REPUBLIC OF ZAMBIA

REPORT

OF THE

COMMITTEE ON MEDIA, INFORMATION AND COMMUNICATION TECHNOLOGIES

ON THE

ELECTRONIC COMMUNICATIONS AND TRANSACTIONS BILL, N.A.B. NO. 29 OF 2020

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

ELECTRONIC COMMUNICATIONS AND TRANSACTIONS BILL, N.A.B. NO. 29 OF 2020

FOR THE

FIFTH SESSION OF THE TWELFTH NATIONAL ASSEMBLY

Table of Contents

REPORT OF THE COMMITTEE ON MEDIA, INFORMATION AND COMMUNICATION TECHNOLOGIES ON THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS BILL, N.A.B. 29 OF 2020, 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); Mrs P Kucheka, MP (Vice Chairperson); 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 D Mumba, MP; Mr C D Miyanda, MP and Mr G K Chisanga, MP.

The Honourable Mr Speaker
National Assembly
Parliament Buildings
LUSAKA

Sir,

The Committee has the honour to present its Report on the Electronic Communications and Transactions Bill, N.A.B. 29 of 2020 for the Fifth Session of the Twelfth National Assembly referred to it by the House on Wednesday, 27th January, 2021.

2.0 FUNCTIONS OF THE COMMITTEE

The functions of the Committee are as set out under Standing Order 157(2) and, among other functions, the Committee is mandated to consider Bills that may be referred to it by the House.

3.0 MEETINGS OF THE COMMITTEE

The Committee held nine meetings to consider the Electronic Communications and Transactions Bill, N.A.B. 29 of 2020.

4.0 PROCEDURE ADOPTED BY THE COMMITTEE

In order to acquaint itself with the ramifications of the Bill, the Committee sought both written and oral submissions from stakeholders listed at Appendix II.

5.0 BACKGROUND TO THE BILL

The African Union Convention on Cyber Security and Protection of Personal Data was adopted by the Assembly of Heads of State and Government of the African Union in June, 2014. On 29th January, 2016, the President of the Republic of Zambia signed the African Union (AU) Convention on Cyber Security and Protection of Personal Data during the 26th Ordinary Session of the Assembly of Heads of State

and Government of the AU. The AU Convention addressed four main areas, namely:

i) electronic transactions;
ii) personal data protection;
iii) electronic Commerce; and
iv) cyber security and cybercrime

The Convention provided a guideline for Member States to formulate appropriate legal frameworks that would empower their citizens and ensure their respective online environment was trusted, safe, beneficial and empowering to all individuals.

In 2017, the Government, through the Ministry of Transport and Communications commenced the process of reviewing the *Electronic Communications and Transactions Act, No 21 of 2009,* in line with the AU Convention on Cyber Security and Data Protection and in harmonisation with the proposed SADC model laws.

In 2018, Government approved the repeal of the *Electronic Communications and Transactions Act*, *No 21 of 2009,* and the replacement of the Act with three standalone laws that would be in line with regional and international best practice and would be responsive to the needs of the Zambian people. Therefore, the *Electronic Communications and Transactions Act, No 21 of 2009,* was to be repealed and replaced with the following laws:

(a) Electronic Communications and Transactions Bill;
(b) Data Protection Bill; and
(c) Cyber Security and Cybercrimes Bill.

In the fourth quarter of 2019, Cabinet approved the Ratification of the Convention on Cyber Security and Data Protection (Malabo Convention) and approved for presentation before Parliament the two bills, namely: Data Protection and Electronic Communications and Transactions. Further, Parliament in November 2020 also approved the ratification of the Convention by Zambia.

In view of this, the Government had introduced the Electronic Communications and Transactions Bill, N.A.B. 29 of 2020.

6.0 OBJECTIVES OF THE BILL

The objectives of the Bill were to:

(a) provide a safe and effective environment for electronic transactions;

(b) promote secure electronic signatures;

(c) facilitate electronic filling of documents by public authorities;

(d) provide for the use, security, facilitation and regulation of electronic communications and transactions;

(e) promote legal certainty and confidence, and encourage investment and innovation in relation to electronic transactions;

(f) regulate the National Public Key Infrastructure;

(g) repeal and replace the *Electronic Communications and Transactions Act, No 21 of 2009*; and

(h) provide for matters connected with, or incidental, to the foregoing.

SALIENT PROVISIONS OF THE BILL

Part I

Clause 1 – Title

This clause provided for the title of the Bill and the commencement of the Bill.

Clause 2 – Interpretation

This clause provided for interpretation of certain selected words and phrases used in the Bill to facilitate understanding of the law.

Clause 3 – Application

This clause provided for an extent to which the law shall apply.

Part II

Clause 4 – Legal requirements for data message

This clause sought to set out conditions that must exist for information to have a legal force and effect.

Clause 5 – Writing

This clause provided for the features that a document or information must have for that document or information to be considered as having met the requirements, in law, to be in writing.

Clause 6 – Use of advanced electronic signature

The clause sought to provide for the use of advanced electronic signature where the signature of a person was required by law and that law did not specify the type of signature.

Clause 7 – Use of electronic signature

The clause sought to provide for the use of electronic signature where an electronic signature was required by the parties to an electronic transaction and the parties had not agreed on the type of electronic signature to be used.

Clause 8 – Determination of originality of data message

The clause sought to set out the manner of determining the originality of a data message.

Clause 9 – Admissibility and evidential weight of data messages

This clause provided for the admissibility of data messages in evidence. It further provided for the factors that must be considered when assessing the evidential weight of a data message.

Clause 10 – Retention of documents or information

The clause sought to provide for instances when information shall be regarded as having been retained where there was a law that required that information be retained.

Clause 11 – Production of document or information

The clause provided for instances when production of a document or information shall be regarded as having been produced where the law required a person to produce a document or information.

Clause 12 – Notarisation acknowledgement and certification

The clause sought to provide for notarisation, certification and acknowledgement of documents using an advanced electronic signature.

Clause 13 – Other legal requirement

This clause sought to provide for other requirements such as a requirement for multiple copies, to have been satisfied by the submission of a single data message that was capable of being reproduced by the addressee.

Clause 14 – Automated transactions

This clause sought to provide for requirements that must be satisfied for an automated transaction to exist.

Clause 15 – Dispatch of electronic record

The clause sought to provide for when dispatch of electronic record would be considered to have occurred between the originator and the addressee unless otherwise agreed by the parties.

Clause 16 – Receipt of electronic record

The clause sought to provide for factors that must exist for an electronic record to be considered as having been received.

Clause 17 – Expression of intent or other statement

The clause sought to provide for the admission of an expression of intent or other electronic representation between an originator and the addressee, where that intent or representation was relevant at law.

Clause 18 – Attribution of electronic records to originator

The clause sought to provide for factors that must exist for an electronic record to be considered to be that of the originator.

Clause 19 – Acknowledgement of receipt of electronic record

The clause sought to provide for methods of giving an acknowledgement of receipt of an electronic record. It also provided for dispensation of the requirement for acknowledgment were parties so agreed.

Part III

Clause 20- Application of Part

The clause sought to provide for the limit of application of the Part.

Clause 21 – Formation and validity of agreements

The clause sought to give validity to agreements that were concluded wholly or partly by means of a data message.

Clause 22 – Expression of intent or other statement

This clause sought to provide for the validity of expression of intent or other statement expressed in a form of a data message or not evidenced by an electronic signature, but by other means.

Clause 23 – Acceptance of electronic filling and issuing of documents

The clause provided for the acceptance of electronic filing by public bodies that, by law, accepted filing of documents.

Clause 24 – Requirements for electronic filing and issuing of documents

This clause mandated public bodies that accepted filing of documents to specify in a Gazette or news paper of daily circulation the manner and format in which a data message shall be filed, the type of electronic signature required and any other requirements for data messages or payments.

Part IV

Clause 25 – National Root Certification Authority

This clause sought to designate the Zambia Information and Technology Authority as the National Root Certification Authority.

Clause 26 – Functions of National Root Certification Authority

This clause set out the functions of the National Root Certification Authority which included regulating the national public key infrastructure.

Clause 27 – Prohibition of providing certification service without license

This clause sought to prohibit any person from offering certification services without a valid license from the Authority.

Clause 28 – License

The clause sought to provide for the procedure of applying for a license for certification services and time-stamping services.

Clause 29 – Certification authority

The clause sought to set out institutions that may apply for a license as a certification authority under the national public key infrastructure.

Clause 30 – Variation of license

The clause mandated a license holder to seek the Authority's approval for any variation of the terms and conditions of a license.

Clause 31 – Surrender of license

The clause mandated a licensee who decided to discontinue providing the services relating to the license, to surrender the license on such terms and conditions as the Authority would determine.

Clause 32 – Transfer, cede or assignment of license

This clause sought to prohibit the transfer, cede, pledging of the license without the approval of the Authority.

Clause 33 – Suspension or cancellation of license

The clause provided for grounds on which the Authority may suspend or cancel a license.

Clause 34 – Registration of cryptography service providers

This clause sought to provide for the registration of cryptography service providers by the Authority. It further prohibited any person from providing cryptography services without registration.

Clause 35 – Recognition or foreign certification authority

This clause sought to empower the National Root Certification Authority, by notice in the Gazette, to recognise a license, accreditation or recognition granted to a foreign certification authority by a foreign country.

Clause 36 – Issue of certificate to subscriber

The clause provided for requirements that an applicant for a certificate must meet before being issued with a certificate.

Clause 37 – Details of certificate

The clause sought to set out what a certificate must contain and it included, the number of the certificate, the name of the certificate holder, the period of validity of the certificate, among other things.

Part V

Clause 38 – Trustworthy system

The clause mandated a certification authority to utilise a trustworthy system in performing its functions.

Clause 39 – Disclosure and compliance with certification practice statement

The clause mandated a certification authority to disclose facts that materially and adversely affected either the reliability or a certificate that the authority had issued or the authority's ability to carry out its obligations.

Clause 40 – Audit services

The clause mandated a certification authority to conduct and submit to the Authority an information system audit annually and an audit report.

Clause 41 – Publication of certificate revocation list

The clause required a certification authority to maintain a certificate revocation list.

Clause 42 – Prohibition of publication of certificate

The clause prohibited any person from publishing a certificate or otherwise making it available to another person other than the person listed in the certificate.

Clause 43 – Representations on issuance of certificate

The clause set out the representations that came with the issuance of a certificate and one of which was that the certification authority had issued the certificate in accordance with the applicable certification practice statement.

Clause 44 – Recommended reliance limits

This clause required a certification authority when issuing a certificate, to specify a recommended reliance limit in the certificate.

Clause 45 – Liability limits for certification authorities

This clause sought to limit the liability of a certification authority unless there was an agreement to the contrary between a certification authority and a subscriber.

Clause 46 – Suspension of certification authority certificate

This clause empowered a certification authority, by court order or on request by a subscriber, to suspend a certificate.

Clause 47 – Notice of suspension

The clause mandated a certification authority after the suspension of a certificate, to publish a signed notice of the suspension in the repository.

Clause 48 – Revocation of certificate

The clause provided for the grounds on which a certification authority may revoke a certificate.

Clause 49 – Revocation without subscriber's consent

This clause empowered a certification authority to suspend a certificate without the consent of a subscriber listed in the certificate.

Clause 50 – Notice of revocation

The clause mandated a certification authority to publish a revocation notice in the repository.

Clause 51 – Appointment of registration authority

This clause empowered the certification authority to appoint registration authorities as may be prescribed.

Clause 52 – Appeals under this Part

The clause sought to provide for the right to appeal to the Authority by any person who was aggrieved by the decision of a certification authority.

Part VI

Clause 53 – Generating key pair

This clause provided for a subscriber to generate a key pair whose public key was to be listed in a certificate and accepted by the subscriber using a trustworthy system. Further, this clause did not apply to a subscriber who generated the key pair using a system approved by a certification authority.

Clause 54 – Obtaining certificate

This clause provided for requirements of obtaining a certificate.

Clause 55 – Acceptance of certificate

This clause sought to provide for instances where a subscriber was deemed to have accepted a certificate, which included a subscriber publishing or authorising the publication of the certificate to one or more persons or in a repository.

Clause 56 – Control of private key

This clause provided for a subscriber to exercise reasonable care in retaining control of the private key corresponding to the public key listed in that certificate and prevent its disclosure to a person not authorised to create that subscriber's digital signature.

Clause 57 – Suspension or revocation of a compromised certificate

This clause sought to provide for suspension or revocation where the private key corresponding to the public key listed in the certificate had been compromised.

Part VI

Clause 58 – Time stamping services

This clause sought to provide for time stamping service and the time stamping service provider shall ensure that the time stamp was linked to data in a manner that precluded the possibility of changing the data undetectably after obtaining the time-stamp.

Clause 59 – Time stamping service providers

This clause sought to provide for time stamping service providers as a public company, private limited company or state body.

Clause 60 – Requirements for time stamping service providers

This clause sought to provide for requirements for a time stamping service providers in accordance with the provision of the Act.

Clause 61 – Duties of time stamping service providers
This clause sought to provide for duties of time stamp service providers.

Part VIII

Clause 62 – Scope of application

This clause sought to provide that the part on consumer protection in relation to Electronic transactions was without prejudice to any other written law.

Clause 63 – Information to be provided by supplier

This clause sought to provide for information to be provided by a supplier of goods or services for sale, hire or exchange by way of an electronic transaction would be made available to a consumer on the website or other electronic media platform where the goods or services were offered.

Clause 64 – Online market

This clause sought to provide for requirements for online marketing of a product or service to a consumer.

Clause 65 – Unsolicited goods, services or communication

This clause sought to provide for unsolicited communication to a consumer and a person shall only send a commercial communication to an address where the option requirement was met.

Clause 66 – Cooling off period

This clause sought to provide for the period within which a consumer may cancel an electronic transaction for goods and services and the provision provided for exceptions on cancelation of an electronic transaction for certain goods and services.

Clause 67 – Performance

This clause sought to provide for the period within which the supplier must execute an order from the consumer and where a supplier failed to execute an order within the agreed period, the consumer may cancel the agreement on giving seven days' written notice.

Clause 68 – Application of foreign law

This clause sought to provide for the application of provisions relating to protection of consumers under Part VIII irrespective of the legal system applicable to the agreement in question.

Clause 69 – Non exclusion

This clause sought to make void, to the extent of the exclusion, a provision in an agreement which excluded a right provided for under Part VIII.

Clause 70 – Complaints to Authority

This clause sought to provide for the procedure of lodging a complaint with the Authority in respect of any noncompliance with the provisions of Part VIII by a supplier and the Authority may investigate and determine any complaint in accordance with the Act and any other applicable written law.

Clause 71 - Directives, code of conduct and guidelines

This clause sought to provide for directives, code of conduct and guideline that the Authority may issue on consumer related matters.

Part IX

Clause 72 – Domain name

This clause sought to provide for the administration and management of the .zm name space and the regulation of licensing of registrars by the Authority.

Clause 73 – Licensing of registers and registries

This clause provided for the licensing of registers and registries that intended to update a registry or administer a licensing of second level domain as a registrar or registry.

Clause 74 – Regulations regarding registrars, etc

This clause provided that the Minister may, in consultation with the Authority, by statutory instrument, make regulations to provide for registrars and any other matter related to .zm domain name space.

Part X

Clause 75 – Definition

This clause sought to provide for the definition of service provider.

Clause 76 – No liability for mere conduit

This clause sought to provide for circumstances under which a service provider shall not be liable for providing access to, or for operating facilities for, information systems or transmitting, routing or storage of data messages through an information system under the service provider's control.

Clause 77 – Caching

This clause provided for circumstances under which a service provider that transmitted data provided by a recipient of the service through an information system under the service provider's control shall not be liable for the automatic, intermediate and temporary storage of that data, where the purpose of storing that data was to make the onward transmission of the data more efficient to other recipients of the service upon their request.

Clause 78 – Hyperlink provider

This clause sought to provide for an internet service provider who enabled the access to information provided by a third person by providing an electronic hyperlink shall not be liable for the information where the internet service provider expeditiously removed or disables access to the information after receiving an order from any court to remove the link.

Clause 79 – Hosting

This clause sought to provide for the circumstance under which a service provider that provided a hosting service, was not liable for damages arising from data stored at the request of the recipient of the service.

Clause 80 – Order by Court to terminate illegal activity

This clause provided for an order by the court for a service provider to terminate or prevent any unlawful activities under this Act or any other written law.

Clause 81 – Use of information location tools by service provider

This clause sought to provide circumstances under which a service provider was not liable for any damage incurred by a person if the service provider referred or linked users to a web page containing an infringing data message or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hyperlink.

Clause 82 – Take down notification

This clause sought to provide for a recipient of service may through a takedown notification, in writing, notify the service provider of any data or activity infringing the rights of the recipient or of a third party.

Clause 83 – No general obligation on service provider to monitor unlawful activities

This clause provided that a service provider had no obligation to monitor the data which the service provider transmitted or stored or actively sought facts or circumstances indicating an unlawful activity**.**

Clause 84 – Savings

This clause provided that nothing in the Act affected the obligation of a service provider under any written law or by a court, to remove, block or deny access to any data message or any right to limitation of liability based on the Constitution**.**

Part XI

Clause 85 - Use of encrypted communication

This clause provided that a person providing an encryption service shall use an encryption, regardless of encryption algorithm selected, encryption key length chosen, or implementation technique or medium used, in the manner provided for under this Act.

Clause 86 – No limitation on encryption function

This clause provided nothing in the Act put a limit or affected the ability of the person to use encryption function**.**

Clause 87 – Prohibition of unauthorised decryption or release of decryption key

This clause provided for prohibition of unauthorised decryption or release of a decryption key.

Clause 88 – Prohibition of disclosure of record or other information by key holder

This clause prohibited a key holder from disclosing a record or any other personal information relating to an owner of a key held or managed by the key holder without the consent of the owner or court order.

Clause 89 – Obstruction of law enforcement officer

This clause provided for an offence for obstructing a law enforcement officer from performing function as provided under the Act.

Clause 90 – Prohibition of disclosure or use of stored recovery information

This clause provided for a recovery agent in implementing technical and organisational measures to comply with the *Data Protection Act, No. 28 2020*, and prohibited disclosure or use of stored recovery information.

Clause 91 – Immunity of recovery agents

This clause sought to provide for immunity of recovery agents.

Part XII

Clause 92 – Appeal

This clause sought to provide for an appeal procedure for a person aggrieved with the decision of the Authority**.**

Clause 93 – Register

This clause provided for the Register of the Authority.

Clause 94 – Offences by body corporate or unincorporated body

This clause sought to provide for the offences by body corporate or unincorporated body**.**

Clause 95 – General penalty

This clause sought to provide for a general penalty for the offence with no penalty under the Act.

Clause 96 – Circumstances under which evidence obtained by unlawful interception admissible in criminal proceedings

This clause sought to provide for circumstances under which evidence obtained by unlawful interception would be admissible in criminal proceedings.

Clause 97 – Guidelines

This clause sought to provide for guidelines issued by the Authority.

Clause 98 – Supervision of compliance with the Act

This clause provided for supervision of compliance of the Act by the Authority.

Clause 99 – Regulations

This clause sought to empower the Minister to issue regulations for the better carrying out of the provisions in this Act.

Clause 100 – Extraterritorial application of offences

This clause provided for extraterritorial application of offences committed outside the Republic.

Clause 101 – Act to bind Republic

This clause provided for the Act to bind the Republic.

Clause 102 – Repeal of Act

This clause sought to repeal the *Electronic Communications and Transactions Act No. 21 of 2009***.**

CONCERNS RAISED BY STAKEHOLDERS

Most stakeholders supported the Electronic Communications and Transactions Bill, N.A.B. No. 29 of 2020, and in supporting the Bill, stakeholders made the following

observations and recommendation which they proposed needed to be addressed before the Bill could be enacted in order to improve the law.

Long title

Stakeholders submitted that the Long Title of the Bill was a summary of the objectives of the Bill which mirrored the memorandum of the Bill. However, the objectives of the Bill contained in its Long Title were different from the objectives contained in the Bill. The proposed Long Title appeared to be providing for the establishment of the Information and Communications Association of Zambia (ICTAZ) and regulation of the attendant professionals. They were of the view that the Long Title be amended to reflect the correct objectives of the Bill.

Clause 2 – Interpretation

Stakeholders also proposed that in the definition of "**ccTLD**" the words "**two**" and "**letter**" should be separated in order to cure the typographical error. It was also proposed that the ISO title be amended from "**31661**" to "**3166**" to correct the standard.

Stakeholders were of the view that the definition of "certification service" should be amended to read as follows: Certification Service means a service of –

(a) issuing certificates necessary for giving digital signatures or digital seals to users;

(b) enabling the verification of digital signatures or digital seals given on the basis of certificates;

(c) implementing procedures for suspension, termination of suspension and revocation of certificates;

(d) checking the revocation status of the certificate and advising the Relying Party; or

(e) issuing cross-pair certificates;

This proposal was meant to provide clarity as certification services included the items in (a) to (e).

New definition

It was proposed that the term "Cross-pair certificates" be included in the definitions and read: "Cross-pair certificates" means certificates that are framed as certificate pairs and are issued by different Certification Authorities. This was meant to define a word that had been used in the Bill but not defined.

It was proposed that "Registration Authority" be included in the definitions and read: "Registration Authority" meant person or entity that was entrusted by the certification authority to register or vouch for the identity of users of a certification authority, but did not sign certificates. This was because the words were used in the Bill but never defined.

Stakeholders proposed that the definition of "collection on delivery" be deleted as the subject covered was catered for in the proposed postal services Bill.

Stakeholders proposed that in the definition of "Computer Network" the word "and" should be replaced with the word "or" after the word media at the end of (a) because it was more appropriate

Under the definition of "Cryptography Product", stakeholders proposed that the word "or" after item (c) in the definition should be replaced by the word "and" because all the elements from (a) to (d) need to be satisfied.

Stakeholders were of the view that in the definition of "Cryptography Service", the use of the word "seller" appeared misplaced. They proposed that the correct word to be used was "sender".

Stakeholders suggested that in the definition of "Electronic Communication", the words "tone" and "only" in (b) of the definition should be separated as that was a typographical error. It was also noted that wherever "photooptical" and "photoelectronic" appear in the Bill, should be separated by a dash as follows "photo-optical" and "photo-electronic".

The definition of "Electronic signature" was proposed by stakeholders to read:
"Electronic signature" means electronic:

(a) sound;
(b) symbol;
(c) process; or
(d) other data created or adopted by a person with the intent to sign a data message.

They argued that the elements in (a) to (d) needed to be in electronic form in order to qualify to be an electronic signature. Further, the use of the words "electronic documents" was found to be limited compared to the use of the words "data massage" which was broader and captured electronic documents. Moreover, data message had been defined while electronic documents had not.

Stakeholders observed that there appeared to be a typographical error in the definition of "electronic transaction". Therefore, the words "non" and "commercial" should be separated.

Stakeholders proposed that the word "infrastructure" should be added to the definition so that it reads as "National Public Key Infrastructure". This was because the word infrastructure was missing in the term being defined.

Under the definition of "recovery information" it was proposed that the word "object" be replaced with the word "hardware" as the use of the word "object" appeared misplaced.

In the definition of "registrant" stakeholders proposed a replacement of the word "of" with the word "for" because the use of the word "of" appeared misplaced.

Stakeholders were of the view that in the interpretation of "secure signature creation device", the word "personal" should be replaced with the word "private" in the last line as the word "personal" appeared misplaced and the correct word to be used being "private".

Clause 4 – Legal Requirements for Data Message

Stakeholders noted that in clause 4(1), that the definition of data included information. They therefore, proposed that the words "information" be replaced with the word "data". The amendment was meant to clarify that the provision related to electronic information and was not intended to render non electronic documents to have no legal effect. They further contended that the word "and" should be replaced with the word "or" between (a) and (b) as the use of the word "and" appeared misplaced. Information has legal force whether (a) or (b) are satisfied.

Clause 9 – Admissibility and evidential weight of data messages

Stakeholder noted that clause 9(3), outlined what should be taken into consideration when any legal proceeding was assessing the evidential weight of a data message. In that regard, they proposed that there was need to clarify the reliability of the data message and how its integrity would be determined and by who.

They further observed that clause 9(4) provided that a data message made by a person in the ordinary course of business, or a copy or printout of, or an extract from, the data message certified to be correct by an officer in the service of that person, shall on its mere production in any civil, criminal, administrative or disciplinary proceedings under a written law, be admissible in evidence against a person and rebuttable proof of the facts contained in a record, copy, printout or extract. Stakeholders proposed that there was need to clarify on how a data message would be certified and who the officer in the service of that person would be.

Clause 11 – Production of document or information and Clause 12 – Notarisation acknowledgement and certification

Stakeholders noted that the clauses appeared to imply that where a law required a person to produce a document or information, that requirement would be met if the

person produced, by means of a data message, an electronic form of that document or information. They were of the view that the Bill should state clearly how verification would be conducted in cases where results or an identity card was required. These could be understood to mean that once, for example, a scanned copy of a certified copy was presented, it could meet the requirements. Therefore, this had to be prevented and proper verification put in place in order to guard against fraud and to detect if any forgeries occurred.

Clause 14 – Automated transactions

Stakeholders noted that the clause used the term "agreement" which had not been defined to state what it meant in the context of the clause. They proposed that the word "agreement" should be clearly defined in that context. With regard to (d) which provided that where the party was not bound by terms of the "agreement" when interacting with an electronic agent, there was need for the Bill to clearly state the issues such as subscriptions or where an electronic agent was used for application of products and services whereby the customer was bound by the owner or provider of the electronic agent's terms and conditions

Clause 18 – Attrition of electronic records to originator

Stakeholders noted that the provision to consider that the dispatch of the electronic record to have "occurred" when it entered an information system outside the control of the originator or his agent placed less than adequate responsibility on the originator in ascertaining that reasonable care was exercised in ascertaining that the record was received by the addressee. They proposed that the phrase "an information system outside the control of the originator or the agent of the originator" be replaced by the words "a designated information system".

Further, stakeholders submitted that clause 18(3), which provided that, "Where a procedure had not been agreed to by both parties to ascertain the originator, the person who appeared to be the originator shall be presumed to be the originator", needed to be amended as follows: "Where a procedure had not been agreed to by both parties to ascertain the originator, the person who appears to be the originator shall be presumed to be the originator if the addressee had made reasonable effort to ascertain the identity of the originator".

Clause 19 – Acknowledgement of Receipt of Electronic Record

Section 19 of the ECT Bill set out the manner in which the recipient of an electronic record may acknowledge receipt. Stakeholders were particularly concerned with clause 19 (2) which provided that an acknowledgment of receipt was not required to give legal effect to a message unless otherwise agreed by the parties. They argued that in Zambia a demand letter for "instance was required to be acknowledged as received for it to be used as evidence in a court of law". They therefore, proposed that for purposes of enforcement in legal proceedings, clause 19(2) above be enhanced to provide as follows:

"an acknowledgment of receipt is not required to give legal effect to a message unless otherwise agreed by the parties. Provided that where a system or server report proves that an electronic record was received by the destination server, such an electronic record will be deemed to have been duly acknowledged as received and may be used as evidence in a court of law."

Clause 25 – National Root Certification Authority

Stakeholders noted that this clause provided for the establishment of the National Root Certification Authority. They were of the view that introduction of another regulatory body would introduce red-tape. The proposed functions could be performed by an already existing body. They also proposed that the National Root Certification Authority could be placed under the Zambia Information and Communications Technology Authority (ZICTA) and hence this provision should be amended to align with this proposition.

Clause 26 – Functions of National Root Certification Authority

Stakeholders observed that clause 26(b) provided for the registration of cryptography service providers. They stated that some organisations had external cryptography service providers and with systems that were located outside the country. They proposed that the Bill should clarify how such organisations would be registered.

With regard to (d), the stakeholders were of the view that there was need to include the formulation of standards and policies to guide the users and also expand on what the audits would be about and the skills needed for these audits. Some stakeholders proposed that ICTAZ be included to ensure that the right skills and competencies were prescribed for such task.

Clause 27 – Prohibition of providing certification service or time-stamping service without licence

Stakeholders observed that clause 27(1), stated that a person shall not provide a certification service or a time-stamping service to an institution with critical information infrastructure. However, the Bill did not define what critical infrastructure was hence the need to define what critical infrastructure was in the Bill to ensure clarity. They further proposed that clause 27(1), should be amended to read as: "A person shall not, without a license issued under this Act, provide a certification service or a time stamping service to an institution with critical information infrastructure". The inclusion of the words "without a license issued under this Act" were meant to make it clear that it was the unlicensed person that was prohibited.

Clause 28 – Licence

Some stakeholders noted that the clause provided the requirements that an applicant needed to meet such as provided in clause 28(a), including financial and technical capability of the applicants, among others. They were of the view that a resource plan and financial assessment could be done to prescribe even a minimum. The financial assessment could ensure that individuals of Zambian origin with low capital were not disadvantaged.

Clause 29 – Certification Authority

Stakeholders observed that the clause 29 provided for listed classes of entities that may apply to be licensed as certification authority under the national public key infrastructure. They argued that for a company to qualify to be a certification authority, it must adopt, implement, and be certified against ISO/IEC 27001 - Information Security Management System. They were of the view that the Bill should include the requirement for certification authorities to be suitably qualified under the best internationally recognised standards and certifications.

Clause 31 – Surrender of Licence

Stakeholders proposed that in clause 31(1), the word "license" should be replaced with "licensee" and read as follows: "a licensee shall, where a licensee decides not to continue…."

Clause 36 – Issue of Certificate to Subscriber

Stakeholders proposed the removal of the word "its" appearing at the beginning of clause 36(a), and the deletion of clause 36(b), because the clause captured internal processes of the Certification Authority which may not need to be in the Bill. Further, the words "certificate authority" should be replaced with the words "Certification Authority" wherever they appeared and capitalise the letters "C" and "A" whenever using the words. It was also proposed that the word "prospective" be removed from section 36(c), and wherever it appeared before the word subscriber" for the sake of clarity.

Clause 39 – Disclosure and Compliance with Certification Practice Statement

Stakeholders were of the view that in clause 39(1)(a), the word "by" should be removed before the word "corresponding" and to remove the comma after the word "certification" from clause 39(1)(b). In clause 39(2)(a), the words "reasonably expected to" should be added to read as follows: " use reasonable efforts to notify any person who was known or likely to be affected by that occurrence; and……This was because the use of the word "foreseeing" made the provision unclear.

Stakeholders also proposed that a new clause 39(1)(d), be added and should read as follows: "its Certification Revocation List to a Validation Authority licenced by National Root Certification Authority" and therefore, the current (d) in the Bill should become (e).

Clause 63 – Information to be provide by supplier

Stakeholders observed that the provision under clause 63(5) stated that "A supplier shall utilise a payment system that was sufficiently secure in accordance with accepted technological standards at the time of the transaction and the type of transaction concerned". However, standards for determining the "accepted technological standards" being referred to were unclear. They proposed that standards should be provided.

Clause 65 – Unsolicited good, services or communications

Stakeholders noted that this clause provided that a person may send one unsolicited commercial communication to a consumer. However, it was unclear as what exactly amounted to commercial communication and the time limit for the proscription not stated. They were of the view that the Bill should state clearly what exactly amounted to commercial communication and the time limit for the proscription not stated.

Clause 68 Application for foreign law

Stakeholders noted that the protection provided to consumers in this Part applied irrespective of the legal system applicable to the agreement in question. They were of the view that this provision was against this power by overriding every legal system applicable to an agreement between consenting parties. They proposed that there should be a provision which put the burden on the service provider.

Clause 70 – Complaints Authority

This clause provided that a consumer may lodge a complaint with the Authority in respect of any noncompliance with the provisions of this Part by a supplier. They were of the view that the provision should have a clause for grievance resolution and timelines before lodging of complaint to the Authority. They proposed an inclusion of a grievance procedure with specific timelines for every service provider.

Clause 86 – No limitation on encryption function

Stakeholders noted that the Bill in clause 86 provided that "Nothing in this Act shall be construed as requiring the use by a person of any form of encryption that:

(a) limits or affects the ability of the person to use encryption without a key escrow function; or

(b) limits or affects the ability of the person who uses encryption with a key escrow function not to use a key holder".

Stakeholders argued that this was not satisfactory in that, encryption would depend on infrastructure and sensitivity of information. They were of the view there was

need to at least have standard encryption algorithms such as the advanced encryption standard (**AES), RSA,** the standard that was invented by (Rivest, Shamir, and Adelman), or data encryption software **(DES)**, which in itself introduced limitations**.**

Clause 87 – Prohibition of unauthorised decryption or release of decryption key

Stakeholders noted that the clause provided that a person who contravened clause(1), committed an offence and was liable, on conviction, in the case of:

(a) an advanced electronic signature private key, to imprisonment for a minimum term of ten years and a maximum period not exceeding twenty-five years without the option of a fine; and

(b) any other electronic signature, to imprisonment for a term not exceeding ten years without the option of a fine.

Stakeholders were of the view that this punishment was outrageous and proposed that the Bill should provide for reduced sentence tenure.

COMMITTEES OBSERVATIONS AND RECOMMENDATIONS

Having interacted with stakeholders, the Committee makes observations and recommendations as outlined below.

1. Long title

The Committee agrees with the stakeholders who noted that the long title of the Electronic Communications and Transactions Bill appears to be providing for the establishment of the Information and Communications Association of Zambia (ICTAZ) and regulation of the attendant professionals. In this regard, the Committee recommends that the long title should be amended to reflect the correct objectives of the Bill.

2. Certification Authority

The Committee observes that the Bill, in clause 29, provides classes of entities that will qualify to apply for a certification authority licence under the National Public Key Infrastructure. The Committee is of the view that for a company to qualify to be a certification authority, it should adopt, implement, and be certified against ISO/IEC 27001 - Information Security Management System. In this vein, the Committee recommends that the Bill should include the requirement for certification authorities to be suitably qualified under the best internationally recognised standards and certifications.

3. Encryption limitations

The Committee observes with concern that clause 86 provides that nothing in the Act shall be construed as requiring the use by a person of any form of encryption that limits or affects the ability of a person to use encryption without a key escrow function. In this regard, the Committee recommends that the standard encryption algorithms designed to limit the encryption of information should be introduced because the objective of encryption is not only to secure data but to also give inspectors and security agencies the ability to urgently have access to information contained on a suspect's encrypted device.

4. Manner of Receipt of Electronic Record

The Committee notes that clause 19(2) provides that an acknowledgment of receipt is not required to give legal effect to a message unless otherwise agreed by the parties. However, it is concerned that for legal proceedings, it may be a requirement for the recipient to acknowledge receipt for an electronic record to be admitted as evidence in a court of law.

The Committee, therefore, recommends that the Bill be harmonised with other legal provisions in order to avoid contradictions with other pieces of legislation especially those that require that documents be physically delivered to the addressee.

CONCLUSION

The National Assembly recently ratified the African Union (AU) Convention on Cyber Security and Personal Data Protection. In this regard, it is necessary that the Convention is domesticated for it to have the force of law in Zambia. The Electronic Communications and Transactions Bill, N.A.B. No. 29 of 2020, if enacted, will provide for the use, security, facilitation and regulation of electronic communications and transactions, and promote legal certainty and confidence, and encourage investment and innovation in relation to electronic transactions.. Its enactment will ensure that there is regulation on the collection, use, transmission and storage of personal data. This Bill is, therefore, progressive.

The Committee wishes to express its gratitude to all stakeholders who appeared before it and tendered both oral and written submissions; and to thank you, Mr Speaker, for affording it an opportunity to scrutinise the Bill. The Committee also appreciates the services rendered by the Office of the Clerk of the National Assembly.

We have the Honour to be, Sir, the Committee on Media, Information and Communication Technologies mandated to consider the Electronic Communications and Transactions Bill, N.A.B. No. 29 of 2020, for the Fifth Session of the Twelfth National Assembly.

Mr G M Imbuwa, MP,
(Chairperson)

Ms P C Kucheka, MP
(Vice-Chairperson)

Mr D M Kundoti, MP
(Member)

Mr M Mukumbuta, MP
(Member)

Dr E I Chibanda, MP
(Member)

Mr M K Tembo, MP
(Member)

Dr F Ng'ambi MP
(Member)

Mr D Mumba, MP
(Member)

Mr C D Miyanda, MP
(Member)

Mr G K Chisanga
(Member)

APPENDIX I – National Assembly Officers

Ms C Musonda, Principal Clerk of Committees
Mr F Nabulyato, Deputy Principal Clerk of Committees (SC)
Mr C K Mumba, Senior Committee Clerk
Ms C R Mulenga, Committee Clerk
Mr Cosmas Bulaya, Committee Clerk
Mr S Samuwika, Committee Clerk
Mrs R Kanyumbu, Typist
Mr D Lupiya, Parliamentary Messenger

APPENDIX II – The Witnesses

PERMANENT WITNESSES

MINISTRY OF JUSTICE
Mrs O Sakala, Deputy Chief Parliamentary Counsel
Ms M Siwiwaliondo, Senior Parliamentary Counsel
Mrs N Nchito, Senior Parliamentary Counsel

MINISTRY OF TRANSPORT AND COMMUNICATIONS
Hon. M Kafwaya, MP, Minister of Transport & Communications
Eng. M Lungu, Permanent Secretary –
Mr Y Bwalya, Director -Communications
Mr S Mbewe, Director Planning & Monitoring
Mr A Sichinga, Assistant Director –Technical
Mr N Nkunika, Assistant Director –Policy
Ms S Musonda, Principal Communications Officer –Infrastructure
Ms C Phiri, Principal Communications Officer -M&E
Ms L M Munyama, Senior Planner

MINISTRY OF FINANCE
Mr C Chikuba, Permanent Secretary – Economic Management and Finance
Mr I Akapelwa, Assistant Director – Economic Management Department
Mr E Sakanyi, Principal Planner – Economic Management Department
Mr M Mweemba, Senior Economist - Economic Management Department
Ms I Kafwenba, Senior Economist - Economic Management Department

MINISTRY OF HEALTH
Dr K Malama, Permanent Secretary, Technical Services
Mr E Ngulube, Permanent Secretary - Administration
Dr C Sichone, Director – Health Policy
Mr P Chishimba, Director, Monitoring and Evaluation
Mr A Kashoka, Assistant Director- ICT
Dr A Kabalo, Health Promotion Environment and Social Determinants
Mr E Malikana, Deputy Director Health Policy

ZAMBIA INFORMATION AND COMMUNICATIONS AUTHORITY
Mr P Mutimushi, Director General
Mr T Malama, Director Legal
Mr M Mutale, Director Technology and Engineering
Mr N Samatebele, Manager Cyber Security
Ms M Chisha, Acting Manager Legal
Mr A Mpondela, Legal Officer

INFORMATION COMMUNICATION TECHNOLOGY ASSOCIATION OF ZAMBIA (ICTAZ)

Mr C Lalusha, Vice-President
Mr C Sinyangwe, Member
Ms S Y Mavula, Chief Executive Officer and Registrar

ZAMBIA STATISTICS AGENCY (ZAMSTATS)
Mr M Musepa, Director General
Mr N Bukoka, Chief Statistician
Mr Kafuli, Assistant Director Population and Social Statistics

NATIONAL PENSION SCHEME AUTHORITY (NAPSA)
Mrs L Chilumba, Director
Mr R Kamanya, Director Strategy and Business Performance
Mrs M Kayombo, Legal Manager Regulatory Enforcement
Mr M Mvula, Area Manager ICT Infrastructure
Ms O Chirwa, Legal Officer Regulatory and Enforcement
Mr B Liyanda, Legal Officer Regulatory and Enforcement
Mr M Kangwa, Senior Manager Information Technology Security
Mr D Chibesakunda, Senior Information Technology Security Officer
Mr D Munyame, Manager, ITC Service Delivery
Mr P Sunkutu, Manager Business Applications

ZAMBIA REVENUE AUTHORITY (ZRA)
Mr K Chanda, Commissioner General
Mr E Phiri, Director, Research

INFRATEL
Mr Bwalya, Chief Executive Officer
Mr Z Mbumwae, Chief Information Officer
Mr S Kaonga, Legal Counsel

COPPERBELT UNIVERSITY (CBU)
Mrs F Bwalya, Manager – ICT Operations
Dr J Kalezhi, Dean – School of ICT
Mr P Hampande, Director – CBU – IBIC
Mr G Phiri, Monitoring and Evaluation Officer
Mrs C Mwembeshi, Manager Quality Assurance and Security Center for ICT

ZCAS UNIVERSITY
Dr E S B Jere, Dean – School of ICT

BLOGGERS OF ZAMBIA
Mr R Mulonga, Chief Executive Officer
Ms B Nkowani, Programmes Coordinator
Ms M Dambwa, Programmes Officer

SMART ZAMBIA INSTITUTE (SZI)
Mr M Makuni, Director, eGovernment
Ms N Mwanza, Assistant Director, Standards

Ms G Nkula, Head Quality Assurance and Security
Mr J Chipeta, Principal Policy
Mr S Mbuzi, Senior Security Officer
Ms C Chipango, Senior Policy Officer

UNIVERSITY OF ZAMBIA (UNZA)
Dr O Muyati, Dean School of Natural Science
Dr M Nyirenda, Head of Department Computer Science
Mr D Zulu, Senior Lecture Computer Science,
Mr D Leza, Acting Director Center for ICT
Mrs C Mwembeshi, Manager Quality Assurance and Security Center for ICT

BANK OF ZAMBIA
Dr F Chipimo, Deputy Director – Operations
Mrs R C Mhango, Deputy Governor – Administration
Mr F Hara, Chief of Staff
Ms G Mposha, Director – Bank Supervision Department
Ms F Tamba, Director – Non-Bank Financial Institutions Department
Mrs C Punabantu, Acting Director – Board Services Department
Mr L Kamamga – Director – Banking Currency and Payment Systems
Mrs H Banda, Deputy General Counsel
Ms B Mwanza, Assistant Director – Communications
Dr J Lungu, Assistant – Governor's Office
Mr C Kapembwa, Executive Assistant – Deputy Governor – Operations
Ms P Sinkamba, Executive Assistant – Deputy Governor - Administration

BANKERS ASSOCIATION OF ZAMBIA
Mr H Kasekende, Standard Chartered Bank (CEO) - Bankers Association of Zambia Chairperson
Ms R Kavimba, Standard Chartered Bank, BAZ Legal Committee Vice Chairperson
Mr W Luwabelwa, Stanbic Bank, Chief Compliance Officer/ BAZ Legal Representative
Ms J Mtaja, Zanaco Bank, Regulatory and Advisory Specialist
Ms A Malama, Standard Chartered Bank, Country Technology Manager
Mr C Lalusha, Absa Bank, Chief Information Officer
Mr A Chisha, Zanaco Bank, Head Core Banking & Enterprise Applications
Ms K Kaulungombe, Zanaco Bank, Company Secretary & Acting Chief Legal Officer
Mr L Mwanza, Bankers Association of Zambia, Chief Executive Officer
Ms M Zimba, Bankers Association of Zambia, Public Relations & Administrative Officer

MULTICHOICE
Ms G Zulu, Head Regulatory Affairs, MulticChoice Zambia
Ms Kate Munuka, MultiChoice Southern Africa Compliance Manager
Mr U Nel, Principal CII Governance MultiChoice Africa
Mr L Momba, Head Regulatory Affairs Southern Region

ICT COLLEGE
Mr G Mumba, Acting Executive Director
Mr J Silungwe, Direct5or ICT

AIRTEL ZAMBIA
Mr J Chulu, Legal Counsel