New Bill
Draft: Cybercrimes and Electronic Evidence Bill, 2024
(Subject to change)
Author: Malawi Communications Regulatory Authority
Date: 6th July, 2024

CYBERCRIMES AND ELECTRONIC EVIDENCE BILL, 2024

MEMORANDUM

This Bill seeks to make provision for criminalizing acts and omissions related to computer systems and information and communication technologies; for procedures for investigation, preservation, collection and use of electronic evidence; for admission, in criminal matters, of electronic evidence; and for facilitating international cooperation in dealing with computer and cybercrimes.

The Bill is divided into six Parts.

Part I provides for preliminary matters, namely; short title, commencement, and interpretation of key words and terms used in the Bill.

Part II provides for various offences, including the offences of unauthorized access, unlawful interception of data, unlawful interference with a computer system, unauthorized interference with a computer program or data, misuse of devices and access codes, child pornography, cyber grooming, cyber harassment, cyber stalking, unlawful use of software and hardware, cyber terrorism, and racist or xenophobic material. The Part also provides for other offences such as attempting, aiding and abetting crime, obstruction of a law enforcement officer or cyber inspection officer. The Part further provides for various penalties for contravention of this Part, and also a general penalty for contravention of any provision of this Act, whose penalty has not specifically been provided in the Act.

Part III provides for procedural powers, including the power to obtain a preservation order, power to demand disclosure of preserved data, powers of access, search and seizure, and powers for real time collection of content or traffic data. The Part also contains provisions relating to non-compliance with an order or notice, scope of procedural powers, obstruction and misuse of power, and provisions on confidentiality and limitation of liability.

Part IV makes provision for admissibility of electronic evidence. The Part further contains provisions on admissibility of evidence based on functional equivalence. The Part provides that in assessing whether evidence is functionally equivalent, the court may take into account a number of factors, including, the reliability and authenticity of the evidence in question, the extent to which the evidence conveys substantially the same information, facts, or substance as the evidence that strictly complies with the prescribed requirements, and the degree to which the evidence maintains the fairness and integrity of the legal proceedings.

Part V contains provisions relating to international cooperation. The Part specifically provides for requests for mutual legal assistance, for expedited preservation of stored data and expedited disclosure of preserved traffic data, for mutual assistance regarding access of stored data, for trans-border access to stored data with consent or where publicly available, for mutual assistance in real time collection of traffic data, and for mutual assistance regarding the interception of data. The Part further provides for the designation of a point of contact to facilitate the provision of, among other things, assistance for purposes of investigations or proceedings concerning criminal offences related to computer systems and data, and for the collection of evidence in electronic form of a criminal offence.

Part VI contains miscellaneous provisions. Specifically, the Part gives the Minister the power to make regulations, on the advice of the Authority, for carrying out or giving effect to the provisions of this Act and for such matters as are envisaged by the provisions of this Act or as the Authority may deem necessary.

CYBERCRIMES AND ELECTRONIC EVIDENCE BILL, 2023

ARRANGEMENT OF SECTIONS

SECTION

PART III — PROCEDURAL POWERS

PART IV - ELECTRONIC EVIDENCE

A BILL

entitled

An Act to make provision for criminalizing acts and omissions related to computer systems and information and communication technologies; for procedures for investigation, preservation, collection and use of electronic evidence; for admission, in criminal matters, of electronic evidence; for facilitating international cooperation in dealing with computer related crimes and cybercrimes; and for matters ancillary thereto or connected therewith.

ENACTED by the Parliament of Malawi as follows —

PART I — PRELIMINARY

Short title and commencement

1. This Act may be cited as the Cybercrimes and Electronic Evidence Act, 2024, and shall come into force on such date as the Minister may appoint by notice published in the Gazette.

Interpretation

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

Cap. 68:01

"Authority" has the meaning ascribed thereto in the Communications Act;

"child pornography" means visual and pornographic material that depicts, presents or represents a –

(a) person under the age of eighteen engaged in sexually explicit conduct;
(b) person appearing to be under the age of eighteen engaged in sexually explicit conduct; or
(c) realistic image representing a person under the age of eighteen engaged in sexually explicit conduct.

"Competent Authority" shall have the meaning ascribed thereto in the Mutual Assistance in Criminal Matters Act; Cap. 8:04

"computer data" means a representation of facts, concepts or information in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

"computer data storage medium" means an apparatus or object from which electronic information is capable of being reproduced, with or without the aid of an article or device;

"computer system" means a device or group of interconnected or related set of integrated devices which, pursuant to a computer program, performs automatic processing of data;

"critical information infrastructure" means the cyber infrastructure that is essential to vital services for public safety, economic stability, national security, international stability and for the sustainability and restoration of critical cyberspace;

"cyber" means the —

(a) computer simulated environment; or

(b) state of connection or association with electronic communication systems or networks including the internet;

"device" includes —

(a) components of computer systems such as graphic cards, memory chips and processors;

(b) storage components such as hard drives, memory cards, compact discs and tapes;

(c) input devices such as keyboards, mouse, trackpad, scanner and digital cameras;

(d) output devices such as printer and screens;

(e) computer program; and

(f) an apparatus which can be used to intercept a wire, oral or electronic communications;

"functional equivalence" means the principle that evidence, which may not strictly conform to the prescribed requirements, may nonetheless be admissible if it serves the same functional purpose as evidence that strictly complies with the specified rules of admissibility; and

“police officer” means a police officer of a rank of sub-inspector and above;

“racist or xenophobic material” includes any image, video, audio recording or any other representation of ideas or theories in electronic form, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent, national or ethnic origin, or religion if used as a pretext for any of these factors; and

“unauthorized” or “without authorization”, in relation to any offence, means any act in relation to a program, computer data or a computer system, if the person doing the act or causing the act to be done -

(a) is not himself a person who has responsibility for the computer system or computer data and is not entitled to determine whether the act may be done; and

(b) does not have consent to do the act from any such person.

PART II — OFFENCES

Unauthorized access

3. - (1) A person who, by himself or another person, intentionally causes, whether temporarily or permanently, a computer system or network to perform a function, by infringing security measures, with intent to secure or gain access to any computer program or computer data held in a computer system, and knowing such access is unauthorized, commits an offence and shall, upon conviction, be liable to a fine of K15,000,000 and to imprisonment for fifteen years.

(2) Access by a person to a computer system or network is unauthorized if the person —

(a) is not entitled to control access of the kind in question to the program or data; or

(b) does not have consent from any person who is entitled to access the computer system through any function to the program or data.

(3) For purposes of subsection (1), a person secures access to a computer program or computer data held in a computer system if by causing the computer system to perform a function, the person -

(a) alters or erases the computer program or computer data;

(b) copies or moves it to any computer data storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses it; or

(d) has it output from the computer system in which it is held, whether by having it displayed or in any other manner.

(4) For purposes of subsection (3) (c), a person uses a computer program if the function he causes the computer system to perform —

(a) causes the computer program to be executed; or

(b) is itself a function of the computer program.

(5) For purposes of subsection (3) (d), the form in which any program or data is output, and in particular, whether or not it represents a form in which, in the case of a program, it is capable of being executed or, in the case of data, it is capable of being processed by a computer, is immaterial.

Access with intent to commit further offence

4. - (1) A person who commits an offence under section 3 with intent to commit a further offence under any law, or to facilitate the commission of a further offence by that person or any other person, commits an offence and shall, upon conviction, be liable to a fine of K15,000,000 and to imprisonment for fifteen years.

(2) For the purposes of subsection (1), it is immaterial that the further offence to which this section applies is committed at the same time when the access is secured or at any other time.

Unlawful interception of data

5. - (1) A person who intentionally and without authority commits unauthorized interception of non-public transmissions of computer data, including electromagnetic emissions from a computer system carrying such data, to, from or within or which is transmitted to or from a computer system through technical means, commits an offence and shall, upon conviction, be liable to a fine of K10,000,000 and to imprisonment for ten years.

(2) A person who intentionally and without authorization possesses data, with the knowledge that such data was obtained by the commission of an offence under this Part, commits an offence and shall, upon conviction, be liable to a fine of K10,000,000 and to imprisonment for ten years.

Unlawful interference with a computer system

6. – (1) A person who, intentionally does any act which causes unauthorized interference with a computer system commits an offence and shall, upon conviction, be liable to a fine of K5,000,000 and to imprisonment for five years.

(2) For purposes of subsection (1), interference with a computer system means to -

(a) interfere, hinder, damage, prevent, suppress, deteriorate, impair or obstruct the functioning of a computer system;

(b) interfere, hinder, damage, prevent, suppress, deteriorate, impair or obstruct communication between or with a computer system;

(c) interfere with or hinder access to any computer system;

(d) impair the operation of any computer system;

(e) impair the reliability of any computer system;

(f) impair the security of any computer system; or

(g) enable any of the things mentioned in subsection (a) to (f) to be done.

Unauthorized interference with a computer program or data

7. - (1) A person who, intentionally and without authority, does any act which causes an unauthorized interference with a computer program or computer data, commits an offence and shall, upon conviction, be liable to a fine of K5,000,000 and to imprisonment for five years.

(2) For purposes of subsection (1), "interference with a computer program or computer data" means to permanently or temporarily —

(a) delete a computer program or computer data;

(b) alter a computer program or computer data;

(c) copy a computer program or computer data;

(d) suppress a computer program or computer data;

(e) render vulnerable, damage or deteriorate a computer program or computer data;

(f) render a computer program or computer data meaningless, useless or ineffective;

(g) obstruct, interrupt or interfere with the lawful use of, a computer program or computer data;

(h) deny or hinder access to a computer program or computer data, held in a computer data storage medium or a computer system; or

(i) enable any of the things mentioned in subsections (a) to (h) to be done.

Misuse of devices and access codes

8. - (1) A person who knowingly manufactures, adapts, sells, procures for use, imports, offers to supply, distributes or otherwise makes available a device, computer password, access code or similar data designed or adapted primarily for the purpose of committing any offence under this Part, commits an offence and shall, upon conviction, be liable to a fine of K10,000,000 and to imprisonment for ten years.

(2) Notwithstanding subsection (1), the activities described under subsection (1) do not constitute an offence if —

(a) the act is intended for the authorized training, testing or protection of a computer system; or

(b) the use of a program or a computer password, access code, or similar data is undertaken in compliance of and in accordance with a court order or in exercise of any power under this Act or any law.

(3) For purposes of subsection (1), possession of any program or a computer password, access code, or similar data includes having —

(a) possession of a computer system which contains the program or a computer password, access code, or similar data;

(b) possession of a data storage device in which the program or a computer password, access code, or similar data is recorded; or

(c) control of a program or a computer password, access code, or similar data that is in the possession of another person.

Child pornography

9. - (1) A person who intentionally –

(a) uses a computer system to produce child pornographic material;

(b) reproduces child pornographic material for the purpose of its distribution through a computer system;

(c) sells, facilitates, offers or makes available any child pornographic material through a computer system;

(d) distributes or transmits any child pornographic material through a computer system;

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

(f) 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 K15,000,000 and to imprisonment for fifteen years.

(2) Subsection (1) shall not apply to a person performing a bona fide law enforcement function.

(3) When prosecuting an offence under this Section, it is a defence for a person older than 14 years of age, and under 18 years of age, to evidence that the production or possession of pornographic material concerning another minor above 14 years, and under 18 years of age, was done with the consent of all parties and was solely for their personal use.

(4) A person providing services of access to a computer system to the public shall use pornography filtering measures.

(5) A person who fails to comply with subsection (4) commits an offence and shall, upon conviction, be liable to a fine of K5,000,000 and to imprisonment for five years.

Cyber grooming

10. A person who, intentionally -

(a) uses a computer system to meet a child for the purpose of committing a sexual related offence;

(b) communicates with a child through a computer system for the purpose of making it easier to procure the child to engage in sexual activity with that person;

(c) attracts a child for the purpose of making it easier to procure the child to engage in sexual activity with that person;

(d) attracts a child for the purpose of making it easier to procure the child to engage in sexual activity with another person;

(e) compels, invites or allows a child to view pornographic material through a computer system;

(f) recruits a child to participate in a pornographic performance that is intended to be produced or recorded through a computer system or computer network with or without the intent to distribute such material; or

(g) communicates, attracts, compels, invites or does anything with a child through a computer system for any other illegal purposes,

commits an offence and shall, upon conviction, be liable to a fine of K50,000,000 and to imprisonment for twenty years.

Revenge pornography

11. – (1) A person who, by means of a computer system, discloses or publishes sexual content without the consent of the person who appears in the content, and with the intention of causing that person distress, commits an offence and shall, upon conviction, be liable to a fine of K15,000,000 and to imprisonment for fifteen years.

Cyber harassment

12. A person who intentionally uses any computer system to initiate any electronic communication with the intent to coerce, intimidate, harass or cause emotional distress to a person, commits an offence and shall, upon conviction, be liable to a fine of K5,000,000 and to imprisonment for five years.

Offensive communication

13. A person who intentionally 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.

Cyber stalking

14. A person who maliciously and repeatedly uses electronic communication to harass another person and makes a threat with the intent to instill fear in that person for his safety or to a member of that person's immediate family, commits an offence and shall, upon conviction, be liable to a fine of K1,000,000 and to imprisonment for twelve months.

Unlawful use of software and hardware

15. A person who, intentionally and without authority, introduces or spreads a computer program referred to under section 7 (1) into a computer system, commits an offence and shall, upon conviction, be liable to a fine of K5,000.000 and to imprisonment for five years.

Cyber terrorism

16. - (1) A person who intentionally commits any offence in this Part in relation to any critical information infrastructure commits an offence and shall, upon conviction, be liable to imprisonment for life.

(2) A person who commits the offence under subsection (1) with the intent to intimidate or coerce a government or its people in furtherance of political or social objectives, and to cause severe disruption or widespread fear in society, uses or causes to be used a computer system for the purposes of cyber terrorism commits an offence and shall, upon conviction, be liable to imprisonment for life.

Intentionally withholding message delivered erroneously

17. A person who intentionally hides or detains any electronic mail, message, electronic payment, credit and debit card which was found by the person or delivered to the person in error and which ought to be delivered to another person, commits an offence and shall, upon conviction, be liable to a fine of K5,000,000 and imprisonment for five years.

Identity related crimes

18. A person who, intentionally and without authority, using a computer system, transfers, possesses, or uses, a means of identification of another person, commits an offence and shall, upon conviction, be liable to a fine of K10,000,000 and to imprisonment for ten years.

Cyber forgery

19. - (1) A person who, intentionally and without authorization inputs, alters, deletes or suppresses computer data, resulting in unauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible, commits an offence and shall, upon conviction, be liable to a fine of K10,000,000 and to imprisonment for five years.

(2) A person who commits an offence under subsection (1), dishonestly or with similar intent —

(a) for wrongful gain;

(b) for wrongful loss to another person; or

(c) for any economic benefit for oneself or for another person,

shall, upon conviction, be liable to a fine of K20,000,000 and to imprisonment for ten years.

Cyber fraud

20. - (1) A person who, with fraudulent or dishonest intent, and without authorization —

(a) occasions loss to another person; or

(b) obtains an economic benefit for oneself or for another person, through any of the means described under subsection (2),

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

(2) For purposes of subsection (1), the word "means" refers to —

(a) any input, alteration, modification, deletion, suppression or generation of any program or data;

(b) any interference, hindrance, impairment or obstruction with the functioning of a computer system;

(c) copying, transferring or moving any data or program to any computer system, data or computer data storage medium other than that in which it is held or to a different location in any other computer system, program, data or computer data storage medium in which it is held; or

(d) use of any data or program, or any data or program output from the computer system in which it is held, by having it displayed in any manner.

Publication of information or data

21. A person who, with intent to compromise the finances, safety or security of any other person, publishes information or data presented in a picture, image, text, symbol, voice or any other form in a computer system, commits an offence and shall, upon conviction, be liable to a fine of K10,000,000 and to imprisonment for ten years.

Publication of false information

22. – (1) A person who knowingly publishes information that is false in print, broadcast, data or over a computer system, that is calculated or results in panic, chaos, or violence, or which is likely to discredit the reputation of a person, commits an offence and shall, upon conviction, be liable to a fine of K10,000,000 and to imprisonment for ten years.

(2) Notwithstanding section 35 of the Constitution, freedom of expression shall be limited in respect of the intentional publication of false, misleading or fictitious data, or misinformation, that is likely to -

(a) propagate war;

(b) incite persons to violence and damage to property;

(c) constitute hate speech;

(d) advocate hatred that constitutes ethnic incitement, vilification of others or incitement to cause harm, or is based on any ground of discrimination specified under section 20 of the Constitution;

(e) negatively affect the rights or reputation of others; or

(f) be prejudicial to the vital interests of the country.

Prohibition of use of computer system for offences

23. - (1) A person shall not use a computer system for any activity which constitutes an offence under any written law and which is not provided under this Act.

(2) A person who contravenes subsection (1) commits an offence and shall, upon conviction, be liable to the punishment specified for that offence in the applicable written law.

Minimization, etc., of genocide and crimes against humanity

24. A person who, knowingly and without authority, distributes or otherwise makes available, through a computer system to the public or another person, material which denies, grossly minimizes, approves or justifies acts constituting genocide or crimes against humanity, commits an offence and shall, upon conviction, be liable to imprisonment for life.

Unlawful disclosure of details of investigation

25. A person who knowingly receives an order related to a criminal investigation and without authority discloses —

(a) the fact that an order has been made;

(b) anything done under the order; or

(c) any data collected or recorded under the order,

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

Racist or xenophobic material

26. A person who, by means of a computer system —

(a) produces racist or xenophobic material;

(b) offers or makes available racist or xenophobic material; or

(c) distributes or transmits racist or xenophobic material,

commits an offence and shall, upon conviction, be liable to a fine of K20,000,000 and imprisonment for ten years.

Racist xenophobic motivated insult

27. A person who, by means of a computer system, insults another person on the basis of race, colour, descent, nationality, ethnic origin, tribe or religion, commits an offence and shall, upon conviction, be liable to a fine of K20,000,000 and imprisonment for ten years.

Offences committed by legal persons

28. – (1) 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 punished and sentenced accordingly.

(2) If any person referred to in subsection (1) commits an offence under this Act for the benefit of a legal person, the legal person may be punished and sentenced with the fine prescribed under the offence.

Attempting, aiding and abetting crime

29. - (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 punishment not exceeding one half of the maximum punishment imposed by the provision creating the complete offence.

(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 punishment imposed by the provision creating the offence for actually committing the offence.

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

Obstruction of a law enforcement officer or cyber inspection officer

30. A person who obstructs or hinders a law enforcement officer, a cyber inspector or any person in the exercise of any powers under this Act, or who neglects or fails to comply with an order, commits an offence and shall, upon conviction, be liable to a fine of K5,000,000 and imprisonment for two years.

Aggravated offences

31. A person who commits an offence under this Part which —

(a) results in a significant financial loss;

(b) damages or compromises critical information infrastructure;

(c) damages or compromises designated critical sites and facilities;

(d) threatens national security;

(e) causes physical or psychological injury or death to any person;

(f) threatens public health or public safety; or

(g) threatens the vital interests of the State.

commits an offence and shall, upon conviction, be liable to a fine of K50,000,000 and to imprisonment for life.

General offence and penalty

32. A person who contravenes 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 five years.

PART III — PROCEDURAL POWERS

Preservation notice

33. - (1) A competent authority may, by a written notice given to a person in possession or control of stored computer data, require the person to ensure that the data specified in the notice is preserved against any modification or deletion, for the period specified in the notice.

(2) The notice referred to under subsection (1) may be issued by the competent authority for a period of up to ninety days and shall be in the form set out in the Schedule.

(3) A competent authority may apply before a Chief Resident Magistrate Court for an extension of the notice issued under subsection (1), and the court may extend the notice for a further period of ninety days.

(4) For purposes of this Part, "competent authority" means, where appropriate, the Office of the Director of Public Prosecutions, the Anti-Corruption Bureau, the Financial

Intelligence Authority, the Reserve Bank of Malawi, the Office of the Registrar General, an immigration officer, a revenue officer and a police officer of the rank of inspector and above, and includes any person the Minister may, by notice published in the Gazette, designate.

Disclosure of preserved data

34. When a notice under section 33 is served on a service provider in relation to traffic data, the service provider shall, upon the competent authority's written request, immediately disclose to the competent authority sufficient traffic data about a specified communication to identify other service providers and the path through which the data was transmitted.

Production order

35. - (1) Where a competent authority has reasonable grounds to believe that stored data or information would be relevant for purposes of an investigation or prosecution of an offence, the competent authority may apply to a court for an order compelling -

(a) a person to submit specified data in his possession or control, which is stored in a computer system; or
(b) a service provider offering its services in Malawi to submit subscriber information in relation to its services in the service provider's possession or control.

(2) Where the data in subsection (1) consists of data stored in an electronic form on a device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

(3) A court may issue a production order if, on application made by a competent authority, the court is satisfied that there are reasonable grounds for believing that—

(a) an offence has been committed;
(b) there is computer data in the possession or control of a person specified in the application which is likely to be of substantial value, whether by itself or together with other material, to the investigation of the offence; and

(c) the computer data in question does not consist of or include items subject to legal privileges.

(4) For purposes of this section, "court" means a court of Resident Magistrate and above.

Access, search and seizure

36. - (1) Where a police officer has reasonable grounds to believe that there may be in a computer system, or part of it, or in a computer data storage medium, stored data that is relevant for purposes of an investigation or prosecution of an offence, he may apply to a court for an order authorizing him to enter any premises where such data might be stored and to access, search and seize it.

(2) Where a police officer applies for an access, search and seizure warrant, he shall—

(a) state the ground on which he makes the application and the law under which the warrant will be issued;

(b) specify the premises where, or the person in whose possession, a specified computer system, or part of it, or a computer data storage medium, may be found;

(c) identify, so far as it is practicable, the data to be sought; and

(d) explain to the court why, in his opinion, a production order may not be practicable or may frustrate an investigation or prosecution.

(3) An application for an order of access, search and seizure shall be made ex-parte, and shall be supported by a sworn statement.

(4) A court may issue an order for access, search and seizure if, on application made by a police officer, the court is satisfied that there are reasonable grounds for believing that—

(a) an offence has been committed;

(b) there is stored computer data which is likely to be of substantial value, whether by itself or together with other material, to an investigation of the offence;

(c) the computer data in question does not consist of or include items subject to legal privileges; and

(d) using a production order is not practicable or may frustrate the investigation or prosecution.

(5) A court order issued under subsection (4) shall —

(a) identify the police officer;

(b) identify the premises where or the person in whose possession a specified computer system, or part of it, or a computer data storage medium, may be found;

(c) identify, so far as it is practicable, the data to be sought; and

(d) authorize the police officer to -

(i) search any person identified in the order;

(ii) enter and search any premises identified in the order; and

(iii) search a computer system, or parts of it, or a computer data storage medium, found in the premises or in possession of a person identified in the order.

(6) A police officer shall, in the execution of an order issued under subsection (4), have the power to -

(a) seize or secure a computer system or computer data storage medium in which the data sought may be stored;

(b) make and retain a copy of such data;

(c) maintain the integrity of the relevant stored data;

(d) print, photograph, copy or make in any other manner for the purpose of maintaining the integrity of the relevant stored data; or

(e) render inaccessible or remove the stored data from the computer system or computer data storage medium.

(7) A police officer shall, in the execution of an order issued under subsection (4), be authorized to -

(a) access and search, and

(b) apply the powers in subsection (6) paragraphs (b), (c), (d) and (e) in relation to computer data stored in any other computer system or part of it, or computer data storage medium which is accessible from or available to the system which is the subject of an order under subsection (4).

(8) A police officer may, in the execution of an order issued under subsection (4), order any person who has knowledge about the functioning of the computer system or the measures used to protect the data contained therein, to provide, as is reasonable, the necessary data and information, and to otherwise provide reasonable assistance, to enable the undertaking of the measures provided under subsection (6).

Real time collection of content or traffic data

37. Where traffic data or content data associated with specific communications are necessary for the purposes of an investigation or the prosecution of an offence, a police officer may apply to a court, ex-parte, for an order -

(a) for the collection or recording of the traffic data or content, in real time, associated with specified communications transmitted by means of a computer system; or

(b) compelling a service provider, within its technical capabilities, to -

(i) effect the collection or recording referred to in paragraph (a), or

(ii) assist the person making the application to effect the collection or recording.

Scope of an order

38. - (1) An order under section 37 may relate to a person who is —

(a) suspected of committing, or of attempting to commit, a serious offence as defined in subsection 2;

(b) aiding or abetting the commission of a serious offence as defined in subsection 2; or

(c) receiving or transmitting messages intended for or originating from a person referred to in paragraph (a) or (b), or allowing the person to use his communication devices.

(2) For purposes of this section, a "serious offence" means any offence that attracts a minimum punishment of five years imprisonment.

Detection, prevention and investigation of serious offences

39. - (1) A police officer may apply for an order under section 37 where he has reasonable grounds to believe that traffic data or content data associated with a person specified in section 38 is necessary for the purposes of detecting, preventing or investigating a serious offence.

(2) Where a police officer applies for an order under section 37, he shall —

(a) specify the purpose for which the order is sought, and explain the factual circumstances of the offence in respect of which the order is sought;

(b) identify the persons, to the extent that they are known and in any case as precisely as possible, and explain how the conditions under section 38 are satisfied;

(c) identify the type of communication subject to the order and give as precise information as possible about the telephone number, internet access point or any other identifier of the connection or the end device in relation to which the order is to be applied;

(d) state whether the order is requested for -

(i) collection or recording of traffic data;

(ii) collection or recording of content data; or

(iii) both;

(e) specify the period for which the collection or recording of traffic or content data is requested; and

(f) explain why what is sought cannot reasonably be achieved by using less intrusive means, and this may include elaborating whether any other investigative procedures have been tried and have failed, or are unlikely to succeed, or whether

the urgency of the matter is such that it would be impracticable to carry out the investigation using any other investigative procedure.

(3) An application for an order under this section shall be supported by a sworn statement.

Issuance of court order

40. - (1) The Resident Magistrate may issue an order under section 39 if, on application made by a police officer, he is satisfied that—

(a) there are reasonable grounds for believing that a serious offence has been committed or is being attempted or planned;

(b) collection or recoding of traffic or content data associated with persons specified in section 38 is likely to be of substantial value, whether by itself or together with other material, for the detection, prevention or investigation of that offence;

(c) the data in question does not consist of or include items subject to legal privileges; and

(d) the collection or recording of the traffic or content data is necessary and cannot be reasonably achieved by less intrusive means.

(2) The order shall be in writing, and it shall include -

(a) the person to whom the order is addressed;

(b) the name and address of the person against whom the measure is directed, where known;

(c) the alleged serious offence, on the basis of which the measure is being ordered;

(d) the telephone number, internet access point or any other identifier of the connection or the end device in relation to which the order is to be applied;

(e) whether the order authorizes -

(i) collection or recording of traffic data;

(ii) collection or recording of content data; or

(iii)both; and

(f) the validity period of the order.

Deletion order

41. The Director of Public Prosecutions or any person authorized by him, in writing, may apply to a court for an order that data in a computer system or any device that stores data which contains pornography, obscene material or child pornography be -

(a) no longer stored on and made available through the computer system or other device; or

(b) deleted or destroyed.

Acting without an order

42. - (1) A police officer may carry out the powers conferred on him under this Act without applying for an order under this Act if such application would result in an undue delay in the investigation of any offence under this Act.

(2) Where a police officer exercises the powers under subsection (1), he shall, within 48 hours thereafter, obtain an appropriate order from the court.

(3) If the police officer does not obtain an appropriate order from the court within 48 hours since the moment when he started applying the power under subsection (1) -

(a) the police officer must ensure that anything in the process of being done under subsection stops immediately;

(b) the police officer must destroy all material which was obtained on the basis of acting under subsection (1), and, in any case;

(c) whatever material was obtained in a procedure under subsection (1) will not be admissible as evidence.

Limited use of disclosed data and information

43. - (1) Data obtained under this Act by a police officer shall be used for the purpose for which the data was originally sought, unless such data is sought in -

(a) accordance with any other written law;

(b) compliance with an order of court;

(c) the prevention of injury or other damage to the health of a person or serious loss of or damage to property; or

(d) the public interest.

(2) Subject to subsection (3), on receipt of a request, in writing, a police officer shall permit a person who had the custody or control of a computer system to access and copy data on the computer system.

(3) A police officer may refuse to give access to data or provide copies of such data if he has reasonable grounds for believing that the giving of access or the provision of copies -

(a) would constitute a criminal offence; or

(b) would prejudice -

(i) the investigation in connection with which the search was carried out;

(ii) another ongoing investigation; or

(iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations.

Non-compliance with order or notice

44. A person who fails to comply with an order or notice issued under this Part commits an offence and shall, upon conviction, be liable to a fine of K10,000,000 and to imprisonment for two years.

Scope of procedural powers

45. - (1) All powers and procedures under this Act are applicable to and may be exercised with respect to any —

(a) criminal offences provided under this Act;

(b) other criminal offences committed by means of a computer system established under any other written law; and

(c) the collection of evidence in electronic form of a criminal offence under this Act or any other written law.

(2) In any proceedings related to any offence under any written law in Malawi, the fact that evidence has been generated, transmitted or seized from, or identified in a search of a

computer system, shall not of itself prevent that evidence from being presented, relied upon or admitted.

(3) The powers and procedures provided under this Part are without prejudice to the powers granted under -

No. 30 of 2018
Cap. 13:01
Cap. 12:01

(a) the National Intelligence Service Act;

(b) the Police Act;

(c) the Defence Force Act; and

(d) any other relevant law.

Obstruction and misuse of power

46. - (1) A person who intentionally –

(a) obstructs the lawful exercise of the powers under this Part; or

(b) destroys data,

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

(2) A police officer who misuses the exercise of powers under this Part commits an offence and shall, upon conviction, be liable to a fine of K10,000,000 and to imprisonment for five years.

Confidentiality and limitation of liability

47. - (1) A service provider shall not be subject to any civil or criminal liability, unless it is established that the service provider had actual notice, actual knowledge, or willful and malicious intent, and not merely through omission or failure to act, had thereby facilitated, aided or abetted the use by any person of any computer system controlled or managed by the service provider in connection with a contravention of this Act or any other written law.

(2) A service provider shall not be liable under this Act or any other written law for the disclosure of any data that the service provider discloses only to the extent required under this Act or in compliance with the exercise of powers under this Part.

PART IV - ELECTRONIC EVIDENCE

Admissibility of electronic evidence

48. - (1) In any criminal proceedings, the rules of evidence shall not be applied so as to deny the admissibility of a data message in evidence -

(a) on the mere grounds that it is constituted by a data message; or

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message shall be given due evidential weight.

(3) In assessing the evidential weight of a data message, regard shall be had to –

(a) the reliability of the manner in which the integrity of the data message was generated, stored or communicated;

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

(c) functional equivalence;

(d) the manner in which its originator was identified; and

(e) any other relevant factor.

Admissibility based on functional equivalence

49. – (1) The determination of functional equivalence shall be made at the discretion of the presiding court, taking into consideration the probative value, relevance and the overall interests of justice.

(2) In assessing whether evidence is functionally equivalent, the following factors may be considered –

(a) the reliability and authenticity of the evidence in question;

(b) the extent to which the evidence conveys substantially the same information, facts, or substance as the evidence that strictly complies with the prescribed requirements;

(c) the degree to which the evidence maintains the fairness and integrity of the legal proceedings; or

(d) any other relevant factors that the court may deem appropriate.

PART V — INTERNATIONAL CO-OPERATION

Requests for mutual legal assistance

50. - (1) This Part shall apply in addition to the Mutual Assistance in Criminal Matters Act and the Extradition Act.

Cap. 8:04
Cap. 8:03

(2) The Competent Authority may make a request for mutual legal assistance in any criminal matter to a requested State for purposes of -

(a) undertaking investigations or proceedings concerning offences related to computer systems or data;

(b) collecting evidence in electronic form; or

(c) obtaining expeditious preservation and disclosure of traffic data, real-time collection of traffic data associated with specified communications, or interception of content data or any other means.

(3) A requesting State may make a request for mutual legal assistance to the Competent Authority in any criminal matter, for the purposes provided in subsection (2).

Cap. 8:04
Cap. 8:03

(4) Where a request has been received under subsection (3), the Competent Authority may, subject to the provisions of the Mutual Assistance in Criminal Matters Act, the Extradition Act, this Act or any other written law –

(a) grant the legal assistance requested; or

(b) refuse to grant the legal assistance requested.

(5) The Competent Authority may require a requesting State to –

(a) keep the data or any information provided pursuant to this Part in a confidential manner;

(b) only use the data or the information provided for the purpose of the criminal matter specified in the request; and

(c) use the data or the information subject to any other specified conditions.

Spontaneous information

51. - (1) The Competent Authority may, subject to this Act and any other written law, without prior request, forward to a foreign State information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the foreign State in initiating or carrying out investigations or proceedings concerning criminal offences, or might lead to a request for co-operation by the foreign State under this Act.

(2) Prior to providing the information under subsection (1), the Competent Authority may request that such information be kept confidential or subject to any other specified conditions.

(3) Where a foreign State cannot comply with the specified conditions specified under subsection (2), the State shall notify the Competent Authority as soon as practicable.

(4) Upon receipt of a notice under subsection (3), the Competent Authority may determine whether to provide such information or not.

(5) Where the foreign State accepts the information subject to the conditions specified by the Competent Authority under subsection (2), that State shall be bound by them.

Expedited preservation of stored data

52. - (1) Subject to section 50, a requesting State which has the intention to make a request for mutual legal assistance for the search or similar access, seizure or similar securing or the disclosure of data, may request the Competent Authority to obtain the expeditious preservation of data stored by means of a computer system, located within Malawi.

(2) When making a request under subsection (1), the requesting State shall specify –

(a) the authority seeking the preservation;

(b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

(c) the stored data to be preserved and its connection to the offence;

(d) any available information identifying the custodian of the stored data or the location of the computer system;

(e) the necessity of the preservation; and

(f) the intention to submit a request for mutual assistance for the search or similar access, seizure or similar securing or the disclosure of the stored data.

(3) Upon receiving the request under this section, the Competent Authority shall take the appropriate measures to preserve the specified data in accordance with the procedures and powers provided under this Act and any other written law.

(4) A preservation of stored data effected under this section shall be for a period of not less than one hundred and twenty days, in order to enable the requesting State to submit a request for the search or access, seizure or securing, or the disclosure of the data.

(5) Upon receipt for a request for preservation of data under this section, the data shall continue to be preserved pending the final decision being made with regard to the request for mutual legal assistance under section 50.

Expedited disclosure of preserved traffic data

53. Where, during the course of executing a request under section 50 with respect to a specified communication, the investigating agency discovers that a service provider in another State was involved in the transmission of the communication, the Competent Authority shall expeditiously disclose to the requesting State a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

Mutual assistance regarding access of stored data

54. - (1) Subject to section 50, a requesting State may request the Competent Authority to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within Malawi, including data that has been preserved in accordance with section 52.

(2) When making a request under subsection (1), the requesting State shall –

(a) give the name of the authority conducting the investigation or proceedings to which the request relates;

(b) give a description of the nature of the criminal matter and a statement setting out a summary of the relevant facts and laws;

(c) give a description of the purpose of the request and of the nature of the assistance being sought;

(d) in the case of a request to restrain or confiscate assets believed on reasonable grounds to be located in the requested State, give details of the offence in question, particulars of the investigation or proceeding commenced in respect of the offence, and be accompanied by a copy of any relevant restraining or confiscation order;

(e) give details of any procedure that the requesting State wishes to be followed by the requested State in giving effect to the request, particularly in the case of a request to take evidence;

(f) include a statement setting out any wishes of the requesting State concerning any confidentiality relating to the request and the reasons for those wishes;

(g) give details of the period within which the requesting State wishes the request to be complied with;

(h) where applicable, give details of the property, computer, computer system or electronic device to be traced, restrained, seized or confiscated, and of the grounds for believing that the property is believed to be in the requested State;

(i) give details of the stored computer data, data or program to be seized and its relationship to the offence;

(j) give any available information identifying the custodian of the stored computer data or the location of the computer system or any device that can store data;

(k) include an agreement on the question of the payment of the damages or costs of fulfilling the request; and

(1) give any other information that may assist in giving effect to the request.

(3) Upon receiving the request under this section, the Competent Authority shall take all appropriate measures to obtain necessary authorization including any warrants to execute

upon the request in accordance with the procedures and powers provided under this Act and any other written law.

(4) Where the Competent Authority obtains the necessary authorization in accordance with subsection (3), including any warrants to execute the request, the Competent Authority may seek the support and cooperation of the requesting State during such search and seizure.

(5) Upon conducting the search and seizure request, the Competent Authority shall, subject to section 52, provide the results of the search and seizure as well as electronic or physical evidence seized to the requesting State.

Trans-border access to stored data with consent or where publicly available

55. A police officer may, subject to any applicable provisions of this Act -

(a) access publicly available stored data, regardless of where the data is located geographically; or

(b) access or receive, through a computer system in Malawi, stored data located in another country, if such police officer obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data through that computer system.

Mutual assistance in real time collection of traffic data

56. - (1) Subject to section 50, a requesting State may request the Competent Authority to provide assistance in real-time collection of traffic data associated with specified communications in Malawi transmitted by means of a computer system.

(2) When making a request under subsection (1), the requesting State shall specify -

(a) the authority seeking the use of powers under this section;

(b) the offence that is the subject of a criminal investigation or proceeding and a brief summary of the related facts;

(c) the name of the authority with access to the relevant traffic data;

(d) the location at which the traffic data may be held;

(e) the intended purpose for the required traffic data;

(f) sufficient information to identify the traffic data;

(g) any further details relevant to the traffic data;

(h) the necessity for use of powers under this section; and

(i) the terms for the use and disclosure of the traffic data to third parties.

(3) Upon receiving the request under this section, the Competent Authority shall take all appropriate measures to obtain necessary authorization including any warrants to execute upon the request in accordance with the procedures and powers provided under this Act and any other written law.

(4) Where the Competent Authority obtains the necessary authorization, including any warrants to execute upon the request, the Competent Authority may seek the support and cooperation of the requesting State during the search and seizure.

(5) Upon conducting the measures under this section, the Competent Authority shall, subject to section 50, provide the results of such measures as well as real-time collection of traffic data associated with specified communications to the requesting State.

Mutual assistance regarding the interception of data

57. - (1) Subject to section 50, a requesting State may request the Competent Authority to provide assistance by intercepting specified communication in Malawi transmitted by means of a computer system.

(2) When making a request under subsection (1), the requesting State shall specify –

(a) the authority seeking the use of powers under this section;

(b) the offence that is the subject of a criminal investigation or proceeding and a brief summary of the related facts;

(c) the name of the authority with access to the relevant communication;

(d) the nature of the communication;

(e) the location of the communication;

(f) the intended purpose for the required communication;

(g) sufficient information to identify the communication;

(h) details of the data of the relevant interception;

(i) the recipient of the communication;

(j) the intended duration for the use of the communication;

(k) the necessity for use of powers under this section; and

(l) the terms for the use and disclosure of the communication to third parties.

(3) Upon receiving the request under this section, the Competent Authority shall take all appropriate measures to obtain necessary authorization including any warrants to execute upon the request in accordance with the procedures and powers provided under this Act or any other written law.

(4) Where the Competent Authority obtains the necessary authorization, including any warrants to execute upon the request, the Competent Authority may seek the support and cooperation of the requesting State during the search and seizure.

(5) Upon conducting the measures under this section, the Competent Authority shall, subject to section 50, provide the results of such measures and the interception of the specified communication to the requesting State.

(6) For purposes of this Part, interception means "real-time collection or recording of content data".

Point of contact

58. - (1) The Competent Authority shall ensure that the agency responsible for investigating cybercrime, shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence, including carrying out the following measures –

(a) the provision of technical advice;

(b) the preservation of data pursuant to section 55; and

(c) the collection of evidence, the provision of legal information, and locating of suspects, within expeditious timelines to be defined by regulations under this Act.

(2) The point of contact shall be resourced with and possess the requisite capacity to securely and efficiently carry out communications with other points of contact in other countries, on an expedited basis.

(3) The point of contact shall have the authority and be empowered to coordinate and enable access to international mutual assistance under this Act.

PART VI — MISCELLANEOUS

Regulations

59. The Minister may, on the advice of the Authority, make regulations for carrying out or giving effect to the provisions of this Act and for such matters as are envisaged by the provisions of this Act or as the Authority may deem necessary.

SCHEDULE (section 33)

PRESERVATION NOTICE

OBJECTS AND REASONS

The object of this Bill is to provide for a comphrehensive legal framework for criminal acts and omissions committed in the cyberspace or using a computer, and provide for procedural powers related to the investigation of the offences and for international cooperation on cybercrimes.

Thabo Chakaka Nyirenda
Attorney General