ESWATINI
GOVERNMENT GAZETTE
EXTRAORDINARY

VOL. LX] MBABANE, Friday, MARCH 4th 2022 [No. 42

CONTENTS

PUBLISHED BY AUTHORITY

PART B

THE COMPUTER CRIME AND CYBERCRIME ACT, 2022

(Act No. 6 of 2022)

I ASSENT

MSWATI III
KING OF THE KINGDOM OF ESWATINI

....., 2022

AN ACT
ENTITLED

AN ACT to criminalize offences committed against, and through the usage of computer systems and electronic communications networks; to provide for investigation and collection of evidence for computer and network related crimes; to provide for the admission of electronic evidence for such offences, to establish the National Cybersecurity Advisory Council, to give powers to the Commission to regulate and coordinate cybersecurity matters and to provide for incidental matters.

ENACTED by the King and the Parliament of the Kingdom of Eswatini.

ARRANGEMENT OF SECTIONS

PART IV
PROCEDURAL LAW

PART V
LIABILITY

PART VI
GENERAL PROVISIONS

PART I
PRELIMINARY PROVISIONS

Short title and Commencement

1. (1) This Act shall be cited as the Computer Crime and Cybercrime Act, 2022.

(2) This Act shall come into operation on the date of publication in the Government Gazette.

Interpretation

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

"abetting" means to encourage or assist someone to commit a crime or other offence;

"access" in relation to section 3 means logging into a computer system;

"access provider" means any person, natural or juristic, providing an electronic data transmission service by transmitting information provided by or to a user of the service in a communication network or providing access to a communication network;

"caching provider" means any person natural or juristic providing an electronic data transmission service by automatic, intermediate and temporary storing information, performed for the sole purpose of making more efficient the information's onward transmission to other users of the service upon their request;

"child" means a person under the age of eighteen (18) years;

"child pornography" means any material that depicts, presents or represents;

(a) a child engaged in sexual conduct, or in the nude without a justifiable cause; or

(b) images representing a child engaged in sexual conduct;

which includes, but is not limited to, any audio, visual or text pornographic material.

"Commission" means the Eswatini Communications Commission established under the Eswatini Communications Commission Act, 2013;

"computer system" or "information system" means a device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data or any other function;

"computer data" means any representation of facts, concepts, information (being either texts, audio, video or images) machine-readable code or instructions, in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

"computer data storage medium" means any article or material from which information is capable of being reproduced, with or without the aid of any other article or device;

"Court" means a Magistrate Court or the High Court;

"critical infrastructure" means computer systems, devices, networks, computer programs, computer data, vital to the country that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on, national or economic security,

national public health and safety, national elections or any combination of those matters; or physical infrastructure, assets or systems declared as such by Government

"cyberbullying" means the use of electronic communication to bully a person typically by sending messages of an intimidating or threatening nature;

"Cybersex" means sexual activity or fantasy which may lead to sexual arousal or pleasure gained through communication, for that purpose, by computer system with another person;

"cyberstalking" means the use of the Internet or other electronic means to inflict repeated unwarranted actions on a natural or juristic person(s). Such actions may include false accusations, defamation, slander, libel, monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten, embarrass or harass; which may result in mental or corporate abuse;

"cyberterrorism" means deliberate actions perpetrated using computer systems with the intention to cause serious harm to human lives, way of life, infrastructure or the economy or to cause fear or terror in a community, nation or group of nations;

"device" includes but is not limited to –

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

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

(c) input devices such as keyboards, mouse, track pad, scanner and digital cameras and any other gadget that can transfer information to a computer system; or

(d) output devices such as printers and screens and any other gadget that is able to receive information from a computer system.

"electronic communication" means any transfer of signs, signals or computer data of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system;

"extortion" means an act of demanding favour or benefit from a person through coercion, or arising from an advantage one holds over the victim, by threatening to inflict harm to his person, family members, reputation or property by unleashing the advantage he holds over the victim;

"hinder" in relation to a computer system includes but is not limited to –

(a) cutting the electricity supply to a computer system;

(b) causing electromagnetic interference to a computer system;

(c) corrupting a computer system by any means; and

(d) inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

"hosting provider" means any natural or legal person providing an electronic data transmission service by storing information provided by a user of the service;

"hyperlink" means characteristic or property of an element such as a symbol, word, phrase, sentence, or image that contains information about another source and points to and causes to display another document when executed;

"hyperlink provider" means any natural or legal person providing one or more hyperlinks;

"interception" includes but is not limited to the acquiring, viewing and capturing of any computer data communication whether by wire, wireless, electronic, optical, magnetic, oral or other means, during transmission through the use of any technical device;

"internet service provider" means any natural or legal person mentioned in sections 33 to 38 that provides users' services;

"law enforcement agent" means personnel employed and representing agencies established under an Act of Eswatini with the requisite power to exercise rights given under that Act when undertaking their responsibilities. These may include Royal Eswatini Police, Anti-Corruption Commission, Eswatini Revenue Authority and Eswatini Communications Commission;

"Minister" means the Minister responsible for Information, Communications and Technology;

"multiple electronic mail messages" means a mail message including e-mail and instant messaging sent to more than one recipient;

"pornography" means a visual, text or audio presentation, simulated or real of –

(a) a person who is, or is depicted as participating in or assisting another person to engage in sexual act or sexual violations or lewd display of nudity which is intended for sexual gratification;

(b) explicit sexual conduct which degrades a person or which constitutes incitement to cause harm; or

(c) a sexual act between a person and an animal.

"racist, xenophobic and hate speech," means any material, including but not limited to any image, video, audio recording or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals; which may be based on race, colour, descent, national or ethnic origin, religion, creed or social or economic standing, political opinion or disability;

"remote forensic tool" means an investigative tool including software or hardware installed on or in relation to a computer system or part of a computer system and used to perform tasks that include but are not limited to keystroke logging or transmission of an IP-address.

"seize" includes: -

(a) activating any onsite computer system and or computer data storage media;

(b) making and retaining a copy of computer data, including by using onsite equipment;

(c) maintaining the integrity of the relevant stored computer data;

(d) rendering inaccessible or removing, computer data in the accessed computer system;

(e) taking a printout of output of computer data; or

(f) securing or taking custody of a computer system or part of it or a computer-data storage medium.

"sexual grooming" means intentionally befriending or establishing an emotional connection with a child, or an adult who is legally not able to consent, to train them to agree to participate, or lower their inhibitions, in acts of sexual abuse or exploitation;

"spamming" or "spam" is the use of messaging systems to send unsolicited mail messages, text messages or adverts, usually for marketing or promotional purposes to customers, former or potential customers or other recipients;

"spoofing" means hiding the actual source address or identity behind another identity to appear as if the email or information is from the legitimate address;

"traffic data" means computer data that relates to a communication by means of a computer system and generated by a computer system that is part of the chain of electronic communication; and may show one or more of the following, the communication's origin, destination, route, time, date, size, duration or the type of underlying services;

"thing" includes but is not limited to –

(a) a computer system or part of a computer system;

(b) another computer system, if-

(i) computer data from that computer system is available to the first computer system being searched; and

(ii) there are reasonable grounds for believing that the computer data sought is stored in the other computer system; or

(c) a computer data storage medium;

"trafficking" means initiating, carrying out, or being party to, actively or passively, an act of moving or facilitating the illegal movement or illegal transportation of people, animals, plants, money or goods within a country or across international borders for trade purposes to fulfil personal goals through the use of a computer system;

"uttering" means the publishing as true a false, forged, altered or counterfeit record, instrument, or other writing knowing it to be false, altered, forged or counterfeit, with intent to injure or defraud;

"website defacement" means the act of attacking a website by changing the visual appearance, adding, changing, deleting or replacing content by a party or parties not authorized by the website owner.

PART II
OFFENCES AND PENALTIES

Illegal Access

3. (1) A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, accesses the whole or any part of a computer system commits an offence, and is liable, on conviction, to a fine not exceeding three hundred (300) thousand Emalangeni or to imprisonment for a period not exceeding three (3) years or both.

(2) Where the person who accesses a computer system in subsection (1) infringes security measures with the intention of obtaining computer data, that person shall on conviction be liable to a fine not exceeding five hundred (5) thousand Emalangeni or to imprisonment not exceeding five (5) years or both.

Illegally remaining logged onto a computer

4. (1) A person who intentionally, without lawful excuse or justification, infringes security measures or with the intention of obtaining computer data or with other dishonest intent, remains logged in a computer system or part of a computer system or continues to use a computer system commits an offence and is liable, on conviction, to a fine not exceeding one hundred (1) thousand Emalangeni or to imprisonment for a period not exceeding three (3) years or both.

Illegal interception

5. (1) A person who intentionally without lawful excuse or justification or in excess of a lawful excuse or justification, intercepts, by electronic means –

(a) any non-public transmission to, from or within a computer system; or

(b) electromagnetic emissions from a computer system -

commits an offence and is liable, on conviction, to a fine not exceeding three hundred (300) thousand Emalangeni or to imprisonment for a period not exceeding three (3) years or both.

Illegal data interference

6. (1) Subject to subsections 2 and 5, a person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification does any of the following acts –

(a) damages or deteriorates computer data;

(b) deletes computer data;

(c) alters computer data;

(d) renders computer data meaningless, useless or ineffective;

(e) obstructs, interrupts or interferes with the lawful use of computer data;

(f) obstructs, interrupts or interferes with any person in the lawful use of computer data; or

(g) denies access to computer data to any person authorized to access it,

commits an offence and is liable, on conviction, to a fine not exceeding five hundred (5) thousand Emalangeni or to imprisonment for a period not exceeding three (3) years or both.

(2) A person, who intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification commits any act described in this section, in order to deny access, including a partial denial of service to any person authorised to access it, commits an offence and is liable, on conviction, to a fine not exceeding five hundred (5) thousand Emalangeni or to imprisonment for a period not exceeding three (3) years or both.

(3) A person who intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification-

(a) communicates, discloses or transmits any computer data, program, access code or command to any person not authorized to access the computer data, program, code or command;

(b) accesses or destroys any computer data, for purposes of concealing information necessary for an investigation into the commission or otherwise of an offence; or

(c) receives computer data that that person is not authorized to receive,

commits an offence and is liable, on conviction, to a fine not exceeding five hundred (5) thousand Emalangeni or to imprisonment for a period not exceeding three (3) years or both.

(4) A person, who intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification destroys or alters computer data where that data is required to be kept or maintained by a law in force or any evidence in relation to any proceeding under this Act by –

(a) creating, destroying, mutilating, removing or modifying data or a program or any other form of information existing within or outside a computer or computer network;

(b) activating, installing or downloading a program that is designed to create, destroy, mutilate, remove or modify data, program or any other form of information existing within or outside a computer or computer network; or

(c) creating, altering, or destroying a password, personal identification number, code or method used to access a computer or computer network,

commits an offence and is liable, on conviction, to imprisonment for a period not exceeding ten (10) years or a fine not exceeding five hundred (5) thousand Emalangeni, or both.

(5) A person shall not be liable under this section where the person –

(a) is acting pursuant to measures that can be taken under Part V of this Act; or

(b) is acting on the basis of any other statutory power.

(6) Where an offence under this section is committed in relation to data that is in a critical database or that is concerned with national security or the provision of an essential service, the person shall be liable, on conviction, to a fine not exceeding one (1) million Emalangeni or to imprisonment for a period not exceeding ten (10) years.

(7) For the purposes of this section, it is immaterial whether an illegal interference or any intended effect of it, is permanent or temporary.

Data espionage

7. A person who, intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification obtains for that person or for another person, computer data which is not meant for that person and which is specially protected against unauthorized access, commits an offence and is liable, on conviction, to a fine not exceeding five hundred (5) thousand Emalangeni or to imprisonment for a period not exceeding four (4) years or both.

Illegal system interference

8. (1) A person who intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification –

(a) hinders or interferes with the functioning of a computer system; or

(b) hinders or interferes with a person who is lawfully using or operating a computer system,

commits an offence and is liable, on conviction, to a fine not exceeding five hundred (5) thousand Emalangeni or to imprisonment for a period not exceeding four (4) years or both.

(2) A person who intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification, seizes or destroys any computer storage medium, commits an offence and is liable on conviction to a fine not exceeding five hundred (500) thousand Emalangeni or to imprisonment for a period not exceeding four (4) years or both.

(3) A person who intentionally without lawful excuse or justification or in excess of a lawful excuse or justification, hinders or interferes with a computer system that is exclusively for the use of critical infrastructure operations, or in the case in which such is not exclusively for the use of critical infrastructure operations, but is used in critical infrastructure operations and that conduct affects that use or impacts the operations of critical infrastructure, commits an offence, and shall on conviction, be liable to a fine not exceeding one (1) million Emalangeni or to imprisonment for a period not exceeding ten (10) years or both.

Illegal devices

9. (1) A person who –

(a) intentionally without lawful excuse or justification or in excess of a lawful excuse or justification, produces, sells, introduces, spreads, procures for use, use imports, exports, distributes or otherwise makes available -

(i) a device, including a computer program, that is designed or adapted for the purpose of committing an offence under this Part; or

(ii) a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed; or

(iii) a software code that damages a computer or computer system –

(aa) with the intent that it be used by any person for the purpose of committing an offence as defined under this Part; or

(bb) has an item mentioned in subparagraph (i) or (ii) in the possession of that person, with the intention that the item be used by any person for the purpose of committing any offence under this Part, commits an offence and is liable on conviction, to a fine not exceeding one million (1) Emalangeni or to imprisonment for a period not exceeding ten (10) years or both.

Computer related forgery and uttering

10. (1) A person, who intentionally without lawful excuse or justification or in excess of a lawful excuse or justification inputs, alters, deletes, or suppresses computer data, resulting in inauthentic data, with the intention 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 a fine not exceeding one hundred (1) thousand Emalangeni or to imprisonment for a period not exceeding two (2) years or both.

(2) If the above-mentioned offence is committed by sending out multiple electronic mail messages from or through a computer system, the penalty shall be, on conviction, be one hundred (1) thousand Emalangeni or to imprisonment for a period not exceeding two (2) years or both.

Computer related fraud

11. A person who intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification causes loss of property to another person by –

(a) any input, alteration, deletion or suppression of computer data; or

(b) any interference with the functioning of a computer system,

with a fraudulent or dishonest intention of procuring, without permission, an economic benefit for that person or for another person, commits an offence, and shall on conviction, be liable to a fine not exceeding five hundred (5) thousand Emalangeni or to two (2) times the value of said property, whichever is higher, or to imprisonment for a period not exceeding three (3) years or both.

Phishing

12. A person who, without a lawful excuse or justification, through-

(a) an email;

(b) spoofed email;

(c) website;

(d) social media; or

(e) text message

lures, deceives or threatens another to give money or other value or to reveal sensitive information, account login details, bank account or credit card information, or the like commits a crime and on conviction is liable to a fine not exceeding one hundred (1) thousand Emalangeni or to imprisonment not exceeding five (5) years or both.

Cyber-terrorism

13. A person who intentionally without legal justification or legal excuse, using a computer system-

(a) through conventional methods, launches an attack on telecommunications or computer networks;

(b) launches attacks using physical devices, computer programs or other electronic means to -

(i) render the financial or banking system of the country or city unusable;

(ii) compromise the defence system of the country;

(iii) seriously disrupt or interfere with the operations of the electricity grid, aviation control system, tax management systems, population register, government payroll and cabinet system; or

(c) funds or raises funds with the purpose of financing carrying out the acts listed in (a) and (b),

commits and offence of cyberterrorism and is liable on conviction to a fine not exceeding five hundred (5) thousand Emalangeni or to imprisonment for a period not ten (10) years or both.

Child pornography

14. (1) A person who intentionally and without lawful excuse or justification –

(a) produces child pornography;

(b) offers or makes available child pornography through a computer system;

(c) distributes or transmits child pornography through a computer system;

(d) procures or obtains child pornography through a computer system for oneself or for another person;

(e) possesses child pornography in a computer system or on a computer-data storage medium; or

(f) knowingly obtains access to child pornography, through information and communication technologies,

commits an offence and is liable, on conviction, to a fine not exceeding one (1) million Emalangeni or to imprisonment for a period not exceeding ten (10) years or both.

(2) It is a defence to a charge of an offence under sub-section (1) (b) to (1) (f) if the person establishes that –

(a) the child pornography was for a bona fide law enforcement purpose; or

(b) the conduct that is alleged to constitute the offence was for a genuine artistic, educational, legal, medical, scientific or public benefit purpose, including Eswatini cultural events.

(3) A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification makes pornography available to one or more children through a computer system or facilitates the access of children to pornography through a computer system commits an offence and is liable, on conviction, to a fine not exceeding one hundred (1) thousand or to imprisonment for a period not exceeding five (5) years or both.

(4) A person who engages in cybersex with a child or any person who is not legally able to consent, commits an offence and is liable on conviction to a fine not exceeding one hundred (1) thousand or imprisonment for a period not exceeding five (5) years or both.

(5) Any person who subjects a child, or an adult who cannot legally consent, to sexual grooming, commits an offence and is liable on conviction, to a fine not exceeding three hundred (3) thousand Emalangeni or imprisonment for a period not exceeding five (5) years or both.

Prohibition of distribution or publication of pornography

15. (1) A person, who -

(a) distributes, publishes, advertises or exposes material which is pornographic to child or an adult without the consent of that adult;

(b) publishes or exhibits any pornographic material without printing in such his or her name and the prescribed particulars of his or her address or without indicating the age restriction or consumer advice; or

(c) broadcasts a pornographic film whether publicly or privately to children or non-consenting adults,

commits an offence and on conviction, shall be liable to pay a fine not exceeding one hundred (1) thousand Emalangeni or to a term of imprisonment not exceeding one (1) year or to both.

(2) Where the person referred to under subsection (1) has parental power or control over that child, and that person commits the offence mentioned in subsection (1), that person shall, on conviction, be liable to pay a fine of not exceeding one hundred (1) thousand Emalangeni or to a term of imprisonment not exceeding one (1) year or both.

Identity related crimes

16. A person who intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification, by using a computer system in any stage of the offence, intentionally transfers, acquires, possesses or uses a means of identification of another person with the intention to commit, or to aid or abet, or in connection with, any unlawful activity that, commits an offence and is liable, on conviction, to a fine not exceeding two hundred (2) thousand Emalangeni or to imprisonment for a period not exceeding five (5) years or both.

Cyberbullying and Cyberstalking

17. (1) A person who intentionally engages or solicits or abets another in the furtherance of cyberbullying of another person commits an offence and is liable, on conviction, to a fine not exceeding one hundred (1) thousand Emalangeni or to imprisonment for a period not exceeding two (2) years or both.

(2) A person who intentionally engages in cyberstalking or solicits or abets another in the furtherance of the act of cyberstalking commits an offence and is liable, on conviction to a fine not exceeding one hundred (1) thousand or to imprisonment for a period not exceeding two (2) years or both.

Extortion

18. Any person who intentionally and unlawfully uses the internet, email or any computer system platform to commit the act of extortion on another person, natural or juristic, commits an offence and is a liable on conviction to a fine not exceeding ten times the amount sought to be extorted or imprisonment for a period not exceeding five (5) years.

Website defacement

19. A person who intentionally or without lawful excuse commits or participate in the website defacement belonging to another entity commits a crime and is on conviction liable to a fine not exceeding one hundred (1) thousand Emalangeni or imprisonment for a period not exceeding two (2) years or both.

Racist, hate speech or xenophobic material

20. A person who intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification –

(a) produces racist, hate speech or xenophobic, material with the intention of distributing it through a computer system;

(b) offers or makes available racist, hate speech or xenophobic material through a computer system; or

(c) distributes or transmits racist, hate speech or xenophobic material through a computer system,

commits an offence and is liable, on conviction, to a fine not exceeding two hundred (2) thousand Emalangeni or to imprisonment for a period not exceeding one (1) year or both.

Racist, hate speech and xenophobic motivated insult

21. A person who intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification publicly, through a computer system, uses language that harms the reputation or feelings of –

(a) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or

(b) a group of persons which is distinguished by any of these characteristics,

commits an offence and is liable, on conviction, to a fine not exceeding one hundred (1) thousand Emalangeni or to imprisonment for a period not exceeding one (1) year or both.

Genocide and crimes against humanity

22. A person who intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification distributes or otherwise makes available, through a computer system to the public or to another person, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity that aids, induces or incites others to commit such acts, or incites, instigates, commands, or procures any other person to commit genocide or crimes against humanity, commits an offence and is liable, on conviction, to a fine not exceeding five (5) million Emalangeni or to imprisonment for a period not exceeding twenty (20) years or both.

Trafficking in humans, endangered species or illegal merchandise

23. A person who without justification or lawful excuse participates in the trafficking of humans, endangered animals, protected plants or any goods that he is not authorised to, using electronic or online methods commits an offence and is liable on conviction to a fine not exceeding one hundred (1) thousand Emalangeni or imprisonment for a period not exceeding five (5) years or both.

Spam or Spamming

24. (1) A person who intentionally and without lawful excuse or justification –

(a) initiates the transmission of spam messages from or through a computer system;

(b) uses a hidden or disguised computer system to relay or retransmit multiple electronic mail messages, with the intention to deceive or mislead users, or any electronic mail or internet service provider, as to the origin of such messages; or

(c) materially falsifies header information in multiple electronic mail messages and intentionally initiates the transmission of such messages,

commits an offence and is liable, on conviction, to a fine not exceeding one hundred (1) thousand Emalangeni or to imprisonment for a period not exceeding two (2) years or both.

(2) It shall not be an offence under this section where –

(a) the transmission of multiple electronic mail messages from, or through such computer system was done within a customer or business relationship; or

(b) the recipient of such electronic mail messages has not opted out of the business or customer relationship.

Denial of service and botnets

25. (1) Any person who, remotely or otherwise takes illegal control of a computer system in a network or an entire network of computer systems or network components, partially or fully, commits an offence and is liable on conviction to a fine not exceeding five (5) million Emalangeni or imprisonment for a period not exceeding ten (10) years or both.

(2) Any person who intentionally, without justification causes or launches an attack with data traffic on a computer system or network so as to overwhelm the network resources, resulting in slowed or denied service, commits an offence and is liable on conviction to a fine not exceeding five (5) million Emalangeni or imprisonment for a period not exceeding ten (10) years or both.

Disclosure of details of an investigation

26. A service provider who receives an order related to a criminal investigation that explicitly stipulates that confidentiality is to be maintained or such obligation is stated by law, and intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification discloses –

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

(b) anything done under the order; or

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

commits an offence and is liable on conviction to a fine not exceeding one hundred (1) thousand Emalangeni or to imprisonment for a period not exceeding two (2) years or both.

Failure to permit assistance

27. A person who intentionally fails, without lawful excuse or justification, or in excess of a lawful excuse or justification to permit or assist a person based on an order specified in sections 29 to 31, commits an offence and is liable on conviction to a fine not exceeding one hundred (1) thousand Emalangeni or to imprisonment for a period not exceeding two (2) years or both.

Harassment utilising means of electronic communication

28. A person who intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification initiates any electronic communication, with the intention to coerce, intimidate, insult, harass, or cause emotional distress to a person, using a computer system, to support hostile behaviour, commits an offence and is liable, on conviction, to a fine not exceeding one hundred (1) thousand Emalangeni or to imprisonment for a period not exceeding five (5) years or both.

Violation of intellectual property rights

29. Any person who uses any computer or electronic device to violate any intellectual property rights protected under any law or treaty applicable to intellectual property rights in the Kingdom of Eswatini, commits an offence under this Act and shall be liable on conviction, in addition to any penalty or relief provided under the intellectual property law in question, to a fine not exceeding one hundred (1) thousand Emalangeni or to imprisonment for a period not exceeding three (3) years or both.

Attempting, abetting or conspiring

30. (1) Any person who attempts to commit any offence under this Act, or aids, abets or does any act preparatory to or in furtherance of the commission of an offence under this Act; or conspires with another to commit any offence under this Act, commits an offence and is liable, on conviction, to the penalty provided for that offence under this Act.

2. For the purposes of this section, "attempt" shall have the meaning ascribed to it under the Criminal Procedure and Evidence Act, 1938.

PART III
EXTRA TERRITORIAL JURISDICTION

Extra territorial jurisdiction

31. (1) The courts in the Kingdom of Eswatini shall have jurisdiction to try any offence under this Act where an act or omission constituting an offence under this Act has been committed wholly or in part –

(a) within the territory of the Kingdom of Eswatini;

(b) on an aircraft or vessel registered in the Kingdom of Eswatini;

(c) by a national of the Kingdom of Eswatini outside the territory of the Kingdom of Eswatini, if the person's conduct would also constitute an offence under a law of the country where the offence was committed;

(d) by a person, irrespective of the nationality or citizenship of the person, when the offence is committed within the territory of the Kingdom of Eswatini or outside the boarders of Eswatini with direct impact to the Kingdom of Eswatini; or,

(e) using equipment, software, or data located within the Kingdom of Eswatini, regardless of the location of the person; or directed against equipment, software, or data located in the Kingdom of Eswatini regardless of the location of the person.

Extradition and mutual legal assistance

32. Any offence under the provisions of this Act shall be considered to be an extraditable crime for which extradition and or mutual legal assistance may be granted or obtained under the applicable laws of Eswatini.

PART IV
PROCEDURAL LAW

Search and seizure

33. (1) If a Court is satisfied on the basis of an application by a law enforcement agent supported by affidavit that there are reasonable grounds to suspect or to believe that there may be in a place a thing or computer data –

(a) that may be material as evidence in proving an offence; or

(b) that has been acquired by a person as a result of an offence,

the Court may issue a warrant authorizing the law enforcement agent, with any assistance that may be necessary, to enter the place to search and seize the thing or computer data, including search or similar access of –

(i) a computer system or part of it and computer data stored therein; or

(ii) a computer-data storage medium in which computer data may be stored in the territory of Eswatini.

(2) If a law enforcement agent undertaking a search under section 25 (1) has grounds to believe that the data sought is stored in another computer system or part of it in another territory, and that data is lawfully accessible from or available to the initial system, the law enforcement agent may expeditiously extend the search or similar accessing of the other system.

(3) A law enforcement agent undertaking a search is empowered to seize or secure computer data accessed under sub-sections (1) or (2).

Assistance

34. (1) If a Court is satisfied on the basis of an application by a law enforcement agent, supported by affidavit that there are reasonable grounds to suspect or to believe that there may be in a place a thing or computer data –

(a) that may be material as evidence in proving an offence; or

(b) that has been acquired by a person as a result of an offence,

the Court may issue a warrant authorizing a law enforcement agent, with any assistance that may be necessary, from any person, who is not a suspect of a crime or otherwise excluded from an obligation to follow that order, but who has knowledge about the functioning of the computer system or measures applied to protect the computer data in the computer system that is the subject of a search under section 25.

(2) Any person, who is not a suspect of a crime or otherwise excluded from an obligation to follow such order, but who has knowledge about the functioning of the computer system or measures applied to protect the computer data in the computer system that is the subject of a search under section 25 shall permit, and assist if reasonably required and requested by the person authorized to make the search by –

(a) providing information that enables the undertaking of measures referred to in section 25;

(b) accessing and using a computer system or computer data storage medium to search any computer data available to or in the system;

(c) obtaining and copying such computer data;

(d) using equipment to make copies; and

(e) obtaining an intelligible output from a computer system in such a format that is admissible for the purposes of legal proceedings.

Production order

35. If a Court is satisfied on the basis of an application by a law enforcement officer or police officer that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the Court may order that –

(a) a person in the territory of Eswatini in control of a computer system produce from the system specified computer data or a printout or other intelligible output of that data; or

(b) a service provider in Eswatini to produce information about persons who subscribe to or otherwise use the service.

Expedited preservation of traffic data

36. (1) If law enforcement agent is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the law enforcement agent may, by written notice given to a person in control of the computer data, require the person to ensure that the data specified in the notice be preserved for a period of up to twenty eight (28) days as specified in the notice.

(2) The period specified in subsection (1) may be extended beyond twenty eight (28) days if, on an application the Court authorizes an extension for a further specified period of time.

Partial disclosure of traffic data

37. If a law enforcement agent is satisfied that computer data is reasonably required for the purposes of a criminal investigation, a law enforcement agent may, by written notice given to a person in control of the computer system, require the person to disclose relevant traffic data about a specified communications to identify the service provider; or the path through which a communication was transmitted.

Collection of traffic data

38. (1) If a Court is satisfied on the basis of an application by a law enforcement agent, supported by affidavit that there are reasonable grounds to suspect or believe that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the Court may order a person in control of that data to –

(a) collect or record traffic data associated with a specified communication during a specified period; or

(b) permit and assist a specified police officer to collect or record that data.

(2) If a Court is satisfied on the basis of an application by a law enforcement agent, supported by affidavit that there are reasonable grounds to suspect or believe that traffic data is reasonably required for the purposes of a criminal investigation, the Court may authorize the law enforcement agent to collect or record traffic data associated with a specified communication during a specified period through application of technical means.

Interception of content data

39. (1) If a Court is satisfied on the basis of an application by a law enforcement agent, supported by affidavit that there are reasonable grounds to suspect or believe that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the Court may –

(a) order a service provider whose service is available in Eswatini through application of technical means, to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or

(b) authorize a law enforcement agent to collect or record that data through application of technical means.

Forensic tool

40. (1) If a Court is satisfied on the basis of an application by a law enforcement agent, supported by affidavit that in an investigation concerning an offence listed in subsection 10, there are reasonable grounds to believe that essential evidence cannot be collected by applying other instruments listed in this Part, but is reasonably required for the purposes of a criminal investigation, the Court may authorize a law enforcement agent to use a remote, or otherwise, forensic tool with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence.

(2) The application under subsection (1) shall contain the following information –

(a) the suspect of the offence, if available with name and address if available;

(b) description of the targeted computer system;

(c) description of the intended measure, extent and duration of the utilization;

(d) reasons for the necessity of the utilization.

(3) It shall be a condition of the authorisation that such investigation shall ensure that modifications to the computer system of the suspect are limited to those modifications essential for the investigation and that any changes if possible can be undone after the end of the investigation.

(4) During the investigation, it shall be necessary to log –

(a) the technical means used and time and date of the application;

(b) the identification of the computer system and details of the modifications undertaken within the investigation; and

(c) any information obtained.

(5) Information obtained by the use of such tool shall be protected against any modification, unauthorized deletion and unauthorized access.

(6) The duration of authorization shall be limited to 3 months, renewable on justifiable grounds, and where the conditions of the authorization are no longer met, the action taken shall be stopped immediately.

(7) The authorization to install the tool shall include remotely accessing the suspect's computer system.

(8) Where the installation process requires physical access to a place, the requirements of section 25 shall be fulfilled.

(9) A law enforcement agent may, pursuant to the order of a court granted under subsection (1) request that a service provider support the installation process.

(10) The offences where subsection (1) is applicable include –

(a) murder or treason;

(b) kidnapping or abduction or human trafficking or child pornography or grooming;

(c) money laundering;

(d) producing, manufacturing, supplying or otherwise dealing in any dangerous drug;

(e) importing or exporting a harmful drug;

(f) importing, exporting or trans-shipping any firearm or ammunition;

(g) manufacture of, or dealing, in firearms or ammunition, or explosives;

(h) illegal possession of a prohibited weapon or any other firearm or ammunition;

(i) an offence under the Prevention of Corruption Act, 2006;

(j) arson;

(k) hijacking and terrorism offences; or

(l) attempting or conspiring to commit, or aiding, abetting, or procuring the commission of, an offence falling within any of the preceding paragraphs.

PART V
LIABILITY

No monitoring obligation

41. When providing the services under this Part –

(1) A service provider shall have no general obligation to monitor the data which it transmits or stores; or actively seek facts or circumstances indicating an unlawful activity.

(2) The Minister may, subject to the provisions of any other law, prescribe procedures for service providers to –

(a) inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service; and

(b) communicate to the competent authorities, at their request, information enabling the identification of recipients of their service.

Access provider

42. (1) An access provider shall not be criminally liable for providing access and transmitting information if the access provider –

(a) does not initiate the transmission;

(b) does not select the receiver of the transmission; or

(c) does not select or modify the information contained in the transmission.

(2) The acts of transmission and provision of access referred to in subsection (1) include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

Hosting provider

43. (1) A hosting provider shall not be criminally liable for the information stored at the request of a user of the service, if –

(a) the hosting provider expeditiously removes or disables access to the information after receiving an order from any public authority or court to remove specific illegal information stored; or

(b) the hosting provider, upon obtaining knowledge or awareness about specific illegal information stored, by other ways than an order from a public authority, expeditiously informs the Commission to enable them to evaluate the nature of the information and if necessary issue an order to remove the content.

(2) Subsection (1) shall not apply when the user of the service is acting under the authority or the control of the hosting provider.

(3) Where the hosting provider removes the content after receiving an order pursuant to sub-section (1) liability shall not arise from contractual obligations with its customer to ensure the availability of the service.

Caching provider

44. A caching provider shall not be criminally liable for the automatic, intermediate and temporary storage of information, performed for the sole purpose of making more efficient the information's onward transmission to other users of the service upon their request, if –

(a) the caching provider does not modify the information;

(b) the caching provider complies with conditions of access to the information;

(c) the caching provider complies with rules regarding the updating of the information, manner widely recognised and used by industry;

(d) the caching provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and

(e) the caching provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or other relevant authority has ordered such removal or disablement.

Hyperlinks provider

45. An Internet service provider who enables access to information provided by a third party by providing an electronic hyperlink shall not be liable for the information where the Internet service provider –

(a) expeditiously removes or disables access to the information after receiving an order from any public authority or court to remove the link; or

(b) upon obtaining knowledge or awareness about specific illegal information stored by other ways than an order from a public authority, expeditiously informs the relevant authority to enable them to evaluate the nature of the information and if necessary issue an order to remove the content.

Search engine provider

46. (1) A service provider who makes or operates a search engine that either automatically or based on entries by others, creates an index of Internet-related content or makes available electronic tools to search for information provided by a third party is not liable for search results if that provider –

(a) does not initiate the transmission;

(b) does not select the receiver of the transmission; or

(c) does not select or modify the information contained in the transmission.

PART VI
GENERAL PROVISIONS

Limitation of Liability

47. Neither the State, members of the Commission nor any public officer or employee shall be liable in respect of the performance of any act or any omission where that act or omission was done in good faith and without gross negligence in accordance with the provisions of this Act.

Forfeiture of assets

48. (1) The Court in imposing sentence on any person who is convicted of an offence under this Act may also order that the convicted person forfeits to the State –

(a) any asset, money or property (whether real or personal) constituting or traceable to the proceeds of the offence; and

(b) any computer, equipment, software or other technology used or intended to be used to commit or to facilitate the commission of the offence.

(2) Any person convicted of an offence under this Act shall forfeit the passport or international travelling document to the State until the person has paid the fines or served the sentence imposed.

(3) Notwithstanding subsection (2), the court may –

(a) for the purposes of allowing the convicted person to travel abroad for medical treatment;

(b) in the interest of the public; and

(c) upon application,

grant an order that the passport or travelling document of the convicted person be released to that person.

General provision on cybercrimes

49. Except as provided for in this Act, any offence under any Act which is committed in whole or in part through the use of a computer, electronic device or in electronic form is deemed to have been committed under that Act and the provisions of that Act shall apply with the necessary modification to the person who commits the offence.

Offence by body corporate and un incorporate

50. If a body corporate or un incorporate is convicted of an offence under this Act, every person who -

(a) is a director of, or is otherwise connected with the management of the body corporate or un-incorporate;

(b) is in the management of the body corporate or un-incorporate; and

(c) knowingly authorised or permitted or condoned the act or omission constituting the offence,

shall be deemed to have committed the same offence and may be proceeded against and punished accordingly.

Admissibility of evidence

51. (1) The best evidence rule in respect of an electronic record is satisfied-

(a) on proof of the integrity of the electronic records system in or by which the data contained in the electronic record was recorded or stored; or

(b) if the electronic record contains a secure electronic signature that was added when the electronic record was first generated in its final form and that can be used to verify that the electronic record has not been changed since that time.

(2) Notwithstanding subsection (1), in the absence of evidence to the contrary, an electronic record in the form of a printout satisfies the best evidence rule if, in any legal proceedings, the printout has been manifestly and consistently acted on, relied on or used as a record of the information recorded or stored in the printout

as evidence has the burden of proving its authenticity by giving evidence capable of supporting a finding that the electronic record is that which the person purports it to be.

Powers of the Commission to Regulate Cybersecurity

52. The Commission shall have the powers to regulate and coordinate matters of cybersecurity and enforce standards applicable to the security of the critical information infrastructures.

Establishment of the Cybersecurity Advisory Council

53. The Prime Minister may, by notice in the Gazette or Government website establish a National Cybersecurity Advisory Council not exceeding fifteen (15) members, coming from a cross section of stakeholders including information communication and technology, legal, finance, education, business, civil society, defence, police, international cooperation, national security, the Commission serving as the secretariat.

Ad Hoc Committees

54. The Minister may establish ad-hoc committees at any time to deal with specific tasks at any given time when there is a need.

Compensation

55. The court may order the guilty party to compensate their victims to the value of damage or loss suffered on any crime committed in this Act.

Regulations

56. (1) The Minister may, in consultation with the Commission make regulations regarding any matter which by this Act is required or permitted to be prescribed or which is necessary or expedient to be prescribed for carrying out or giving effect to the provisions of this Act and may include regulations on –

(a) interception of computer data communication including but not limited to the security, functional and technical requirements for interception;

(b) the declaration of critical information infrastructure, including but not limited to, the identification, securing the integrity and authenticity of, registration, and other procedures relating to critical information infrastructure;

(c) the liability of access providers which may include the security, functional and technical requirements for the purposes of Part VI of this Act.

(2) The Commission may, with the approval of the Minister, issue any guidelines that may be required for the carrying out of the provisions of this Act.

The Government Printer, Mbabane