New Bill
Draft: Cybercrimes Bill, 2023
(Subject to change)
Author: Malawi Communications Regulatory Authority
Date: 15th November, 2023

CYBERCRIMES BILL, 2023

MEMORANDUM

This Bill seeks to make provision for criminalizing offences 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 acts in respect of software or hardware, unlawful use of software and hardware, cyber terrorism, 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 inspector 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 BILL, 2023

ARRANGEMENT OF SECTIONS

SECTION

PART I — PRELIMINARY

PART II — OFFENCES

PART IV - ELECTRONIC EVIDENCE

PART V — INTERNATIONAL CO-OPERATION

PART VI — MISCELLANEOUS

A BILL

entitled

An Act to make provision for criminalizing offences 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 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 Act, 2023, 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;

Cap. 8:04

"Competent Authority" means the appropriate authority designated pursuant to section 4 of the Mutual Assistance in Criminal Matters Act;

"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 set of integrated devices that input, output, process, and store data and information including internet;

“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; and

(e) 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;

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

"racist or xenophobic material" includes any image, video, audio recording or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin.

PART II — OFFENCES

Unauthorized access

3. - (1) A person who by himself or another person causes, whether temporarily or permanently, a computer system or network to perform a function, by infringing security measures, with intent to gain access, 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 —

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

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

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, intercepts data, including electromagnetic emissions from a computer system carrying such data, within or which is transmitted to or from 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.

(2) A person who, intentionally and without authority, possesses data, with the knowledge that such data was intercepted unlawfully as provided for under subsection (1), commits an offence and shall, upon conviction, be liable to a fine of K10,000,000 and to imprisonment for ten years.

(3) A person found in possession of data, in regard to which there is a reasonable suspicion that such data was intercepted unlawfully as provided for under subsection (1), and who is unable to give a satisfactory exculpatory account of such possession, commits an offence and shall, upon conviction, be liable to a fine of K5,000,000 and to imprisonment for five years.

Unlawful interference with a computer system

6. – (1) A person who, intentionally and without authority, does any act which causes an unlawful 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 this section, an interference is unlawful if the person whose act causes the interference —

(a) is not entitled to cause that interference; or

(b) does not have consent to interfere from a person who is so entitled.

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 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 this section "interference with a computer program or data" includes to permanently or temporarily —

(a) delete a computer program or data;

(b) alter a computer program or data;

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

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

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

(f) deny access to a computer program or data,

held in a computer data storage medium or a computer system.

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, program, 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) A person who knowingly receives, or is in possession of, a program or a computer password, device, access code, or similar data from any action specified under subsection (1) and intends to use it to commit or assist in 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.

(3) Notwithstanding subsections (1) and (2), the activities described under subsections (2) and (3) 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.

(4) For purposes of subsections (1) and (2), 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 knowingly –

(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) A person providing public internet access points shall use child pornography filtering measures.

(4) A person who fails to comply with subsection (3) 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, knowingly -

(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;

(e) 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 K2,000,000 and to imprisonment for two 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 instil 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 acts in respect of software or hardware

15. – (1) A person who, intentionally and without authority, uses any software or hardware tool for purposes of contravening section 3 (1) commits an offence and shall, upon conviction, be liable to a fine of K1,000,000 and to imprisonment for twelve months.

(2) For purposes of subsection (1) "software or hardware tool" means any electronic, mechanical or other instrument, device, equipment, apparatus or a substantial component thereof or a computer program, which is designed or adapted primarily for the purposes of -

(a) unauthorized access as provided in section 3 (1);

(b) unlawful interception of data as provided in section 5 (1);

(c) unlawful interference with a computer system as provided in section 6 (1);

(c) unauthorized interference with a computer program or data as provided in section 7 (1); or

(e) manufacturing, making available or using a password, access code or similar data or devices as provided in section 8 (1).

(3) For purposes of subsection (2) (e) "password, access code or similar data or devices" include –

(a) a secret code or pin;

(b) an image;

(c) a security token;

(d) an access card;

(e) any device;

(f) biometric data; or

(g) a word or string of characters or numbers,

used for financial transactions or user authentication in order to access or use data, computer program, or a computer system.

Unlawful use of software and hardware

16. A person who, without authority, accesses any computer system, or knowingly introduces or spreads malware into a computer system or network, commits an offence and shall, upon conviction, be liable to a fine of K5,000.000 and to imprisonment for five years.

Unlawfully disabling a computer system

17. A person who, intentionally 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 five years.

Cyber terrorism

18. - (1) A person who 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.

(2) In this section, "cyber terrorism" means the unlawful use of computers and information technology to unlawfully attack or threaten to attack computers, networks and the information stored therein, 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.

Intentionally withholding message delivered erroneously

19. 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.

Cyber extortion

20. A person who, through a computer system with intent to extort or gain anything from any person —

(a) accuses or threatens to accuse any person of committing a crime or offering or making any solicitation or threat to any person as an inducement to commit or permit the commission of a crime;

(b) threatens that any person shall be accused by another person of the commission of an offence;

(c) knowing the contents of a writing, causes any person to receive the writing containing such accusation or threat;

(d) knowingly transmits any communication containing any threat to cause damage to a computer system with the intent to extort from any person any money or other thing of value;

(e) obtains any advantage from another person; or

(f) compels another person to perform or to abstain from performing any act,

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

Identity related crimes

21. A person who, knowingly and without lawful 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.

Cybersquatting

22. A person who, intentionally takes or makes use of a Country Code Top-Level Domain ".mw" registered, owned or in use by another person on the internet, without

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

Cyber forgery

23. - (1) A person who, intentionally 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

24. - (1) A person who, with fraudulent or dishonest intent —

(a) unlawfully gains;

(b) occasions unlawful loss to another person; or

(c) 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) an unauthorized access to a computer system, program or data;

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

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

(d) 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

(e) 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

25. A person who, with intent to compromise the safety and 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

26. – (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.

Unsolicited electronic messages

27. - (1) A person who, knowingly and without lawful excuse or justification —

(a) initiates the transmission of multiple electronic communications from or through a computer system; or

(b) uses a computer system to relay or retransmit multiple electronic communications, with the intent to deceive or mislead users, as to the origin of such messages,

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

(2) Notwithstanding subsection (1), it shall not be an offence under this section if —

(a) the transmission of multiple electronic communications from or through such computer system is done within customer, business or any other relationships where a person would reasonably be expected to transmit multiple electronic mail messages;

(b) the recipient of such electronic communications has not opted out of the business, customer or other relationship; or

(c) the transmission is by public institutions and is for purposes of raising awareness or collecting information with regard to education, health, security, safety outages and emergencies.

Prohibition of use of computer system for offences

28. - (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

29. A person who, knowingly and without lawful excuse, 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

30. A person who receives an order related to a criminal investigation and without lawful excuse 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

31. A person who, by means of a computer or 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

32. A person who, by means of a computer or 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

33. 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.

Prohibition of illegal trade and commerce

34. 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 a fine of K10,000,000 and imprisonment for ten years.

Attempting, aiding and abetting crime

35. - (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 law enforcement officer or cyber inspection officer

36. 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

37. 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

38. 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 order

39. A police officer may, upon confirmation by the court and as soon as reasonably practicable to do so, order for the preservation of data that has been stored or processed by means of a computer system or any other information and communication technology, where there are reasonable grounds to believe that such data is vulnerable to loss or modification.

Disclosure of preserved data

40. A police officer may, by written notice given to a person in control of a computer system, require the person to -

(a) ensure that the data specified in the notice is preserved for the period specified in the notice; or

(b) disclose sufficient traffic data about a specified communication to identify the service provider or the path through which the data was transmitted.

Production order

41. - (1) A police officer may apply to a court for an order compelling -

(a) a person to submit specified data in that person's possession or control, which is stored in a computer system; or

(b) a service provider to submit subscriber information in relation to its services in that 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.

Access, search and seizure

42. - (1) Where a police officer has reasonable grounds to believe that stored data or information would be relevant for the purposes of an investigation or the prosecution of an offence, he may apply to a court for an order to enter any premises to access, search and seize such data or information.

(2) A police officer shall, in the execution of an order issued under subsection (1) -

(a) seize or secure a computer system or any device that stores data;

(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 doing an act referred to in paragraph (a); or

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

(3) A police officer may, in the execution of an order issued under subsection (1), order any person who has knowledge about the functioning of the computer system or the measures provided under subsection (2) to protect the data contained therein in order to provide, as is reasonable, the necessary data to enable the undertaking of the measures provided under subsection (2).

Real time collection of content or traffic data

43. A police officer may apply to a court, ex-parte, for an order -

(a) for the collection or recording of content or traffic data, 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 such collection or recording referred to in paragraph (a), or

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

Deletion order

44. 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

45. - (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.

Limited use of disclosed data and information

46. - (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

47. 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

48. - (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 -

(a) the National Intelligence Service Act (No. 30 of 2018);

(b) the Police Act (Cap. 13:01);

(c) the Defence Force Act (Cap. 12:01); and

(d) any other relevant law.

Obstruction and misuse of power

49. - (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

50. - (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

51. - (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

52. – (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

Cap. 8:04
Cap. 8:03

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

(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).

(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 –

Cap. 8:04
Cap. 8:03

(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

54. - (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

55. - (1) Subject to section 53, 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 53.

Expedited disclosure of preserved traffic data

56. Where, during the course of executing a request under section 53 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

57. - (1) Subject to section 53, 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 55.

(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 55, 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

58. 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

59. - (1) Subject to section 53, 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 53, 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

60. - (1) Subject to section 53, 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 53, 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

61. - (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

62. 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.

OBJECTS AND REASONS