THE REPUBLIC OF KENYA

LAWS OF KENYA

THE COMPUTER MISUSE AND CYBERCRIMES ACT

CHAPTER 79C

Revised Edition 2022

Published by the National Council for Law Reporting
with the Authority of the Attorney-General

www.kenyalaw.org

CHAPTER 79C

COMPUTER MISUSE AND CYBERCRIMES

ARRANGEMENT OF SECTIONS

PART I – PRELIMINARY

Section

SPENT

CHAPTER 79C

COMPUTER MISUSE AND CYBERCRIMES

[*Date of assent: 16th May, 2018*.]

[*Date of commencement: 30th May, 2018*.]

An Act of Parliament to provide for offences relating to computer systems; to enable timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes; to facilitate international co-operation in dealing with computer and cybercrime matters; and for connected purposes

[Act No. 5 of 2018.]

PART I – PRELIMINARY

1. Short title

This Act may be cited as the Computer Misuse and Cybercrimes Act.

2. Interpretation

In this Act, unless the context otherwise requires—

"access" means gaining entry into or intent to gain entry by a person to a program or data stored in a computer system and the person either—

(a) alters, modifies or erases a program or data or any aspect related to the program or data in the computer system;

(b) copies, transfers or moves a program or data to—

(i) any computer system, device or storage medium other than that in which it is stored; or

(ii) to a different location in the same computer system, device or storage medium in which it is stored;

(c) causes it to be output from the computer in which it is held, whether by having it displayed or in any other manner; or

(d) uses it by causing the computer to execute a program or is itself a function of the program;

"Authority" means the Communications Authority of Kenya;

"authorised person" means an officer in a law enforcement agency or a cybersecurity expert designated by the Cabinet Secretary responsible for matters relating to national security by notice in the *Gazette* for the purposes of Part III of this Act;

"blockchain technology" means a digitized, decentralized, public ledger of all crypto currency transactions;

"Cabinet Secretary" means the Cabinet Secretary responsible for matters relating to internal security;

"Central Authority" means the Office of the Attorney-General and Department of Justice;

"Committee" means the National Computer and Cybercrimes Co-ordination Committee established under section 4;

"computer data storage medium" means a device, whether physical or virtual, containing or designed to contain, or enabling or designed to enable storage of data, whether available in a single or distributed form for use by a computer, and from which data is capable of being reproduced;

"computer system" means a physical or virtual device, or a set of associated physical or virtual devices, which use electronic, magnetic, optical or other technology, to perform logical, arithmetic storage and communication functions on data or which perform control functions on physical or virtual devices including mobile devices and reference to a computer system includes a reference to part of a computer system;

"content data" means the substance, its meaning or purport of a specified communication;

"critical information infrastructure system or data" means an information system, program or data that supports or performs a function with respect to a national critical information infrastructure;

"critical infrastructure" means the processes, systems, facilities, technologies, networks, assets and services essentials to the health, safety,

security or economic well-being of Kenyans and the effective functioning of Government;

"cybersquatting" means the acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, or deprive another from registering the same, if the domain name is—

(a) similar, identical or confusingly similar to an existing trademark registered with the appropriate government agency at the time of registration;

(b) identical or in any way similar with the name of a person other than the registrant, in case of a personal name; or

(c) acquired without right or intellectual property interests in it;

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

"interception" means the monitoring, modifying, viewing or recording of non-public transmissions of data to or from a computer system over a telecommunications system, and includes, in relation to a function of a computer system, listening to or recording a function of a computer system or acquiring the substance, its meaning or purport of such function;

"interference" means any impairment to the confidentiality, integrity or availability of a computer system, or any program or data on a computer system, or any act in relation to the computer system which impairs the operation of the computer system, program or data;

"mobile money" means electronic transfer of funds between banks or accounts' deposit or withdrawal of funds or payment of bills by mobile phone;

"national critical information infrastructure" means a vital virtual asset, facility, system, network or process whose incapacity, destruction or modification would have—

(a) a debilitating impact on the availability, integrity or delivery of essential services including those services, whose integrity, if compromised, could result in significant loss of life or casualties; or

(b) significant impact on national security, national defense, or the functioning of the state;

"network" means a collection of hardware components and computers interconnected by communications channels that allow sharing of resources and information;

"password" means any data by which a computer service or a computer system is capable of being obtained or used;

"pornography" includes the representation in books, magazines,

photographs, films, and other media, telecommunication apparatus of scenes of sexual behaviour that are erotic or lewd and are designed to arouse sexual interest;

"premises" includes land, buildings, movable structures, a physical or virtual space in which data is maintained, managed, backed up remotely and made available to users over a network, vehicles, vessels or aircraft;

"program" means data representing instructions or statements that, if executed in a computer system, causes the computer system to perform a function and reference to a program includes a reference to a part of a program;

"requested State" means a state being requested to provide legal assistance under the terms of this Act;

"requesting State" means a state requesting for legal assistance and may for the purposes of this Act include an international entity to which Kenya is obligated;

"seize" with respect to a program or data includes to—

(a) secure a computer system or part of it or a device;

(b) make and retain a digital image or secure a copy of any program or data, including using an on-site equipment;

(c) render the computer system inaccessible;

(d) remove data in the accessed computer system; or

(e) obtain output of data from a computer system;

"service provider" means—

(a) a public or private entity that provides to users of its services the means to communicate by use of a computer system; and

(b) any other entity that processes or stores computer data on behalf of that entity or its users;

"subscriber information" means any information contained in the form of data or any form that is held by a service provider, relating to subscribers of its services, other than traffic data or content data, by which can be established—

(a) the type of communication service used, the technical provisions taken thereto and the period of service;

(b) the subscriber's identity, postal, geographic location, electronic mail address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; or

(c) any other information on the site of the installation of telecommunication apparatus, available on the basis of the service agreement or arrangement;

"telecommunication apparatus" means an apparatus constructed or adapted for use in transmitting anything which is transmissible by a telecommunication system or in conveying anything which is transmitted through such a system;

"telecommunication system" means a system for the conveyance, through the use of electric, magnetic, electro-magnetic, electro-chemical or electro-mechanical energy, of—

(a) speech, music or other sounds;

(b) visual images;

(c) data;

(d) signals serving for the impartation, whether as between persons and persons, things and things or persons and things, of any matter otherwise than in the form of sound, visual images or data; or

(e) signals serving for the activation or control of machinery or apparatus and includes any cable for the distribution of anything falling within paragraphs (a), (b), (c) or (d);

"traffic data" means computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or the type of underlying service; and

"trust accounts" means an account where a bank or trust company is holding funds in relation to mobile money on behalf of the public depositors.

3. Objects of the Act

The objects of this Act are to—

(a) protect the confidentiality, integrity and availability of computer systems, programs and data;

(b) prevent the unlawful use of computer systems;

(c) facilitate the prevention, detection, investigation, prosecution and punishment of cybercrimes;

(d) protect the rights to privacy, freedom of expression and access to information as guaranteed under the Constitution; and

(e) facilitate international co-operation on matters covered under this Act.

PART II – THE NATIONAL COMPUTER AND CYBERCRIMES CO-ORDINATION COMMITTEE

4. Establishment of Committee

There is established the National Computer and Cybercrimes Co-ordination Committee.

5. Composition of the Committee

(1) The Committee shall comprise of—

(a) the Principal Secretary responsible for matters relating to internal security or a representative designated and who shall be the chairperson;

(b) the Principal Secretary responsible for matters relating to information, communication and technology or a representative designated in writing by the Principal Secretary responsible for information, communication and technology;

(c) the Attorney-General or a representative designated in writing by the Attorney-General;

(d) the Chief of the Kenya Defence Forces or a representative designated in writing by the Chief of the Kenya Defence Forces;

(e) the Inspector-General of the National Police Service or a representative designated in writing by the Inspector-General of the National Police Service;

(f) the Director-General of the National Intelligence Service or a representative designated in writing by the Director-General of the National Intelligence Service;

(g) the Director-General of the Communications Authority of Kenya or a representative designated in writing by the Director-General of the Communications Authority of Kenya;

(h) the Director of Public Prosecutions or a representative designated in writing by the Director of Public Prosecutions;

(i) the Governor of the Central Bank of Kenya or a representative designated in writing by the Governor of the Central Bank of Kenya; and

(j) the Director who shall be the secretary of the Committee and who shall not have a right to vote.

(2) The Committee shall report to the Cabinet Secretary responsible for matters relating to internal security.

6. Functions of the Committee

(1) The Committee shall—

(a) advise the Government on security related aspects touching on matters relating to blockchain technology, critical infrastructure, mobile money and trust accounts;

(b) advise the National Security Council on computer and cybercrimes;

(c) co-ordinate national security organs in matters relating to computer and cybercrimes;

(d) receive and act on reports relating to computer and cybercrimes;

(e) develop a framework to facilitate the availability, integrity and confidentiality of critical national information infrastructure including telecommunications and information systems of Kenya;

(f) co-ordinate collection and analysis of cyber threats, and response to cyber incidents that threaten cyberspace belonging to Kenya, whether such threats or incidents of computer and cybercrime occur within or outside Kenya;

(g) co-operate with computer incident response teams and other relevant bodies, locally and internationally on response to threats of computer and cybercrime and incidents;

(h) establish codes of cyber security practice and standards of performance for implementation by owners of critical national information infrastructure;

(i) develop and manage a national public key infrastructure framework;

(j) develop a framework for training on prevention, detection and mitigation of computer and cybercrimes and matters connected thereto; and

(k) perform any other function conferred on it by this Act or any other written law.

(2) Subject to the provisions of this Act, the Committee shall regulate its own procedure.

7. Secretariat of the Committee

(1) There shall be a Secretariat which shall comprise of the Director and such number of public officers that, subject to the approval of the Committee, the Cabinet Secretary responsible for matters relating to internal security in consultation with the Cabinet Secretary responsible for matters relating to information, communications and technology may deploy to the Secretariat.

(2) The Director shall be—

(a) the head of the Secretariat; and

(b) responsible to the Committee for the day to day administration of the affairs of the Secretariat and implementation of the decisions arising from the Committee.

(3) Without prejudice to the generality of the provisions of subsection (2), the Director shall be responsible for—

(a) the implementation of the decisions of the Committee;

(b) the efficient administration of the Secretariat;

(c) the management of staff of the Secretariat;

(d) the maintenance of accurate records on financial matters and resource use;

(e) the preparation and approval of the budget for the required funding of the operational expenses of the Secretariat; and

(f) the performance of any other duties as may be assigned to him or her by the Committee.

(4) The Director shall be appointed for a single term of four years and shall not be eligible for reappointment.

8. Reports by the Committee etc

The Committee shall submit quarterly reports to the National Security Council.

9. Critical information infrastructure

(1) The Director shall, by notice in the *Gazette*, designate certain systems as critical infrastructure.

(2) The Director shall designate a system as a critical infrastructure if a disruption of the system would result in—

(a) the interruption of a life sustaining service including the supply of water, health services and energy;

(b) an adverse effect on the economy of the Republic;

(c) an event that would result in massive casualties or fatalities;

(d) failure or substantial disruption of the money market of the Republic; and

(e) adverse and severe effect of the security of the Republic including intelligence and military services.

(3) The Director shall, within a reasonable time of designating a system as critical infrastructure, inform the owner or operator of the system the reasons for the designation of the system as a critical infrastructure.

(4) The Director shall, within a reasonable time of the declaration of any information infrastructure, or category or class of information infrastructure or any part thereof, as a critical information infrastructure, in line with a critical infrastructure framework issue directives to regulate—

(a) the classification of data held by the critical information infrastructure;

(b) the protection of, the storing of and archiving of data held by the critical information infrastructure;

(c) cyber security incident management by the critical information infrastructure;

(d) disaster contingency and recovery measures, which must be put in place by the critical information infrastructure;

(e) minimum physical and technical security measures that must be implemented in order to protect the critical information infrastructure;

(f) the period within which the owner, or person in control of a critical information infrastructure must comply with the directives; and

(g) any other relevant matter which is necessary or expedient in order to promote cyber security in respect of the critical information infrastructure.

10. Protection of critical information infrastructure

(1) The Committee shall within reasonable time and in consultation with the owner or a person in control of an identified critical information infrastructure, submit to the National Security Council its recommendations of entities to be gazetted as critical information infrastructures.

(2) The Committee shall, after the gazettement under subsection (1), in consultation with a person that owns or operates the critical information infrastructure—

(a) conduct an assessment of the threats, vulnerabilities, risks, and probability of a cyberattack across all critical infrastructure sectors;

(b) determine the harm to the economy that would result from damage or unauthorized access to critical infrastructure;

(c) measure the overall preparedness of each sector against damage or unauthorized access to critical infrastructure including the effectiveness of market forces driving security innovation and secure practices.

(d) identify any other risk-based security factors appropriate and necessary to protect public health and safety, or national socio-economic security; and

(e) recommend to the owners of systems designated as critical infrastructure, methods of securing their systems against cyber threats.

11. Reports on critical information infrastructure

(1) The owner or operator of a system designated as critical infrastructure shall report to the Committee any incidents likely to constitute a threat in the nature of an attack that amounts to a computer and cybercrime and the action the owner or operator intends to take to prevent the threat.

(2) Upon receipt of a report by the Committee, under subsection (1), the National Security Council shall provide technical assistance to the owner or operator of a critical infrastructure to mitigate the threat.

(3) The Director may institute an investigation of a computer and cybercrime attack on his or her own volition and may take necessary steps to secure any critical infrastructure without reference to the entity.

(4) The Director shall submit a report on any threat in the nature of a computer and cybercrime reported by the owners or operators of critical infrastructure periodically to the National Security Council.

12. Information sharing agreements

(1) A private entity may enter into an information sharing agreement with a public entity on critical information infrastructure.

(2) An agreement under subsection (1) shall only be entered into for the following purposes and in line with a critical infrastructure framework—

(a) to ensure cyber security;

(b) for the investigation and prosecution of crimes related to cyber security;

(c) for the protection of life or property of an individual; and

(d) to protect the national security of the country.

(3) Prior to the sharing of information under subsection (1), a party to an agreement shall review the information and ascertain whether the information contains personal details that may identify a specific person not directly related to a threat that amounts to a computer and cybercrime and remove such information.

(4) A person shall not, under this Part, share information relating to the health status of another person without the prior written consent of the person to whom the information relates.

13. Auditing of critical information infrastructures to ensure compliance

(1) The owner or person in control of a critical information infrastructure shall annually submit a compliance report on the critical information infrastructure to the Committee in line with a critical infrastructure framework in order to evaluate compliance.

(2) The Director, shall within a reasonable time before an audit on a critical information infrastructure or at any time there is an imminent threat in the nature of an attack that amounts to a computer and cybercrime, notify the owner or person in control of a critical information infrastructure in writing—

(a) the date on which an audit is to be performed; and

(b) the particulars and contact details of the person who is responsible for the overall management and control of the audit.

(3) The Director shall monitor, evaluate and report on the adequacy and effectiveness of any audit.

(4) The Director may request the owner or person in control of a critical information infrastructure to provide such additional information as may be necessary within a specified period in order to evaluate the issues raised from the audit.

(5) An owner or authorised person in control of a critical information infrastructure commits an offence and if convicted is liable to a fine not exceeding two hundred thousand shillings or to term of imprisonment not exceeding five years or both if the owner or authorized person—

(a) fails to file a compliance report and fails to cooperate with an audit to be performed on a critical information infrastructure in order to evaluate compliance with the directives issued;

(b) fails to provide to the Director such additional information as may be necessary within a specified period in order to evaluate the report of an audit in line with the critical infrastructure after he or she has been requested to do so to the Director;

(c) hinders, obstructs or improperly attempts to influence any member of the Committee, person or entity to monitor, evaluate and report on the adequacy and effectiveness of an audit;

(d) hinders, obstructs or improperly attempts to influence any person authorized to carry out an audit;

(e) fails to co-operate with any person authorized to carry out an audit; or

(f) fails to assist or provide technical assistance and support to a person authorized to carry out an audit.

(6) A person shall not perform an audit on a critical information infrastructure unless he or she—

(a) has been authorized in writing by the Director to perform such audit; or

(b) is in possession of a certificate of appointment, in the prescribed form, issued by the Director, which certificate must be submitted to the owner or person in control of a critical information infrastructure at the commencement of the audit.

PART III – OFFENCES

14. Unauthorised access

(1) A person who causes, whether temporarily or permanently, a computer system to perform a function, by infringing security measures, with intent to gain access, and knowing such access is unauthorised, commits an offence and is liable on conviction, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.

(2) Access by a person to a computer system is unauthorised if—

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

(b) that person 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 the purposes of this section, it is immaterial that the unauthorised access is not directed at—

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer system.

15. Access with intent to commit further offence

(1) A person who commits an offence under section 14 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 is liable, on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding ten years, or to both.

(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.

16. Unauthorised interference

(1) A person who intentionally and without authorisation does any act which causes an unauthorised interference to a computer system, program or data, commits an offence and is liable on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both.

(2) For the purposes of this section, an interference is unauthorised, if the person whose act causes the interference-

(a) is not entitled to cause that interference;

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

(3) A person who commits an offence under subsection (1) which—

(a) results in a significant financial loss to any person;

(b) threatens national security;

(c) causes physical injury or death to any person; or

(d) threatens public health or public safety,

is liable on conviction to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.

(4) For the purposes of this section, it is immaterial whether or not the unauthorised interference is directed at—

(a) any particular computer system, program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer system.

(5) For the purposes of this section, it is immaterial whether an unauthorised modification or any intended effect of it is permanent or temporary.

17. Unauthorised interception

(1) A person who intentionally and without authorisation does any act which intercepts or causes to be intercepted, directly or indirectly and causes the transmission of data to or from a computer system over a telecommunication system commits an offence and is liable, on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both.

(2) A person who commits an offence under subsection (1) which—

(a) results in a significant financial loss;

(b) threatens national security;

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

(d) threatens public health or public safety, is liable, on conviction to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.

(3) For the purposes of this section, it is immaterial that the unauthorised interception is not directed at—

(a) a telecommunication system;

(b) any particular computer system data;

(c) a program or data of any kind; or

(d) a program or data held in any particular computer system.

(4) For the purposes of this section, it is immaterial whether an unauthorised interception or any intended effect of it is permanent or temporary.

18. Illegal devices and access codes

(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 is liable, on conviction, to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.

(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 that it be used to commit or assist in commission of an offence under this Part commits an offence and is liable on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both.

(3) Despite subsections (1) and (2), the activities described under the subsections do not constitute an offence if—

(a) any act intended for the authorised 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 the terms of a judicial order issued or in exercise of any power under this Act or any law.

(4) For the 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.

19. Unauthorised disclosure of password or access code

(1) A person who knowingly and without authority discloses any password, access code or other means of gaining access to any program or data held in any computer system commits an offence and is liable, on conviction, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.

(2) A person who commits the offence under subsection (1)—

(a) for any wrongful gain;

(b) for any unlawful purpose; or

(c) to occasion any loss,

is liable, on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both.

20. Enhanced penalty for offences involving protected computer system

(1) Where a person commits any of the offences specified under sections 14, 15, 16 and 17 on a protected computer system, that person shall be liable, on conviction, to a fine not exceeding twenty five million shillings or imprisonment for a term not exceeding twenty years or both.

(2) For purposes of this section—

"protected computer system" means a computer system used directly in connection with, or necessary for,—

(a) the security, defence or international relations of Kenya;

(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;

(c) the provision of services directly related to communications infrastructure, banking and financial services, payment and settlement systems and instruments, public utilities or public transportation, including government services delivered electronically;

(d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services;

(e) the provision of national registration systems; or

(f) such other systems as may be designated relating to the security, defence or international relations of Kenya, critical information, communications, business or transport infrastructure and protection of public safety and public services as may be designated by the Cabinet Secretary responsible for matters relating to information, communication and technology.

21. Cyber espionage

(1) A person who unlawfully and intentionally performs or authorizes or allows another person to perform a prohibited act envisaged in this Act, in order to—

(a) gain access, as provided under section 14, to critical data, a critical database or a national critical information infrastructure; or

(b) intercept data, as provided under section 17, to, from or within a critical database or a national critical information infrastructure, with

the intention to directly or indirectly benefit a foreign state against the Republic of Kenya,

commits an offence and is liable, on conviction, to imprisonment for a period not exceeding twenty years or to a fine not exceeding ten million shillings, or to both.

(2) A person who commits an offence under subsection (1) which causes physical injury to any person is liable, on conviction, to imprisonment for a term not exceeding twenty years.

(3) A person who commits an offence under subsection (1) which causes the death of a person is liable, on conviction, to imprisonment for life.

(4) A person who unlawfully and intentionally possesses, communicates, delivers or makes available or receives, data, to, from or within a critical database or a national critical information infrastructure, with the intention to directly or indirectly benefit a foreign state against the Republic of Kenya, commits an offence and is liable on conviction to imprisonment for a period not exceeding twenty years or to a fine not exceeding ten million shillings, or to both.

(5) A person who unlawfully and intentionally performs or authorizes, or allows another person to perform a prohibited act as envisaged under this Act in order to gain access, as provided under section 14, to or intercept data, as provided under section 17, which is in possession of the State and which is exempt information in accordance with the law relating to access to information, with the intention to directly or indirectly benefit a foreign state against the Republic of Kenya, commits an offence and is liable, on conviction, to a fine not exceeding five million shillings or to imprisonment for a period not exceeding ten years, or to both.

22. False publications

(1) A person who intentionally publishes false, misleading or fictitious data or misinforms with intent that the data shall be considered or acted upon as authentic, with or without any financial gain, commits an offence and shall, on conviction, be liable to a fine not exceeding five million shillings or to imprisonment for a term not exceeding two years, or to both.

(2) Pursuant to Article 24 of the Constitution, the freedom of expression under Article 33 of the Constitution shall be limited in respect of the intentional publication of false, misleading or fictitious data or misinformation that—

(a) is likely to—
  (i) propagate war; or
  (ii) incite persons to violence;
(b) constitutes hate speech;
(c) advocates hatred that—
  (i) constitutes ethnic incitement, vilification of others or incitement to cause harm; or
  (ii) is based on any ground of discrimination specified or contemplated in Article 27(4) of the Constitution; or
(d) negatively affects the rights or reputations of others.

23. Publication of false information

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 among citizens of the Republic, or which is likely to discredit the reputation

of any person commits an offence and shall on conviction, be liable to a fine not exceeding five million shillings or to imprisonment for a term not exceeding ten years, or to both.

24. Child pornography

(1) A person who intentionally—

(a) publishes child pornography through a computer system;

(b) produces child pornography for the purpose of its publication through a computer system;

(c) downloads, distributes, transmits, disseminates, circulates, delivers, exhibits, lends for gain, exchanges, barters, sells or offers for sale, lets on hire or offers to let on hire, offers in another way, or make available in any way from a telecommunications apparatus pornography; or

(d) possesses child pornography in a computer system or on a computer data storage medium,

commits an offence and is liable, on conviction, to a fine not exceeding twenty million or to imprisonment for a term not exceeding twenty five years, or both.

(2) It is a defence to a charge of an offence under subsection (1) that a publication which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, art, representation or figure is in the interest of science, literature, learning or other objects of general concerns.

(3) For purposes of this section—

"child" means a person under the age of eighteen years;

"child pornography" includes data which, whether visual or audio, depicts—

(a) a child engaged in sexually explicit conduct;

(b) a person who appears to be a child engaged in sexually explicit conduct; or

(c) realistic images representing a child engaged in sexually explicit conduct;

"publish" includes to—

(a) distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way;

(b) having in possession or custody, or under control, for the purpose of doing an act referred to in paragraph (a); or

(c) print, photograph, copy or make in any other manner whether of the same or of a different kind or nature for the purpose of doing an act referred to in paragraph (a).

25. Computer forgery

(1) A person who intentionally inputs, alters, deletes, or suppresses computer data, resulting in inauthentic 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 is liable, on conviction, to fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both.

(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,

is liable, on conviction, to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.

26. Computer fraud

(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 in subsection (2),

commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or imprisonment term for a term not exceeding ten years, or to both.

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

(a) an unauthorised 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) uses any data or program, or has any data or program output from the computer system in which it is held, by having it displayed in any manner.

27. Cyber harassment

(1) A person who, individually or with other persons, wilfully communicates, either directly or indirectly, with another person or anyone known to that person commits an offence, if they know or ought to know that their conduct—

(a) is likely to cause those persons apprehension or fear of violence to them or damage or loss on that persons' property; or

(b) detrimentally affects that person; or

(c) is in whole or part, of an indecent or grossly offensive nature and affects the person.

(2) A person who commits an offence under subsection (1) is liable, on conviction, to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.

(3) A person may apply to Court for an order compelling a person charged with an offence under subsection (1) to refrain from—

(a) engaging or attempting to engage in; or

(b) enlisting the help of another person to engage in, any communication complained of under subsection (1).

(4) The Court—

(a) may grant an interim order; and

(b) shall hear and determine an application under subsection (4) within fourteen days.

(5) An intermediary may apply for the order under subsection (4) on behalf of a complainant under this section.

(6) A person may apply for an order under his section outside court working hours.

(7) The Court may order a service provider to provide any subscriber information in its possession for the purpose of identifying a person whose conduct is complained of under this section.

(8) A person who contravenes an order made under this section commits an offence and is liable, on conviction to a fine not exceeding one million shillings or to imprisonment for a term not exceeding six months, or to both.

28. Cybersquatting

A person who, intentionally takes or makes use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by another person on the internet or any other computer network, without authority or right, commits an offence and is liable on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or both.

29. Identity theft and impersonation

A person who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person commits an offence and is liable, on conviction, to a fine not exceeding two hundred thousand shillings or to imprisonment for a term not exceeding three years or both.

30. Phishing

A person who creates or operates a website or sends a message through a computer system with the intention to induce the user of a website or the recipient of the message to disclose personal information for an unlawful purpose or to gain unauthorized access to a computer system, commits an offence and is liable upon conviction to a fine not exceeding three hundred thousand shillings or to imprisonment for a term not exceeding three years or both.

31. Interception of electronic messages or money transfers

A person who unlawfully destroys or aborts any electronic mail or processes through which money or information is being conveyed commits an offence and is liable on conviction to a fine not exceeding two hundred thousand shillings or to a term of imprisonment not exceeding seven years or to both.

32. Willful misdirection of electronic messages

A person who willfully misdirects electronic messages commits an offence and is liable on conviction to a fine not exceeding one hundred thousand shillings or to imprisonment for a term not exceeding two years or to both.

33. Cyber terrorism

(1) A person who accesses or causes to be accessed a computer or computer system or network for purposes of carrying out a terrorist act, commits an offence and shall on conviction, be liable to a fine not exceeding five million shillings or to imprisonment for a term not exceeding ten years, or to both.

(2) For the purpose of this section, "terrorist act" shall have the same meaning as assigned under the Prevention of Terrorism Act (Cap. 59B).

34. Inducement to deliver electronic message

A person who induces any person in charge of electronic devices to deliver any electronic messages not specifically meant for him commits an offence and is liable on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or to both.

35. Intentionally withholding message delivered erroneously

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 is liable on conviction a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or to both.

36. Unlawful destruction of electronic messages

A person who unlawfully destroys or aborts any electronic mail or processes through which money or information is being conveyed commits an offence and is liable on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or to both.

37. Wrongful distribution of obscene or intimate images

A person who transfers, publishes, or disseminates, including making a digital depiction available for distribution or downloading through a telecommunications network or though any other means of transferring data to a computer, the intimate or obscene image of another person commits an offence and is liable, on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or to both.

38. Fraudulent use of electronic data

(1) A person who knowingly and without authority causes any loss of property to another by altering, erasing, inputting or suppressing any data stored in a computer,

commits an offence and is liable on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or to both.

(2) A person who sends an electronic message which materially misrepresents any fact upon which reliance by another person is caused to suffer any damage or loss commits an offence and is liable on conviction to imprisonment for a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or to both.

(3) A person who with intent to defraud, franks electronic messages, instructions, subscribes any electronic messages or instructions, commits an offence and is liable on conviction a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or to both.

(4) A person who manipulates a computer or other electronic payment device with the intent to short pay or overpay commits an offence and is liable on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or to both.

(5) A person convicted under subsection (4) shall forfeit the proprietary interest in the stolen money or property to the bank, financial institution or the customer.

39. Issuance of false e-instructions

A person authorized to use a computer or other electronic devices for financial transactions including posting of debit and credit transactions, issuance of electronic instructions as they relate to sending of electronic debit and credit messages or confirmation of electronic fund transfer, issues false electronic instructions, commits an offence and is liable, on conviction, a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or to both.

40. Reporting of cyber threat

(1) A person who operates a computer system or a computer network, whether public or private, shall immediately inform the Committee of any attacks, intrusions and other disruptions to the functioning of another computer system or network within twenty four hours of such attack, intrusion or disruption.

(2) A report made under subsection (1) shall include—

(a) information about the breach, including a summary of any information that the agency knows on how the breach occurred;

(b) an estimate of the number of people affected by the breach;

(c) an assessment of the risk of harm to the affected individuals; and

(d) an explanation of any circumstances that would delay or prevent the affected persons from being informed of the breach.

(3) The Committee may propose the isolation of any computer systems or network suspected to have been attacked or disrupted pending the resolution of the issues.

(4) A person who contravenes the provisions of subsection (1) commits an offence and is liable upon conviction a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or to both.

41. Employee responsibility to relinquish access codes

(1) An employee shall, subject to any contractual agreement between the employer and the employee, relinquish all codes and access rights to their employer's computer network or system immediately upon termination of employment.

(2) person who contravenes the provision of this subsection (1) commits an offence and shall be, liable on conviction, to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or to both.

42. Aiding or abetting in the commission of an offence

(1) A person who knowingly and willfully aids or abets the commission of any offence under this Act commits an offence and is liable, on conviction, to a fine not exceeding seven million shillings or to imprisonment for a term not exceeding four years, or to both.

(2) A person who knowingly and willfully attempts to commit an offence or does any act preparatory to or in furtherance of the commission of any offence under this Act, commits an offence and is liable, on conviction, to a fine not exceeding seven million shillings or to imprisonment for a term not exceeding four years, or to both.

43. Offences by a body corporate and limitation of liability

(1) Where any offence under this Act has been committed by a body corporate–

(a) the body corporate is liable, on conviction, to a fine not exceeding fifty million shillings; and

(b) every person who at the time of the commission of the offence was a principal officer of the body corporate, or anyone acting in a similar capacity, is also deemed to have committed the offence, unless they prove that the offence was committed without their consent or knowledge and that they exercised such diligence to prevent the commission of the offence as they ought to have exercised having regard to the nature of their functions and to prevailing circumstances, and is liable, on conviction, to a fine not exceeding five million shillings or imprisonment for a term not exceeding three years, or to both.

(2) If the affairs of the body corporate are managed by its members, subsection (1)(b) applies in relation to the acts or defaults of a member in connection with their management functions, as if the member was a principal officer of the body corporate or was acting in a similar capacity.

44. Confiscation or forfeiture of assets

(1) A court may order the confiscation or forfeiture of monies, proceeds, properties and assets purchased or obtained by a person with proceeds derived from or in the commission of an offence under this Act.

(2) The court may, on conviction of a person for any offence under this Act make an order of restitution of any asset gained from the commission of the offence, in accordance with the provisions and procedures of the Proceeds of Crime and Anti-Money Laundering Act (Cap. 59A).

45. Compensation order

(1) Where the court convicts a person for any offence under this Part, or for an offence under any other law committed through the use of a computer system, the court may make an order for the payment by that person of a sum to be fixed by the court as compensation to any person for any resultant loss caused by the commission of the offence for which the sentence is passed.

(2) Any claim by a person for damages sustained by reason of any offence committed under this Part is deemed to have been satisfied to the extent of any amount which they have been paid under an order for compensation, but the order shall not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order.

(3) An order of compensation under this section is recoverable as a civil debt.

46. Additional penalty for other offences committed through use of a computer system

(1) A person who commits an offence under any other law through the use of a computer system commits an offence and shall be liable on conviction to a penalty similar to the penalty provided under that law.

(2) A Court shall, in determining whether to sentence a person convicted of an offence under this section, consider—

(a) the manner in which the use of a computer system enhanced the impact of the offence;

(b) whether the offence resulted in a commercial advantage or financial gain;

(c) the value involved, whether of the consequential loss or damage caused, or the profit gained from commission of the offence through the use of a computer system;

(d) whether there was a breach of trust or responsibility;

(e) the number of victims or persons affected by the offence;

(f) the conduct of the accused; and

(g) any other matter that the court deems fit to consider.

PART IV – INVESTIGATION PROCEDURES

47. Scope of procedural provisions

(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 law; and

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

(2) In any proceedings related to any offence, under any law of Kenya, 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 (Cap. 206);

(b) the National Police Service Act (Cap. 84);

(c) the Kenya Defence Forces Act (Cap. 199); and

(d) any other relevant law.

48. Search and seizure of stored computer data

(1) Where a police officer or an authorised person has reasonable grounds to believe that there may be in a specified computer system or part of it, computer data storage medium, program, data, that—

(a) is reasonably required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence; or

(b) has been acquired by a person as a result of the commission of an offence, the police officer or the authorised person may apply to the court for issue of a warrant to enter any premises to access, search and similarly seize such data.

(2) A search warrant issued under subsection (1) shall—

(a) identify the police officer or authorised person;

(b) direct the police officer or authorised person under paragraph (a) to seize the data in question; or

(c) direct the police officer or authorised person to–

(i) search any person identified in the warrant;

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

(iii) search any person found on or at such premises.

(3) A search warrant may be issued on any day and shall be of force until it is executed or is cancelled by the issuing court.

(4) A police officer or an authorised person shall present a copy of the warrant to a person against whom it is issued.

(5) A person who—

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

(b) compromises the integrity or confidentiality of a computer system, data, or information accessed or retained under this section; or

(c) misuses the powers granted under this section,

commits an offence and is liable on conviction to a fine not exceeding five million shillings or to a term of imprisonment not exceeding three years or to both.

49. Record of and access to seized data

(1) Where a computer system or data has been removed or rendered inaccessible, following a search or a seizure under section 48, the person who made the search shall, at the time of the search or as soon as practicable after the search—

(a) make a list of what has been seized or rendered inaccessible, and shall specify the date and time of seizure; and

(b) provide a copy of the list to the occupier of the premises or the person in control of the computer system referred to under paragraph (a).

(2) Subject to subsection (3), a police officer or an authorised person shall, on request, permit a person who—

(a) had the custody or control of the computer system;

(b) has a right to any data or information seized or secured; or

(c) has been acting on behalf of a person under subsection (1)(a) or (b),

to access and copy computer data on the system or give the person a copy of the computer data.

(3) The police officer or authorised person may refuse to give access or provide copies under subsection (2), if they have reasonable grounds for believing that giving the access or providing the copies, may—

(a) constitute a criminal offence; or

(b) prejudice—

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

(ii) an ongoing investigation; or

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

(4) Despite subsection (3), a court may, on reasonable grounds being disclosed, allow a person who has qualified under subsection (2)(a) or (b) to—

(a) access and copy computer data on the system; or

(b) obtain a copy of the computer data.

50. Production order

(1) Where a police officer or an authorised person has reasonable grounds to believe that—

(a) specified data stored in a computer system or a computer data storage medium is in the possession or control of a person in its territory; and

(b) specified subscriber information relating to services offered by a service provider in Kenya are in that service provider's possession or control and is necessary or desirable for the purposes of the investigation, the police officer or the authorised person may apply to court for an order.

(2) The Court shall issue an order directing—

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

(b) a specified service provider offering its services in Kenya to submit subscriber information relating to such services in that service provider's possession or control.

51. Expedited preservation and partial disclosure of traffic data

(1) Where a police officer or an authorised person has reasonable grounds to believe that—

(a) any specified traffic data stored in any computer system or computer data storage medium or by means of a computer system is reasonably required for the purposes of a criminal investigation; and

(b) there is a risk or vulnerability that the traffic data may be modified, lost, destroyed or rendered inaccessible, the police officer or an authorised person shall serve a notice on the person who is in possession or control of the computer system, requiring the person to—

(i) undertake expeditious preservation of such available traffic data regardless of whether one or more service providers were involved in the transmission of that communication; or

(ii) disclose sufficient traffic data concerning any communication in order to identify the service providers and the path through which communication was transmitted.

(2) The data specified in the notice shall be preserved and its integrity shall be maintained for a period not exceeding thirty days.

(3) The period of preservation and maintenance of integrity may be extended for a period exceeding thirty days if, on an application by the police officer or authorised person, the court is satisfied that—

(a) an extension of preservation is reasonably required for the purposes of an investigation or prosecution;

(b) there is a risk or vulnerability that the traffic data may be modified, lost, destroyed or rendered inaccessible; and

(c) the cost of the preservation is not overly burdensome on the person in control of the computer system.

(4) The person in possession or control of the computer system shall be responsible to preserve the data specified—

(a) for the period of notice for preservation and maintenance of integrity or for any extension thereof permitted by the court; and

(b) for the period of the preservation to keep confidential any preservation ordered under this section.

(5) Where the person in possession or control of the computer system is a service provider, the service provider shall be required to—

(a) respond expeditiously to a request for assistance, whether to facilitate requests for police assistance, or mutual assistance requests; and

(b) disclose as soon as practicable, a sufficient amount of the non-content data to enable a police officer or an authorised person to identify any other telecommunications providers involved in the transmission of the communication.

(6) The powers of the police officer or an authorised person under subsection (1) shall apply whether there is one or more service providers involved in the transmission of communication which is subject to exercise of powers under this section.

52. Real-time collection of traffic data

(1) Where a police officer or an authorised person has reasonable grounds to believe that traffic data associated with specified communications and related to the person under investigation is required for the purposes of a specific criminal investigation, the police officer or authorised person may apply to the court for an order to—

(a) permit the police officer or authorised person to collect or record through the application of technical means traffic data, in real-time;

(b) compel a service provider, within its existing technical capability—

(i) to collect or record through application of technical means traffic data in real time; or

(ii) to cooperate and assist a police officer or an authorised person in the collection or recording of traffic data, in real-time, associated with specified communications in its jurisdiction transmitted by means of a computer system.

(2) In making an application under subsection (1), the police officer or an authorised person shall—

(a) state the grounds they believe the traffic data sought is available with the person in control of the computer system;

(b) identify and explain, the type of traffic data suspected to be found on such computer system;

(c) identify and explain the subscribers, users or unique identifier the subject of an investigation or prosecution suspected as may be found on such computer system;

(d) identify and explain the offences identified in respect of which the warrant is sought; and

(e) explain the measures to be taken to prepare and ensure that the traffic data shall be sought—

(i) while maintaining the privacy of other users, customers and third parties; and

(ii) without the disclosure of data to any party not part of the investigation.

(3) Where the court is satisfied with the explanations provided under subsection (2), the court shall issue the order provided for under subsection (1).

(4) For purposes of subsection (1), real-time collection or recording of traffic data shall be ordered for a period not exceeding six months.

(5) The court may authorize an extension of time under subsection (4), if it is satisfied that—

(a) such extension of real-time collection or recording of traffic data is reasonably required for the purposes of an investigation or prosecution;

(b) the extent of real-time collection or recording of traffic data is commensurate, proportionate and necessary for the purposes of investigation or prosecution;

(c) despite prior authorisation for real-time collection or recording of traffic data, additional real-time collection or recording of traffic data is necessary and needed to achieve the purpose for which the warrant is to be issued;

(d) measures taken to prepare and ensure that the real time collection or recording of traffic data is carried out while maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation;

(e) the investigation may be frustrated or seriously prejudiced unless the real-time collection or recording of traffic data is permitted; and

(f) the cost of such preservation is not overly burdensome upon the person in control of the computer system.

(6) A court may, in addition to the requirement specified under subsection (3)

require the service provider to keep confidential the order and execution of any power provided under this section.

(7) A service provider who fails to comply with an order under this section commits an offence and is liable on conviction—

(a) where the service provider is a corporation, to a fine not exceeding ten million shillings; or

(b) in case of a principal officer of the service provider, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.

53. Interception of content data

(1) Where a police officer or an authorised person has reasonable grounds to believe that the content of any specifically identified electronic communications is required for the purposes of a specific investigation in respect of an offence, the police officer or authorised person may apply to the court for an order to—

(a) permit the police officer or authorised person to collect or record through the application of technical means;

(b) compel a service provider, within its existing technical capability—

(i) to collect or record through the application of technical means; or

(ii) to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications within the jurisdiction transmitted by means of a computer system.

(2) In making an application under subsection (1), the police officer or an authorised person shall—

(a) state the reasons he believes the content data being sought is in possession of the person in control of the computer system;

(b) identify and state the type of content data suspected to be found on such computer system;

(c) identify and state the offence in respect of which the warrant is sought;

(d) state if they have authority to seek real-time collection or recording on more than one occasion is needed, and shall specify the additional number of disclosures needed to achieve the purpose for which the warrant is to be issued;

(e) explain measures to be taken to prepare and ensure that the real-time collection or recording is carried out—

(i) while maintaining the privacy of other users, customers and third parties; and

(ii) without the disclosure of information and data of any party not part of the investigation;

(f) state how the investigation may be frustrated or seriously prejudiced unless the real time collection or recording is permitted; and

(g) state the manner in which they shall achieve the objective of the warrant, real time collection or recording by the person in control of the computer system where necessary.

(3) Where the court is satisfied with the grounds provided under subsection (2), the court shall issue the order applied for under subsection (1).

(4) For purposes of subsection (1), the real-time collection or recording of content data shall not be ordered for a period that exceeds the period that is necessary for the collection thereof and in any event not for more than a period of nine months.

(5) The period of real-time collection or recording of content data may be extended for such period as the court may consider necessary where the court is satisfied that—

(a) such extension of real-time collection or recording of content data is required for the purposes of an investigation or prosecution;

(b) the extent of real-time collection or recording of content data is proportionate and necessary for the purposes of investigation or prosecution;

(c) despite prior authorisation for real-time collection or recording of content data, further real-time collection or recording of content data

is necessary to achieve the purpose for which the warrant is to be issued;

(d) measures shall be taken to prepare and ensure that the real-time collection or recording of content data is carried out while maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation;

(e) the investigation may be frustrated or seriously prejudiced unless the real-time collection or recording of content data is permitted; and

(f) the cost of such real-time recording and collection is not overly burdensome upon the person in control of the computer system.

(6) The court may also require the service provider to keep confidential the order and execution of any power provided for under this section.

(7) A service provider who fails to comply with an order under this section commits an offence and is liable, on conviction—

(a) where the service provider is a corporation, to a fine not exceeding ten million shillings;

(b) in case of an officer of the service provider, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.

54. Obstruction and misuse of power

(1) A person who obstructs the lawful exercise of the powers under this Part, including destruction of data, or fails to comply with the requirements of this Part is liable, on conviction, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.

(2) A police officer or an authorised person who misuses the exercise of powers under this Part commits an offence and is liable, on conviction, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.

55. Appeal

Any person aggrieved by any decision or order of the Court made under this Part, may appeal to the High Court or Court of Appeal as the case may be within thirty days from the date of the decision or order.

56. Confidentiality and limitation of liability

(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 a 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 law for maintaining and making available the provision of their service.

(3) A service provider shall not be liable under this Act or any other law for the disclosure of any data or other information 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 V – INTERNATIONAL CO-OPERATION

57. General principles relating to international cooperation

(1) This Part shall apply in addition to the Mutual Legal Assistance Act (Cap. 75A) and the Extradition (Contiguous and Foreign Countries) Act (Cap 76).

(2) The Central 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, electronic communications or data;

(b) collecting evidence of an offence 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, power, function or provisions under this Act.

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

(4) Where a request has been received under subsection (3), the Central Authority may, subject to the provisions of the Mutual Legal Assistance Act (Cap. 75A), the Extradition (Contiguous and Foreign Countries) Act (Cap. 76), this Act and any other relevant law—

(a) grant the legal assistance requested; or

(b) refuse to grant the legal assistance requested.

(5) The Central Authority may require a requested State to—

(a) keep the contents, any information and material provided in a confidential manner;

(b) only use the contents, information and material provided for the purpose of the criminal matter specified in the request; and

(c) use it subject to other specified conditions.

58. Spontaneous information

(1) The Central Authority may, subject to this Act and other relevant 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 Central Authority may request that such information be kept confidential or only subject to other specified conditions.

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

(4) Upon receipt of a notice under subsection (3), the Central 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 Central Authority, that State shall be bound by them.

59. Expedited preservation of stored computer data

(1) Subject to section 57, 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 Central Authority to obtain the expeditious preservation of data stored by means of a computer system, located within the territory of Kenya.

(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 computer data to be preserved and its connection to the offence;

(d) any available information identifying the custodian of the stored computer 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 computer data.

(3) Upon receiving the request under this section, the Central 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 relevant law.

(4) A preservation of stored computer data effected under this section, shall be for a period of not less 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 under this section, the data shall continue to be preserved pending the final decision being made with regard to that request.

60. Expedited disclosure of preserved traffic data

Where during the course of executing a request under section 57 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 Central 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.

61. Mutual assistance regarding accessing of stored computer data

(1) Subject to section 57, a requesting State may request the Central Authority to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of Kenya, including data that has been preserved in accordance with section 60.

(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, computer system or electronic device;

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

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

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

(4) Where the Central Authority obtains the necessary authorisation in accordance with subsection (3), including any warrants to execute the request, the Central 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 Central Authority shall, subject to section 59, provide the results of the search and seizure as well as electronic or physical evidence seized to the requesting State.

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

A police officer or authorised person may, subject to any applicable provisions of this Act—

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

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

63. Mutual assistance in the real-time collection of traffic data

(1) Subject to section 57, a requesting State may request the Central Authority to provide assistance in real-time collection of traffic data associated with specified communications in Kenya 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 proceedings 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 Central Authority shall take all appropriate measures to obtain necessary authorisation including any warrants to execute upon the request in accordance with the procedures and powers provided under this Act and any other relevant law.

(4) Where the Central Authority obtains the necessary authorisation including any warrants to execute upon the request, the Central 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 Central Authority shall, subject to section 57, provide the results of such measures as well as real-time collection of traffic data associated with specified communications to the requesting State.

64. Mutual assistance regarding the interception of content data

(1) Subject to section 57, a requesting State may request the Central Authority to provide assistance in the real-time collection or recording of content data of specified communications in the territory of Kenya transmitted by means of a computer system.

(2) When making a request under subsection (1), a 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 proceedings and a brief summary of the related facts;

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

(d) the location at which or nature of the communication;

(e) the intended purpose for the required communication;

(f) sufficient information to identify the communications;

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

(h) the recipient of the communication;

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

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

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

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

(4) Where the Central Authority obtains the necessary authorisation, including any warrants to execute upon the request, the Central 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 Central Authority shall subject to section 57, provide the results of such measures as well as real-time collection or recording of content data of specified communications to the requesting State.

65. Point of contact

(1) The Central Authority shall ensure that the investigation 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 sections 59 and 60;

(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 territories, 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 – GENERAL PROVISIONS

66. Territorial jurisdiction

(1) Any court of competent jurisdiction shall try any offence under this Act where the act or omission constituting the offence is committed in Kenya.

(2) For the purposes of subsection (1), an act or omission committed outside Kenya which would if committed in Kenya constitute an offence under this Act is deemed to have been committed in Kenya if—

(a) the person committing the act or omission is–

(i) a citizen of Kenya; or

(ii) ordinarily resident in Kenya; and

(b) the act or omission is committed–

(i) against a citizen of Kenya;

(ii) against property belonging to the Government of Kenya outside Kenya; or

(iii) to compel the Government of Kenya to do or refrain from doing any act; or

(c) the person who commits the act or omission is, after its commission or omission, present in Kenya.

67. Forfeiture

The court before which a person is convicted of any offence may, in addition to any other penalty imposed, order the forfeiture of any apparatus, device or thing to the Authority which is the subject matter of the offence or is used in connection with the commission of the offence.

68. Prevailing Clause

Whenever there is a conflict between this Act and any other law regarding cybercrimes, the provisions of this Act shall supersede any such other law.

69. *Spent*

PART VII – PROVISIONS ON DELEGATED POWERS

70. Regulations

(1) The Cabinet Secretary may make regulations generally for the better carrying into effect of any provisions under this Act.

(2) Without prejudice to the foregoing, regulations made under this section may provide for—

(a) designation of computer systems, networks, programs, data as national critical information infrastructure;

(b) protection, preservation and management of critical information infrastructure;

(c) access to, transfer and control of data in any critical information infrastructure;

(d) storage and archiving of critical data or information;

(e) audit and inspection of national critical information infrastructure;

(f) recovery plans in the event of disaster, breach or loss of national critical information infrastructure or any part of it;

(g) standard operating procedures for the conduct, search, seizure and collection of electronic evidence; and

(h) mutual legal assistance.

(3) For the purposes of Article 94 (6) of the Constitution—

(a) the purpose and objective of delegation under this section is to enable the Cabinet Secretary to make regulations to provide for the better carrying into effect of the provisions of this Act and to enable the Authority to discharge its functions more effectively;

(b) the authority of the Cabinet Secretary to make regulations under this Act will be limited to bringing into effect the provisions of this Act and to fulfil the objectives specified under this section;

(c) the principles and standards applicable to the regulations made under this section are those set out in the Interpretation and General Provisions Act (Cap. 2) and the Statutory Instruments Act (Cap. 2A).

SCHEDULE

[s. 69]

SPENT