CYBERCRIME AND CYBERSECURITY BILL, 2017

ARRANGEMENT OF SECTIONS

PART I

PRELIMINARY

Section

PART II

ESTABLISHMENT OF CYBERSECURITY CENTRE

PART III

OFFENCES RELATING TO COMPUTER SYSTEMS, COMPUTER DATA, DATA STORAGE MEDIUMS, DATA CODES AND DEVICES

PART IV

OFFENCES RELATING TO ELECTRONIC COMMUNICATIONS AND MATERIALS

BILL

To provide for and to consolidate cyber-related offences with due regard to the Declaration of Rights under the Constitution and the public and national interest; to establish a Cyber Security Centre and to provide for its functions; provide for investigation and collection of evidence of cyber-crime; to provide for the admissibility of electronic evidence for such offences; to create a technology-driven business environment; to encourage technological development and the lawful use of technology; to amend section 162 and to repeal sections 163 to 166 of the Criminal Code (Codification and Reform) Act [*Chapter 9:23*]; and to provide for matters connected with or incidental to the foregoing.

ENACTED by the Parliament and the President of Zimbabwe.

PART I

PRELIMINARY

1 Short title and date of commencement

(1) This Act may be cited as the Cyber-crime and Cyber-security Act, 2017.

(2) This Act shall come into operation on a date to be fixed by the President by notice in the *Gazette.*

2 Objects of Act

The objects of the Act are to curb cybercrime and increase cybersecurity in order to build confidence and trust in the secure use of information and communications technologies.

3 Interpretation

(1) In this Act—

"**access provider**" means any person providing—

(a) an electronic data transmission service by transmitting information provided by, or to, a user of the service in a communication network; or

(b) access to a communication network;

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

"**child**" means any person under the age of eighteen years;

"child pornography" means pornography involving a child;

"**computer device**" means any portable and non-portable electronic programmable device used or designed, whether by itself or as part of a computer network, a database, a critical database, an electronic communications network or critical information infrastructure or any other device or equipment or any part thereof, to perform predetermined arithmetic, logical, routing or storage operations in accordance with set instructions and includes—

(a) input devices;

(b) output devices;

(c) processing devices;

(d) computer data storage mediums;

(e) programmes; and

(f) other equipment and devices,

that are related to, connected or used with, such a device or any part thereof and "**device**" shall be construed accordingly;

"**computer data storage medium**" means any device or location from which data is capable of being reproduced or on which data is capable of being stored, by a computer device, irrespective of whether the device is physically attached to or connected with the computer device;

"**computer system**" means interconnected or related computer devices, one or more of which uses a programme to perform the automatic processing of data, exchange data with each other or any other computer system or connect to an electronic communications network;

"**Criminal Law Code**" means Criminal Law (Codification and Reform) Act [*Chapter 9:23*];

"**critical database**" means a computer data storage medium or any part thereof which contains critical data;

"**critical information infrastructure**" means computer systems, devices, networks, computer programmes, computer data, so vital to the country that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on security, defence, economic and international affairs, public health and safety, or to essential services as defined in section 19 of the Criminal Law Code including the banking system and "**critical data**" shall be construed accordingly;

"**cybercrime**" means any offence under this Act;

"**data**" means any representation of facts, concepts, information, whether in text, audio, video, images, machine-readable code or instructions, in a form suitable for communications, interpretation or processing in a computer device, computer system, database, electronic communications network or related devices and includes a computer programme and traffic data;

"**electronic communications network**" means any electronic communications infrastructures and facilities used for the conveyance of data;

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

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

"information and communications technologies" mean a device or inter-connected or related devices that are used or that are responsible for the creation, transmission, receiving, processing and/or collation of digital data by making use of computer, software, networking, telecommunications, Internet, programming and information system technologies;

"**information system**" means a device or inter-connected or related devices, one or more of which uses a programme to automatically processes computer data as well as computer data stored, processed, retrieved or transmitted by that device or inter-connected or related devices for the purposes of its or their operation, use, protection or maintenance;

"**Minister**" means the Minister responsible for information and communications technologies;

"**pornography**" includes any representation, through publication, exhibition, cinematography, electronic means or any other means whatsoever, of a person engaged in real or simulated explicit sexual activity, or any representation of the sexual parts of a person for primarily sexual purposes;

"**programme**" means data or a set of instructions which, when executed in a computer, causes the computer to perform a function;

"**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 keystroke logging or transmission of an IP-address;

"**service provider**" means—

(a) any person that provides to users of its service the ability to communicate by means of information communication technology systems, and

(b) any person that processes or stores information and communications data on behalf of such communications service or users of such service;

and includes—

(c) access, caching and hosting provider;

"**system**" means an arrangement of data or one or more programmes which, when executed, performs a function;

"**traffic data**" means data relating to a communication by means of an information communications system or generated by an information communications system that forms a part of the chain of communications indicating the communication's origin, destination, route, format, time, date, size, duration or type of the underlying service;

"**utilize**" in relation to a remote forensic tool includes—

(a) developing a remote forensic tool;

(b) adopting a remote forensic tool; and

(c) purchasing a remote forensic tool;

(2) In addition to section 4 (Application of Code to other enactments) of the Criminal Law Code, Chapter XIII (Participation or assistance in the commission of crimes) of the Criminal Law Code shall apply, *mutatis mutandis*, with respect to offences in terms of this Act.

PART II

ESTABLISHMENT OF CYBERSECURITY CENTRE

4 Establishment of Cybersecurity Centre

The Minister shall, in consultation with the Minister responsible for Finance, establish a Cybersecurity Centre.

5 Cybersecurity Committee

(1) The Cybersecurity Centre shall be managed by a committee to be known as the Cybersecurity Committee which will report to the Minister.

(2) The Cybersecurity Committee shall consist of eleven members chosen for their computer and telecommunications, law and policy knowledge and skills in respect of any aspect dealt with in this Act as follows--

(a) one representative nominated by each of the following--

(i) the Postal and Telecommunications Regulatory Authority of Zimbabwe;

(ii) the ministry responsible for information and communications technologies;

(ii) the ministry responsible for science and technology;

(iii) the ministry responsible for justice;

(iv) the Zimbabwe Republic Police;

(v) the National Prosecution Authority;

(vi) the ministry responsible for defence;

(vii) the Central Intelligence Organisation;

(viii) the Prisons and Correctional Service;

(b) one representative chosen by organizations representing the information technology communications sector and computer professionals; and

(c) one person with appropriate information and communications technology expertise chosen by the National Association of Non-Governmental Organisations to represent civic society.

(3) The functions of the Cybersecurity Centre shall be to—

(a) advise Government and implement Government policy on cybercrime and cybersecurity;

(b) identify areas for intervention to prevent cybercrime;

(c) coordinate cybersecurity and establish a national contact point available daily around-the-clock;

(d) establish and operate a protection-assured whistle-blower system that will enable members of the public to confidentially report to the Committee cases of alleged cybercrime;

(e) promote and coordinate activities focused on improving cybersecurity and preventing cybercrime by all interested parties in the public and private sectors;

(f) provide guidelines to public and private sector interested parties on matters relating to awareness, training, enhancement, investigation, prosecution and combating cybercrime and managing cybersecurity threats;

(g) oversee the enforcement of the Act to ensure that it is enforced reasonably and with due regard to fundamental human rights and freedoms;

(h) provide technical and policy advice to the Minister;

(i) advise the Minister on the establishment and development of a comprehensive legal framework governing cyber security matters.

(4) The Committee shall, not later than 31 March in each year, submit to the Minister—

(a) an annual report on the Committee's activities during the previous calendar year, detailing fully its operations and activities, in particular the impact of the implementation of the Act on the freedom of expression and the right to privacy;

(b) such other reports as the Minister may require or as the Committee considers advisable.

(5) The Minister—

(a) shall table the annual report;

(b) may table any other reports submitted to him;

before the National Assembly on one of the ten days on which the Assembly next sits following receipt of the reports.

PART III

OFFENCES RELATING TO COMPUTER SYSTEMS, COMPUTER DATA, DATA STORAGE MEDIUMS, DATA CODES AND DEVICES

6 Unlawful access

(1) Any person who unlawfully and intentionally secures unauthorised access to data, a computer programme, a computer data storage medium or the whole or any part of a computer system shall be guilty of unlawful access and liable to a fine not exceeding level fourteen or to imprisonment for a period not exceeding five years or both such fine and such imprisonment.

(2) For the purposes of this section "access" includes—

(a) to obtain;

(b) to make use of;

(c) gain entry to;

(d) view;

(e) display;

(f) instruct or communicate with;

(g) to store data in or retrieve data from;

(h) to copy, move, add, change or remove data, critical data or a critical database, or otherwise to make use of, configure or reconfigure any resources of a computer device, a computer network, a database, a critical database, an electronic communications network, a critical information infrastructure, whether in whole or in part, including their logical, arithmetical, memory, access codes, transmission, data storage, processor or memory function, whether physical, virtual, by direct or indirect means or by electronic, magnetic, audio, optical or any other means.

(3) Any person who contravenes subsection (1) in any of the aggravating circumstances described in section 13 shall be liable to a fine not exceeding level fourteen or imprisonment for a period not exceeding ten years or to both such fine and such imprisonment.

7 Unlawful interception of data

(1) Any person who, unlawfully and intentionally, intercepts by technical or any other means—

(a) any private transmission of computer data to, from or within a computer network, computer device, database or information system; or

(b) electromagnetic emissions from a computer or information system carrying such computer data;

shall be guilty of unlawful interception of data and liable to a fine not exceeding level ten or to imprisonment not exceeding five years or to both such fine and such imprisonment.

(2) Any person who contravenes subsection (1) in any of the aggravating circumstances described in section 13 shall be liable to a fine not exceeding level fourteen or to imprisonment for a period not exceeding ten years or to both such fine and such imprisonment.

8 Unlawful acquisition of data

(1) Any person who unlawfully and intentionally—

(a) overcomes or circumvents any protective security measure intended to prevent access to data; and

(b) acquires data within a computer system or data which is transmitted to or from a computer system;

shall be guilty of unlawful acquisition of data and shall be liable to a fine not exceeding level fourteen or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

(2) Any person who unlawfully and intentionally possesses data knowing that such data was acquired unlawfully shall be guilty of unlawful possession of data and liable to a fine not exceeding level fourteen or to imprisonment not exceeding five years or to both such fine and such imprisonment.

(3) For the purposes of this section "acquire" includes to use, examine, capture, copy, move to a different location or divert data to a destination other than its intended location.

(4) Any person who contravenes this section in any of the aggravating circumstances described in section 13 shall be liable to a fine not exceeding level fourteen or to imprisonment for a period not exceeding ten years or to both such fine and such imprisonment.

9 Unlawful interference with data or data storage medium

(1) Any person who unlawfully and intentionally interferes with computer data or a data storage medium by—

(a) damaging, corrupting, impairing or deteriorating computer data; or

(b) deleting computer data ; or

(c) altering computer data; or

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

(e) obstructing, interrupting or interfering with the lawful use of computer data; or

(f) obstructing, interrupting or interfering with any person in the lawful use of computer data; or

(g) denying, hindering, blocking access to computer data to any person authorized to access it; or

(h) maliciously creating, altering or manipulating any data, programme or system in whole or in part which is intended for installation in a computer;

shall be guilty of an offence and liable to a fine not exceeding level ten or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

(2) Any person who contravenes subsection (1) in any of the aggravating circumstances described in section 13 is liable to a fine not exceeding level fourteen or to imprisonment for a period not exceeding ten years or to both such fine and such imprisonment.

10 Unlawful interference with computer system

(1) Any person who unlawfully and intentionally interferes with the use of a computer or information system, computer device, an electronic communications system or critical information infrastructure by blocking, hindering, impeding, interrupting, altering or impairing the functioning of, access to or the integrity of, a computer device, computer or information system, an electronic communications network or critical information infrastructure shall be guilty of unlawful interference with computer or information system and liable to a fine not exceeding level fourteen or to imprisonment not exceeding ten years or to both such fine and such imprisonment.

(2) Any person who contravenes subsection (1) in any of the aggravating circumstances described in section 13 is liable to a fine not exceeding level fourteen or to imprisonment for a period not exceeding twenty years or to both such fine and such imprisonment.

11 Unlawful disclosure of data code

(1) Any person who unlawfully and intentionally—

(a) communicates, discloses or transmits any computer data, programme, access code or command or any other means of gaining access to any programme or data held in a computer or information system to any person not authorized to access the computer data, programme, code or command for any purpose;

(b) activates or installs or downloads a programme that is designed to create, destroy, mutilate, remove or modify any data, programme or other form of information existing within or outside a computer or computer system; or

(c) creates, alters or destroys a password, personal identification number, code or any method used to access a computer or computer network;

shall be guilty of an offence and liable to a fine not exceeding level twelve or imprisonment for a period not exceeding ten years or both such fine or such imprisonment.

(2) A person shall not be liable under this section if the action is—

(a) pursuant to measures that can be taken in terms of section 39; or

(b) authorised under the law.

(3) Where an offence under this section is committed in relation to data that forms part of a database or that involves national security or the provision of an essential service, the penalty shall be imprisonment for a period not exceeding ten years.

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

12 Unlawful use of data or devices

(1) Any person who unlawfully and intentionally acquires, possesses, produces, sells, procures for use, imports, distributes, supplies, uses or makes available an access code, password, a computer programme designed or adapted for the purpose of committing an offence or similar data or device by which the whole or any part of a computer or information system is capable of being accessed, for purposes of the commission or attempted commission of an offence in terms of this Act, shall be guilty of an offence and liable to a fine not exceeding level twelve or imprisonment for a period not exceeding ten years or both such fine or such imprisonment.

(2) Any person who unlawfully and intentionally assembles, obtains, sells, purchases, possesses, makes available, advertises or uses malicious software, programmes or devices for purposes of causing damage to data, computer or information systems and networks, electronic communications networks, critical information infrastructure or computer devices shall be guilty of an offence and liable to a fine not exceeding level ten or imprisonment for a period not exceeding five years or both such fine and such imprisonment.

(3) Any person who contravenes this section in any of the aggravating circumstances described in section 13 shall be liable to a fine not exceeding level twelve or imprisonment for a period not exceeding ten years or to both such fine and such imprisonment.

13 Aggravating circumstances

In this Part, an offence is committed in aggravating circumstances if—

(a) committed in connection with or in furtherance of the commission or attempted commission of a crime against the State specified in Part III of the Criminal Law Code;

(b) it is intended for or results in damaging, destroying or prejudicing the safe operation of an aircraft;

(c) it is intended to conceal or disguise the proceeds of unlawful dealing in dangerous drugs or the enjoyment thereof;

(d) it results in defeating or obstructing the course of justice;

(e) it seriously prejudices the enforcement of the law by any law enforcement agencies;

(f) any computer, computer network, information communications network data, programme or system involved is owned by the State, a law enforcement agency, the Defence Forces, the Prison Service, a statutory corporation or a local authority;

(g) the offence results in considerable material prejudice or economic loss to the owner of the computer, computer network, data, programme or system;

(h) the offence seriously interferes with or disrupts an essential service; or

(i) the offence was committed in furtherance of organised crime or the perpetrator was part of organised criminal gang.

PART IV

OFFENCES RELATING TO ELECTRONIC COMMUNICATIONS AND MATERIALS

14 Transmission of data message inciting violence or damage to property

Any person who unlawfully by means of a computer or information system makes available, transmits, broadcasts or distributes a data message to any person, group of persons or to the public with intend to incite such persons to commit acts of violence against any person or persons or to cause damage to any property shall be guilty of an offence and liable to a fine not exceeding level ten or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

15 Sending threatening data message

Any person who unlawfully and intentionally by means of a computer or information system sends any data message to another person threatening harm to the person or the person's family or friends or damage to the property of such persons shall be guilty of an offence and liable to a fine not exceeding level ten or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

16 Cyber-bullying and harassment

Any person who unlawfully and intentionally by means of a computer or information system generates and sends any data message to another person, or posts on any material whatsoever on any electronic medium accessible by any person, with the intent to coerce, intimidate, harass, threaten, bully or cause substantial emotional distress, or to degrade, humiliate or demean the person of another or to encourage a person to harm himself or herself, shall be guilty of an offence and liable to a fine not exceeding level ten or to imprisonment for a period not exceeding ten years or to both such fine and such imprisonment.

17 Transmission of false data message intending to cause harm

Any person who unlawfully and intentionally by means of a computer or information system makes available, broadcasts or distributes data to any other person concerning an identified or identifiable person knowing it to be false with intend to cause psychological or economic harm

shall be guilty of an offence and liable to a fine not exceeding level ten or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

18 Spam

Any person who intentionally and without lawful excuse—

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

(b) uses a protected computer system to relay or retransmit multiple electronic mail messages, with the intent to deceive or mislead recipients 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 initiates the transmission of such messages;

shall be guilty of an offence and liable to a fine not exceeding level five or to imprisonment for a period not exceeding one year or to both such fine and such imprisonment.

Provided that it shall not be an offence under this section if the transmission of multiple electronic mail messages is done within a customer or business relationships.

19 Transmission of intimate images without consent

(1) Any person who unlawfully and intentionally by means of a computer or information system makes available, broadcasts or distributes a data message containing any intimate image of an identifiable person without the consent of the person concerned causing the humiliation or embarrassment of such person shall be guilty of an offence and liable to a fine not exceeding level ten or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

(2) For the purposes of subsubsection (1) "intimate image" means a visual depiction of a person made by any means in which the person is nude, the genitalia or naked female breasts are exposed or sexual acts are displayed.

20 Production and dissemination of racist and xenophobic material

Any person who unlawfully and intentionally through a computer or information system—

(a) produces or causes to be produced racist or xenophobic material for the purpose of its distribution;

(b) offers, makes available or broadcasts or causes to be offered, made available or broadcast racist or xenophobic material;

(c) distributes or transmits or causes to be distributed or transmitted racist or xenophobic material;

(d) uses language that tends to lower the reputation or feelings of persons for the reason that they belong to a group of persons distinguished on the grounds set out in section 56 (3) of the Constitution or any other grounds whatsoever, if used as a pretext for any of these factors;

shall be guilty of an offence and liable to a fine not exceeding level fourteen or to imprisonment for a period not exceeding ten years or to both such fine and such imprisonment.

PART V

OFFENCES INVOLVING DISHONESTY

21 Cyber-fraud

Any person who unlawfully and with the intention to defraud makes a misrepresentation by means of—

(a) data or a computer programme or by the alteration or deletion of data or a computer programme;

(b) interference with the functioning of a computer system or a computer data storage medium;

and causes actual or potential prejudice to another person shall be guilty of an offence and liable to a penalty in terms of section 136 of the Criminal Law Code.

22 Unlawful remaining

Any person who unlawfully and with intent to defraud—

(a) exceeds his or her lawful authority to access a computer or information system by unlawfully remaining or attempting to remain logged in to a computer or information system or part of a computer or information system; or

(b) continues to use a computer or information system beyond the authorised period or purpose;

shall be guilty of an offence and liable to a fine not exceeding level ten or imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

23 Cyber-forgery and transmission thereof

(1) Any person who unlawfully and with intent to defraud—

(a) falsifies data by altering data or deleting any of the data in order to deceive another into believing that the data is authentic, whether or not the data is directly readable and intelligible;

(b) by creating a false computer programme;

and the false data or false computer programme causes actual or potential prejudice to another, shall be guilty of an offence and liable to a penalty in terms of section 137 of the Criminal Law Code.

(2) Any person who unlawfully and with intent to defraud transmits data or a computer programme knowing it to be forged or realising the real possibility that it is forged and causes actual or potential prejudice to another is guilty of cyber-fraud and liable to a penalty in terms of section 137 of the Criminal Law Code.

(3) Notwithstanding subsections (1) and (2), if the offence involves a public document or public data, the penalty shall be a fine not exceeding level fourteen or imprisonment for a period not exceeding twenty years or to both such fine and such imprisonment.

24 Computer related financial offences

(1) Any person who unlawfully and intentionally acquires by any means, possesses, uses or provides to another person the financial information of another for the purpose of committing any offence shall be guilty of an offence and liable to a fine not exceeding level fourteen or imprisonment for a period not exceeding ten years or to both such fine and such imprisonment.

(2) Any person who unlawfully and intentionally is in possession of the financial information of another person in regard of which there is a reasonable suspicion that such financial information was acquired, is possessed or provided to another for purposes of committing an offence or was used or may be used to commit an offence under this Act shall be guilty of an offence and is liable to a fine not exceeding level fourteen or imprisonment for a period not exceeding ten years or to both such fine and such imprisonment.

25 Violation of intellectual property rights

Any person who unlawfully and intentionally appropriates in any manner rights in property which rights are vested in another person or where copyright exists in respect of any work without the authority of the owner of the rights by means of a computer or electronic communications system which the person knows is the subject of intellectual property protection shall be guilty of an offence and, in addition to any penalty or relief provided under any relevant intellectual property laws, liable to a fine not exceeding level ten or imprisonment for a period not exceeding five years or both such fine and such imprisonment.

26 Identity-related offence

Any person who unlawfully and intentionally by using a computer or information system acquires, transfers, possesses or uses any means of identification of another person with the intent to commit, or to assist in connection with the commission of an offence shall be guilty of an offence and liable to a fine not exceeding level ten or imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

27 Cyber-extortion

(1) Any person who unlawfully and intentionally through a computer or information system exerts illegitimate pressure on another to obtain an advantage from the other person or compels or abstains from the performance of any act shall be guilty of cyber-extortion and liable to a penalty in terms of section 134 of the Criminal Law Code.

(2) For the purposes of subsection (1), “illegitimate pressure” includes infecting a computer or computer system with a virus or any other malware which prevents the user from accessing the computer files and demanding a payment of money in return for the removal of the virus or other malware to allow access to the files.

PART VI

CYBER-RELATED TERRORISM AND SABOTAGE

28 Cyber-terrorism and sabotage of critical infrastructure

(1) Any person who unlawfully and intentionally—

(a) uses computers, computer networks or information infrastructure networks;

(b) possesses, receives or makes available data, any software or hardware tool, malware, a password, access code or similar data and device, or computer data, computer device, computer network or information infrastructure network;

for the purposes of committing, inciting the commission of, conspiring to commit or attempting to commit acts of insurgency, banditry, sabotage or terrorism defined in section 23 of the Criminal Law Code shall be guilty of cyber-terrorism and liable to the penalties set out in the said section 23 of the Criminal Law Code.

(2) Any person who unlawfully and seriously damages or destroys a computer or information infrastructure network, a computer programme or a data storage medium under the control of the State or a critical information infrastructure in unlawful pursuit of political, religious, social and ideological objectives shall be guilty of an offence and liable to the penalties set out in the said section 23 of the Criminal Law Code.

29 Cyber-related foreign and international terrorism

Any person who uses any computer or computer or information infrastructure network for the purpose of committing, inciting the commission of, conspiring to commit or attempting to commit any offence in terms of the Suppression of Foreign and International Terrorism Act [*Chapter 11:21*] shall be guilty of an offence and liable to the appropriate penalty in terms of that Act.

PART VII

OFFENCES AGAINST CHILDREN

30 Child pornography

Any person who unlawfully and intentionally, through a computer or information system—

(a) produces child pornography for the purpose of distribution of the material;

(a) offers or makes available child pornography;

(b) distributes or transmits child pornography;

(c) procures or obtains child pornography for oneself or for another person;

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

(e) knowingly obtains, accesses or procures child pornography;

shall be guilty of an offence and liable to a fine not exceeding level fourteen or to imprisonment for a period not exceeding ten years, or both such fine and such imprisonment.

31 Exposing children to pornography

Any person who unlawfully and intentionally through a computer or information system—

(a) makes pornographic material available to any child; or

(b) facilitates access by any child to pornography or displays pornographic material to any child;

with or without the intention of lowering the child's inhibitions in relation to sexual activity or inducing the child to have sexual relations with that person;

shall be guilty of an offence and liable to a fine not exceeding level fourteen or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

PART VIII

PROCEDURAL LAW

32 Application of procedural law

The powers and procedures provided for under this Act shall apply to-

(a) any offence in terms of this Act;

(b) any other offence involving computer or other information system in contravention of any other law;

(c) the collection of evidence in electronic form for any offence under this Act or any other offence involving computer or other information and communications technology system in contravention of any other law.

33 Search and seizure

(1) In this section "seize" includes—

(a) taking possession of or securing a computer;

(b) securing a computer system or part thereof or a computer-data storage medium;

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

(d) making and retaining a copy of computer data, including through the use of use of onsite equipment;

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

(f) maintaining the integrity of any stored relevant computer data;

(g) rendering inaccessible or removing computer data in the accessed computer system.

(2) A magistrate may, on an application by a police officer in the prescribed form, that specified computer data or a printout or other information is reasonably required for the purpose of a criminal investigation or criminal proceedings, order that—

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

(b) an electronic communications service provider in Zimbabwe produce information about persons who subscribe to or otherwise use the service.

(3) An application referred to in subsection (1) shall be supported by an affidavit in which the police officer shall set out the offence being investigated, the computer system in which it is suspected to be stored, the reasonable grounds upon which the belief is based, the measures that will be taken in pursuance of the investigation and the period over which those measures will the taken.

(4) A police officer granted a warrant in terms of this section may—

(a) if there are reasonable grounds to believe that computer data concerned is susceptible to loss, alteration, deletion, impairment or modification, by written notice given to a person in control of the computer data, require the person in control of the data to ensure that the data specified in the notice is preserved for a period not exceeding seven days as may be specified in the notice which period may be extended, on an application to a magistrate, for such period as the magistrate may grant;

(b) by written notice to a person in control of the computer system or information system concerned, require the person in control thereof to disclose relevant traffic data concerning specified communications in order to identify--

(i) the service providers; or

(ii) the path through which the communication was transmitted.

34 Expedited preservation

(1) A magistrate may, on an application by a police officer in the prescribed form, that there are reasonable grounds to suspect or believe that traffic data associated with a specified communication is required for the purposes of a criminal investigation--

(a) order any person in control of such data to--

(i) collect, record or preserve the traffic data associated with a specified communication during a specified period; or

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

(b) authorize the police officer to collect or record traffic data associated with a specified communication during a specified period through the use of any appropriate technological means.

(2) Subsection (3) of section 33 shall apply *mutatis mutandis* to an application in terms of this section.

35 Partial disclosure of traffic data

(1) A magistrate may, on an application by a police officer, in the prescribed form, that there are reasonable grounds to suspect or believe that the content of specified electronic communications is required for the purposes of a criminal investigation, order a service provider operating in Zimbabwe or authorize the police officer, to collect or record or to permit or assist the police officer to collect or record, through the use of appropriate technological means, the data associated with specified communications transmitted by the service provider.

(2) Subsection (3) of section 33 shall apply *mutatis mutandis* to an application in terms of this section.

36 Collection of traffic data

(1) A magistrate may, on an application by a police officer in the prescribed form, that in an investigation relating to or concerning an offence listed in subsection (10) or as may be prescribed, there are reasonable grounds to believe that essential evidence cannot be collected in any other way provided for in this Part but is reasonably required for the purposes of a criminal investigation, authorize the police officer to utilize remote forensic tools and such application shall be supported by an affidavit stating--

(a) the name and address of the suspect;

(b) the description of the targeted computer system,

(c) the description of the intended measures and the extent and duration of the use of the remote forensic tools, and

(d) the reasons for the proposed use of the remote forensic tools.

(2) It shall be a condition of the authorization that the investigation shall ensure that modifications to the computer system of the suspect are limited to those modifications essential for the investigation.

(3) During the conduct of the investigation, the police officer shall record--

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

(b) the identity of the computer system and details of the modifications undertaken during the investigation; and

(c) any information obtained;

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

(5) The duration of authorization in terms of this section shall not exceed three months.

(6) The authorization to install the tool shall include remotely accessing the targeted computer system.

(7) A police officer may, in addition to the authority sought in terms of subsection (1), request that the authorization direct a specified service provider to support and assist the installation process.

(10) The offences referred to in subsection (1) are--

(a) murder;

(b) treason;

(c) kidnapping or abduction;

(d) money laundering as provided for in the Money Laundering and Proceeds of Crime Act [*Chapter 9:24*] and Suppression of Money laundering Act [*Chapter 24:*24];

(e) production, manufacture, supply, importation, exportation or otherwise dealing in any dangerous drug in contravention of the Dangerous Drugs Act [*Chapter 15:02*];

(f) importation, exportation or trans-shipment, manufacture of, dealing in, illegal possession of any firearm or ammunition or of any prohibited weapon in contravention of the Firearms Act [*Chapter 10:09*];

(g) any offence under the Prevention of Corruption Act [*Chapter 9:16*];

(h) any offence under the Trafficking in Persons Act [*Chapter 9:25*];

(i) the offence of insurgency, banditry, sabotage or terrorism as defined in section 23 of the Criminal Law Code;

(j) arson;

(k) offences relating to hijacking and terrorism;

(l) offences under the Suppression of Foreign and International Terrorism Act [*Chapter 11:21*];

(m) attempting or conspiring to commit, or aiding, abetting, concealing or procuring the commission of the foregoing offences.

PART IX

OBLIGATIONS OF SERVICE PROVIDERS

37 Obligations of service providers

(1) An electronic communications network or access service provider shall not be criminally liable for providing access or transmitting information through its system if such service provider has not--

(a) initiated the transmission; or

(b) selected the receiver of the transmission; or

(c) selected or modified the information contained in the transmission.

(2) The provision of access or the transmission referred to in subsection (1) shall 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 the information is not stored for any period longer than is reasonably necessary for the transmission.

(3) A hosting provider shall not be criminally liable for the information stored at the request of a user of the service if the hosting provider--

(a) promptly removes or disables access to the information after receiving an order from any court of law to remove specific stored illegal information; or

(b) in any other manner, obtains knowledge or becomes aware of any illegal information stored, promptly informs the appropriate authority to enable it to evaluate the nature of the information and if necessary, issue an order for its removal.

(4) Subsection (3) shall not apply where the user of the service is acting under the authority or the control of the hosting provider.

(5) Where the hosting provider removes the content after receiving an order pursuant to sub-section (3), no liability shall arise from the contractual obligations with the user with regard to the availability of the service.

(6) A hosting provider who fails to remove or disable access to information in terms of subsection (3) shall be guilty of an offence and liable to a fine not exceeding level eight or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment.

(7) A caching provider shall not be criminally liable for the automatic, intermediate or temporary storage of information where the caching was performed for the sole purpose of making the onward transmission of the information to other users of the service upon their request more efficient if the caching provider--

(a) does not modify the information;

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

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

(d) 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) acts promptly to remove or to disable access to the information it has stored upon obtaining knowledge that the information has been removed from the network at the initial source of the transmission, or that access to it has been disabled, or that a court or an appropriate public authority has ordered such removal or disablement.

(8) A caching provider who contravenes the conditions set out in subsection (7) shall be guilty of an offence and liable to a fine not exceeding level eight or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment.

(9) An internet service provider who enables access to information provided by a third person by providing an electronic hyperlink shall not be criminally liable with respect to the information if the internet service provider--

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

(b) through other means, obtains knowledge or becomes aware of stored specific illegal information promptly informs the appropriate authority to enable it to evaluate the nature of the information and if necessary issue an order for its removal.

(10) An internet service provider who fails to promptly remove or disable access to information in terms of subsection (9) shall be guilty of an offence and liable to a fine not exceeding level eight or to imprisonment for a period not exceeding two years or both such fine and such imprisonment.

(11) Any service provider who knowingly enables access to, stores, transmits or provides an electronic hyperlink to, any information with knowledge of the unlawfulness of the content of any such information shall be guilty of an offence and liable to a fine not exceeding level fourteen or to imprisonment not exceeding a period of ten years or to both such fine and such imprisonment.

PART X

GENERAL PROVISIONS

38 Jurisdiction

(1) A court in Zimbabwe shall have jurisdiction to try any offence under this Act where the offence was committed wholly or in part—

(a) within Zimbabwe or by any person in or outside Zimbabwe using a computer or information system or device, software or data located in Zimbabwe; or

(b) on a ship or aircraft registered in Zimbabwe; or

(c) by a national or permanent resident of Zimbabwe or a person carrying on business in Zimbabwe, whether or not the offence is committed in Zimbabwe; or

(d) by a national or permanent resident of Zimbabwe or a person carrying on business in Zimbabwe and the offence is committed outside Zimbabwe, if the person's conduct also constitutes an offence under the law of the country where the offence was committed and harmful effects were caused in Zimbabwe; or

(e) by any person, regardless of the location, nationality or citizenship of the person--

(i) using a computer or information system or device, software, or data located within Zimbabwe; or

(ii) directed against a computer or information system or device, software or data located in Zimbabwe.

39 Extradition

Any offence in terms of this Act shall be subject to extradition in terms of the Extradition Act [*Chapter 9:08*] provided that a person may not be extradited to or from Zimbabwe unless his or her conduct is criminal in both Zimbabwe and the other country.

40 Admissibility of electronic evidence

(1) In any criminal proceedings for an offence in terms of this Act, evidence generated from a computer system or by means of information and communications technologies or electronic communications systems shall be admissible in court.

(2) In assessing the admissibility or evidential weight of the evidence, regard shall be given to—

(a) the reliability of the manner in which the evidence was generated, stored or communicated;

(b) the integrity of the manner in which the evidence was maintained;

(c) the manner in which the originator or recipient of the evidence was identified; and

(d) any other relevant factors.

(4) The authentication of electronically generated documents shall be as prescribed in rules of evidence regulating the integrity and correctness of any other documents presented as evidence in a court of law.

(5) This section shall apply in addition to and not in substitution of any other law in terms of which evidence generated by computer systems or information and communications technologies or electronic communications systems or devices may be admissible in evidence.

41 Forfeiture

A court convicting any person of an offence under this Act may order the forfeiture to the State of--

(a) any money, asset or property constituting or traceable to the gross proceeds of such offence; and

(b) any computer or information system, software or other devices used or intended to be used to commit or to facilitate the commission of such offence.

42 Regulations

(1) The Minister may, in consultation with the Cybersecurity Committee, make regulations providing for all matters which by this Act are required or permitted to be prescribed or which, in his or her opinion, are necessary or convenient to be provided for in order to carry out or give effect to the provisions of this Act.

(2) Regulations made in terms of subsection (1) may provide for—

(a) 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;

(b) the penalties for contraventions of the regulations:

Provided that no such penalty shall exceed a fine of level ten or imprisonment for a period exceeding five years or both such fine and such imprisonment.

4 Guidelines

The Cybersecurity Committee may, with the approval of the Minister, issue such guidelines as may be necessary for the carrying out of the provisions of this Act as it relates to its functions under this Act.

45 Amendment of Cap. 9:23.

The Criminal Law (Codification and Reform) Act [*Chapter 9:23*] is amended—

(a) in section 162 by the repeal of the definitions of "computer virus", "data", "essential service" and "owner";

(b) by the repeal of sections 163 to 166.

(c)