REPUBLIC OF ZAMBIA

REPORT

OF THE

COMMITTEE ON MEDIA, INFORMATION AND COMMUNICATION TECHNOLOGIES

ON THE

RATIFICATION OF THE AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION FOR THE FIFTH SESSION OF THE TWELFTH NATIONAL ASSEMBLY

Published by the National Assembly of Zambia

REPORT

OF THE

COMMITTEE ON MEDIA, INFORMATION AND COMMUNICATION TECHNOLOGIES

ON THE

RATIFICATION OF THE AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION FOR THE FIFTH SESSION OF THE TWELFTH NATIONAL ASSEMBLY

Table of Contents

REPORT OF THE COMMITTEE ON MEDIA, INFORMATION AND COMMUNICATION TECHNOLOGIES ON THE RATIFICATION OF THE AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION FOR THE FIFTH SESSION OF THE TWELFTH NATIONAL ASSEMBLY

1.0 MEMBERSHIP OF THE COMMITTEE

The Committee consisted of Mr G M Imbuwa, MP (Chairperson); Ms P C Kucheka, MP (Vice-Chairperson); Mr R Mwewa, MP; Mr D M Kundoti, MP; Mr M Mukumbuta, MP; Dr E I Chibanda, MP; Mr M K Tembo, MP; Dr F Ng'ambi, MP; Mr C D Miyanda, MP; and Mr D Mumba, MP.

The membership of the Committee changed after the demise of Mr R Mwewa, MP, who was replaced by Mr K G Chisanga, MP.

The Honourable Mr Speaker
National Assembly
Parliament Buildings
LUSAKA

Sir

The Committee has the honour to present its Report on the ratification of the African Union Convention on Cyber Security and Personal Data Protection.

2.0 FUNCTIONS OF THE COMMITTEE

Pursuant to Article 63(2)(e) of the *Constitution of Zambia, Chapter 1 of the Laws of Zambia,* as amended by Act No. 2 of 2016, section 5(1*)* of the *Ratification of International Agreements Act*, *No. 34 of 2016* and the National Assembly Standing Orders No. 158 and 159, the National Assembly is vested with the power to oversee the performance of Executive functions by, among other things, approving international agreements and treaties before they are acceded to or ratified. Thus, the Committee was mandated to consider submissions and make recommendations to the House on the proposal to ratify the African Union Convention on Cyber Security and Personal Data Protection.

3.0 COMMITTEE'S PROGRAMME OF WORK

The Committee held ten meetings to consider the African Union Convention on Cyber Security and Personal Data Protection.

4.0 PROCEDURE ADOPTED BY THE COMMITTEE

In order to acquaint itself with the provisions and ramifications of the international agreement under consideration, the Committee sought both written and oral submissions from stakeholders. The stakeholders, who virtually appeared before the Committee, are listed at Appendix II.

5.0 GENERAL BACKGROUND

The African Union (AU) is an intergovernmental regional body that unites sovereign states on the African continent. Currently, the AU comprised fifty-five sovereign African States. The aims of the AU were, among others, to accelerate the political and socio-economic integration of the African states; promote economic development and the integration of African economies; and coordinate and harmonise the policies between the existing and future regional economic communities for the gradual attainment of the objectives of the Union. These aims, which formed the core mandate of the AU as enshrined in its constitutive document, created a broad legal basis for the AU and its institutions to establish regional policy and regulatory regimes on issues that affected Africa's economic integration and development, such as Information Communication Technologies (ICTs) and cyber security governance.

From the onset of the 21st century, the African continent had continued to witness tremendous growth in ICT and internet penetration. Recent statistics on the use of the internet indicated that Africa's internet user population grew from about 4.515 million people in 2000 to 453.3 million people in December, 2017, representing approximately 35.2 per cent of Africa's entire population estimate. This phenomenal growth, which still continued into the future, had been linked to factors such as the liberalisation of telecommunications markets in African states, the wide spread proliferation of mobile telecommunication technologies, and the increasing availability of broadband capacity. However, the spread of ICTs and internet penetration in Africa had also raised concerns over the need to promote cyber security governance and cyber stability on the continent.

This concern prompted the AU at its 23rd Ordinary Session held from 20th to 27th June, 2014, to establish a regional cyber security treaty known as the African Union (AU) Convention on Cyber Security and Personal Data Protection, at Malabo, Equatorial Guinea. The Convention imposed obligations on Member States to establish legal, policy and regulatory measures to promote cyber security governance and control cyber crime. Currently, fourteen member states of the African Union including Zambia had signed the Convention, and only eight member states have ratified the Convention which require, fifteen members states to ratify and come into force.

6.0 OBJECTIVE

The overall objective of the Convention was to harmonise legislation in the area of cyber security in Africa. The goal of the Convention, over and above the need to harmonise legislation, was to establish in each member state a mechanism capable of combating violations of privacy that may be generated by personal data collection, processing, transmission, storage and use. The Convention guaranteed that whatever form of data processing used shall respect the basic freedoms and rights of individuals while also taking into account the prerogatives of states, the rights of local communities, interests of business and take on board internationally-recognised best practices.

7.0 PROVISIONS OF THE CONVENTION

7.1 Key Provisions

The Convention under Article 8, required members states to promote cyber stability by establishing an appropriate cyber security legal framework aimed at strengthening fundamental rights and freedoms, particularly the protection of physical data and punish any violation of privacy without prejudice to the principle of free flow of personal data.

Further, Article 24 obliged Member States to establish a national cyber security framework that comprised a national cyber security policy and a national cyber security strategy. A Member State's national cyber security policy was required to recognise the importance of national Critical Information Infrastructure (CII) and identify related risks using the all-hazards approach, while also outlining how the objects of such policy were to be achieved.

7.1.1 How to become a party

Article 35 provided that the Convention would be open to all Member States of the Union, for signature, ratification or accession, in conformity with their respective constitutional procedures.

7.1.2 Reservations

A reservation to a treaty or an international agreement was a unilateral statement, however phrased or named, made by a state, when signing, ratifying, accepting, approving or acceding to a treaty, whereby it purported to exclude or to modify the legal effect of certain provisions of the treaty in their application to that state. In this regard, a reservation was permissible because the Convention did not expressly prohibit it.

7.1.3 Denunciation withdrawal

Article 38(2) of the Convention provided for a state party to withdrawal from the Convention by giving a one year written notice to the Chairperson of the Commission of the African Union.

8.0 Specific provisions of the convention

PREAMBLE

The preamble was an introduction highlighting what led to states parties to come up with the Convention.

Article 1 - Definitions

This Article provided for the definition of terms used in the Convention. It defined technical and non technical terms like child pornography, critical cyber, cryptology and cryptology activity.

8.1 CHAPTER 1 – ELECTRONIC TRANSACTIONS

Section I: Electronic Commerce

Article 2 – Scope of application of electronic commerce

Article 2(1) provided that state parties would ensure that e-commerce activities were exercised freely in their territories except:

(a) gambling, even in the form of legally authorised betting and lotteries;

(b) legal representation and assistance activities; and

(c) activities exercised by notaries or equivalent authorities in application of extant texts.

The import of Article 2(1) was that acts of gambling, legal representation and other activities exercised by notaries were precluded from the scope of e-commerce activities by member states.

Further, Article 2(2) obliged state parties to ensure that a person exercising e-commerce activities provided to the consumers information regarding: his or her name and address; where the person was subject to taxes; the licensing regime of the activity undertaken; and where the person was a member of a regulated profession, that person would indicate the professional title and the state party which had granted such

authorisation. The regulated professional would also indicate the professional body to which she or he was registered.

Additionally, Article 2(3) provided that a person involved in e-commerce activities would clearly state the price inclusive of taxes and other costs.

Article 3 – Contractual liability of the provider of goods and services by electronic means

This Article provided that e-commerce activities would be subject to the law of the state party in whose territory the person exercising such activity was established, subject to the intention expressed in common by the said person and the recipient of goods or services.

Article 4 – Advertising by electronic means

This Article provided that advertisements accessible through online communication services would clearly identify the individual or corporate body on whose behalf the advertisement was made. It also provided that conditions governing promotional offers and conditions for participating in promotional offers or games that were electronically disseminated would be clearly spelt out and easily accessible.

Further, Article 4(3) obliged state parties to prohibit direct marketing through any kind of communication using particulars of an individual who had not given prior consent to receiving the said direct marketing through such means. The Article obliged state parties to prohibit transmission, for the purposes of direct marketing, of messages by means of any form of indirect electronic communication without indicating valid particulars to which the addressee may send a request to stop such communications without incurring charges other than those arising from the transmission of such a request.

Furthermore, Article 4(6) provided that state parties would prohibit concealment of the identity of the person on whose behalf the advertisement accessed by an online communication service was issued.

Section II: Contractual Obligations in Electronic Form

Article 5 – Electronic contracts

This Article provided that information requested for the purpose of concluding a contract might be transmitted by electronic means if the recipients agreed to use those means. It also provided that a service provider or supplier, who offered goods and services in a professional capacity by electronic means, would make available the applicable contractual conditions directly or indirectly, in a way that facilitated the

conservation and reproduction of such conditions according to national legislation.

Further, the Article provided that for a contract to be validly concluded, the offeree would have had an opportunity to verify details of his or her order, before confirming the said order and signifying his or her acceptance.

Additionally, the Article also provided for instances where a party to a contract might not be held liable for breach of contract if the failure to perform was as a result of a *force majeure*.

Force majeure means an event which was beyond the reasonable control of a party to a contract, and which made a Party's performance of its obligations in the agreement impossible or so impracticable as reasonably to be considered impossible in the circumstances, and included, but was not limited to war, riots, civil disorder, earthquake, fire, explosions, storm, flood or other adverse weather conditions, strikes, lockouts or other industrial action.

Article 6 – Writing in electronic form

This Article provided that no person would be compelled to take legal action by electronic means. It also stated that in instances where a paper document was required to validate an act, state parties would establish conditions that could equally make electronic communication to have the same effect as a paper-based document. Further, it provided for methods to be implemented in order to fulfil the tax purposes of an invoice and management controls which created a reliable audit trail between an invoice and a supply of goods or services.

Furthermore, Article 6 provided for qualified electronic signature and Electronic Data Interchange (EDI) as examples of controls that would be used to authenticate the origin and integrity of content of an electronic invoice. Article 6(5) stated that a written document in electronic form was admissible in evidence in the same way as the paper-based document, provided that the author of the document could be duly identified and that it had been made out and retained in a manner that guaranteed its integrity.

Section III: Security of Electronic Transactions

Article 7 – Ensuring the security of electronic transactions

This Article provided for measures to be put in place to ensure that there was security of electronic transactions. It stated that the supplier of goods would allow the clients to make payments using electronic payment

methods approved by the state in line with the regulations of each state party. The Article also provided that the court would resolve proof related conflicts by determining all possible means in instances where there was no valid agreement between the parties.

Further, Article 7(3) stated that a copy or any other reproduction of contracts signed by electronic means would have the same effect as the original, where a copy had been certified as a true copy.

Furthermore, Article 7(4) provided for electronic signature. It stated that an electronic signature created by a secure device which the signatory was able to keep under his or her exclusive control and was appended to a digital certificate would be admissible as a signature just like a hand written one.

8.2 CHAPTER II – PERSONAL DATA PROTECTION

Section I: Personal Data Protection

Article 8 – Objective of the Convention with respect to personal data

Article 8 provided that each state party would establish a legal framework aimed at strengthening fundamental rights and public freedoms, particularly, the protection of physical data, and punish any violation of privacy without prejudice to the principle of free flow of data. It also stated that the legal framework established would ensure that any form of data processing respected the fundamental freedoms and rights of natural persons while recognising the prerogatives of the state, the rights of local communities and the purpose for which the business was established.

Article 9 – Scope of application of the Convention

Article 9 provided for acts that would be subject to the Convention and also instances when the Convention would not be applicable. Article 9(1) stated that an act of collection, processing, transmission, storage or use of personal data by a natural person, state, local communities and public or private corporate bodies would be subject to the Convention. Other actions that would be subject to the Convention included: automated or non-automated processing of data contained in a file or meant to be part of a file; any processing of data undertaken in the territory of a state party; and any processing of data relating to public security, defence, research criminal prosecution or state security.

Article 9 also provided for acts that were not applicable to the Convention. These included data processing undertaken by a natural person within the context of his or her personal or house hold activities, and temporary

copies produced within the context of technical activities for transmission and access to digital network with a view to automatic, immediate and temporary storage and data for the sole purpose of offering beneficiaries of the service the best possible information so transmitted.

Article 10 – Preliminary personal data processing formalities

This Article provided for actions that were exempted from preliminary formalities in personal data processing. These included processing undertaken by a non-profit making organisation with a religious, philosophical, political or trade union aim, provided such information was not disclosed to third parties.

Article 10 also stated that personal data processing would be subjected to a declaration before the protection authority except cases that were exempted in Article 10.1, 10.4 and 10.5 of the Convention. Further, Article 10 provided for actions that would be undertaken after authorisation by the national protection authority.

Section II: Institutional framework for the protection of personal data

Article 11 – Status, composition and organisation of national personal data protection authorities

This Article provided for an institutional framework for personal data protection. The Article also provided, *inter-alia*, that each state party would establish an authority in charge of protecting personal data. The Article further provided for how the authority would operate and the role of the state with regard to the National Personal Data Protection Authority.

Article 12 – Duties and powers of the national personal data protection authorities

This Article provided that the National Protection Authority would ensure that the processing of personal data was consistent with the provisions of the Convention. The Article also provided for what a National Protection Authority would do to ensure that information and communication technologies did not constitute a threat to public freedoms and other private life of citizens.

Section III: Obligations relating to conditions governing personal Data Processing

Article 13 – Basic principles of governing and legitimacy of professional data processing

Article 13 set out the basic principles that governed processing of personal data. This entailed that, firstly, the data subject would be given notice that certain personal data would be collected and processed. The data subject would then consent to it. Thereafter, in line with what the notice stated, the processing of the data would be done lawfully and for the purpose it was being acquired. It would be stored for a specified period in an accurate, transparent and in a confidential and secure manner.

Article 14 – Specific principles for the processing of sensitive data

Article 14 set out specific principles relating to the processing of sensitive data. Article 14(1) stated that parties prohibited the collection and processing of data relating to, *inter alia,* race, religion, political opinions and health of the data subject in order to avoid discrimination or profiling of certain individuals but with exceptions.

Article 14(2) set out the exceptions to the prohibitions to include data which the subject personally made public, where the data subject consented to the collection and processing of his or her sensitive data.

Article 15 – Interconnection of personal files

This Article provided that the interconnection of files laid down in the Convention would help to achieve the legal or statutory objectives which were of legitimate interest to data controllers.

Section IV: The data subjects' rights

This section provided for the rights of the data subject in relation to the processing of his or her data. Some of these rights included: the right to be kept informed under Article 16 and the right of access under Article 17. It also provided for the right to object under Article 18 and the right to rectification or erasure under Article 19, where it was found to be inaccurate or incomplete.

Section V: Obligations of the personal data controller

This section provided for the obligations placed on the data controller in the processing of personal data. The data controller was obliged to treat all personal data as confidential. Further, the data would be kept in a

secure place, for a specified period and in a user friendly manner. The obligations included confidentiality obligations, security obligations, storage obligations and sustainability obligations.

8.3 CHAPTER III – PROMOTING CYBER SECURITY AND COMBATING CYBERCRIME

Section I: Cyber security measures to be taken at national level

Article 24 provided for the cyber security framework to be developed at national level. This included developing a national policy and adopting strategies on how to implement the policy.

Article 25 provided for all legal measures to be undertaken by state parties. The Article recognised the need to criminalise cybercrime or to strengthen existing laws.

Article 26 placed the responsibility of promoting a culture of cyber security at national level, by ensuring that state parties engaged stakeholders in all sectors.

Article 26(3) provided for the development of public-private partnerships.

Article 27 – National cyber security monitoring structures

Article 27 provided that each state party would adopt the necessary measures to establish appropriate institutional mechanisms responsible for cyber security governance. Therefore, a state party was expected to ensure that institutions were established to ensure that cybercrime was combated in a coordinated manner nationally and regionally.

Article 28 – International cooperation

The Article provided for four elements within the international cooperation as set out below.

(i) Harmonisation

This section required harmonisation of legislative measures or regulations by state parties against cybercrime. The adoption of such measures was expected to strengthen regional harmonisation of these measures and enhancement of the principle of double criminal liability.

(ii) Mutual legal assistance

State parties that did not have agreements on mutual assistance in cybercrime were obliged to sign such agreements in conformity with the principle of double criminal liability. Doing so promoted the exchange of information as well as the efficient sharing of data between organisations of State Parties on a bilateral and multilateral basis.

(iii) Exchange of information

The Convention encouraged the establishment of institutions that exchanged information on cyber threats and vulnerability assessment such as the Computer Emergency Response Team (CERT).

(iv) Means of cooperation

State parties were obliged to make use of existing means for international cooperation with a view to responding to cyber threats, improving cyber security and stimulating dialogue between stakeholders. These may be international, nongovernmental or regional or based on private and public partnerships.

Section II: Criminal Provisions

Article 29 – Offences specific to Information and Communication Technologies

This Article provided for four elements of specific offences to ICTs as set out below.

(i) Attacks on computer systems

This section provided that state parties would take the necessary legislative or regulatory measures to criminalise certain offences. Such offences included one's attempt to enter or enter data fraudulently in a computer system or the gaining or attempt to gaining unauthorised access to part or all of a computer system or exceed authorised access, among others.

(ii) Computerised data breaches

The provision criminalised offences such as knowingly using data obtained fraudulently from a computer system or the processing or having personal data processed without complying with the preliminary formalities for the processing.

(ii) Content-related offences

This segment provided that state parties shall take the necessary legislative or regulatory measures to criminalise certain offences. Some of the offences included: the possession of an image or representation of child pornography in a computer system or on a computer data storage medium and deliberately deny, approve or justify acts constituting genocide or crimes against humanity through a computer system.

(iii) Offences relating to electronic message security measures

The provision required state parties to take necessary legislative or regulatory measures to ensure that digital evidence in criminal cases was admissible to establish offences under national criminal laws. This was achieved when the evidence had been presented during proceedings and discussed before the judge, that the originator could be identified and that its integrity could be established.

Article 30 – Adapting certain offences to information and communication technologies

This Article provided for two elements of the adaptation of certain offences to ICT as outlined below.

(i) Property Offences

This segment provided that state parties would take necessary legislative or regulatory measures to criminalise the violation of property such as theft, fraud and handling of stolen property. In addition, state parties would also consider as aggravated circumstances, the use of ICT to commit offences such as theft and fraud, among others.

(ii) Criminal Liability for Legal Persons

The section provided that state parties would take the necessary legislative or regulatory measures to ensure that legal persons other than the state, local communities and public institutions could be held responsible for the offences as provided under Article 29. Further, the provision did not exclude natural person who were perpetrators of or accomplices in the same offence.

Article 31 – Adapting certain sanctions to information and communication technologies

This Article provided for three elements of the adaptation of certain sanctions to ICT as set out hereunder.

(i) Criminal sanctions

The segment provided that state parties would ensure that measures were undertaken to provide punishment that was effective, proportionate and dissuasive criminal penalties for the offences under the Convention. Further, that the member states would also provide appropriate penalties under their national legislations.

(ii) Other criminal sanctions

This section provided for other sanctions for offences committed through digital communication medium and breach of confidentiality of data stored in a computer system. The Convention empowered competent courts to hand down additional sanctions. Further, it provided that a judge may order the mandatory dissemination of an extract of the decision through the same medium and according to modalities prescribed by the law of member states.

(iii) Procedural law

The provision provided that necessary measures would be made by member states to ensure that courts carried out searches on data stored in a computer system or medium where computerised data could be stored in the territory of a state party. This was achieved by establishing the truth. As such, data could be retrieved through another computer system. Additionally, member states would ensure that legislative measures were available for judicial authorities in charge of investigations or execution of a judicial delegation was empowered to carry out the operations under the Convention. Further, that such investigating judge was empowered to compel a service provider within the framework of his or her technical capacities to collect and record the computerised data.

8.4 CHAPTER IV – FINAL PROVISIONS

Article 32 – Measures to be taken at the level of the African Union

This Article empowered the Chairperson of the Commission to report to the Assembly on the establishment and monitoring of the operational mechanism of the Convention. The mechanism established was created

to ensure that member states were encouraged to adopt and implement measures to strengthen cyber security in electronic services, among others.

Article 33 – Safeguard provisions

The Article provided that the interpretation of the Convention would not be at variance with the relevant principles of international and customary law.

Article 34 – Settlement of disputes

Article 34 encouraged member states to settle any dispute through negotiations between states. The Article also encouraged members states to resolve disputes through other peaceful means such as mediation and conciliation where negotiations failed.

Article 35 – Signature, ratification or accession

The Article provided that the Convention would be open to all member states for signature, ratification or accession, in conformity with their respective constitutional procedures.

Article 36 – Entry to force

The Article provided that the Convention would enter into force thirty days after the date of the receipt by the Chairperson of the Commission of the African Union on the Fifteenth Instrument of ratification.

Article 37 – Amendment

The Article enabled state parties to submit proposals for any amendment or revision of the Convention. It further provided for the procedure to be followed by the Commission of the African Union once the proposals were received. The procedure entailed that the amendments or revisions once adopted would enter into force in accordance with the provisions of Article 36.

Article 38 – Depository

The Article provided that the state parties would deposit the instruments of ratification or accession with the Chairperson of the Commission of the African Union. The Article further enabled a state party to withdraw from the Convention if it so wished by giving prior written notice of one year in advance. The provision also obliged the Chairperson to register the amendment or withdrawal from the Convention with the Secretary General of the United Nations.

9.0 BENEFITS OF RATIFYING THE CONVENTION

The Committee was informed that ratifying the African Union Convention on Cyber Security and Data Protection would benefit member states and Zambia, in particular, in many ways including:

(a) ensuring that the country developed a legal framework that was harmonised with the regional aspirations and structures for cyber security and data protection;

(b) establishing a mechanism capable of combating violations of privacy that may be generated by personal data collection, processing, transmission, storage and use by proposing a type of institutional framework;

(c) guaranteeing that whatever form of data processing used would respect the basic freedoms and rights of individuals while also taking into account the prerogatives of the state, the rights of local communities and the interests of businesses and take on board internationally recognised best practices; and

(d) enabling member states to harmonise laws on cyber security and personal data protection.

10.0 STAKEHOLDERS' SPECIFIC CONCERNS ON THE PROVISIONS OF THE CONVENTION

The Committee interacted with various stakeholders with a view to broadening the consultative process on the proposal to ratify the African Union Convention on Cyber Security and Personal Data Protection. All stakeholders who appeared before the Committee supported the proposal by the Executive to ratify the African Union Convention on Cyber Security and Personal Data Protection. However, some stakeholders raised concerns as outlined below.

Title of the Convention

Stakeholders noted that although the Convention was titled African Union Convention on Cyber Security and Personal Data Protection, the Convention's scope and contents extended beyond cyber security and personal data protection as it also covered electronic commerce. In this regard, they noted that the entire Chapter I focused on electronic commerce. Thus, in their view, the Convention ought to have been aptly titled: "African Union Convention on Cyber-Security, Personal Data Protection and Electronic Commerce" in order to be inclusive of the entire scope of the content.

Article 1 – Definitions

Child pornography

Stakeholders were concerned with the phrase "and exploited with or without the child's knowledge" in the definition of child pornography because it could open up a loophole and possible debate regarding what was meant by "exploited." The phrase "and exploited" also made the exploitation of the minor's organs a vital component of the offence without which an accused person could not be successfully prosecuted. They were of the view that child pornography would still be pornography when images of a minor engaging in a sexual act were generated or when a minor's sexual organs were produced or used for primarily sexual purposes. Stakeholders were concerned that the Article also placed more emphasis on child pornography and not the circulation of general pornographic content of any nature on digital platforms as a cybercrime.

Communication with the public by electronic means

Stakeholders also proposed that the definition of communication with the public by electronic means in the Convention be expanded so as to read "Provision to the public or segments of the public, of signs, signals, writing, images, sounds, data or intelligence of any nature, transmitted in whole or in part by radio, electro-magnetic, photo electronic or photo optical system in order for it to be inclusive.

Damage

Stakeholders proposed that the word "means" be inserted between the word "Damage and any" so that the definition reads as Damage "means" any impairment to the integrity or availability of data, a program, a system, or information because in the definition the word means was missing.

Health data

Stakeholders noted that health data in the Convention was defined as information relating to the physical or mental state of the data subject, including the aforementioned genetic data. They were of the view that the definition was too wide and could include the physical state of a person and might not be reflective of a person's status. They submitted that the definition could state that "personal data related to the physical or mental health of a natural person including the provision of health care services, where such information revealed information about that natural person's health status."

Definition of sensitive data

Stakeholders noted that the definition of sensitive data in the Convention was narrow and submitted that this definition could be expanded so as to read "sensitive data means any personal data which had the potential of being the basis upon which the data subject might be discriminated against and included personal data relating to religious, philosophical, political and trade union opinions and activities as well as to sex life or race, health, social measures, legal proceedings and penal or administrative sanctions."

Article 2(1) – Scope of application of electronic commerce

Stakeholders noted that the provision sought to prohibit online gambling even in the form of legally authorised betting and lotteries. They argued that this provision needed to be measured against the current Government Policy as reflected by the current pieces of legislation, namely: *the State Lotteries Act, Chapter 328 of the Laws of Zambia; the Casino Act, Chapter 157 of the Laws of Zambia and the Betting Control Act, Chapter 166 of the Laws of Zambia*. This was because in Zambia, authorised betting took place even on digital platforms and a number of applications related to sports betting were easily and freely accessible. Therefore, this provision in the Convention would be in contradiction to what the law provided for in Zambia. They were of the view that there was need for the Executive to review the current relevant Zambian laws that regulated gambling and betting using digital platforms to align them to the Convention. Alternatively, this provision in the Convention should be struck off to allow for individual member states to determine what was applicable in their respective jurisdictions regarding betting.

Some stakeholders were also wary that the gambling industry was cash-intensive, thereby making it vulnerable to illicit activities such as money laundering and tax evasion. They were of the view that uncontrolled growth of the industry may result in irresponsible gambling which may breed addiction and loss of welfare to society.

Article 2 (b) – Provision of legal services and assistance activities

Stakeholders were concerned with the provision to exclude e-commerce activities relating to, the provision of legal services and assistance activities which in their view could be at variance with the intentions of the agreement establishing the Tripartite Free Trade Area among the Common Market for Eastern and Southern Africa (COMESA), the East African Community (EAC) and the Southern African Development Community (SADC) protocol on Trade in Services. The protocol allowed member states of the regional bodies to trade freely in services and made no exclusion to the nature of services regardless of the mode of their

delivery. They were of the view that the Tripartite Free Trade Area and the Convention be analysed together to ensure that the provisions were not in conflict.

Article 2 (c) – Online notaries

Stakeholders noted that the provision sought to restrict the free exercise of e-commerce activities relating to online notaries or equivalent authorities in application of extant texts. They appreciated the fact that the prohibition related only to extant texts, but argued that this provision was contrary to the provisions of the *Electronic Communications and Transactions Act No. 21 of 2009*. This was because this piece of legislation introduced a concept referred to as "functional equivalence" which sought to equate, for purposes of legal efficacy, online data and activities to hard copy data and physical activities. Notarisation and certification of documents as true copies were two of the activities expressly mentioned in the Act as not being affected by the fact that they were being performed online.

Article 2 (2) – Information to consumers

In addition to Article 2(2), stakeholders proposed that the information to consumers being referred to could also be intelligible, legible and in a language widely used by prospective consumers. The information would, therefore, read as "easy, direct and uninterrupted access using non-proprietary standards regarding information which should be in an intelligible and legible format." They further suggested that the provision must also mandate providers of online services to provide information regarding an adequate description of the goods or services for consumers to be able to make an informed decision regarding whether or not to enter into a contract with the supplier of such goods or services.

Article 4 – Advertising by electronic means

Stakeholders were of the view that the provisions of Article 4(2), which provided that direct marketing by electronic mail would be permissible where particulars of the addressee had been obtained directly from him or her. However, they were of the view that the proposal may also provide that the prospective customer be provided with an option to opt out of a transaction.

Article 4(3) – Unsolicited direct marketing messages

Stakeholders noted that notwithstanding provisions of Article 4(4), unsolicited direct marketing messages were still being sent to individuals either by email or text. They observed that ZICTA had in the past censored mobile network operators for this behaviour. However, this

concern had gone on unabated, creating a perception that it had now been allowed by the regulator. Stakeholders were of the view that ZICTA may have to state clearly what the position on the issue would be in the proposed laws. The proposed laws would also have to be aligned to the requirement being proposed in the AU Convention.

Article 12 – Duties and powers of National Protection Authority

Stakeholders noted that some of the duties specified in Article 12 may be in conflict with the provisions of the *Zambia Statistics Agency Act, No. 13 of 2018;* the *Zambia Information and Communications Technology Authority Act, No.15 of 2009* and the *National Health Research Act, No. 2 of 2013,* which had elements requiring approval on access to personal data, especially for research purposes. Therefore, they proposed that once the Convention was ratified, the laws needed to be aligned to the provisions in the Convention.

Article 14 – Specific principles for the processing of sensitive personal data

Stakeholders were concerned with the provision for processing of personal information without the consent of the data subject where processing was necessary for the performance of a task being carried out in the public interest or in the exercise of official authority or as assigned by a public authority vested in the controller or in a third party to whom data was disclosed. Stakeholders were of the view that there was need to emphasise that where processing of personal data was being executed following an assignment of a task by a public authority, both the person assigning the task as well as the assignee would, by law, be either compelled or expressly be allowed to process the data. Where this was not the case and consent had not been obtained, such processing would be prohibited. In the view of the stakeholders, it would not be enough to process personal data merely because a task was assigned to someone by a public authority. They proposed that the power to authorise should be provided for in a particular piece of legislation authorising the public authority as well as the person to whom the public authority delegated the processing of the personal data.

Article 14(6)(b) – Transfer of personal data

Stakeholders noted that this provision indicated that transfer of personal data to certain third countries may be done following authorisation by the National Protection Authority. However, they were of the view that it may be necessary to underscore the fact that transfer of personal data to third countries may, or may not, depending on policy, still occur notwithstanding the absence of authorisation from the National Protection Authority where the data subject consented to the transfer unless the

data in question had been declared critical to the security or economic wellbeing of the state. They proposed that the transfer of data could be done either with the consent of the owner of the data or the dictates of the National Protection Authority.

Article 27 – National cyber security monitoring structures

Stakeholders welcomed the provision for the Convention to allow all member states the flexibility to develop a strategy to combat cybercrime at national level. This would ensure that each member state responded to its own unique circumstances. However, they proposed that the AU must develop a general framework to act as a guideline for its members so that their policies could be harmonised.

Article 31 – Adapting certain sanctions to Information and Communication Technologies

Stakeholders noted that Article 31(3) conferred broad authority on courts to access databases and conduct surveillance of networks if necessary in establishing the truth. They were of the view that this provision would be in direct conflict with the country's legislation and was impractical as the stated function was the preserve of the Executive. They argued that the provision would negate the separation of powers and the adversarial nature of the court system. In their view, giving a judge the duty to institute an investigation into ICT offences and collect and preserve evidence, among other duties, would be a complete realignment of the structure of the Government.

11.0 GENERAL SUBMISSION

Available legal provisions

Stakeholders submitted that in Zambia, the mandate to regulate, protect and police the cyberspace fell clearly within the ambit of the Zambia Information and Communications Technology Authority (ZICTA). Currently, ZICTA was being governed by four pieces of legislation, namely the:

(a) *Electronic Communications and Transactions Act, No. 21 of 2009*;

(b) *Information and Communication Technologies Act, No. 9 of 2009*;

(c) *Information and Communication Technologies Amendment Act, No. 3 of 2010*; and

(d) *Postal Services Act, No. 22 of 2009*.

Stakeholders submitted that the *Electronic Communications and Transactions Act*, dealt with issues pertaining to cybercrime and personal data protection. They argued that the legal framework provided for in this Act may not be sufficient to deal with the complexities associated with modern day cybercrime and the purveyance of electronically generated data. However, they also acknowledged that ZICTA had advanced in revising the Act and was proposing to have three laws enacted in its place, namely:

(a) Cyber Security Act;
(b) E-Commerce Act; and
(c) Data Privacy Act.

Stakeholders were of the view that once enacted, the above proposed laws would adequately deal with all issues pertaining to cybercrime, e-commerce and data privacy. The proposed laws were also meant to align to the African Union Convention on Cybercrime and Personal Data Protection.

General challenges

Stakeholders observed that there were a few challenges that may impede the application of the obligations under the Convention for the purpose of promoting regional cyber stability. The peculiar challenges arose from the absence of requisite institutional capacities in terms of cyber security governance and cybercrime law enforcement in the AU member states. For instance, law enforcement authorities in many African countries lacked capacities to detect, investigate and prosecute cybercrime. However, Zambia had designed programmes and initiatives to build capacities in law enforcement authorities, Judiciary and the establishment of the Zambia Cyber Security Agency under the proposed but yet to be introduced Cyber Security and Cyber Crime Bill, 2020. Stakeholders were of the view that the Government needed to upscale the enhancement of the continuous institutional and human resources capacity building programmes in cyber security and combating of cybercrime in order to realise the objectives and outcomes of the African Union Convention on Cyber Security and Personal Data Protection.

12.0 COMMITTEE'S OBSERVATIONS AND RECOMMENDATIONS

Following interactions with stakeholders, the Committee makes observations and recommendations as outlined below.

(a) Article 1 – Definition of Child Pornography

The Committee agrees with the stakeholders who stated that child pornography is still pornography when images of a minor engaging in a sexual act are generated or when a minor's sexual organs are produced or used for primarily sexual purposes hence the need to clearly define child pornography. They are also concerned that the definition also places more emphasis on child pornography and not the circulation of general pornographic content of any nature on digital platforms as a cybercrime. The Committee, therefore, recommends that pornography be clearly defined in order to come up with an all encompassing definition to avoid the loopholes that may arise during prosecution.

(b) *Article 2(1) – Scope of application of electronic commerce*

The Committee agrees with stakeholders who stated that this Article seems to suggest that gambling by electronic means should not be exercised freely. However, in Zambia, authorised betting takes place even on digital platforms using a number of applications related to sports betting which are easily and freely accessible online. Therefore, this provision in the Convention will be in contradiction to what the law provides for in Zambia.

In view of the foregoing, the Committee recommends that the Executive should review the currently fragmented legislative framework that regulates gambling and betting using digital platforms to align it to the Convention.

(c) *Harmonisation of the current pieces of legislation*

The Committee notes that some of the provisions in Article 12 may be in conflict with the provisions of the *Zambia Statistics Agency Act, No. 13 of 2018;* the *Zambia Information and Communications Technology Authority Act, No.15 of 2009;* and the *National Health Research Act, No. 2 of 2013,* that allow for access to personal data especially for research purposes.

In this regard, the Committee recommends that once the Convention is ratified, the pieces of legislation should be amended so as to align them to the provisions in the Convention before they are domesticated.

(d) Unbundling of the *Electronic Communications and Transactions Act, No. 12 of 2009*

While acknowledging that the *Electronic Communications and Transactions Act, No. 12 of 2009*, deals with issues pertaining to cybercrime and personal data protection, the legal framework provided for in this Act may not be sufficient to deal with the complexities associated with modern day cybercrime and the purveyance of electronically generated data.

In this vein, the Committee urges the Executive, as matter of urgency, to expedite the process of drafting the proposed three pieces of legislation, namely: cyber security, e-commerce and data privacy act. This is because once these laws are enacted, they will help to address concerns pertaining to cybercrime, e-commerce and data privacy and will be aligned to the African Union Convention on Cyber Crime and Personal Data Protection.

Given the foregoing, the Committee recommends that the House do approve the African Union Convention on Cyber Crime and Personal Data Protection.

13.0 CONCLUSION

The Committee notes that the African Union Convention on Cyber Security and Personal Data Protection holds several prospects towards promoting regional cyber stability in Africa. Such prospects arise from the fact that the establishment of the Convention increases policy and regulatory awareness on cyber security governance, while also improving the harmonisation of national cyber security model frameworks within the AU member states. The Committee is aware that there may be challenges that will impede the application of the obligations under the Convention, such as the absence of capacity in terms of expert personnel to facilitate the development and implementation of national policy and regulatory frameworks for cyber security governance. Overall, the Convention is progressive.

G M Imbuwa, MP
CHAIRPERSON

November, 2020
LUSAKA

APPENDIX –NATIONAL ASSEMBLY OFFICIALS

National Assembly

Ms C Musonda, Principal Clerk of Committees
Mr H Mulenga, Deputy Principal Clerk of Committees (FC)
Mrs C K Mumba, Senior Committee Clerk (FC)
Ms C R Mulenga, Committee Clerk
Mr C Bulaya, Committee Clerk
Mrs R M Kanyumbu, Typist
Mr M Chikome, Committee Assistant

Appendix II

LIST OF WITNESSES

1. MINISTRY OF JUSTICE
Ms M S Mutale – Parliamentary Counsel

2. MINISTRY OF TRANSPORT AND COMMUNICATIONS
Mr S Mbewe – Acting Permanent Secretary
Mr Y Bwalya – Director Communications
Mrs I Tembo – Acting Director Planning
Mr A Sichinga – Assistant Director Communications
Mr K Nkunika – Assistant Director Communications
Mr M Chisulo – Planner
Ms C Malama – Intern Planner

3. MINISTRY OF INFORMATION AND BROADCASTING SERVICES
Mr A Malupenga – Permanent Secretary
Dr R Mulenga – Director Planning
Mr M Mayembe – Director Press and Media Development

4. MINISTRY OF AGRICULTURE
Mrs P Mlewa – Director, Policy and Planning
Mr E Mushota – Assistant Director, ICT
Mr M Chulu – Acting Principal Policy Analyst

5. MINISTRY OF HIGHER EDUCATION
Ms K Siame – Permanent Secretary
Mr S Mubanga – Director Planning and Information
Mr B Mutale – Senior Planner Cabinet and Parliamentary Affairs

6. MINISTRY OF HEALTH
Ms K Mulalelo – Permanent Secretary, Administration
Dr C Sichone – Director, Health Policy
Mr S Phiri – Principal ICT Officer
Mr E Malikana – Deputy Director, Healthy Policy/Parliamentary Liaison Officer
Mr R Tumeo – Senior ICT Officer

7. MINISTRY OF HOME AFFAIRS (DEPARTMENT OF IMMIGRATION)
Mr M W Banda – Permanent Secretary
Mr A Mukisi – Parliamentary Liaison Officer
Mr D Chimota – Superintendent, Zambia Police

8. MINISTRY OF LANDS AND NATURAL RESOURCES
Mr N Yumba – Permanent Secretary

Ms L Siwale – Acting Director Planning and Information
Mrs N P Chella – Senior Planner/Parliamentary Liaison Officer

9. ZAMBIA REVENUE AUTHORITY (ZRA)

Mr K Chanda – Director General
Mr L Simbeye – Assistant Director, Research

10. ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY(ZICTA)

Dr P Mutimushi – Director General
Mr T Malama – Director legal and Regulatory Affairs

11. SMART ZAMBIA INSTITUTE

Mr M Makuni, Director e-government
Mr S Mbuzi, Senior Cyber Security Officer
Mr C Kayamba, Senior Cyber Security Officer

12. INFRATEL

Mr F Bwalya – Chief Executive Officer
Mr Z Mbumwae – Chief Information Officer

13. ZAMBIA STATISTICAL AGENCY (ZSA)

Mr M J J Musepa – Interim Statistician General
Mr D Kafuli – Deputy Director, Social Statistics

14. BANKERS ASSOCIATION OF ZAMBIA (BAZ)

Mr L Mwanza – Chief Executive Officer
Mr C Lalusha – Head of Information Technology
Mr J Njovu – Head of Fraud Prevention and Security
Ms M Zimba – Public Relations and Administrative Officer

15. ROAD TRANSPORT AND SAFETY AGENCY (RTSA)

Mr G Banda – Director and Chief Executive Officer
Mr C Kanchele – Head, Planning, Research and Development
Mr A Tembo – Legal Counsel
Mr B Sikute – Head, Information and Communication Technology

16. INFORMATION AND COMMUNICATIONS TECHNOLOGY ASSOCIATION OF ZAMBIA (ICTAZ)

Mr K Mutembo – President
Mr C Sinyangwe – Chairperson Membership
Mr K Sokoni – Member

17. BONGO HIVE

Ms L Kapiyha – Hub Manager, Social Enterprise Academy Programme
Mr S Maboshe – Consultant Lead and Co-founder

18. ICT UNIVERSITY COLLEGE

Mrs B S Bweupe – Executive Director
Mr J Silungwe, Head, ICT

19. UNIVERSITY OF ZAMBIA (UNZA)

Mr D Leza – Acting Director, Centre for Information and Communication
Mrs C S Mwembeshi – Manager, Quality Assurance and Security

20. COPPERBELT UNIVERSITY (CBU)

Mr S Zulu – Business development officer
Mr P Hampande – Director CBU, ICT Business and Innovation Centre
Mr N Mazyopa – Head, Systems Development
Dr J Kaleshi – Dean, School of ICT
Dr N Chaamwe – Directorate of ICT

21. ZAMBIA CENTRE FOR ACCOUNTANCY (ZCAS)

Dr E S B Jere – Dean, School of ICT

22. AIRTEL

Mrs S N Akatama – Legal and Regulatory Director

23. LIQUID TELECOM

Mr M Mazaba – Chief Finance Officer (Acting Chief Executive Officer)
Ms P Nyati – Head of Legal and Regulatory Affairs
Mr M Ketani – Chief Network Officer

24. BLOGGERS OF ZAMBIA

Mr M Mulonga – Chief Executive Officer
Ms B T Nkowani – Programme Officer

25. LAW ASSOCIATION OF ZAMBIA

Mr I Nonde – Member of LAZ
Mr L Zulu – Vice President
Ms H Ndao – Member of LAZ