SPECIAL ISSUE

Kenya Gazette Supplement No. 156 (National Assembly Bills No. 41)

REPUBLIC OF KENYA

KENYA GAZETTE SUPPLEMENT

NATIONAL ASSEMBLY BILLS, 2024

NAIROBI, 9th August, 2024

CONTENT

PRINTED AND PUBLISHED BY THE GOVERNMENT PRINTER, NAIROBI

THE COMPUTER MISUSE AND CYBERCRIMES (AMENDMENT) BILL, 2024

A Bill for

AN ACT of Parliament to amend the Computer Misuse and Cybercrimes Act, Cap 79C and for connected purposes

ENACTED by the Parliament of Kenya, as follows—

Short title.

1. This Act may be cited as the Computer Misuse and Cybercrimes (Amendment) Act, 2024.

Amendment of section 2 of Cap 79C.

2. Section 2 of the Computer Misuse and Cybercrimes Act (in this Act referred to as "the principal Act"), is amended—

(a) in the definition of "access" by inserting the words "through a program or a device or" immediately after the words "by a person"; and

(b) by inserting the following new definitions in their proper alphabetical sequence—

"asset" includes all property movable or immovable, physical or virtual and all estates, easements and rights whether equitable or legal in, over or out of property, choses-in-action, money or goodwill whether situated in Kenya or elsewhere;

Cap 411A.

Cap 59B.

"identity theft" means the use of another person's personal identification information including the name, identification number, SIM-card, bank card, bank account information, address or any other subscriber information;

"SIM-card" has the meaning assigned to it under the Kenya Information and Communications Act, 1998;

"terrorist act" has the meaning assigned to it under the Prevention of Terrorism Act, 2012;

"virtual account" means a digital account acquired through virtual representation.

Amendment of section 6 of Cap 79C.

3. Section 6 of the principal Act is amended in subsection (1) by inserting the following new paragraphs immediately after paragraph (j)—

(ja) where it is proved that a website or application promotes illegal activities, child pornography, terrorism, extreme religious and cultic practices, issue a directive to render the website or application inaccessible.

Amendment of section 27 of Cap 79C.

4. Section 27 of the principal Act is amended in subsection (1) by inserting the words "or is likely to cause them to commit suicide" immediately after the word "person" appearing in paragraph (b).

Amendment of section 30 of Cap 79C.

5. Section 30 of the principal Act is amended—

(a) by inserting the words "or makes a call" immediately after the words "sends a message"; and

(b) by inserting the words "or call" immediately after the words "recipient of the message".

Insertion of a new section 42A in Cap 79C.

6. The principal Act is amended by inserting the following new section immediately after section 42—

Unauthorized SIM-card swap.

42A. A person who willfully causes unauthorized alteration and unlawfully takes ownership of another person's SIM-card with intent to commit an offence, is liable on conviction, to a fine not exceeding Kenya Shilling two hundred thousand or to imprisonment for a term not exceeding two years, or to both.

MEMORANDUM OF OBJECTS AND REASONS

Statement of the Objects and Reasons for the Bill

The principal object of the Bill is to amend the Computer Misuse and Cybercrimes Act, Cap 79C.

The Bill seeks to prohibit the use of electronic mediums to promote terrorism and extreme religious and cultic practices. The Bill in particular proposes the following amendments—

Clause 1 provides the short title of the Bill.

Clause 2 seeks to amend section 2 of the Act in order to provide a clearer definition of the term "access" to a computer system that is unauthorized. The Bill also introduces new definitions to align with the provisions of the Act.

Clause 3 seeks to amend section 6 of the Act to give the National Computer and Cybercrimes Co-ordination Committee an additional function of issuing directives on websites and applications that may be rendered inaccessible within the country where the website or application promotes illegal activities, child pornography, terrorism and extreme religious and cultic practices.

Clause 4 seeks to amend section 27 of the Act to expand the scope of the offence of cyber harassment.

Clause 5 seeks to amend section 30 of the Act to expand the scope of the offence of phishing.

Clause 6 seeks to introduce a new section 42A for the offence of unauthorized SIM-swap.

Statement on the delegation of legislative powers and limitation of fundamental rights and freedoms.

This Bill does not delegate legislative powers nor does it limit fundamental rights and freedoms.

Statement as to whether the Bill concerns county governments

Paragraph 13 of Part 2 of the Fourth Schedule to the Constitution provides that the control of pornography is a function of the county governments.

Therefore, the Bill concerns county governments in terms of Article 110(1)(a) of the Constitution as it contains provisions that affect the functions and powers of the county governments as set out in the Fourth Schedule to the Constitution.

Statement as to whether the Bill is a money Bill within the meaning of Article 114 of the Constitution

The enactment of this Bill shall not occasion additional expenditure of public funds.

Dated the 28th June, 2024.

ADEN DAUDI MOHAMED,
Member of Parliament.

Section 2 of Cap 79C which is intended to be amended—

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 Coordination 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.

Section 6 of Cap 79C which is intended to be amended—

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.

Section 27 of Cap 79C which is intended to be amended—

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.

Section 30 of Cap 79C which is intended to be amended—

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.

Section 42 of Cap 79C which is intended to be amended—

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.