right to personal security - **Section 52** on, and
27.3. Right to privacy - **Section 57**, and
27.4. Freedom of expression and freedom of the media - **Section 61**, and
27.5. Access to Information - **Section 62**, and
27.6. Right to administrative justice - **Section 68**, and
27.7. Right to a fair hearing - **Section 69**, and
27.8. Rights of accused persons - **Section 70**, and
27.9. Rights of children - **Section 81**.

28. The first listed objective of the Bill make it clear that the primary purpose of the law-maker is to create a criminal law relating to computers and computer networks; that is, a cybercrime statute. Other cyber-law dimensions such as Intellectual Property Rights, e-Commerce, and free speech, are overlooked. This leads to the criminalization of non-criminal spheres of societal enterprise, notably including free speech and media operations.

29. After considering the content of the 35 clauses of this Bill, it is not clear whether the draft law is a criminal or a civil statute; and as pointed in earlier paragraphs of this analysis, that in itself is a major problem.

30. As an instrument of Criminal Law, the Bill falls short of the basic standards for the definition of crimes. The Bill fails to clearly identify or define the various cybercrimes that are known at law in other jurisdictions, or to spell out the elements that constitute those crimes.

iv) **Clause 3 – Definitions**

31. The Interpretation section of the Bill proffers a wide range of definitions, and this is useful in making the proposed law clearer. However, a number of important terms are omitted, while certain terms that are included are inadequately defined, for instance:

31.1. “Data Contoller,” and

31.2. “Health Professional,” or

31.3. “Whistleblowing.”

v) Clause 4 – Application of Statute

32. Application of the proposed law is subjected to a yet to be published law, that is: "the Protection of Personal Information Act [Chapter ….]"

32.1. This means the introduction of H.B. 18, 2019 is premature. The Minister ought to have waited until the law referred to was on the statute book. It will be difficult for legislators and the general populace to definitively assess the quality of the proposed cybersecurity, without knowing the contents of the reported "Protection of Personal Information Act."

32.2. The Bill's intention to introduce extraterritorial jurisdiction through Clause 4 (2) (b) is questionable. Without entering into an effective multinational concord[7] or Mutual Assistance arrangements of countries hosting the "controller who is not permanently established in Zimbabwe," enforcing Clause 4 (2) (b) of the Bill could be highly challenging, if not impossible.

32.3. The threat of litigation to data controllers under Clause 4 (3) is clumsily placed in this Part of the Bill, and it does not add value to the proposed law.

vi) Clauses 5 and 6 – POTRAZ as Cyber Security Centre, and Data Protection Authority

33. The Bill proposes to designate the Postal and Telecommunications Regulatory Authority (POTRAZ) as:

33.1. the Cyber Security Centre (Clause 5), and

[7] as was done by European nations through the Council of Europe Convention on Cybercrime (Budapest, 23.XI.2001).

33.2. the Data Protection Authority.

34. These designations create quite a behemoth out of POTRAZ, a situation that probably compromises the efficiency of the organization. POTRAZ is created under the Postal and Telecommunications Act [Chapter 12:05] wherein a total of fifteen (15) functions are assigned to this Authority. An additional nine (9) functions are listed in the Bill, in respect of POTRAZ's supplementary role as a Cyber Security Centre, and ten (10) other roles in its third designation as a Data Protection Authority.

35. Regulatory convergence is, in general terms, progressive. However, the legislature must be careful to avoid creating loaded, and therefore, inefficient governance and supervisory institutions.

36. POTRAZ in its current configuration is ill-suited to serve as a fitting and effective Authority, Regulator or protector of fundamental rights because:

36.1. It is not an independent institution. Its Board is appointed by the President in consultation with the Minister.[8]

36.2. The competencies listed under section 6 (2) of the Postal and Telecommunications Act are not broad enough to address all the key functions that are assigned to POTRAZ by that statute, and by the Bill under review. For instance, knowledge and/ experience in the field of human rights, is not listed as part of the criteria for selection and appointment to the POTRAZ Board.

37. **RECOMMENDATION**: To improve on the efficiency and effectiveness of POTRAZ, the Cyber Security Centre, and the Data Protection Authority, it would be useful for the lawmaker to:

[8] See section 6 (1) of the Postal and Telecommunications Act [Chapter 12:05].

37.1. Streamline the functions of these bodies, and

37.2. Consider their separation into distinct bodies with clearly defined roles and functions. To avoid the multiplicity of regulatory authorities, the regulation of Cyber Security and Data Protection activities could be assigned to POTRAZ departments or committees, and

37.3. Transform POTRAZ into a truly independent institution, for instance through adopting appointment procedures that relate to Constitutional Commissions, and

37.4. Expand the criteria to appointment to the reformed POTRAZ so as to cover all the functional roles that are listed in this Bill for execution by the expanded POTRAZ, and

37.5. Assign some of the listed functions to existing institution e.g guidelines for investigation to be left with the Police, for prosecution with the National Prosecuting Authority, and complaints regarding fundamental human rights and freedoms with the Human Rights Commission. In the Republic of Ireland, they have gone as far as establishing a Data Protection Commission. In the Zimbabwean context, where numerous constitutional commissions are already in place, the Human Rights or Media Commissions could play some role in the regulation of data management issues.

vii) **Clauses 9 – 16: Quality of Data, and General Rules on Data Processing**

38. The Bill's description of date quality required from a controller, is deficient in a number of ways, including the omission of the following important features: i)

transparency/openness, ii) purpose limitation, and iii) accountability[9] on the part of data controllers.

39. The inadequacy of the Bill's Clause 9 threatens therefore threatens the right of privacy of persons whose data is in the custody of a controller.

40. **Clause 14** of the Bill refers to **Genetic, Biometric Sensitive Data and Health Data**. Although **sub-clause (1)** establishes the concept of data subject consent, that right is quickly and decisively snuffed out through **sub-clause (3)** which prioritizes a whopping ten (10) justifications for the disregard of a data subject's consent, privacy rights, dignity, and administrative justice. This, of course, means the Bill does not pass constitutional muster.

41. **RECOMMENDATIONS**:

41.1. The expansion of Clause 9 (on **Data Quality**), to include other widely recognized characteristics (for instance by infusing additional features of the GDPR) of acceptable data quality, would be useful.

41.2. The concept of data subject participation must also be infused into the Bill beyond the token reference to consent in Clause 12. The data subject must be afforded the right to request confirmation of whether a responsible party holds personal information about him/ her.

41.3. The data subject must also be afforded the right to request a record or description of the personal information about the data subject being held by a data processor, as well as information concerning the identity of all third parties who have had access to the data subject's personal information.

[9] Article 5 of the European Union General Data Protection Regulation (GDPR) for a comprehensive list of data [processing principles.

41.4. An improved Bill would carry clauses allowing a data subject to request that a data processor:

a) correct or delete personal information about the data subject that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or unlawfully obtained; and

b) delete or destroy personal information that the responsible party is no longer authorized to retain.[10]

42. Issues pertaining Genetic, Biometric Sensitive Data and Health Data, and the protection thereof, should probably regulated from a separate statute so as to avoid the dilution of data subjects' fundamental rights.

viii) <u>Clauses 18 – 19: Security</u>

43. The data controller's obligation to safeguard the security, integrity and confidentiality of day is established in very broad terms, whose lack of specificity weakens the effectiveness of these provisions. Clause 18 compels the controller to "***take appropriate technical and organizational measures that are necessary***." Such general language is insufficient, especially when one considers the importance of data security, in the context of relevant personal rights.

44. The Clause regarding the Data Controller's obligations (i.e Clause 18 of the Bill) ought to be more specific about what the said "***technical and organizational measures***" should look like. For example, under Irish law controllers should design their processes so that they collect only the data absolutely necessary for their purposes, and access to personal data should be limited to only those necessary for processing. Controllers may also temporarily anonymise personal data."

[10] The recommendation on data subject rights are largely drawn from South Africa's Protection of Personal Information Act, 2013 (POPIA).

45. The proposed Zimbabwean cyber law lacks in oversight or adequate accountability provisions. While Clause 19 compels the controller to notify the Authority of any data breach, that duty to report refers only to the Authority, not to the data subject. This shows the drafters' scant regard for the persons that the draft law purports to protect. As a result of that shortcoming, the Bill fails to proffer adequate protection or recourse for potential victims of breaches emanating from the Controller's negligence or incompetence.

46. **RECOMMENDATIONS** (Data Controller Obligations):

46.1. The section relating to the Data Controller's obligations must be more specific as to what the required "***technical and organizational measures***" should be.

46.2. To ensure the adequacy of those measures, Controllers must be compelled to submit their technical and organizational plans to a higher Authority, for assessment and approval. Under that assessment and approval mechanism, a Controller would have to secure certification from the supervisory authority, after demonstrating that their processes are designed to comply with the Authority/ Commission's minimum standards.

46.3. In order to afford data subjects greater protection, and to encourage Controllers to be more vigilant when dealing with information, the law must spell out consequences for avoidable breaches e.g by providing Compensation to a data subject whose information was not adequately protected. This could be an adaptation from Section 43A India's IT Act, which provides for compensation in the event one is negligent in using reasonable security practices and procedures (RSPP) in protecting sensitive personal data and information (SPDI) and this results in a wrongful gain or wrongful loss.

47. In the event of a data breach, the Controller should be obliged to report that breach, not only to the Authority, but also to the data subject.

ix) Clauses 25 –27: Data Subject

48. These Clauses zero-in on the issue of the Data Subjects, that is, an identifiable person in respect of whom specific data is concerned. These sections do not go far enough in defining measures of protection to be extended to Data Subjects.

49. **RECOMMENDATIONS** (on Data Subjects Issues):

49.1. The lawmaker should aim to synthesize all the key provisions relating to Data Subjects, in a more concise and focused manner, as opposed to the current format in the Bill, whereby these provisions are scattered in numerous parts of the Bill.

49.2. Protections for Data Subjects should also be clearer under this segment of the proposed law. For instance, it must be made unequivocally clear that a Data Subject has the right to suspend, withdraw or order the blocking, removal or destruction of personal data. The Subject may exercise that right upon discovery and reasonable proof that the relevant personal data is incomplete, outdated, false, or was unlawfully obtained.

49.3. International best practice and the Bill of Rights under Zimbabwe's Constitution are also important sources of the other rights that must be listed in the Data Subjects portion of the Bill.

x) Clause 30: Code of Conduct

50. In advanced democracies, Codes of Conduct in the context of Cyber Law and Regulation relate to voluntary sets of rules that assist members of that Code with data protection compliance and accountability in specific sectors or relating to particular processing operations. However, under the Bill under review, the Code referred to is a document drafted or provided by the Authority.

51. The Bill makes a feeble reference to 'consultation' in the Code-making process. To say "if it deems it fit, the Authority shall seek the views of the affected,"[11] falls short of the constitutional standard of a genuinely consultative law-making process.

52. **RECOMMENDATION** (on Codes of Conduct): Unconditional consultation, and opportunities for voluntary rule-making processes, should be at the core of the rule-making/ Codes-making process.

xi) Clause 31: Whistleblowing System

53. The protection offered to whistle-blowers under this section is inadequate. The Bill presents broad principles for the protection of whistle-blowers, but is very thin on details.

54. **RECOMMENDATION** (Whistleblower Protection):

54.1. In order to strengthen the protection framework, all protection arrangements should include a legal obligation for public officials to report misconduct and/or procedures for protecting whistleblowers and enforcing fair treatment after a disclosure has been made.

54.2. Clear legislation that offers comprehensive protection to whistleblowers.[12]

Clause 35: Amendment of the Criminal Code

55. The proposed amendments Chapter VIII of the Criminal Code which presently regulates Cybercrime in Zimbabwe, are not well thought out. For instance:

[11] Clause 30 (4) of the Bill.
[12] That is the case in Italy, the United States, Australia, France, among numerous other nations.

55.1. Numerous definitions are still vague and therefore unhelpful to persons who might wish to rely on the proposed law for guidance and protection. For instance, "cybercrime" is defined as "any offence under this Act."[13]

55.2. The Bill also omits numerous important definitions, and crimes, such as:

a) Definitions: modification, unauthorized access, or asymmetric cryptosystem," and

b) Crimes: Cyber terrorism, Fraudulent issuance of e-instructions, and Cyberextortion.

56. Section 166D makes reference to a Cyber Security Committee, yet another layer of regulation in addition to be ones stipulated in earlier sections of the Bill.

RECOMMENDATION (Amendments to the Criminal Code): The proposed amendments must be comprehensive, and result in the effective updating of the cyber-related aspects of Zimbabwe's criminal law.

xii) <u>CONCLUSION</u>

57. While the Bill carries various useful sections that will go a long way in updating Zimbabwe's cyber and data protection laws, the Bill, in its present form, still needs significant improvements in respect of presentation style, protection of fundamental rights, and its expansiveness in terms of covering pertinent issues.

[13] Compare this with the Kingdom of Saudi Arabia's Anti-Cyber Crime Law (Royal Decree No. M/17) of March 2007, which defines the same term to mean: "Any action which involves the use of computers or computer networks, in violation of the provisions of this Law."