

MALAWI GOVERNMENT

(Published 4th November, 2016)

ACT

No. 33 of 2016

I assent

PRO. ARTHUR PETER MUTHARIKA

PRESIDENT

20th October, 2016

ARRANGEMENT OF SECTIONS

SECTION

PART I—PRELIMINARY PROVISIONS

1. Short title and commencement
2. Interpretation
3. Objective of the Act
4. Principles
5. Implementation of this Act

PART II—ADMINISTRATION

6. Establishment of the Malawi CERT

PART III—FORMATION AND VALIDITY OF ELECTRONIC TRANSACTIONS

7. Recognition of electronic writing
8. Electronic signature
9. Equal treatment of digital signatures
10. Conduct of a person relying on a digital signature
11. Bearing legal consequences of relying on electronic signature
12. Recognition of digital signature certificates and digital signatures
13. Notarization, acknowledgement and certification
14. Other requirements
15. Determination of originality of an electronic message
16. Admissibility and evidential weight of electronic messages
17. Storage of electronic messages
18. Secure electronic record
19. Validity of a contract executed in electronic form

SECTION

20. Time and place of dispatch and receipt of an electronic message
21. Offer and acceptance
22. Attribution of electronic messages to sender
23. Acknowledgement of receipt of an electronic message

PART IV—LIABILITY OF ONLINE INTERMEDIARIES AND CONTENT EDITORS AND PROTECTION OF ONLINE USERS

24. Freedom of communication and its limitations
25. Liability of an intermediary service provider
26. Liability for being a conduit
27. Liability for caching services
28. Liability for the supply of hosting services
29. Saving of data
30. Takedown notification
31. Online content editors
32. Right to reply

PART V—ELECTRONIC COMMERCE

33. Information to be provided by supplier
34. Formation of electronic contracts with consumers
35. Cooling off period
36. Performance of an electronic transaction
37. Default in contract performance
38. Review and cancellation of contract by a consumer
39. Cancellation of payment
40. Prohibition of misleading advertising
41. Identification of advertisement content
42. Unsolicited communication
43. Scope of application of financial provisions
44. Identity of a provider of financial or banking services
45. Right of withdrawal from a contract

PART VI—SECURITY AND DIGITAL ECONOMY

46. Use, supply, transfer, etc.
47. Presumptions regarding digital signature certificates
48. Unreliable digital signatures
49. Reliance on digital signature and certificate
50. Requirements to publish digital signature certificate

SECTION

51. The Authority to appoint a certification authority
52. Encryption
53. Trustworthy system
54. Disclosure
55. Issuing a digital signature certificate
56. Representations upon issuance of a digital signature certificate
57. Suspension of a digital signature certificate
58. Revocation of a digital signature certificate
59. Revocation without a subscriber's consent
60. Notice of suspension of digital signature certificate
61. Notification of revocation of a digital signature certificate
62. Generating a key pair
63. Accurate and complete representations
64. Acceptance of a digital signature certificate
65. Control of a private key
66. Requesting for suspension or revocation
67. Provision of encryption services
68. Administrative sanctions
69. Appointment of cyber inspectors
70. Powers and functions of a cyber inspector

PART VII—DATA PROTECTION AND PRIVACY

71. Processing of personal data
72. Rights of a data subject
73. Accuracy and completeness of information
74. Security obligations

PART VIII—DOMAIN NAME AND MANAGEMENT

75. Appointment of the Registrar of domain names
76. Functions of the Registrar
77. Recommendations relating to domain names
78. Offence of administering domain name without authority
79. Dispute resolution concerning domain names

PART IX—ELECTRONIC-GOVERNMENT TRANSACTIONS

80. Requirement of electronic filing and issuing of documents
81. Specific guidelines to public bodies
82. Implementation of e-government

SECTION

PART X—OFFENCES

83. Search warrant
84. Unauthorized access, interception or interference with data
85. Child pornography
86. Prohibition of cyber harassment
87. Prohibition of offensive communication
88. Prohibition of cyber stalking
89. Prohibition of hacking, cracking and introduction of viruses
90. Unlawfully disabling a computer system
91. Prohibition of spamming
92. Prohibition of illegal trade and commerce
93. Attempting, aiding and abetting crimes
94. Offences committed by legal persons
95. General offence and penalty

PART XI—GENERAL PROVISIONS

96. Lodging of complaints to the Authority
97. Public education programmes
98. Intermediary services providers' levy
99. Codes of conduct
100. Act to prevail in case of inconsistency
101. Administrative penalties
102. Regulations
103. Exemption orders
104. Transitional provision

An Act to make provision for electronic transactions; for the establishment and functions of the Malawi Computer Emergency Response Team (MCERT); to make provision for criminalizing offences related to computer systems and information communication technologies; and provide for investigation, collection and use of electronic evidence; and for matters connected therewith and incidental thereto.

ENACTED by the Parliament of Malawi as follows—

PART I—PRELIMINARY PROVISIONS

1. This Act may be cited as the Electronic Transactions and Cyber Security Act, 2016, and shall come into operation on such date as the Minister may appoint, by notice published in the *Gazette*. Short title and commencement

2. In this Act, unless the context otherwise requires— Interpretation

“Authority” means the Malawi Communications Regulatory Authority established under section 3 of the Communications Act; Cap 68:01

“CCTLD” means the Country Code Top Level Domain which is at the top level of the internet domain name, system assigned according to the two letter codes in the international standards ISO3166–1 by ICANN;

“certification authority” means a trusted third party organization or company licensed or authorized by the Authority to issue digital certificates used to create digital signatures and public-private key pairs;

“child pornography” means visual and pornographic material that depicts, presents or represents a person under the age of eighteen engaged in sexually explicit conduct or an image representing a person under the age of eighteen engaged in sexually explicit conduct;

“comparative advertising” means any advertising which explicitly or impliedly identifies a competitor, or goods or services offered by a competitor;

“computer system” means a device or a group of interconnected or related devices, one or more of which performs automatic processing of data pursuant to a program;

“consumer” means any person who enters or intends to enter into a contract by electronic means with a supplier as the end-user of the goods or services offered by the supplier and acts, for that purpose, outside his trade, business or profession;

“content provider” means a person or organization who supplies information for use on a website or an electronic media platform;

“critical data” means data which is declared by the Minister in accordance with this Act, to be of importance to the protection of national security of the Republic or the economic and socio well being of its citizens;

“cryptography” means the method of storing and transmitting data by transferring it into unreadable format so that only those for whom it is intended can process and read it;

“cyber inspector” means a person appointed as such under section 69;

“data” means electronic presentation of information in any form;

“data controller” means a person who, acting either alone or in common with other persons, determines the purpose for which, and the manner in which, any personal data is processed, or is to be processed and thus, controls and is responsible for the keeping and using of personal data, and the term includes a person who collects, processes or stores personal data;

“data subject” means a person from whom data relating to that person is collected, processed or stored by a data controller;

“digital certificate” means an electronic document to prove ownership of a public key, and certificate includes information about the key owners’ identity and the digital signature if an entity that has verified the certificates contents are correct;

“digital signature” means an electronic signature consisting of a transformation of an electronic message using an asymmetric crypto system and a hash function such that a person having the initial and transformed electronic message and the signatory’s public key can accurately determine—

(a) whether the transformation was created using the private key that corresponds with the signatory's public key; and

(b) whether the initial electronic message is as it was after the transformation was made;

“digital signature certificate” means a record which is issued by the Authority for the purpose of supporting a digital signature;

“distance contract” means any contract concluded between a supplier and a consumer under an organized remote sales or service-provision scheme run by the supplier, who, for the purpose of that contract, makes exclusive use of one or more electronic means up to and including the time at which the contract is concluded;

“domain name” means an alphanumeric designation that is registered or assigned in respect of an electronic address or other resources on the internet;

“e-government service” means a public service provided by electronic means;

“electronic commerce” means any economic activity provided by electronic means, including remote services and products, particularly services that consist of providing online information,

commercial communications, research tools, or access to, or downloading of, online data, access to a communication network or the hosting of information;

“electronic message” means any communication created, sent, received or stored by electronic communication means, such as computerized data exchange system, electronic mail system and instant messaging;

“electronic record” means a record created, generated, sent, communicated, received and maintained by electronic means;

“electronic signature” means data attached to, incorporated in, or logically associated with, other data and which is intended by the user to serve as a signature;

“encryption” means a method of transforming signals or messages in a systematic way so that the signal would be unintelligible without a suitable receiving apparatus;

“financial services” has the meaning ascribed to the term under section 2 of the Financial Services Act; Cap. 44:05

“financial services law” has the meaning ascribed to the term under section 2 of the Financial Services Act; Cap. 44:05

“ICANN” means Internet Corporation for Assigned Name and Numbers;

“information system” means a system for generating, sending, receiving, storing, displaying or otherwise processing electronic messages, including internet;

“intermediary service provider” means any person or entity that provides electronic communications services consisting of the provision of access to communications networks, storage, hosting or transmission of information through communication networks;

“internet” means the interconnected system of networks that connects computers around the world using Transmission Control Protocol/Internet Protocol (TCP/IP) or other protocols, and includes future versions thereof;

“Internet Service Provider (ISP)” means a company that provides access to the internet and other related services such as website building and virtual hosting to individuals or other companies;

“key” means a piece of information that determines the functional output of a cryptographic algorithm;

“key pair” means a pair of keys used for cryptography;

“Malawi CERT” means the Malawi Computer Emergency Response Team established under section 6;

“misleading advertising” means any advertising which in any way, including its presentation, deceives or is likely to deceive a person to whom it is addressed or whom it reaches and which, by reason of its deceptive nature, is likely to affect his economic behaviour or which, for those reasons, injures or is likely to injure a competitor’s economic or business interests;

“online public communication” means any transmission of digital data, signs, signals, texts, images, sounds or messages, of whatever nature, that are not private correspondence, by electronic communication means that enable a reciprocal exchange of information between an issuer and a receiver;

“opt-in” means a system where a consumer gives consent to an electronic communication service provider to receive any other communication;

“open standard” means any protocol for communication, interconnection or exchange and any format of interoperable data whose technical specifications are public and the access or use thereto is not restricted;

“personal data” means any information relating to an individual who—

(a) may be directly identified; or

(b) if not directly identified, may be identifiable by reference to an identification number or one or several elements related to his physical, physiological, genetic, psychological, cultural, social, or economic identity;

“place of business” means a place where a person has established, in a stable and lasting way, his activity whatever it is, and as regards a legal person, the place where its registered office is located or where it has its principal activity;

“pornography” means visual material that depicts images of a person engaged in sexually suggestive or explicit conduct;

“private key” means the key of a pair of an isometric cryptal system used to create a digital signature by a holder of the digital signature which is exclusively known by the holder and is not made available to anyone;

“processing of data” means any operation or set of operations which is performed upon data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

“public key” means a key of a pair of an isometric cryptal system used to verify a digital signature that the holder of a digital signature makes available to the public or intended recipients;

“recipient” means a person to whom a sender intends to send an electronic communication, but does not include an intermediary for that communication;

“record” means recorded information, in any form, including data in computer systems, created or received and maintained by a public body in the course of official duties and kept as evidence of such activity;

“record keeping” means making and maintaining a complete, accurate and reliable evidence of official formalities in the form of recorded information;

“Registrar” means an entity designated by the Authority to manage and maintain the reservation of domain names and domain name registry;

“registry” means a central place where domain names are kept and maintained in an organized way;

“sender” means a person by whom, in whose name, or on whose behalf an electronic communication is sent or created before being stored, where necessary, but does not include an intermediary for that communication;

“signatory” means a person who holds a digital signature creation device and acts either on his own behalf or on behalf of a person he represents;

“subscriber” means a person who agrees to receive or be allowed to access electronic texts or services by subscription;

“supplier” means a person or entity that is the source for goods or services;

“Transmission Control Protocol/Internet Protocol (TCP/IP)” means a system of digital rules for data exchange within or between computers; and

“virus” means a malicious program or script that negatively affects the functioning of a computer by creating files, moving files, erasing files or consuming computer memory, causing the computer not to function properly.

3. The objectives of this Act are—

Objectives

(a) to set up a responsive information and communication technology legal framework that shall facilitate competition, development of information and communication technology and

the participation of Malawi in the information age and economy and in particular—

(i) to ensure that the development, deployment and exploitation of information and communication technology within the economy and society and related legal provisions shall balance as well as protect community and individual interests, including privacy and data protection issues;

(ii) to address ethical issues in the use of information and communication technology in order to protect the rights of children and the under-privileged;

(iii) in liaison with the Malawi Revenue Authority, to create a legal framework for favourable tax policies that promote information and communication technology products and services that originate from within Malawi; and

(iv) to provide a responsive and efficient regulatory environment, promote economic subsectors, asset accumulation and tax activities that arise from the use of information and communication technology;

(b) to ensure that information and communication technology users are protected from undesirable impacts of information and communication technology, including the spread of pornographic material, cyber-crime and digital fraud; and

(c) to put in place mechanisms that safeguard information and communication technology users from fraud, breach of privacy, misuse of information and immoral behaviour brought by the use of information and communication technology.

Principles

4. The following principles shall, at all times, be adhered to in the implementation and application of this Act—

(a) e-transactions shall benefit from a secure legal framework that recognizes the legal value of electronic transactions and electronic documents;

(b) freedom of communication over electronic networks shall be promoted, with the exception of specific reasons as provided for in this Act;

(c) there shall be clear and fair specification of responsibilities of intermediaries and editors; and

(d) consumer's rights shall be respected, protected and upheld.

Implementation
of this Act

5. Unless otherwise provided in this Act, the Authority shall be responsible for the implementation of this Act.

PART II—ADMINISTRATION

6.—(1) There is hereby established the Malawi CERT which shall be a unit under the Authority.

Establishment of the Malawi CERT

(2) The Malawi CERT shall take charge of its information infrastructure protection actions and serve as a base for national coordination to respond to information and communication technology security threats.

(3) The Authority shall ensure that the Malawi CERT is capable of providing reactive and proactive services, communicating timely information on recent relevant threats and, whenever necessary, bringing its assistance to bear for response to incidents.

(4) The Authority shall ensure that the Malawi CERT executes the following minimum services—

(a) reactive services earl warning and precaution notice, incidents processing, incidents analysis, incident response

facility, incidents response coordination, incident response on the web, vulnerability treatment, vulnerability analysis, vulnerability response and vulnerability response coordination;

(b) proactive services public notice, technological surveillance, security audit and assessment, security installations and mainte-nance, security tools development, intrusion detection servicesand security information dissemination;

(c) artefacts treatment artefacts analysis, response to artefacts,coordination of response to artefacts, risk analysis, continuationand resumption of activities after disaster, security consultationand sensitization campaign, education or training and product appraisal or certification; and

(d) do anything incidental to the functions of Malawi CERT.

PART III—FORMATION AND VALIDITY OF ELECTRONIC TRANSACTIONS

7. Notwithstanding the contrary intention of any written law, where a law requires that certain information or any other matter be in writing, typewritten or printed form, the requirement shall be satisfied if the information or the matter is—

Recognition of electronic writing

(a) rendered or made available in an electronic form;

(b) accessible; and

(c) capable of being retained for a subsequent reference.

Electronic
signature

8.—(1) Where a law requires a document to be signed, an electronic form of the document shall satisfy the requirement if an electronic signature is used.

(2) An electronic signature shall be authentic if—

(a) the means of creating the electronic signature is, within the context in which it is used, linked to the signatory and not any other person;

(b) the means of creating the electronic signature, was at the time of signing, under the control of the signatory and not any other person and was done without duress and undue influence; and

(c) any alteration made to the electronic signature after signing is detectable.

(3) Subsection(2) does not limit the right of a person—

(a) to prove the authenticity of an electronic signature in any other lawful way; or

(b) to adduce evidence in respect of non-authenticity of an electronic signature.

Equal
treatment of
electronic
signature

9. Except as otherwise provided for in this Act, the provisions of this Act shall not exclude, restrict or affect the legality of any method of creating an electronic signature which—

(a) satisfies the requirements of this Act;

(b) meets the requirements of other statutory provision; or

(c) is provided for under a contract.

Conduct of
a person
relying on
a digital
signature

10. A person may sign an electronic record by affixing a personal digital signature or using any other recognized, secure and verifiable mode of signing agreed by parties or recognized by a particular industry to be safe, reliable and acceptable.

Bearing legal
consequences
of relying on
electronic
signature

11. A person who relies on a digital signature shall bear the legal consequences of failure to—

(a) take reasonable steps to verify the authenticity of the digital signature; or

(c) take reasonable steps where a digital signature is supported by a certificate, to—

(i) verify the validity of the certificate; or

(ii) observe any limitation with respect to the certificate.

12.—(1) Unless otherwise prescribed by law, a person may decide the use of a digital signature, digital signature certificate or any other mode of authentication, of his choice.

Recognition of digital signature certificates and digital signatures

(2) The Authority may, by notice published in the *Gazette*, approve digital signatures, certification authorities offering digital certificates, or authentication of a foreign information security service provider, for use by the public.

(3) The Authority shall ensure that digital certificates comply with international best practices and standards.

(4) A certification authority shall be liable for damages incurred by any person who reasonably relied on a digital certificate issued by the certification authority if—

(a) all or part of the information contained in the digital certificate on the date of issuance was incorrect;

(b) all or part of the data required for the digital certificate to be regarded as qualified were incomplete;

(c) the digital certificate has been issued without checking that the signatory is duly entitled to receive such digital certificate;

or

(d) the certification authority has not registered the revocation of the digital certificate or has not made this information available to third parties or both.

(5) A certification authority shall not be responsible for damage caused by the use of a digital certificate that exceeds fixed limits on the use or the value of transactions for which the digital certificate has been used, if this condition has been made available to the users prior to the use of the certificate.

13.—(1) Where a law requires a signature, statement or document to be notarized, acknowledged, verified or made under oath, that requirement shall be satisfied if the electronic signature of the person authorized to perform those acts is affixed to an electronic record.

Notarization, acknowledgment and certification

(2) Where a law requires or permits a person to provide a certified copy of a document and the document exists in paper or in another physical form, that requirement shall be satisfied if an electronic copy of the document is certified to be a true copy by using an electronic signature of the certifying person.

14.—(1) A requirement in any written law for multiple copies of a document to be submitted to a single recipient at the same time shall be satisfied by the submission of a single electronic record of

Other requirements

such document that is capable of being reproduced by the recipient.

(2) Where a corporate seal is required to be affixed to a document, the requirement shall be satisfied if the electronic signature of the corporate body is affixed to the electronic record in accordance with the provisions relating to the use of the corporate seal.

Determination
of originality
of an electronic

15.—(1) Where any written law requires information to be presented or retained in its original form, the requirement shall be satisfied by an electronic record if—

(a) there is reliable assurance of the integrity of the electronic record; and

(b) the electronic record is capable of being displayed to the person to whom it is to be presented.

(2) For the purposes of this section—

(a) criteria for assessing integrity of information shall be whether it has remained complete and unaltered, save from the addition of any endorsement and of any change which may arise in the normal course of communication, storage and display; and

(b) the standard of reliability required shall be assessed in the light of the purpose for which the information was created and in the light of all the circumstances thereof.

Admissibility
and evidential
weight of
electronic
messages

16.—(1) An electronic message shall be admissible as evidence in court proceedings as provided for in this Act.

(2) In assessing the evidential weight of an electronic message, the court shall have regard to the following—

(a) the reliability of the manner in which the electronic record was generated, displayed, stored or communicated;

(b) the reliability of the manner in which the integrity of the information was maintained;

(c) the manner in which the originator of the electronic message was identified; and

(d) any other facts that the court may consider relevant.

Storage of
electronic
messages

17.—(1) Where any written law requires that a document, record or information shall be retained, that requirement shall be satisfied if the document, record or information is held in electronic form, and—

(a) is accessible;

(b) is capable of retention for subsequent reference;

(c) is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(d) is retained to enable the identification of the origin and destination of the electronic record and the date and time when it was sent or received.

(2) A document, record or information referred to in subsection (1) shall be kept in electronic form for at least seven years.

(3) The obligation to retain a document, record or information under this section shall not extend to information whose purpose is only to enable the message to be sent or received.

(4) The provisions of this section may be satisfied by the use of services of another party as long as all the provisions of the section are complied with.

18.—(1) Where a security procedure has been applied to an electronic record at a specific point in time, the record shall be a secure electronic record from the time the security procedure has been applied.

Secure electronic record

(2) An unauthorized alteration of a security procedure shall render the record invalid.

(3) An alteration shall be unauthorized if it is done by a person without the lawful authority of the person who originally applied a security procedure.

19. Validity of a contract shall not be affected by the sole reason that it is executed in electronic form, if the contract has fulfilled all other requirements for formation of such type of contract.

Validity of a contract executed in electronic form

20.—(1) Unless otherwise agreed by the parties, the dispatch of an electronic message shall occur when such message leaves an information system under the control of the sender or an agent of the sender.

Time and place of dispatch and receipt of an electronic message

(2) Unless otherwise agreed by the parties, receipt of an electronic message shall occur—

(a) where the recipient has designated an information system for the purpose of receiving the electronic message, when the electronic message has entered the designated information system; or

(b) where the recipient has not designated an information system, when the electronic message enters an information system through which the recipient retrieves the electronic message.

(3) Unless otherwise agreed by the parties, an electronic message shall be dispatched at the sender's registered place of business and shall be received at the recipient's registered place of business.

(4) Where a sender or recipient has more than one registered place of business, his retained place of business shall be the one having the closest link with his underlying operation or, in the absence of such underlying operation, with the principal place of business.

(5) If a sender or recipient does not have a place of business, the place of usual domicile shall be taken into consideration.

(6) The provisions of this section shall apply even though the information system supporting the electronic address of the recipient differs from the place where an electronic message is considered to be received under this section.

Offer and
acceptance

21.—(1) Unless otherwise agreed by the parties, an offer and acceptance of the offer may be wholly or partly expressed by electronic means.

(2) A contract concluded between parties by means of electronic messages shall be concluded at the time when, and place where, the acceptance of the offer was received by the recipient:

Provided that parties may agree that the contract was concluded at the place of residence of one party or the place of location of the legal entity, who accepted the offer.

Attribution of
electronic
messages to
sender

22.—(1) An electronic message shall be considered to be that of the sender, if it was sent—

(a) by the sender personally;

(b) by an agent of the sender; or

(c) by an information system programmed by the sender or on behalf of the sender to send electronic messages automatically.

(2) The recipient of an electronic message shall justifiably consider that the electronic message came from the sender and act accordingly if—

(a) the recipient properly applied a procedure previously agreed with the sender for this purpose; or

(b) the electronic messages received by the recipient results from the actions of a person whose relationship with the sender or with an agent of the sender, enabled the recipient to gain access to a method used by the sender to identify an electronic message as that of the sender.

(3) Where parties have not agreed on a procedure of ascertaining the sender of an electronic message, the sender shall be presumed to be the person who objectively appears to be the sender.

(4) The presumption in subsection (3) shall not apply in the following circumstances—

(a) where a recipient of an electronic message was timely notified by the sender that an electronic message did not emanate from the sender;

(b) where a recipient of an electronic message has received notice from the sender that the electronic message was issued without the knowledge or consent of the sender;

(c) where a recipient of an electronic message knew or should have reasonably known, if he had used an agreed procedure that the electronic message did not come from the sender, or that the person who sent the electronic message did not have the authority of the sender to issue or send the electronic message; or

(d) the recipient of an electronic message knew or should have reasonably known that the electronic message resulted from a transmission error.

(5) A recipient of an electronic message shall be entitled to consider each electronic message received as a separate electronic message and act accordingly, unless it duplicates another electronic message which the recipient knew or should have known after taking reasonable steps or complying with an agreed procedure that the electronic message was a duplicate.

23.—(1) Where acknowledgment of an electronic message is required, a sender of the message shall indicate this requirement to the recipient of the message on or before sending the message.

Acknowledgment of receipt of an electronic message

(2) Where a sender of an electronic message has not specified a particular form of acknowledgement, the recipient may apply one of the following methods—

(a) any communication by automated means or any other means, which originated from the recipient; or

(b) any act of the recipient, reasonably sufficient to notify the sender that the electronic message was received.

(3) Where a sender of an electronic message states that an electronic message shall be valid on receipt of acknowledgement by the recipient, the electronic message shall not be considered as sent until the acknowledgement is received.

(4) Where a sender of an electronic message receives a recipient's acknowledgement of receipt of the message, it shall be presumed that the message has reached the recipient, but this presumption shall not mean that the electronic message corresponds to the message received.

(5) Where a party has not indicated that the communication of the electronic message is conditional on receipt of an electronic message, and acknowledgement has not been received by the recipient within the time specified or agreed, or if no time has been specified or agreed, within a reasonable time—

(a) the sender of the electronic message may notify the recipient that no acknowledgement has been received and specify a reasonable time by which the acknowledgement shall be received; and

(b) if the acknowledgement of receipt is not received within the specified period stipulated in paragraph (a), the sender of the electronic message may, upon notice to the recipient, treat the electronic message as though it has never been sent, or exercise any other right that the sender may have.

(6) Where an acknowledgement of receipt indicates that an electronic message complies with the technical conditions, prescribed either by an agreement or by applicable law, these conditions shall be deemed to be fulfilled.

(7) Except insofar as it relates to the sending or receipt of an electronic message, this section shall not affect the legal consequences that may flow either from that message or from the acknowledgement of its receipt.

PART IV—LIABILITY OF ONLINE INTERMEDIARIES AND CONTENT EDITORS AND PROTECTION OF ONLINE USERS

Freedom of communication and its limitations

24.—(1) Subject to this Act, there shall be no limitations to online public communication.

(2) Notwithstanding the provisions of subsection (1), online public communication may be restricted in order to—

(a) prohibit child pornography;

(b) prohibit incitement on racial hatred, xenophobia or violence;

- (c) prohibit justification for crimes against humanity;
- (d) promote human dignity and pluralism in the expression of thoughts and opinions;
- (e) protect public order and national security;
- (f) facilitate technical restriction to conditional access to online communication; and
- (g) enhance compliance with the requirements of any other written law.

25.—(1) An intermediary service provider shall not be liable in any civil or criminal proceedings for any information contained in an electronic message in respect of which he provides services, if the intermediary service provider—

Liability of
an
intermediary
service
provider

- (a) has not initiated the transmission of the message;
- (b) has no actual knowledge of the act or omission that gives rise to the civil or criminal liability as the case may be, in respect of the message; and
- (c) has no knowledge of any facts or circumstances from which the likelihood of such civil or criminal liability ought reasonably to have been known.

(2) Nothing in this section shall be construed as—

- (a) requiring an intermediary to monitor any information contained in any electronic message, in order to establish knowledge of any act, omission, fact, or circumstance giving rise to civil or criminal liability or imputing knowledge of such liability; or
- (b) relieving an intermediary from complying with any law, court order, ministerial direction, or contractual obligation in respect of an electronic message.

(3) If in relation to information contained in an electronic message in respect of which an intermediary service provider renders his services, the intermediary service provider has—

- (a) actual knowledge of the act or omission that gives rise to civil or criminal liability, as the case may be, in respect of the message; or
- (b) knowledge of any fact or circumstance from which the likelihood of such civil or criminal liability ought reasonably to have been known, he shall forthwith remove the document from any electronic communication system within his control and shall cease to provide services in relation to the message.

(4) An intermediary service provider shall not be liable for any act done in good faith pursuant to this section.

Liability for
being a conduit

26.—(1) An intermediary service provider shall not, when supplying services of transmission of information, or when offering access to online public communication, be held liable for the information transmitted on condition that the intermediary service provider—

(a) does not monitor the online communication;

(b) does not initiate the transmission;

(c) does not select the receiver of the transmission; or

(d) does not select or modify the information contained in the transmission.

(2) The acts of transmission, routing and provision of access include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place—

(a) for the sole purpose of carrying out the transmission in the information system;

(b) in a manner that makes it ordinarily inaccessible to anyone other than an anticipated recipient; and

(c) for storage for a period not longer than is reasonably necessary for the transmission.

Liability for
caching
services

27. An intermediary service provider shall not be liable for the automatic intermediate and temporary storage of the electronic message, where the intention of such storage is for its onward transmission to other recipients who requested it, if the intermediary service provider—

(a) does not modify the electronic message;

(b) complies with the conditions on access to electronic message;

(c) complies with rules regarding updating of the electronic message, specified in a manner widely recognized and used by the information and communication technology industry;

(d) does not interfere with the lawful use of technology that is widely recognized and used by the information and communication technology industry, to obtain information on the use of electronic message;

(e) acts expeditiously to remove or to disable access to the information it has shared upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed or access to it has been disabled or that a court

or an administrative authority has ordered such removal or disablement; and

(f) removes or disables access to the electronic messages it has stored upon receiving a takedown notice.

28. An intermediary service provider who provides a service comprising storage of electronic messages shall not be liable for the information stored if—

Liability for the supply of hosting services

(a) he was not aware of the unlawful character of the stored information; or

(b) immediately after becoming aware of the unlawful character of the stored information, he took all necessary measures to withdraw the information or to make access to such information impossible; or

(c) upon receipt of the takedown notice issued under this Act, he expeditiously removes or disables access to the information.

29.—(1) An intermediary service provider shall, while exercising the activities prescribed in section 30, maintain and preserve the data that permits the identification of any person who contributed to the creation of all or part of the content relating to the services rendered by such intermediary service provider.

Saving of data

(2) The High Court may require from the intermediary service provider communication of the data referred to in subsection (1).

(3) The Authority may issue regulations governing the retention of data referred to in this section.

30.—(1) An intermediary service provider offering access to online public communication services shall provide, and inform its subscribers of the existence of any technical means which permit restriction of access to certain services.

Takedown notification

(2) An intermediary service provider shall set up an easily accessible and visible system to enable any person inform the intermediary service provider of any content which is unlawful or infringes, or may infringe, on such person's rights.

(3) An intermediary service provider shall—

(a) inform promptly the Authority or its organs of any illegal content reported as indicated in subsection (2) and made available online by the beneficiaries of their services; and

(b) make public the means taken to fight against the dissemination of such illegal content.

(4) Any person who claims that a published electronic message is unlawful or infringes on his right, shall notify the intermediary service provider of such message.

(5) A notification stipulated in subsection (4) shall be in permanent medium addressed by the complainant to the intermediary service provider, and shall include the following information—

- (a) the full name and address of the complainant;
- (b) the written or electronic signature of the complainant;
- (c) the right that has been infringed;
- (d) identification of the material or activity that is claimed to be the subject of the infringing or unlawful activity;
- (e) the remedial action required to be taken by the intermediary service provider in respect of the complaint;
- (f) telephone and electronic mail contacts;
- (g) a statement that the complainant is acting in good faith; and
- (h) a statement by the complainant that the information is true and correct.

(6) Any person who notifies an intermediary service provider of an infringement or unlawful activity or content knowing that the notification is false, commits an offence and is liable to a fine of K1,000,000 and imprisonment for twelve months.

(7) An intermediary service provider shall not be liable for a takedown in response to a wrongful or false notification.

31.—(1) An online content provider shall display in a conspicuous manner, the following information on its webpage—

- (a) in case of a natural person, full name, domicile, telephone number, and email address, of the editor;
- (b) in case of a legal entity, corporate name, postal and physical address of the registered office, telephone number, email address, authorized share capital, and registration number, of the editor;
- (c) where applicable, the name of the corporate officer appointed as director of the publication of the online public communication and the editor in chief; and
- (d) the name, title, corporate name, postal and physical address and telephone number, email address of the intermediary service provider prescribed in this section.

(2) A person editing online public communication on a non-professional basis may make publicly available his name as

well as the name and address of the intermediary service provider prescribed in this Act:

Provided that the person has duly communicated to the intermediary service provider the particulars of personal identification prescribed by subsection (1).

(3) Any intermediary service provider identified in this section shall be subject to professional secrecy as regards disclosure of the particulars of personal identification or of any information sufficient to identify the source of online content.

(4) A person may act as an editor of an online public communication, and as an intermediary service provider, if his activities fall under both regimes.

(5) Where a person acts as an editor of an online public communication and as an intermediary service provider as provided in subsection (4), legal obligations of both regimes shall apply respectively to each activity.

(6) An intermediary service provider exercising the activities prescribed in this section shall provide to editors of online content under this section the technical means to comply with the requirements of identification prescribed in this section.

32.—(1) A person who can be directly or indirectly identified in an online public communication, shall have the right to demand a publication of his response, without prejudice to his right to request correction or deletion of the content. Right of reply

(2) A request stipulated in subsection (1) shall be addressed to the editor in chief designated in section 31(1) (c).

(3) In the event that a person editing an online public communication on a non-professional basis elects to remain anonymous, the complainant shall directly address the request to the hosting intermediary service provider.

(4) An online editor shall publish the response stipulated in subsection (1) within twenty four hours of receipt of the request in subsection (1).

(5) A person who contravenes subsection (4) commits an offence and is liable to a fine of K1,000,000 and imprisonment for twelve months.

(6) A right of reply shall be exercised free of charge.

PART V—ELECTRONIC COMMERCE

Information to be provided by a supplier

33.—(1) A supplier of goods or services through electronic commerce (in this Act otherwise referred to as a “supplier”) shall make available the following information to consumers—

(a) full name and legal personality;

(b) postal and physical address and telephone number;

(c) website address and e-mail address;

(d) in case of a corporate entity, its registration number, name of its office bearers and its place of registration;

(e) if the supplier is subject to a tax on consumer goods and services, his tax personal identification number;

(f) details of membership to any regulatory or accreditation body to which the supplier belongs or subscribes to, and contact information of such body;

(g) if the activity of the supplier is subject to any professional regulation, reference to the applicable professional rules, his professional title, the place where such title was granted, or organization to which the person is registered;

(h) if the supplier belongs to a self-regulatory body, to a professional association, to an organisation for dispute settlement, or to any other relevant certification organization, the supplier shall provide adequate information and ensure easy means of verification of such belonging and of access to the codes and practices applicable to that body, association or organisation; and

(i) physical address where the supplier receives service of legal documents.

(2) A supplier shall, before conclusion of a contract, provide to consumers the following information regarding the terms, conditions and costs associated with the transaction—

(a) sufficient description of goods or services subject of the contract;

(b) instructions for use and, in particular, the warnings related to security and health;

(c) restrictions, limitations or conditions related to the purchase, such as an agreement of a parent or of a guardian, and any territorial or temporal restrictions;

(d) details of full costs, including taxes and costs of shipping and delivery to be paid by the consumer, and terms and conditions of payment;

(e) conditions of delivery or execution such as the time of delivery of goods or provision of services:

Provided that—

(i) unless otherwise agreed by the parties, the supplier shall be bound to deliver the goods or to provide the services immediately upon conclusion of the contract; and

(ii) where the supplier fails to deliver the goods and provide the services as stipulated in subparagraph (i), the consumer shall be entitled to terminate the contract;

(f) mode of payment;

(g) information regarding available after-sale service;

(h) details and conditions of withdrawal, denunciation, return, cancellation or reimbursement, in accordance with the provisions of sections 36, 37, 38 and 39;

(i) warranty conditions;

(j) return, exchange and refund policy of the supplier;

(k) manner and the period within which the consumer can maintain a full record of the transaction;

(l) any alternative dispute resolution code to which the supplier subscribes and how the details and content of that code may be accessed electronically by the consumer; and

(m) security procedures and privacy policy of the supplier in respect of payment, payment information and personal information of the consumer.

34.—(1) A very contract with a value exceeding K5,000,000.00, or a value as will be prescribed by the Minister by notice published in the *Gazette*, concluded by electronic means shall be achieved by the supplier for a period of not less than seven years from the date when the contract was formed.

Formation of
electronic
contracts
with
consumers

(2) A supplier shall ensure that the terms and conditions referred to in subsection (1)—

(a) specify the time and manner the contract is formed; and

(b) are in a form that guarantees their preservation and production.

(3) A supplier shall—

(a) provide the technical means which permit the consumer to review the transaction and correct any errors made;

(b) indicate the languages in which the contract shall be formed;

(c) in case the contract is archived, provide the conditions of such archiving by the supplier and the conditions of access to the archived contract; and

(d) if applicable, provide the way to access, through electronic means, professional and commercial rules that the supplier considers binding.

(4) Every contract with a value exceeding K5,000,000 concluded by electronic means shall be archived by the supplier for a period of not less than seven years from the date when the contract was formed.

Cooling-off
period

35.—(1) A consumer shall be entitled to exercise the right of withdrawal from a contract concluded by electronic means without giving reasons and without penalties—

(a) with respect to goods, within seven days of receipt of the goods or a period as agreed by the two parties in the agreement;

(b) with respect to services, within seven days of the formation of the contract or a period as agreed by the two parties in the agreement.

(2) Where consumer has cancelled a contract under this section, the consumer may, if necessary, bear return costs for the goods supplied or services rendered.

(3) After a consumer has cancelled a contract under this section, a supplier shall, within fourteen days of cancellation of the contract by the consumer, reimburse to the consumer all sums paid.

(4) After expiry of the period specified in subsection (3), the sum due shall attract interest at the prevailing bank rate as specified by the Reserve Bank of Malawi.

(5) A supplier shall reimburse to a consumer, all sums due, in a payment mode agreed by the parties:

Provided that in the event that the parties fail to agree on the mode, the reimbursement shall be made in the same mode in which the consumer paid the supplier.

(6) Notwithstanding subsection (1), a consumer shall not withdraw from a contract concluded by electronic means where—

(a) the provision of services started with the consumer's consent, before the end of the seven day period;

(b) the price of the goods or services depends on the fluctuations of financial market rates and the price is not in the control of the supplier;

(c) the provision of goods was made according to the consumer's own specifications or clearly personalized, or goods which by their nature cannot be returned or are liable to deteriorate rapidly;

(d) the contract relates to the provision of audio or video recording or software;

(e) the contract relates to the provision of newspapers, periodicals or magazines; and

(f) the contract relates to the provision of betting and authorized lotteries.

36.—(1) A supplier shall put technical measures on his electronic platform that will enable a consumer to verify the accuracy of the details of an order, failing which an electronic transaction made on the platform shall be invalid.

Performance of an electronic transaction

(2) A supplier shall acknowledge receipt of the order electronically within forty eight hours of receipt of the order.

(3) Unless the parties agree otherwise, a supplier shall execute the order within thirty days of receipt of the order.

(4) Where a supplier has failed to execute an order within the thirty days or within the agreed period, the consumer may, after the expiration of that period, cancel the contract upon giving a seven days' written notice.

(5) The order, the acceptance of the order, and the acknowledgement of receipt of such acceptance of the order, shall be considered received in accordance with section 20.

(6) For the purposes of this section, an "order" shall amount to an "offer".

37.—(1) Where a supplier fails to perform his part of the contract, the supplier shall inform the consumer of the failure and the supplier shall refund the consumer any sums paid within seven days of notifying the consumer of his failure or at the expiry of the thirty days or at the expiry of the period agreed by the parties, whichever comes first.

Default in contract performance

(2) Where a supplier fails to refund a consumer as required by subsection (1), interest shall accrue on the sum at the applicable bank rate as specified by the Reserve Bank of Malawi.

(3) Where a consumer is contractually required to bear costs of returning goods that the supplier has delivered to a consumer, the supplier shall inform the consumer of this fact in advance.

38.—(1) A supplier shall provide to a consumer with an opportunity to do the following—

Review and cancellation of contract by a consumer

- (a) review the entire electronic transaction;
- (b) correct any errors; and

(c) withdraw from the transaction before finally placing an order.

(2) Where a supplier's transaction fails to comply with subsection (1), a consumer is entitled to cancel the transaction within fourteen days after receiving the goods, services or facilities to which the transaction applies.

(3) Where a transaction is cancelled under subsection (2)—

(a) a consumer shall return the goods and cease using the services or facilities supplied pursuant to the transaction, as the case may require; and

(b) a supplier shall refund all payments made by the consumer in respect of the transaction.

(4) A supplier shall utilize a payment system that is sufficiently secure having regard to—

(a) accepted technological standards at the time of the transaction; and

(b) the type of transaction concerned.

(5) A supplier shall be liable for any damage suffered by a consumer due to a failure by the supplier to comply with subsection (4).

Cancellation of payment

39. A consumer may require the cancellation of a payment in case of fraudulent use of his payment for the purposes of execution of a contract by electronic means, and in such a case the sums paid shall be reimbursed to the consumer.

Prohibition of misleading advertising

40.—(1) A person dealing on online communication shall not advertise in a misleading manner.

(2) In determining whether online advertising is misleading, account shall be taken of all its features, and in particular, of any information it contains concerning—

(a) the characteristics of goods or services, such as their availability, nature, execution, composition, method and date of manufacture or provision, fitness for purpose, uses, quantity, specification, geographical or commercial origin, the results to be expected from their use, or the results and material features of tests or checks carried out on the goods or services;

(b) the price or the manner in which the price is calculated, and the conditions on which the goods are supplied or the services provided; and

(c) the nature, attributes and rights of the advertiser, such as its identity, assets, qualifications, ownership of industrial, commercial or intellectual property rights or its awards and distinctions.

(3) Comparative advertising shall, as far as the comparison is concerned, be permitted if the advertising—

(a) is not misleading within the meaning of subsections(1) and (2);

(b) compares goods or services meeting the same needs or intended for the same purpose;

(c) objectively compares one or more material, relevant, verifiable and representative features of those goods and services, which may include price;

(d) does not discredit or denigrate the trade marks, trade names, other distinguishing marks, goods, services, activities or circumstances of a competitor;

(e) for products with designation of origin, relates in each case to products with the same designation;

(f) does not take unfair advantage of the reputation of a trade mark, trade name or other distinguishing marks of a competitor or of the designation of origin of competing products;

(g) does not present goods or services as imitations or replicas of goods or services bearing a protected trade mark or trade name; and

(h) does not create confusion among traders, between the advertiser and a competitor or between the advertiser's trademarks, trade names, other distinguishing marks, goods or services and those of a competitor.

41.—(1) Subject to the Consumer Protection Act and any other written law, any advertisement made by electronic means shall be clearly identifiable as such and the natural or legal person for whom the advertisement is placed shall be clearly identifiable.

Identification of advertisement content
Cap. 48:10

(2) The terms and conditions for benefiting from promotional offers and for participating in sweepstakes, lotteries or in other promotional games shall be clearly and precisely indicated and easily accessible.

42.—(1) Except in the case of a notice sent by an electronic communications provider to a customer in relation to services, a person shall not send unsolicited electronic communications to a consumer without obtaining the prior consent of the consumer.

Unsolicited communications

(2) A person who sends electronic commercial communication to a consumer shall provide the consumer—

(a) with an option to unsubscribe from the mailing list of that person; and

(b) at the request of the consumer, the identifying particulars of the source from which that person obtained the consumer's personal information.

(3) A recipient shall have the opportunity to object, free of charge, to the use of his personal data for prospection purposes by a data controller.

(4) A person who contravenes subsection (1) commits an offence and shall, upon conviction, be liable to a fine of K2,000,000 and imprisonment for five years.

(5) A person who sends unsolicited commercial communications to another person or who continues to send unsolicited commercial communications to a person after unsubscribing in accordance with subsection (2)(a) commits an offence and shall, upon conviction, be liable to a fine of K1,000,000 and imprisonment for twelve months.

(6) The provisions of subsection (1) and (2) shall not apply where—

(a) the sender of the electronic message has obtained the personal data of the recipient in the course of negotiations for the sale of the product or the provision of the service referred to in the electronic message; or

(b) the commercial solicitation is directly linked to the product or the service.

43.—(1) Subject to the Payment Systems Act, 2016, and any financial services law, the provisions of this Part shall apply to any supply of electronic financial services without prejudice to application of—

(a) specific legal and regulatory obligations applicable to certain financial products, instruments or services; and

(b) other provisions applicable to contracts concluded between natural persons or a supplier and a consumer.

(2) The Minister of Finance, on recommendation from the Authority and the Governor of the Reserve Bank of Malawi, shall make regulations defining specific obligations with regards to online banking.

44.—(1) Before a conclusion of a distance contract or acceptance of an offer, a consumer shall receive from the supplier the information indicated in section 33, and where applicable—

Identity of a provider of financial or banking services

(a) when the supplier uses the services of a representative, the supplier shall communicate to the consumer the identity of the representative and his address and the following information—

(i) the fact that financial services are linked to instruments involving special risks related to their specific features or the operations to be executed or the fact that their price depends on fluctuations in the financial markets outside the supplier's control;

(ii) the fact that past performances do not allow to predict future performances; and

(iii) any limitation of the term during which the information provided is valid, the conditions of payment and execution and, if necessary, the existence of any specific additional costs for the consumer arising out of the use of electronic communication;

(b) where necessary, the existence of a right of withdrawal as prescribed by section 35, its duration, the possible pecuniary consequences of its exercise, as well as the address to be used by the consumer to notify the supplier of his decision;

(c) in a case where the right of withdrawal is not exercisable, the supplier shall inform the consumer about that and the consequences.

(2) For a contract with a withdrawal period, the supplier shall inform the consumer that without his express consent, the contract may not be executed before expiry of the withdrawal period.

(3) The terms and conditions of the contract and in particular the information indicated in subsections (1) and (2) shall be—

(a) provided in a clear and comprehensible manner and in any way appropriate to the means of electronic communication used;

(b) communicated to a consumer in writing prior to the conclusion of the contract; and

(c) communicated to a consumer in writing upon the consumer's request at any time during the contractual relations.

45.—(1) Notwithstanding the provisions of section 35, a consumer entering into a distant contract for the provision of financial services shall have twenty calendar days unless otherwise agreed by the parties, within which he may exercise his right to

Right of withdrawal from a contract

withdraw from the contract without penalty and without giving reasons.

(2) The period referred to in subsection (1) shall be extended to forty five calendar days for distance contracts relating to life insurance and retirement.

(3) The term during which the right of withdrawal may be exercised starts—

(a) either from the day when the distance contract was concluded, except the case of the life insurance with respect to which the term of withdrawal starts from the date when the consumer became aware of the conclusion of a distance contract; or

(b) from the day when the consumer received the terms and conditions of the contract, if the period is later than the period prescribed under subsection (1).

(4) The right of withdrawal shall not apply—

(a) to financial services having prices dependent on fluctuations of the financial market on which the supplier has no influence and which are susceptible to occur during the withdrawal period;

(b) to insurance of travel or luggage, or similar types of short-term insurance not exceeding one month; and

(c) to contracts—

(i) executed exclusively by the supplier and the consumer;

(ii) executed upon the express request of the consumer; and

(iii) where the consumer has not yet exercised the right of withdrawal.

(d) to online auctions;

(e) to supply of food stuffs, beverages and other goods intended for daily consumption;

(f) where audio or video recordings or computer software were downloaded, or unsealed by the consumer;

(g) to sell of newspapers, periodicals, magazines and books;

(h) to the provision of gaming and rotary services;

(i) to online gambling;

(j) to the provision of accommodation, transport and catering services; and

(k) to start up transactions as the Minister may by Notice published in the *Gazette* prescribe.

(5) Unless otherwise agreed by the parties, where a consumer exercises the right of withdrawal, he may only be required to pay, within seven days, for the financial services already provided by a supplier pursuant to the distant contract and the execution of a contract may only start upon consent of the consumer, and the amount due—

(a) has not exceeded the amount proportionate to the service already rendered as compared to the services to be rendered under the contract; and

(b) is not, under any circumstances, of such value or nature as to constitute a penalty.

(6) A supplier may not require a consumer to pay an amount due under subsection (5) unless the supplier proves that the consumer was duly notified of the amount.

(7) Where a supplier has started to execute a contract before expiry of the term of withdrawal, the supplier may not, under any circumstances, require the consumer to process the payment.

(8) Unless otherwise agreed by the parties, a supplier shall be required to reimburse to a consumer, not later than fourteen days, all sums which were paid by the consumer under a distant contract.

(9) The fourteen day period referred to in subsection (8) shall commence once a supplier receives a notification of a decision by a consumer to withdraw from the contract.

(10) Unless otherwise agreed by the parties, where a supplier fails to reimburse to a consumer the sums due within the period of fourteen days, the amount shall attract interest at the prevailing bank rate as specified by the Reserve Bank of Malawi.

(11) A consumer shall return to the supplier not later than fourteen days or such period as agreed by the parties and the calculation of time under this section shall start from when the goods received from the supplier and the fourteen day period shall start from the day when the consumer has sent a notification of withdrawal to the supplier.

PART VI—SECURITY AND DIGITAL ECONOMY

46.—(1) Where any portion of an electronic message is signed with a digital signature, the digital signature shall be treated as a secure electronic signature with respect to such portion of the message if—

Use, supply,
transfer, etc

(a) the digital signature was created during the operational period of a valid digital signatures certificate and is verified by reference to the public key listed in such certificate;

(b) the public key of the signatory has the same identity as the certificate based on the fact that—

(i) the digital signature certificate was issued by a competent licensed certification authority;

(ii) the digital signature certificate was issued by a certification authority outside Malawi recognized for this purpose by the Authority;

(iii) the digital signature certificate was issued by an organ licensed by the Authority to act as a certification authority in accordance with this Act ; and

(iv) the sender and the recipient have expressly agreed between themselves to use digital signatures as a security procedure, and the digital signature was properly verified by reference to the sender's public key.

Presumptions
regarding
digital
signature
certificates

47. Except for information identified as subscriber information which has not been verified, any other information included in a digital signature certificate issued by a licensed certification authority shall be deemed correct if the subscriber accepted the digital signature certificate, unless evidence to the contrary is adduced.

Unreliable
digital
signatures

48.—(1) Unless otherwise provided for by any written law or contract, a person relying on a digitally signed electronic message shall bear the risk that the digital signature is invalid as a signature or authentication of the signed electronic message, if reliance on the digital signature is not reasonable under the circumstances having regard to the following factors—

(a) acts which the person relying on the digitally signed electronic message knows or has notice of, including all facts listed in the digital signature certificate or incorporated in it by reference;

(b) the value or importance of the digital signed electronic message, if known;

(c) the course of dealing between the person relying on the digital signed electronic message and the subscriber and any available indication of reliability or unreliability apart from the digital signature; and

(d) any usage of trade, particularly trade conducted by trustworthy systems or other electronic means.

Reliance on
digital
signature and
certificate

49. A person who relies on a digital signature shall be deemed to have relied on a valid certificate containing the public key by which the digital signature may be verified.

50. A digital signature certificate may be published where—

- (a) it has been issued by a competent authority;
- (b) the subscriber mentioned on that digital signature certificate has accepted it; and
- (c) the digital signature certificate has not been revoked or suspended.

Requirements to publish digital signature certificate

51.—(1) The Authority shall accredit certification authorities.

Authority to appoint a certification authority

(2) the Minister shall, from time to time issue certification authorities accreditation regulations in consultation with the Authority which may include—

- (a) application procedures accreditation;
- (b) applicable fees.
- (c) terms and conditions for accreditation;
- (d) standards to be maintained by accreditation authorities;
- (e) any other terms deemed necessary.

(3) The authority shall—

- (a) keep and maintain a register of certification authorities; and
- (b) do such things as necessary for the implementation of this Act.

52.—(1) A person shall not provide cryptograph services or products in Malawi without registration under this Part.

Encryption

(2) Registration for provision of cryptograph services or products shall be made—

- (a) to the Authority;
- (b) in the prescribed manner and form; and
- (c) upon payment of applicable fees.

(3) The Minister in consultation with the Authority shall issue regulations—

- (a) in respect of use, importation and exportation of encryption programmes and encryption products; and
- (b) prohibiting the exportation of encryption programmes or other encryption products from Malawi generally or subject to such restrictions as may be prescribed.

(4) For the avoidance of doubt, subject to any regulations made under subregulation (1), it is lawful for any person to use encryption programme or product provided that it has lawfully come into possession of that person.

Trustworthy
system

53.—(1) A certification authority shall utilize a trustworthy system in performing its services.

(2) the registration for the provision of cryptographic services or products shall be made—

- (a) to the Authority;
- (b) in the prescribed manner and form; and
- (c) upon payment of prescribed fees.

(3) the minister in consultation with the Authority shall issue regulations—

(a) in respect of use, importation and exportation of inscription programmes and products; and

(b) prohibiting the exportation of inscription programmes or other inscription products from Malawi generally, or subject to such restrictions, as may be prescribed.

(4) For the avoidance of doubt, subject to any regulations made under subregulation (1), it is lawful for any person to use encryption programme or product provided that it has lawfully come into possession of that person.

Disclosure

54.—(1) A certification authority shall disclose—

(a) its digital signature certificate that contains the public key corresponding to the private key used by that certification authority to digitally sign another digital signature certificate;

(b) any relevant certification practice statement;

(c) notice of the revocation or suspension of its certification authority certificate; and

(d) any other fact that materially and adversely affects either the reliability of a digital signature certificate that the authority has issued or the authority's ability to perform its services.

(2) In case of an occurrence that materially and adversely affects a certification authority trustworthy system or its certification, the certification authority shall—

(a) use reasonable efforts to notify any person who is known to be foreseeably affected by that occurrence; and

(b) act in accordance with procedures governing such an occurrence specified in its certification practice statement.

Issuance of a
digital
signature
certificate

55.—(1) A certification authority may issue a certificate to a prospective subscriber only after—

(a) it has received a request from the prospective subscriber; and

(b) the prospective subscriber has a certification practice statement in compliance with the content of such statement including procedures regarding identification of the prospective subscriber.

(2) In the absence of a certification practice statement, the certification authority shall confirm by itself or through an authorized agent that—

(a) the prospective subscriber is the person to be listed in the digital signature certificate to be issued;

(b) if the prospective subscriber is acting through one or more agents, the subscriber authorized the agent to have custody of the subscriber's private key and to request issuance of a digital signature certificate listing the corresponding public key;

(c) the information in the digital signature certificate to be issued is accurate;

(d) the prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the digital signature certificate;

(e) the prospective subscriber holds a private key capable of creating a digital signature; and

(f) the public key indicated in the digital signature certificate is capable of verifying a digital signature affixed by the public key.

56.—(1) By issuing a digital signature certificate, a certification authority represents any person who relies on the digital signature certificate or a digital signature verifiable by the public key indicated in the certificate in accordance with any applicable certification practice statement.

Representations upon issuance of a digital signature certificate

(2) In the absence of such certification practice statement, the representing certification authority confirms that—

(a) the certification authority has complied with all applicable requirements of this Act in issuing the digital signature certificate, but where the certification authority has published or submitted it to such relying person, it shall confirm that the subscriber listed in the digital signature has accepted it;

(b) the subscriber identified in the certificate holds the private key corresponding to the public key listed in the digital signature certificate;

(c) the subscriber's public key and private key constitute a functioning key pair;

(d) all information in the digital signature certificate is accurate, unless the certification authority has stated in the digital signature certificate or incorporated by reference in the

certificate a statement that the accuracy of specified information is not confirmed; and

(e) the certification authority has no knowledge of any material fact which if it had been included in the digital signature certificate would adversely affect the reliability of the representations above mentioned.

Suspension of a digital signature certificate

57. A certification authority that issued a digital signature certificate shall suspend the certificate after receiving a request by—

- (a) a subscriber listed in the digital signature certificate; or
- (b) a person acting on behalf of a subscriber, where the subscriber is not available.

Revocation of digital signature certificate

58. A certification authority shall revoke a digital signature certificate that it issued—

- (a) upon request by the subscriber or his representative;
- (b) upon receipt of a certified copy confirming that the subscriber is dead;
- (c) upon presentation of documents effecting a dissolution of the subscriber; or
- (d) upon confirming by other evidence that the subscriber has been dissolved or has ceased to exist.

Revocation without a subscriber's consent

59. A certification authority shall revoke a digital signature certificate, regardless of whether the subscriber listed in the certificate consents, if the certification authority confirms that—

- (a) a material fact represented in the digital signature certificate is false;
- (b) a requirement for issuance of the digital signature was not satisfied;
- (c) the certification authority's private key or trustworthy system was compromised in a manner materially affecting the digital signature certificate's reliability; or
- (d) a subscriber has ceased his activities.

Notice of suspension of digital signature certificate

60.—(1) Immediately upon suspension of a digital signature certificate by a certification authority, the certification authority shall publish a signed notice of the suspension.

(2) A certification authority shall keep and maintain a register containing notices of suspended digital signature certificates, which registers shall be open for inspection by the public.

Notification of revocation of a digital signature certificate

61.—(1) Immediately upon revocation of a digital signature certificate by a certification authority, the certification authority shall publish a signed notice of the revocation.

(2) A certification authority shall keep and maintain a register containing notices of revoked digital signature certificates which shall be open for inspection by the public.

62.—(1) If a subscriber generates a key pair whose public key is to be listed in a digital signature certificate issued by a certification authority and accepted by the subscriber, the subscriber shall generate the key pair using a trustworthy system.

Generating a key pairs

(2) This section shall not apply to a subscriber who generates a key pair using a system approved by a certification authority.

63. A subscriber shall not make material representations to a certification authority for purposes of obtaining a digital signature certificate, including all information known to the subscriber and represented in the certificate, unless the representations are accurate and complete.

Accurate and complete representations

64.—(1) A subscriber shall be deemed to have accepted a digital signature certificate if he publishes in writing or authorizes the publication of a digital signature certificate—

Acceptance of digital signature certificate

(a) to one or more persons;

(b) in a register; or

(d) where another digital signature certificate is produced or proved by written evidence.

(2) By accepting a digital signature certificate issued by a subscriber or a certification authority, the subscriber listed in the certificate certifies to all who reasonably rely on the information contained in the certificate that—

(a) the subscriber rightfully holds the private key corresponding to the public key listed in the digital signature certificate; and

(b) all representations made by the subscriber to the certification authority and material to the information listed in the digital signature certificate are true.

65.—(1) By accepting a digital signature certificate issued by a certification authority, the subscriber identified in the certificate shall assume a duty to exercise reasonable care to retain control of the private key corresponding to the public key listed in such digital signature certificate and shall prevent its disclosure to a person not authorized to create the subscriber's digital signature.

Control of a private key

(2) The duty referred to in subsection (1) shall continue during the operational period of the digital signature certificate and during any period of suspension of the certificate.

66. A subscriber who has accepted a digital signature certificate shall, as soon as possible, request the issuing certification authority

Requesting for suspension or revocation

to suspend or revoke the certificate if the private key corresponding to the public key listed in the certificate has been compromised.

Provision of encryption services

67.—(1) A person who provides encryption services shall declare to the Authority the technical characteristics of the encryption means as well as the source code of the software used.

(2) Regulations made under this Act shall define the conditions for making declarations referred to in subsection (1), and may define encryption services whose technical characteristics or conditions of supply are such that, with regard to national defence or internal security interests, their provision shall not require any prior formality.

(3) An encryption services provider shall be bound by professional secrecy.

(4) Unless it is proved that no intentional wrongful conduct or negligence was involved, a provider of encryption services for confidentiality purposes shall be liable, notwithstanding any contractual provision to the contrary, for the damage suffered by the persons that entrusted the management of their confidential conventions to them in case of violation of the integrity, confidentiality or availability of the data object of such convention.

Administrative sanctions

68.—(1) Without prejudice to applicable criminal sanctions, where a supplier of encryption, including free of charge encryption, does not comply with its obligations under this Act, the Authority may, after having given the supplier the opportunity to give its observations, prohibit the distribution of the concerned encryption.

(2) The prohibition of distribution shall entail an obligation for the supplier to withdraw—

- (a) from distribution networks, the prohibited encryption; and
- (b) materials constituting encryption whose distribution has been prohibited and that have been acquired against payment directly or through distribution networks.

Appointment of cyber inspectors

69.—(1) The Authority shall appoint any person as a cyber inspector to perform the functions provided for in this Part for a term of two years, renewable for another term of two years.

(2) A person may be appointed as a cyber inspector if that person—

- (a) is a citizen and a resident of Malawi;
- (b) possesses qualifications, expertise and experience in any fields of communications technology, law, economics or finance; and
- (c) is an individual who is committed to fairness, openness,

accountability and to principles by which the Authority is guided.

(3) A person shall be disqualified from being appointed as a cyber inspector if he—

- (a) is a Member of Parliament;
- (b) is a Minister or Deputy Minister; or
- (c) is a member of a committee of a political party.

(4) The Authority shall provide any person appointed as a cyber inspector with a certificate of appointment.

(5) The certificate of appointment referred to in subsection (4) may be accompanied by a digital signature of the Authority.

(6) A cyber inspector shall, in performing any function under this Act—

- (a) be in possession of the certificate of appointment referred to in subsection (4); and
- (b) upon request by a person who is subject to investigations or an employee of that person, show the certificate of appointment to that person.

70.—(1) A cyber inspector shall have the following powers and functions—

Powers and
functions of
a cyber
inspector

(a) to monitor and inspect any website database with critical data or activity on an information system in the public domain and report any unlawful activity to the Authority;

(b) in respect of suppliers of encryption and encryption service providers—

(i) to investigate the activities of suppliers of encryption and of encryption service providers in relation to compliance with this Act; and

(ii) to issue orders in writing to suppliers of encryption and encryption service providers to comply with the provisions of this Act;

(c) in the performance of his functions, at any reasonable time, without prior notice, and under the authority of a search warrant issued by a court, to enter any premises or access any information system and—

(i) search the premises or the information system;

(ii) search any person on the premises if there are reasonable grounds to believe that the person has possession of a document, record or any element that is connected to an investigation;

(iii) take extracts from, or make copies of, any book, document, record or any element that is in the premises or in the information system and has a bearing on an investigation;

(iv) demand the production of, and inspect, relevant authorizations, declarations and certificates;

(v) inspect any facilities on the premises, which are linked or associated with the information system;

(vi) access and inspect the operation of any computer or equipment forming part of an information system and any associated apparatus or material which the cyber inspector has reasonable cause to believe is, or has been used in, connection with the commission of any offence;

(vii) use or cause to be used any information system or part thereof to search any data contained in or available to such information system;

(viii) require the person by whom, or on whose behalf, the cyber inspector has reasonable cause to suspect the computer or information system is or has been used, or require any person in control of, or otherwise involved with the operation of the computer or information system, to provide the cyber inspector with such reasonable technical and other assistance as the cyber inspector may require for the purposes of this part; or

(ix) make such inquiries as may be necessary to ascertain whether the provisions of this Act or any other written law on which an investigation is based, have been complied with.

(2) A person who—

(a) hinders or obstructs a cyber inspector in the performance of his powers and functions under this Part;

(b) refuses to co-operate with a cyber inspector; or

(c) falsely holds himself out as a cyber inspector,

commits an offence and shall, upon conviction, be liable to a fine of K5,000,000 and imprisonment for seven years.

(3) For the proper performance of his functions under this Act, a cyber inspector maybe accompanied by a police officer.

PART VII—DATA PROTECTION AND PRIVACY

71.—(1) A data controller shall ensure that personal data is—

(a) processed fairly and legally;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and processed;

(d) accurate and, where necessary, kept up to date;

(e) every reasonable step shall be taken to ensure that data which is inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, is erased or rectified; and

(f) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed.

(2) Personal data may be processed only if—

(a) the data subject has unambiguously given his consent;

(b) the processing is necessary for the performance of a contract to which a data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) the processing is necessary for compliance with a legal obligation to which a data controller is subject;

(d) the processing is necessary in order to protect the vital interests of a data subject;

(e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in a data controller or in a third party to whom the data is disclosed; or

(f) the processing is necessary for the purposes of the legitimate interests pursued by a data controller or by the third party or parties to whom the data is disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

(3) For purposes of this section, “consent” means any freely given specific and informed indication by a data subject, of his wishes, by agreement, to his personal data being collected, processed or stored.

72.—(1) A data subject shall be entitled to obtain from a data controller, without constraint or unreasonable delay and at no expense—

Rights of a
data subject

(a) confirmation as to whether or not the data relating to him is being processed;

(b) communication to him of the data undergoing processing and of their source; and

(c) communication for the purposes of the processing and the recipients to whom the data is disclosed.

(2) A data subject shall be entitled to object at any time on legitimate grounds relating to his situation to the processing of data

relating to him and where there is a justifiable objection, the processing instigated by the data controller may no longer involve such data.

(3) A data subject shall be entitled to obtain from a data controller, as appropriate, the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Act, in particular because of the incomplete or inaccurate nature of the data.

Accuracy and completeness of information

73.—A data controller shall provide a data subject from whom data relating to himself is collected with at least the following information—

(a) the identity of the data controller and of his representative, if any;

(b) the purposes of the processing for which the data is intended;

(c) the existence of the right of access to and the right to rectify the data concerning him; and

(d) the existence of the right to object to the processing of the data concerning him.

Security obligations

74.—(1) A data controller shall implement technical and organizational measures enabling to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

(2) Having regard to the state of the art (2) and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

PART VIII—DOMAIN NAME AND MANAGEMENT

Appointment of the Registrar of domain names

75.—(1) The Authority shall appoint a Registrar who shall administer and manage the “.mw” domain name space and any other Malawian names to be used for domain names (in this Act, otherwise referred to as the “Registrar”).

(2) A person holding the office of the Registrar shall hold the office for such duration as the Authority, in its discretion, may determine.

Functions and powers of the Registrar

76.—(1) Without prejudice to generality of section 75, a person holding the office of the Registrar shall perform the following functions—

(a) ensuring compliance by users with international best practices in the administration of the “.mw” domain name space and any other Malawian names to be used for domain names; and

(b) publishing guidelines on—

(i) the general administration and management of the “.mw” domain name space and any other Malawian names to be used for the domain names;

(ii) the requirements and procedures for domain name registration; and

(iii) the maintenance of, and public access to, a registry.

(2) The Registrar shall enhance public awareness on the economic and commercial benefits of domain name registration.

(3) The Registrar, in relation to domain name regulation—

(a) may conduct such investigations as he may consider necessary;

(b) shall conduct research into, and keep abreast of, developments in Malawi and elsewhere on the domain name system and identifiers;

(c) shall continually survey and evaluate the extent to which the “.mw” domain-name space and any other Malawian names to be used for domain names meet the needs of the citizens of Malawi; and

(d) may issue information on the registration of domain names in Malawi.

(4) The Registrar may—

(a) liaise, consult and co-operate with any person or other authorities in various fields which he deems fit for the purpose of implementing this Act; and

(b) appoint experts and other consultants on such conditions as the Authority may determine.

77.—(1) The Authority may make recommendations to the Minister in relation to policy on any matter relating to the “.mw” domain name space and any other Malawian names to be used for domain names.

Recommendations relating to domain names

(2) The Authority shall continually evaluate the effectiveness of this Act and the management of the “.mw” domain name space and any other Malawian names to be used for domain names.

(3) The Authority shall, in relation to the “.mw” domain name space and any other Malawian names to be used for domain names existing prior to the coming into force of this Act, uphold the

vested rights and interests of any party involved in the management and administration of the “.mw” domain name space and any other Malawian names to be used for domain names at the date of its establishment:

Provided that—

(a) such party shall be granted a period of six months during which they may continue to operate in respect of their existing delegated sub-domains; and

(b) the Authority may, among other persons, consider the existing registrars for appointment to the post of registrar after the expiry of the six months.

Offence of administering domain name without authority

78. A person who administers, manages or operates second level domain name without authority commits an offence and shall, upon conviction, be liable to a fine of K5,000,000 and to imprisonment for seven years.

Dispute resolution concerning domain names
Cap. 6:03

79. Any unresolved dispute under this Part shall be submitted to arbitration in accordance with the Arbitration Act.

PART IX—ELECTRONIC-GOVERNMENT TRANSACTIONS

Requirement of electronic filing and issuing of documents

80.—(1) A public body shall take steps including entering into an arrangement to ensure that its functions are carried out, delivered or accessed electronically or online in full compliance with internationally recognized best practices.

(2) The Department of E-government shall assist and supervise public bodies in the establishment and delivery of e-government services.

(3) Where a law provides that a public body may—

(a) accept the filing of a document or requires that a document be created or retained;

(b) issue a permit, licence or an approval; or

(c) provide for the making of a payment, the public body may—

(i) accept the document to be filed, created or retained in the form of an electronic message;

(ii) issue the permit, licence or approval in an electronic form; or

(iii) make or receive payment by electronic means.

(4) A public body shall treat as official records, electronic records generated or received by a public body in the course of official duties.

(5) A public body shall maintain electronic records in a reliable record keeping system as defined in regulations made under this Act.

81. The Department of E-government shall, for the purposes of section 80, from time to time, publish guidelines specifying—

Specific guidelines to public bodies

(a) the manner and format in which the electronic message shall be filed, created or retained;

(b) the manner and format in which the permit, licence or approval shall be issued;

(c) where the electronic message has to be signed, the type of digital signature required;

(d) the manner and format in which the digital signature shall be attached to or incorporated into the electronic message;

(e) the appropriate control process and the procedure to ensure adequate integrity, security and confidentiality of an electronic messages or a payment; and

(f) any other requirements in respect of the electronic message or payment.

82. The application of the provisions of this Part shall be subject to the adoption of necessary regulations made by the Minister, which shall establish—

Implementation of e-government

(a) the legal framework to ensure security, storage, confidentiality and integrity of acts and exchanges done by electronic means; and

(b) the legal framework to ensure confidentiality of personal data and guaranteeing inviolability of private life.

PART X—OFFENCES

83.—(1) A court may, on application by a cyber inspector, issue a search warrant.

Search warrant

(2) For the purposes of this section, a court may issue a warrant where—

(a) an offence has been committed in Malawi; or

(b) the subject of an investigation is—

(i) a Malawian or a person ordinarily resident in Malawi;

(ii) present in Malawi at the time when the warrant is applied for; or

(iii) information relevant to an investigation is accessible from within the area of jurisdiction of the court.

(3) A warrant to enter, search and seize may be issued at any time and shall—

(a) identify the premises or information system that may be entered and searched; and

(b) specify which acts may be performed by a cyber inspector in accordance with this Part.

(4) A warrant to enter and search shall be valid—

(a) subject to paragraph (d), until the warrant has been executed;

(b) until the warrant is cancelled by the court which issued it;

(c) until the purpose for issuing the warrant has lapsed; or

(d) until one month has passed from the date on which the warrant was issued.

(5) A warrant to enter and search premises may be executed only during the day, unless the court that issued it authorizes that it may be executed at any other time.

(6) Prohibition of disclosure of information to unauthorized persons shall be governed by the following provisions—

(a) except for the purposes of this Act or for the prosecution of an offence or pursuant to an order of a court, a person who has, pursuant to any powers conferred under this Part, obtained access to any information shall not disclose such information to any other person; and

(b) any person who contravenes paragraph (a), commits an offence and shall, upon conviction, be liable to a fine of K 2,000,000 and to imprisonment for five years.

Unauthorized access, interception or interference with data

84.—(1) A person shall not gain unauthorized access to, or intercept, or interfere with, data.

(2) The Minister shall, by regulations, come up with specific cases where unauthorized access to, or interception of, or interference with, data may be permitted in specific conditions set out in the regulations.

(3) Any person who intentionally accesses or intercepts any data without authority or permission to do so, or who exceeds the authorized access, commits an offence and shall, upon conviction, be liable to a fine of K2,000,000 and to imprisonment for five years.

(4) Any person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, commits an offence and shall, upon conviction, be liable to a fine of K2,000,000 and to imprisonment for five years.

(5) Any person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program, a component or a phone, which is designed primarily to overcome security measures for the protection of data, or performs any of these acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilizing such item, commits an offence and shall, upon conviction, be liable to a fine of K2,000,000 and to imprisonment for five years.

(6) Any person who utilizes any device or computer program referred to in subsection (5) in order to unlawfully overcome security measures designed to protect such data or access thereto, commits an offence and shall, upon conviction, be liable to a fine of K2,000,000 and to imprisonment for five years.

(7) Any person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users commits an offence and shall be liable, upon conviction, to a fine of K2,000,000 and to imprisonment for five years.

(8) Any person who—

(a) communicates, discloses or transmits any data, information, program, access code or command to any person not entitled or authorized to access the data, information, program, code or command;

(b) knowingly introduces or spreads a software code that damages a computer, computer system or network;

(c) accesses or destroys any files, information, computer system or device without authorisation; or for the purposes of concealing information necessary for an investigation into the commission, or otherwise, of an offence; or

(d) damages, deletes, alters suppresses any communication or data without authorisation,

commits an offence and shall, upon conviction, be liable to a fine of K2,000,000, and to imprisonment for five years.

(9) Any person who knowingly receives data which he is not authorized to receive commits an offence and shall, upon conviction, be liable to a fine of K2,000,000 and to imprisonment for five years.

(10) Where an offence under this section is committed in relation to data that is concerned with national security or the provision of an essential service, the person shall, upon conviction, be liable to imprisonment for a term of not less than ten years, but not exceeding fifteen years.

Child
pornography

85.—(1) Child pornography in an electronic form is prohibited under this Act.

(2) Any person who—

(a) produces pornographic material for the purpose of its distribution through a computer system;

(b) reproduces pornographic material for the purpose of its distribution through an information system;

(c) offers or makes available any pornographic material through an information system;

(d) exposes a child to pornographic material through an information system;

(e) distributes or transmits any pornographic material through an information system;

(f) procures any pornographic material through a computer system for oneself or for another person; or

(g) possesses any child pornographic material in a computer system or on a computer data storage medium,

commits an offence and shall, upon conviction, be liable to a fine of K10,000,000 and to imprisonment for fifteen years.

(3) For the sake of protecting children from pornography as provided in subsection (1)—

(a) establishments serving the public, and places open to the public proposing access to internet shall use an adequate pornography filtering software as defined by subsidiary legislation made under this Act;

(b) failure to comply with the obligation provided in this subsection shall be an offence punishable, upon conviction, with a fine of K10,000,000 and to imprisonment for fifteen years.

Prohibition of
cyber
harassment

86. Any person who uses any computer system and continues—

(a) making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent; or

(b) threatening to inflict injury or physical harm to the person or property of any person; or

(c) knowingly permits any electronic communications device to be used for any of the above-mentioned purposes,

commits an offence known as cyber harassment and shall, upon conviction, be liable to a fine of K2,000,000 and to imprisonment for five years.

87. Any person who wilfully and repeatedly uses electronic communication to disturb or attempts to disturb the peace, quietness or right of privacy of any person with no purpose of legitimate communication whether or not a conversation ensues, commits a misdemeanour and shall, upon conviction, be liable to a fine of K1,000,000 and to imprisonment for twelve months.

Prohibition of offensive communication

88. Any person who wilfully, maliciously, and repeatedly uses electronic communication to harass another person and makes a threat with the intent to instil reasonable fear in that person for his safety or to a member of that person’s immediate family, commits an offence known as cyber stalking and shall, upon conviction, be liable to a fine of K1,000,000 and to imprisonment for twelve months.

Prohibition of cyber stalking

89. Any person who hacks into any computer system, or knowingly introduces or spreads a virus into a computer system or network, commits an offence and shall, upon conviction, be liable to a fine of K5,000.00 and to imprisonment for seven years.

Prohibition of hacking, cracking and introduction of viruses

90. Any person who wilfully or maliciously renders a computer system incapable of providing normal services to its legitimate users, commits an offence and shall, upon conviction, be liable to a fine of K5,000,000 and to imprisonment for seven years.

Unlawfully disabling a computer system

91. Any person who transmits any unsolicited electronic information to another person for the purposes of illegal trade or commerce, or other illegal activity, commits an offence and shall, upon conviction, be liable to a fine of K2,000,000 and to imprisonment for five years.

Prohibition of spamming

92. Any person who uses the internet as a medium for any illegal activity or trade, fraudulent transaction or as a means of procuring any internet related fraud, commits an offence and shall, upon conviction, be liable to imprisonment for ten years.

Prohibition of illegal trade and commerce

93.—(1) A person who attempts to commit an offence under any provision of this Act, commits an offence and shall, upon conviction, be liable to a penalty not exceeding one half of the maximum penalty imposable by the provision creating the complete offence.

Attempting, aiding and abetting crime

(2) A person who aids or abets any other person to commit any of the offences under this Act, commits an offence and shall, upon

conviction, be liable to a penalty imposable by the provision creating the offence for actually committing the offence.

(3) The provisions of this section making reference to penalties imposed upon conviction shall apply *mutatis mutandis* to administrative monetary penalties imposable by the Authority under this Act and any regulations made under the Act.

Offences committed by legal persons

94. Where a legal person is convicted of an offence under this Act, every person who—

(a) is a director of, or is otherwise concerned with the management of, the legal person; and

(b) knowingly authorized or permitted the act or omission constituting the offence,

commits the same offence which the legal person is guilty of, and may be proceeded against and be sentenced accordingly.

General offence and penalty

95. A person who violates any provision of this Act, whose penalty has not been provided, commits an offence and shall, upon conviction, be liable to a fine of K5,000,000 and to imprisonment for seven years.

PART XI—GENERAL PROVISIONS

Lodging of complaints to the Authority

96.—(1) Any person affected by a criminal offence defined under this Act may lodge a complaint to the Authority which shall direct a cyber inspector to assess the relevance of the complaint and, if the complaint is considered relevant and reasonable, proceed with investigations.

(2) Any interested organization whose members are affected by a criminal offence defined under this Act is entitled to lodge a complaint with the Authority.

(3) The Authority shall ensure that the complaining organization is kept informed of the investigations.

Public education programmes

97. The Authority shall implement public educational programs on the safe use of internet focusing in particular on—

(a) scope of cybercrimes;

(b) tips on safe cyber experience;

(c) promotion of educational uses of Internet; and

(d) remedies and procedures when affected by cybercrime.

Intermediary services providers' levy

98. For the purposes of implementing the public educational programmes referred to in section 97, the Authority may impose intermediary service providers' levy on intermediary service providers who offer access to communications networks.

99.—(1) In order to promote the development and the use of information technologies and electronic communications in Malawi and contribute to effective application of this Act, professional associations and organizations shall be encouraged to develop codes of conduct.

Codes of
conduct

(2) A code of conduct shall in particular facilitate—

(a) the implementation of self-regulation practices with the assistance of representatives of consumers;

(b) access by consumers to information and advice regarding e-commerce;

(c) the setting up of alternative dispute resolution mechanisms between professionals and consumers at no fee to consumers; and

(d) communication, cooperation, elaboration and effective implementation of joint initiatives between companies, representative consumer associations and the Government to fight against fraudulent, misleading and unfair practices.

(3) A code of conduct shall be notified to the Authority and enter into force upon publication in the *Gazette*.

100. Where any inconsistency arises between a provision of this Act and a provision of any other written law relating to the regulation of electronic transactions, the provisions of this Act shall prevail to the extent of the inconsistency.

Act to prevail
in case of
inconsistency

101. The Authority may in its discretion impose administrative penalties to persons who violate a provision of this Act or the regulations made under it by imposing a fine not exceeding K5,000, 000.

Administrativ
e penalties

102.—(1) The Minister may, in consultation with the Authority, by notice published in the *Gazette*, make regulations for carrying out the purpose and provisions of this Act into effect and prescribing all matters which are necessary or convenient to be prescribed for the better carrying out of the provisions of this Act and, without derogation from the generality of the foregoing, such regulations may provide for—

Regulations

(a) the requirements and standards which registries and the registrar shall meet in order to operate with operational accuracy, stability, robustness and efficiency;

(b) the circumstances and manner in which registrations may be assigned, registered, renewed, refused, or revoked by the registries;

(c) the pricing policy;

(d) the provisions for the restoration of a domain name registration and penalties for late payments;

(e) the terms of the domain name registration agreement which registries and the registrar shall adopt and use in registering domain names, including issues in respect of privacy, consumer protection and alternative dispute resolution;

(f) the processes and procedures to avoid unfair and anticompetitive practices, including bias to, or preferential treatment of actual or prospective registrants, registries or the registrar, protocols or products;

(g) the requirements to ensure that each domain name contains an administrative and technical contact;

(h) the creation of new sub-domains;

(i) the procedures for ensuring the monitoring of compliance with this Act, including compliance with regular “.mw” domain name and any other Malawian names to be used for domain names space technical audits;

(j) any other matter relating to the “.mw” domain name space and any other Malawian names to be used for domain names as may be necessary to achieve the objectives of this Act;

(k) declaring certain classes of information to be critical data;

(l) establishing procedures for identification of database with critical data;

(m) the registration of database with critical data;

(n) prescribing minimum standards regarding management, access to transfer and control of databases with critical data;

(o) the inspection of databases by the Authority; and

(p) any other matter relating to management, protection, recovery and control of databases with critical data.

(2) Notwithstanding section 21 (e) of the General Interpretation Act, the regulations, made under this Act may create offences in respect of any contravention to the regulations, and may for any such contravention impose a fine of up to K5,000,000 and to imprisonment for up to seven years.

103. The Minister may, in consultation with the Authority, by notice published in the *Gazette*, make an order to exempt certain transactions from the application of the requirements of some provisions of this Act. Exemption orders

104. The Minister shall, by order published in the *Gazette*, appoint a date or dates beyond which stakeholders affected by this Act, shall be required to comply with this Act. Transitional provision

Passed in Parliament this fourth day of July, two thousand and sixteen

FIONA KALEMBA
Clerk of Parliament