SPECIAL ISSUE

Kenya Gazette Supplement No. 110 (Senate Bills No. 12)

REPUBLIC OF KENYA

KENYA GAZETTE SUPPLEMENT

SENATE BILLS, 2016

NAIROBI, 5th July, 2016

CONTENT

Bill for Introduction into the Senate—

PRINTED AND PUBLISHED BY THE GOVERNMENT PRINTER, NAIROBI

CYBER SECURITY AND PROTECTION BILL, 2016

ARRANGEMENT OF CLAUSES

Clause

CYBER SECURITY AND PROTECTION BILL, 2016

A Bill for

AN ACT of Parliament to provide for the enhancement of security in cyberspace; to provide for the prohibition, prevention, detection, response, investigation and prosecution of cybercrimes; to establish the national cyber security response unit; and for connected purposes.

ENACTED by the Parliament of Kenya, as follows-

PART I — PRELIMINARY

Short title.

1. This Act may be cited as the Cyber Security and Protection Act, 2016.

Interpretation.

2. In this Act-

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

"child" means an individual who has not attained the age of eighteen years;

"computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, software and communication facilities which are connected or related as a system or network;

"critical infrastructure" means vital virtual systems and assets whose incapacity or destruction would have a debilitating impact on the security, economy, public health and safety of the country;

"cybersecurity threat" means an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system;

"Director" means a person appointed under section 3;

"intimate image" means any photograph, motion picture film, videotape, digital image, or any other recording or transmission of another person who is identifiable from the image itself or from information

displayed with or otherwise connected to the image, and that was taken in a private setting, is not a matter of public concern, and depicts sexual activity, including sexual intercourse or a person's intimate body parts, whether nude or visible through less than opaque clothing, including the genitals; and

"Unit" means the National Cyber Threat Response Unit established under section 3.

PART II — CYBER SECURITY AND PROTECTION

National Computer Threat Response Unit.

3. (1) There is established the National Cyber Threat Response Unit.

(2) The unit shall be a department within the Ministry responsible for matters relating to information and technology and shall comprise-

(a) a Director appointed by the cabinet secretary;

(b) a representative of the National Intelligence Service designated by the Director-General of the Service;

(c) a representative of the Communications Authority of Kenya designated by the chairperson of the Board of the Authority;

(d) a representative of the Office of the Director of Public Prosecutions designated by the Director of Public Prosecutions; and

(e) such other officers as the cabinet secretary may appoint to the unit.

(3) A person is qualified for appointment under subsection (2) (a) if that person-

(a) holds at least a degree in information, communication and technology security or a related field from a university recognized in Kenya;

(b) has at least ten-year's experience in the detection, investigation or prosecution of crimes related to cyber security; and

(c) meet the requirements of Chapter six of the Constitution.

4. The functions of the Unit shall be to— Functions of the unit.

(a) receive reports of interruptions, disruptions or interference with computer systems or networks;

(b) investigate the interruption, disruption or any other unlawful interference with a computer system or network;

(c) advise on measures to prevent and combat computer related offences, cybercrimes, threats to national cyberspace and other cyber security related matters;

(d) establish and maintain a national computer forensic laboratory and coordinate utilization of the facility by all law enforcement, security and intelligence agencies;

(e) coordinate the country's involvement in international cyber security cooperation to ensure the integration of the country's into the global frameworks on cyber security;

(f) establish a program to award grants to institutions of higher learning that establish cyber security research centers;

(g) coordinate the sharing of information related to cybersecurity risks and incidents between the public and private sector;

(h) conduct analysis of cybersecurity risks and incidents;

(i) provide timely technical assistance, risk management support, and incident response measures to public and private entities with respect to cybersecurity risks and incidents;

(j) develop procedures for the sharing of-

(i) cyber threat indicators with public and private entities; and

(ii) cyber security best practices that are developed based on ongoing analysis of cyber threat indicators and information including the challenges faced by small businesses in accessibility and

implementation of measures to combat cyber crimes.

Cooperation.

5. The Director shall ensure that the Unit cooperates and liaises with other government entities involved in cybersecurity matters including the ministry responsible for matters relating to information, communication and technology.

Critical infrastructure.

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

(2) The Cabinet Secretary 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 country;

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

(d) failure or substantial disruption of the country's money market; and

(e) adverse and severe effect of the country's security including intelligence and military services.

(3) The Cabinet Secretary shall, within seven days of designating a system as critical infrastructure, inform the owner or operator of the system designated as critical infrastructure of the reasons why the system has been designated as critical infrastructure.

Duties of the Cabinet Secretary

7. The Cabinet Secretary shall, in consultation with entities that own or operate critical infrastructure-

(a) conduct an assessment of the cybersecurity 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 at driving security innovation and secure practices;

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

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

Duties of owners or operators.

8. (1) The owner or operator of a system designated as critical infrastructure shall report to the Cabinet Secretary any incidents likely to constitute a cyber threat and the action the owner or operator intends to take to prevent the threat.

(2) Upon receipt of a report under subsection (1) the Cabinet Secretary shall provide the necessary assistance, including financial and technical assistance, to the owner or operator of a critical infrastructure.

(3) Notwithstanding the provisions of subsection (2) the Cabinet Secretary may institute an investigation of a cyber threat and may take necessary steps to secure any critical infrastructure.

(4) The Cabinet Secretary shall submit to Parliament a report of the cyber threats reported by the owners or operators of critical infrastructure and the action taken to deal with the threat.

Information sharing agreements.

9. (1) Private entities may enter into information sharing agreements with public entities or with each other.

(2) An agreement under subsection (1) shall only be entered into for the following purposes-

(a) to ensure cybersecurity;

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

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

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

Review of information.

10. Prior to the sharing of information under section 9, 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 cyber security threat, and if so, remove such information.

Protection of certain information.

11. A person shall not, pursuant to an information sharing agreement 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.

PART IV — OFFENCES AND PENALTIES

Unlawful access to a computer system.

12. (1) A person who, without authorization intentionally accesses in whole or in part, a computer system or network, commits an offence and is liable on conviction to a term of imprisonment not exceeding five years or to a fine not exceeding one hundred thousand shillings or both.

(2) A person who knowingly and intentionally traffics in any password or similar information through which a computer may be accessed without lawful authority, commits an offence and is liable on conviction to a fine not exceeding one hundred thousand shillings or to a term of imprisonment not exceeding three years or both.

(3) A person who, with the intent to commit an offence under this section, uses any device to avoid detection or otherwise prevent identification or attribution with the act or omission, 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 three years or both.

System interference.

13. A person who without lawful authority, intentionally causes the hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or any other form of interference with the computer system, which prevents the computer system or any part of the computer from functioning in accordance with its intended purpose, commits an offence and is liable on conviction to imprisonment for a term not exceeding three years or to a fine not exceeding two hundred thousand shillings or both.

Unlawful interceptions.

14. (1) A person, who intentionally and without authorization, intercepts by technical means, non-public transmissions of computer data, content, or traffic data,

including electromagnetic emissions or signals from a computer, computer system or network carrying or emitting signals, to or from a computer, computer system or connected system or network, commits an offence and is liable on conviction to imprisonment for a term of not more than five years or to a fine of not more than one hundred thousand shillings or both.

(2) 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 imprisonment for a term not exceeding two years or to a fine not exceeding one hundred thousand shillings or both.

(3) 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 to imprisonment for one year or a fine not exceeding one hundred thousand shillings or both.

Interception of electronic messages or money transfers.

15. 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 term of imprisonment not exceeding seven years or to a fine not exceeding two hundred thousand shillings or both.

Wilful misdirection of electronic messages.

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

Forgery.

17. A person who inputs, alters, deletes or suppresses any data in a computer or computer network resulting in inauthentic data with the intention that such inauthentic data will be considered or acted upon as if it were authentic or genuine, commits an offence and is liable on conviction to imprisonment for a term of not less than three years or to a fine not exceeding three hundred thousand shillings or both.

Fraud.

18. (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 imprisonment for a term not exceeding five years or to a fine not exceeding five hundred thousand shillings or both.

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

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

(5) A person convicted under subsection (3) shall forfeit the proprietary interest in the stolen money or property to the bank, financial institution or the customer.

Unauthorized modification of data.

19. A person who with intent and without lawful authority directly or indirectly modifies or causes modification of any data held in any computer system or network, commits an offence and is liable on conviction to imprisonment for a term of not more than three years or to a fine not exceeding two hundred thousand shillings or both.

Cyber terrorism.

20. (1) A person who accesses or causes to be accessed a computer or computer system or network for purposes of terrorism, commits an offence and is liable upon conviction to life imprisonment.

(2) For the purpose of this section, "terrorism" shall have the same meaning under the Prevention of Terrorism Act. No. 30 of 2012

Issuance of false e-instructions.

21. A person authorized to use a computer or other electronic devices for financial transactions including posting of debit and credit, 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, to a fine not exceeding one hundred thousand shillings or to a term of imprisonment not exceeding five years or both.

Phishing.

22. 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 a term of imprisonment for a term not exceeding three years or both.

Reporting of cyber threat.

23. (1) A person who operates a computer system or a computer network, whether public or private, shall immediately inform the Unit of any attacks, intrusions and other disruptions to the functioning of another computer system or network within seven days 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 the date on which notification is provided about how the breach occurred;

(b) an estimate of the number of people affected by the breach and an assessment of the risk of harm to the affected individuals; and

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

(3) The unit 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.

Identity theft and impersonation.

24. 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 a term of imprisonment not exceeding three years or both.

Electronic distribution of pornography.

25. (1) A person who intentionally uses a computer system or network for producing, offering or making available, distributing or transmitting, storing, procuring or possessing pornography commits an offence and shall be liable, upon conviction to a term of imprisonment not exceeding twenty years or a fine not exceeding two hundred thousand shillings or both fine and imprisonment.

Child exploitation.

26. A person who, through any computer system or network, proposes, grooms or solicits to meet a child for the purpose of engaging in sexual activities with the child, commits an offence and shall be liable upon conviction to a term of imprisonment not exceeding twenty five years or to a fine not exceeding two hundred and fifty thousand shillings or both.

Cyber-bullying

27. A person who intentionally transmits or causes the transmission of any communication through a computer system or network to bully, threaten or harass another person, where such communication places another person in fear of death, violence or bodily harm, commits an offence and is liable on conviction to a term of imprisonment not exceeding five years or a fine not exceeding two hundred thousand shillings or both.

Wrongful distribution of intimate images

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

Cyber squatting

29. 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 imprisonment for a term not exceeding two years or a fine of not exceeding two hundred thousand shillings or both.

Importation and fabrication of e-tools.

30. A person who unlawfully produces, supplies, adapts, manipulates or procures for use, imports, exports, distributes, offers for sale or otherwise makes available any device, including a computer program, a computer password, access code or similar data by which the whole or any part of a computer system may be accessed without authorization, commits an offence and shall be liable, on conviction, to a fine not exceeding one hundred thousand shillings or to a term of imprisonment not exceeding two years or both.

Employee responsibility.

31. (1) Without prejudice to any contractual agreement between the employer and the employee, an employee shall relinquish all codes and access rights to their employer's computer network or system immediately upon termination of employment.

(2) A person who contravenes the provision of this section commits an offence and shall be liable, on conviction, to a fine not exceeding fifty thousand shillings or to a term of imprisonment not exceeding one year or both.

PART III — MISCELLANEOUS PROVISIONS

Report.

32. The Cabinet Secretary shall submit an annual report to the National Assembly and the Senate of-

(a) measures put in place to enhance cyber security;

(b) the cyber threat incidents reported within the relevant period to which the report relates;

(c) an assessment of the information sharing relationship between Kenya and other countries relating to cyber threats;

(d) an assessment of technologies or capabilities that would enhance the country's ability to prevent and respond to cybersecurity threats;

(e) an assessment of any technologies or practices used by the private sector that could be employed

to assist the government in preventing and responding to cybersecurity threats; and

(f) any other information requested by either house of Parliament.

Regulations.

33. The Cabinet Secretary shall make regulations for the better carrying out of the provisions of this Act.

Amendments to Cap. 411A.

34. (1) Section 83C of the Kenya Information and Communication Act is amended by-

(a) in subsection (1) by deleting paragraph (g) and (h);

(b) repealing subsection (2) and substituting therefor the following new subsection-

(2) The Cabinet Secretary may, in consultation with the Authority, make Regulations with respect to the functions of the Authority relating to cyber security under this Act.

Repeals. Cap. 411A.

35. The Kenya Information and Communication Act is amended by-

(a) repealing section 83W;

(b) repealing section 83X;

(c) repealing section 83Y;

(d) repealing section 83Z;

(e) repealing section 84A;

(f) repealing section 84B;

(g) repealing section 84C

(h) repealing section 84D;

(i) repealing section 84E;

(j) repealing section 84F; and

(k) repealing section 84G.

MEMORANDUM OF OBJECTS AND REASONS

Statement of the Objects and Reasons for the Bill

The principal object of this Bill is to provide increased security in cyberspace and to provide for the prohibition of certain acts in the use of computers. The world is increasingly run through the use of computer technology. Through this virtual system, people are able to send money, store large amount of data, communicate across continents at the touch of a button, control security infrastructure, run businesses and enhance human connectivity.

However while computers have increased human connectivity and have a direct impact on development, they also pose a risk to the users. At a larger scale they may be used to disrupt the delivery of essential services and in effect cause irreparable harm to the economy and lives of people. At a small scale they may be used as a means to harass and intimidate individuals. Therefore, while computers have increased human connectivity, played a major role in development and ensured the effective delivery of certain services, they have also exposed society to certain vulnerabilities. This Bill therefore seeks to address and prohibit any activity the proper functioning of computer systems or the improper use of computer systems in order to protect life and property.

The Bill proposes to establish a national cyber security response unit in the Ministry responsible for matters relating to security. The unit will be responsible for receiving and investigating reports on cyber threat incidences, running a national computer forensic lab for the benefit of law enforcement agencies, advising on measures to combat cyber threats and supporting research into cyber security. The Bill also proposes a mechanism to enable the sharing of information between private entities on cyber threats under certain circumstances. This is intended to enhance awareness and preparedness in combating cyber threats.

The Bill further proposes the identification and designation of certain systems as critical infrastructure. This is in appreciation of the vital role such systems play in the security and economic well-being of the country and is intended to ensure that the owners of such systems receive the necessary support from the State.

The Bill also proposes to proscribe certain conduct in order to ensure the safety of computer systems and that such systems are not used for unlawful purposes.

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

Clause 31 of the Bill provides for the power of the Cabinet Secretary to make Regulations for the better carrying out of the provisions of the legislative proposal.

The Bill provides for the sharing of data by private entities, between themselves or with the government, but only for the purpose of ensuring cyber security. The Bill however prohibits the sharing of certain types of information for instance information relating to the health status of another person without the prior consent of that person.

Statement on how the Bill concerns county governments

Computer systems and the internet are increasingly being relied upon for the delivery of certain services such as commerce, communication, data storage and social activities. County governments are not exempt from this virtual revolution. County governments rely on the proper functioning of computer systems to deliver services in the areas assigned to them under Part 2 of the Fourth Schedule to the Constitution.

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

Statement that the Bill is not a money Bill within the meaning of Article 114 of the Constitution

This Bill proposes to establish a national cybercrime response unit which will be an office in the Ministry responsible for matters relating to security. The Bill seeks to take advantage of existing administrative and financial structures and any monies required for the running of the unit shall be met by the funds appropriated by the National Assembly to the parent Ministry.

This Bill is therefore not a money Bill within the meaning of Article 114 of the Constitution.

Dated the 4th July, 2016.

MUTAHI KAGWE,
Chairperson, Committee on Information and Technology.