CYBER AND DATA PROTECTION ACT [*CHAPTER 12:07*]

ARRANGEMENT OF SECTIONS

PART I

PRELIMINARY

Section

1. Short title.
2. Object.
3. Interpretation.
4. Application.

PART II

DATA PROTECTION AUTHORITY

5. Designation of Postal and Telecommunications Regulatory Authority as Data Protection Authority.
6. Functions of Data Protection Authority.

PART III

QUALITY OF DATA

7. Quality of data.

PART IV

GENERAL RULES ON THE PROCESSING OF DATA

8. Generality.
9. Purpose.
10. Non-sensitive data.
11. Sensitive information.
12. Genetic data, biometric sensitive data and health data.

PART V

DUTIES OF DATA CONTROLLER AND DATA PROCESSOR

13. Duties of Data Controller.
14. Rights of Data Subject.
15. Disclosures when collecting data directly from data subject.
16. Disclosures when not collecting data directly from data subject.
17. Authority to process.
18. Security.
19. Security breach notification.
20. Obligation of notification to Authority.
21. Content of notification.
22. Authorisation.
23. Openness of processing.
24. Accountability.

PART VI

DATA SUBJECT

Section

25. Decision taken on basis of Automatic Data Processing.
26. Representation of data subjection who is a child.
27. Representation of physically, mentally or legally incapacitated data subjects.

PART VII

TRANSBORDER FLOW

28. Transfer of personal information outside Zimbabwe.
29. Transfer to country outside the Republic of Zimbabwe which does not assure adequate level of protection.

PART VIII

CODE OF CONDUCT

30. Code of conduct.

PART IX

WHISTLEBLOWING

31. Whistleblower.

PART X

GENERAL PROVISIONS

32. Regulations.
33. Offences and penalties.
34. Appeals.

PART XI

CONSEQUENTIAL AMENDMENTS

35. Amendment of Chapter VIII of Cap. 9:23.
36. Amendment of Cap. 9:07.
37. Amendment of Cap. 11:20.



ZIMBABWE

ACT

An Act to provide for data protection with due regard to the Declaration of Rights under the Constitution and the public and national interest; to establish a Cyber Security Centre; a Data Protection Authority and to provide for their functions; to create a technology driven business environment and encourage technological development and the lawful use of technology; to amend sections 162 to 166 of the Criminal Code (Codification and Reform) Act [*Chapter 9:23*] to provide for investigation and collection of evidence of cyber crime and unauthorised data collection and breaches, and to provide for admissibility of electronic evidence for such offences 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

This Act may be cited as the Cyber and Data Protection Act [*Chapter 12:07*].

2 Object

The object of this Act is to increase cyber security in order to build confidence and trust in the secure use of information and communication technologies by data controllers, their representatives and data subjects.

Printed by the Government Printer, Harare

3 Interpretation

In this Act—

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

"code of conduct" refers to the Data Use Charters drafted by the data controller in order to institute the rightful use of IT processes, the Internet, and electronic communications of the structure concerned, and which have been approved by the Data Protection Authority;

"consent" refers to any manifestation of specific unequivocal, freely given, informed expression of will by which the data subject or his or her legal, judicial or legally appointed representative accepts that his or her data be processed;

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

"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;

"data controller" or "controller"—

(a) refers to any natural person or legal person who is licensable by the Authority;

(b) includes public bodies and any other person who determines the purpose and means of processing data;

"data controller's representative" or "controller's representative" refers to any natural person or legal person who performs the functions of the data controller in compliance with obligations set forth in this Act;

"Data processor" refers to a natural person or legal person, who processes data for and on behalf of the controller and under the controller's instruction, except for the persons who, under the direct employment or similar authority of the controller, are authorised to process the data;

"Data Protection Authority" or "Authority" refers to Postal and Telecommunications Regulatory Authority of Zimbabwe established in terms of section 5 of the Postal and Telecommunications Act [*Chapter 12:05*];

"data protection officer" or "DPO" refers to any individual appointed by the data controller and is charged with ensuring, in an independent manner, compliance with the obligations provided for in this Act;

"data subject" refers to an individual who is an identifiable person and the subject of data;

"disproportionate effort" means effort that is so labour intensive as to consume a lot of time, money and manpower resources;

"electronic communications network" means any electronic communication infrastructure and facilities used for the conveyance of data;

"genetic data: refers to any personal information stemming from a Deoxyribonucleic acid (DNA) analysis;

"health professional" refers to any individual determined as such by Zimbabwean law;

"identifiable person" means a person who can be identified directly or indirectly, in particular by reference to an identification number or to one or more

factors specific to his or her physical, physiological, mental, economic, cultural or social identity;

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

"personal information" means information relating to a data subject, and includes—

(a) the person's name, address or telephone number;

(b) the person's race, national or ethnic origin, colour, religious or political beliefs or associations;

(c) the person's age, sex, sexual orientation, marital status or family status;

(d) an identifying number, symbol or other particulars assigned to that person;

(e) fingerprints, blood type or inheritable characteristics;

(f) information about a person's health care history, including a physical or mental disability;

(g) information about educational, financial, criminal or employment history;

(h) opinions expressed about an identifiable person;

(i) the individual's personal views or opinions, except if they are about someone else; and

(j) personal correspondence pertaining to home and family life;

"processing" refers to any operation or set of operations which are performed upon data, whether or not by automatic means, such as obtaining recording or holding the data or carrying out any operation or set of operations on data, including—

(a) organisation, adaptation or alteration of the data;

(b) retrieval, consultation or use of the data; or

(c) alignment, combination, blocking, erasure or destruction of the data;

"recipient" a natural or legal person, agency or any other body to whom personal information is disclosed by a data controller, whether a third party or not; however, persons who receive personal information in the framework of a particular legal inquiry shall not be regarded as recipients;

"sensitive data" refers to—

(a) information or any opinion about an individual which reveals or contains the following—

(i) racial or ethnic origin;

(ii) political opinions;

(iii) membership of a political association;

(iv) religious beliefs or affiliations;

(v) philosophical beliefs;

(vi) membership of a professional or trade association;

(vii) membership of a trade union;

(viii) sex life;

(ix) criminal educational, financial or employment history;

(x) gender, age, marital status or family status;

(b) health information about an individual;

(c) genetic information about an individual; or

(d) any information which may be considered as presenting a major risk to the rights of the data subject;

"third party" refers to any natural or legal person or organisation other than the data subject, the controller, the processor and anyone who, under the direct authority of the controller or the processor, is authorised to process the data;

"transborder flow" refers to international flows of data by the means of transmission including data transmission electronically or by satellite;

"whistleblowing" refers to legal provisions permitting individuals to report the behaviour of a member of their organisation which, they consider contrary to a law or regulation or fundamental rules established by their organisation.

4 Application

(1) This Act shall apply to matters relating to access to information, protection of privacy of information and processing and storage of data wholly or partly by automated means: and shall be interpreted as being in addition to and not in conflict or inconsistent with the Protection of Personal Information Act [*Chapter 10:27*].

(2) Subject to subsection (1) this Act shall be applicable—

(a) to the processing of data carried out in the context of the effective and actual activities of any data controller;

(b) to the processing and storage of data by a controller who is not permanently established in Zimbabwe, if the means used, whether electronic or otherwise is located in Zimbabwe, and such processing and storage is not for the purposes of the mere transit of data through Zimbabwe.

(3) In the circumstances referred to in subsection (2)(b), the controller shall designate a representative established in Zimbabwe, without prejudice to legal proceedings that may be brought against the controller.

PART II

DATA PROTECTION AUTHORITY

5 Designation of Postal and Telecommunications Regulatory Authority as Data Protection Authority

The Postal and Telecommunications Regulatory Authority established in terms of the Postal and Telecommunications Act [*Chapter 12:05*] is hereby designated as the Data Protection Authority.

6 Functions of Data Protection Authority

(1) The Authority shall perform the following functions—

(a) to regulate the manner in which personal information may be processed through the establishment of conditions for the lawful processing of data;

(b) to promote and enforce fair processing of data in accordance with this Act;

(c) to issue its opinion either of its own accord, or at the request of any person with a legitimate interest, on any matter relating to the application of the

fundamental principles of the protection of privacy, in the context of this Act;

(d) to submit to any Court any administrative act which is not compliant with the fundamental principles of the protection of the privacy in the framework of this Act as well as any law containing provisions regarding the protection of privacy in relation to the processing of data in consultation with Minister responsible for Information, Publicity and Broadcasting Services;

(e) to advise the Minister on matters relating to right to privacy and access to information;

(f) to conduct inquiries or investigations either of its own accord or at the request of the data subject or any interested person, and in relation thereto may call upon the assistance of experts to carry out its functions and may request the disclosure of any documents that may be of use for their inquiry or investigation;

(g) to receive, by post or electronic means or any other equivalent means, the complaints lodged against data processing and give feed-back to the claimants or complainants;

(h) to investigate any complaint received in terms of this Act howsoever received;

(i) to conduct research on policy and legal matters relating to the development of international best practices on the protection of personal information in Zimbabwe and advise the Minister accordingly;

(j) in consultation with the Minister, to facilitate cross border cooperation in the enforcement of privacy laws and participating at national, regional and international forums mandated to deal with the protection of personal information initiatives.

(2) Subject to this Act, the Authority shall not, in the lawful exercise of its functions under this Act, be subject to the direction or control of any person or authority.

PART III

QUALITY OF DATA

7 Quality of Data

(1) The data controller shall ensure that data processed is—

(a) adequate, relevant and not excessive in relation to the purposes for which it is collected or further processed;

(b) accurate and, where necessary, kept up-to-date;

(c) retained in a form that allows for the identification of data subjects, for no longer than necessary with a view to the purposes for which the data is collected or further processed.

(2) The data controller shall take all appropriate measures to ensure that data processed shall be accessible regardless of the technology used and ensure that the evolution of technology shall not be an obstacle to the access or processing of such data.

(3) The controller shall ensure compliance with the obligations set out in subsections (1) and (2) by any person working under his or her authority and any subcontractor.

PART IV

GENERAL RULES ON THE PROCESSING OF DATA

8 Generality

The data controller shall ensure that the processing of data is necessary and that the data is processed fairly and lawfully.

9 Purpose

(1) The data controller shall ensure that data is collected for specified, explicit and legitimate purposes and, taking into account all relevant factors, especially the reasonable expectations of the data subject and the applicable legal and regulatory provisions, that the data is not further processed in a way incompatible with such purposes.

(2) Under the conditions established by the Authority, further processing of data for historical, statistical or scientific research purposes is not considered incompatible.

10 Non-sensitive data

(1) Personal information may only be processed if the data subject or a competent person, where the data subject is a child, consents to the processing of such data.

(2) The consent referred to in subsection (1) may be implied where the data subject is an adult natural person or has a legal persona and has full legal capacity to consent.

(3) The processing of non-sensitive data is permitted, without the consent of the data subject, where necessary for purposes of—

(a) being material as evidence in proving an offence; or

(b) compliance with an obligation to which the controller is subject by or by virtue of a law; or

(c) protecting the vital interests of the data subject; or

(d) performing a task carried out in the public interest, or in the exercise of the official authority vested in the controller, or in a third party to whom the data is disclosed; or

(e) promoting the legitimate interests of the controller or a third party to whom the data is disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject claiming protection under this Act.

(4) The Authority may specify the circumstances in which the condition stipulated under subsection (3)(e) are considered as having been met.

11 Sensitive information

(1) No data controller shall process sensitive data unless the data subject has given consent in writing for such processing;

(2) The consent to the processing of data may be withdrawn by the data subject at any time and without any explanation and free of charge;

(3) The Authority shall determine the circumstances in which the prohibition to process the data referred to in this subsection (1) cannot be lifted even with the data

subject's consent (taking into account the factors surrounding the prohibition and the reasons for collecting the data).

(4) The Minister responsible for the Cyber security and Monitoring Centre in consultation with the Minister, may give directions on how to implement this section with respect to sensitive information affecting national security or the interests of the State.

(5) The provisions of subsection (1) shall not apply where—

(a) the processing is necessary to carry out the obligations and specific rights of the controller in the field of employment law; or

(b) the processing is necessary to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving his or her consent or is not represented by his or her legal, judicial or agreed representative; or

(c) the processing is carried out in the course of its legitimate activities by a foundation, association or any other non-profit organisation with a political, philosophical, religious, health-insurance or trade-union purpose and on condition that the processing relates solely to the members of the organisation or to persons who have regular contact with it in connection with such purposes and that the data is not disclosed to a third party without the data subjects' consent; or

(d) the processing is necessary to comply with national security laws; or

(e) the processing is necessary, with appropriate guarantees, for the establishment, exercise or defence of legal claims; or

(f) the processing relates to data which has been made public by the data subject; or

(g) the processing is necessary for the purposes of scientific research:

Provided the Authority shall be entitled to specify the conditions under which such processing may be carried out; or

(h) the processing of data is authorised by a law or any regulation for any other reason constituting substantial public interest.

(6) Without prejudice to the application of sections 5 to 8, the processing of data relating to sex life is authorised if—

(a) it is carried out by an association with a legal personality or by an organisation of public interest whose main objective, according to its Memorandum and Articles of Association, is the evaluation, guidance or treatment of persons of such sexual conduct, and who is recognised by a competent public body as being responsible for the welfare of such persons;

(b) the objective of the processing of the data consist of the evaluation, guidance and treatment of the persons referred to in this section, and the processing of data relates only to the afore-mentioned persons:

Provided that the competent public body referred to in paragraph (a) grants a specific, individualised authorisation, having received the opinion of the Authority.

(7) The authorisation referred to in this section shall specify the duration of the authorisation, the conditions for supervision of the authorised association or organisation by the competent public body, and the way in which the processing must be reported to the Authority.

12 Genetic data, biometric sensitive data and health data

(1) The processing of genetic data, biometric data and health data is prohibited unless, the data subject has given consent in writing to the processing.

(2) The consent referred to in subsection (1) can be withdrawn by the data subject at any time without any reasons and free of charge.

(3) The provisions of subsection (1) shall not apply where—

(a) the processing is necessary to carry out the specific obligations and rights of the controller in the field of employment law; or

(b) the processing is necessary to comply with national security laws; or

(c) the processing is necessary for the promotion and protection of public health, including medical examination of the population; or

(d) the processing is required by or by virtue of a law or any equivalent legislative act for reasons of substantial public interest; or

(e) the processing is necessary to protect the vital interests of the data subject or another person, where the data subject is physically or legally incapable of giving his or her consent or is not represented by his or her legal, judicial or agreed representative; or

(f) the processing is necessary for the prevention of imminent danger or the mitigation of a specific criminal offence; or

(g) the processing relates to data which has apparently been made public by the data subject; or

(h) the processing is necessary for the establishment, exercise or defense of legal rights; or

(i) the processing is required for the purposes of scientific research; or

(j) the processing is necessary for the purposes of preventive medicine or medical diagnosis, the provision of care or treatment for the data subject or to one of his or her relatives, or the management of health-care services in the interest of the data subject, and the data is processed under the supervision of a health professional.

(4) Health-related data may only be processed under the responsibility of a health-care professional, except if the data subject has given his or her written consent or if the processing is necessary for the prevention of imminent danger or for the mitigation of a specific criminal offence.

(5) The Authority shall be entitled to specify the conditions under which such processing may be carried out.

(6) Health related data may only be collected from other sources where the data subject is incapable of providing the data.

(7) For the purposes of processing personal information under this section, the health professional and his or her agents are subject to the duty of professional secrecy.

(8) The processing of genetic data, shall be authorised if it is processed for what it reveals or contains and data concerning health shall be processed only if a unique patient identifier is given to the patient which is distinct from any other identification number, issued by the public authority established for this purpose.

(9) The association of the unique patient identifier with any other identifier which permits the identification of the data subject as provided for in section 8 is permissible only with the express authorisation of the Authority.

(10) The data of a child shall be processed subject to section 26.

PART V

DUTIES OF DATA CONTROLLER AND DATA PROCESSOR

13 Duties of Data Controller

Every data controller or data processor shall ensure that personal information is—

(a) processed in accordance with the right to privacy of the data subject;

(b) processed lawfully, fairly and in a transparent manner in relation to any data subject;

(c) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;

(d) adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;

(e) collected only where a valid explanation is provided whenever information relating to family or private affairs is required;

(f) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay; and

kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected.

14 Rights of Data Subject

A data subject has a right to—

(a) be informed of the use to which their personal information is to be put;

(b) access their personal information in custody of data controller or data processor;

(c) object to the processing of all or part of their personal information;

(d) correction of false or misleading personal information; and;

(e) deletion of false or misleading data about them.

15 Disclosures when collecting data directly from data subject

(1) When obtaining data directly from the data subject, the controller or the controller's representative shall provide the data subject with at least the following information, unless the data subject has already received such information—

(a) the name and address of the controller and of his or her representative, if any;

(b) the purposes of the processing;

(c) the existence of the right to object, by request and free of charge, to the intended processing of data relating to him or her, if it is obtained for the purposes of direct marketing;

(d) whether compliance with the request for information is compulsory or not, as well as what the consequences of the failure to comply are;

(e) taking into account the specific circumstances in which the data is collected, any supporting information, as necessary to ensure fair processing for the data subject, such as—

(i) the recipients or categories of recipients of the data;

(ii) whether it is compulsory to reply, and what the possible consequences of the failure to reply are;

(iii) the existence of the right to access and rectify the data relating to him or her except where such additional information, taking into account the specific circumstances in which the data is collected is not necessary to guarantee accurate processing.

(f) other information dependent on the specific nature of the processing, as specified by the Authority.

16 Disclosures when not collecting data directly from data subject

(1) Where the data is not collected from the data subject, the controller or his or her representative shall provide the data subject with at least the information set out below when recording the data or considering communication to a third party, unless it is established that the data subject is in receipt of such information—

(a) the name and address of the controller and of his or her representative, if any;

(b) the purposes of the processing;

(c) whether compliance with the request for information is compulsory or not, as well as what the consequences of the failure to comply are;

(d) the existence of the right to object, by request and free of charge, to the intended processing of data relating to him or her, if it is obtained for the purposes of direct marketing; in which case, the data subject shall be informed prior to the first disclosure of the data to a third party or prior to the first use of the data for the purposes of direct marketing on behalf of third parties;

(e) taking into account the specific circumstances in which the data is collected, any supporting information, as necessary to ensure fair processing such as—

(i) the categories of data concerned;

(ii) the recipients or categories of recipients of the data;

(iii) the existence of the right to access and rectify the data relating to him/her, unless such additional information, taking into account the specific circumstances in which the data is provided, is not necessary to guarantee fair processing with respect to the data subject;

(f) other information dependent on the specific nature of the processing, which is specified by the Authority.

(2) The provisions of subsection (1) shall not apply where—

(a) informing the data subject proves impossible or would involve a disproportionate effort, in particular for data collected for statistical purposes or for the purpose of historical or scientific research, or for the purpose of medical examination of the population with a view to protecting and promoting public health; or

(b) data is recorded or provided in terms of the law;

(3) The Authority shall establish the conditions for the application of this section.

17 Authority to process

Any person having access to the data and acting under the authority of the controller or of the processor, as well as the processor himself or herself, may process data only as instructed by the controller, without prejudice to any duty imposed by law.

18 Security

(1) In order to safeguard the security, integrity and confidentiality of the data, the controller or his or her representative, if any, or the processor, shall take the appropriate technical and organisational measures that are necessary to protect data from negligent or unauthorised destruction, negligent loss, unauthorised alteration or access and any other unauthorised processing of the data.

(2) These measures referred to in subsection (1) must ensure an appropriate level of security taking into account the state of technological development and the cost of implementing the measures on the one hand, and the nature of the data to be protected and the potential risks to the data subject on the other hand.

(3) The Authority may issue appropriate standards relating to information security for all or certain categories of processing.

(4) The data controller shall appoint a data processor who shall provide sufficient guarantees regarding the technical and organisational security measures employed to protect the data associated with the processing undertaken and ensure strict adherence to such measures.

(5) The data controller shall enter into a written contract or any other legal instrument with the data processor which ensures that the data processor maintains security measures on data.

19 Security breach notification

The data controller shall notify the Authority within twenty-four (24) hours of any security breach affecting data he or she processes.

20 Obligation of notification to Authority

(1) Prior to any wholly or partly automated operation or set of operations intended to serve a single purpose or several related purposes, the controller or his or her representative, if any, must notify the Authority.

(2) Any modification to the information provided according to section 16 must be notified to the Authority.

(3) The provisions of subsection (1) shall not apply to operations having the sole purpose of keeping a register that is intended to provide information to the public by virtue of operation of law and that is open to access by the general public or by any person demonstrating a legitimate interest.

(4) The Authority may exempt certain categories from notification under this section if—

(a) taking into account the data being processed, there is no apparent risk of infringement of the data subjects' rights and freedoms, and if the purposes of the processing, the categories of data being processed, the categories of data subjects, the categories of recipients and the data retention period are specified;

(b) the data controller has appointed a data protection officer.

(5) The appointment of the data protection officer shall be duly notified to the Authority.

(6) The Authority shall provide guidelines that provide for the qualifications and functions of data protection officer and such data protection officer's duties shall include—

(a) ensuring compliance by the data controller with the provisions of this Act and regulations made thereunder;

(b) dealing with requests made to the data controller pursuant to this Act;

(c) working with the Authority in relation to the performance of its functions in relation to the data controller.

(7) If exemption from the duty of notification has been granted for automatic processing in accordance with the subsection (3), the data controller may disclose the items of information mentioned in section 16 to any person entitled to receive such information.

21 Content of notification

(1) The notification referred to in section 20 shall state, at least—

(a) the date of notification and the law or regulatory instrument permitting the automatic processing of data;

(b) the surname, first names and complete address or the name and registered offices of the controller and of his or her representative, if any;

(c) the denomination of the automatic processing;

(d) the purpose or the set of related purposes of the automatic processing;

(e) the categories of data being processed and a detailed description of the sensitive data being processed;

(f) a description of the category or categories of the data subjects;

(g) the safeguards that must be linked to the disclosure of the data to third parties;

(h) the manner in which the data subjects are informed, the service providing for the exercise of the right to access and the measures taken to facilitate the exercise of that right;

(i) the inter-related processing planned or any other form of linking with other processing;

(j) the period of time after the expiration of which the data may no longer be stored, used or disclosed;

(k) a general description containing a preliminary assessment of whether the security measures provided for pursuant to section 13 above are adequate;

(l) the recourse to a data processor, if any;

(m) the transfers of data to a third party as planned by the data controller.

(2) The Authority may prescribe other information which shall be mentioned in the notification.

(3) Where the Authority is of the opinion that the processing or transfer of data by a data controller entails specific risks to the privacy rights of data subjects, he or she may inspect and assess the security and organisational measures prior to the commencement of the processing or transfer.

(4) The Authority may, during working hours, carry out further inspection and assessment of the security and organisational measures employed by a data controller subject to reasonable notification to the data controller of the Authority's intended inspection and assessment.

22 Authorisation

(1) The Authority shall establish the categories of data processing which represent specific risks to the fundamental rights of the data subject and which require specific authorisation from the Authority.

(2) Such authorisation shall only be provided following receipt of notification from the data controller or from the data protection officer pursuant to sections 15 and 16.

23 Openness of processing

(1) The Authority shall keep a register of all automatic processing operations of data.

(2) Any entry in the register referred to in subsection (1) must include the information mentioned in section 16(1).

(3) The register shall be available for inspection by members of the public, in the manner determined by the Authority.

(4) In case of the processing of data exempted from notification by this Act, the Authority may, either by virtue of its office or at the data subject's request, impose upon the controller the obligation to disclose to the data subject all or part of the information mentioned in section 16(1).

24 Accountability

The data controller shall—

(a) take all the necessary measures to comply with the principles and obligations set out in this Act; and

(b) have the necessary internal mechanisms in place for demonstrating such compliance to both the data subjects and the Authority in the exercise of its powers.

PART VI

DATA SUBJECT

25 Decision taken on basis of Automatic Data Processing

(1) The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

(2) The right referred to in subsection (1) shall not be applicable if the decision based solely on automated processing is taken on the basis of the data subject having consented to such decision or is based on a provision established by law.

26 Representation of data subject who is child

Where the data subject is a child, his or her rights pursuant to this law may be exercised by his or her parents or legal guardian.

27 Representation of physically, mentally or legally incapacitated data subjects

(1) A data subject who is physically, mentally or legally incapable of exercising the rights given under this Act and who is not subject to the provisions of section 26, may exercise such rights through a parent or guardian or as provided for by law or as designated by a Court of competent jurisdiction.

(2) Incapacity as referred to in subsection (1) shall be proven by a physician or a person legally competent to do so.

PART VII

TRANSBORDER FLOW

28 Transfer of personal information outside Zimbabwe

(1) Subject to the provisions of this Act, a data controller may not transfer personal information about a data subject to a third party who is in a foreign country unless an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data is transferred solely to allow tasks covered by the competence of the controller to be carried out.

(2) The adequacy of the level of protection afforded by the third party or international organisation in question shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; with particular consideration being given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the recipient third party or recipient international organisation, the laws relating to data protection in force in the third party or international organisation in question and the professional rules and security measures which are complied with in that third party or international organisation.

(3) The Authority shall lay down the categories of processing operations for which and the circumstances in which the transfer of data to countries outside the Republic of Zimbabwe is not authorised.

(4) The Minister responsible for the Cyber security and Monitoring Centre in consultation with the Minister, may give directions on how to implement this section with respect to transfer of personal information outside of Zimbabwe.

29 Transfer to country outside Zimbabwe which does not assure adequate level of protection

A transfer or a set of transfers of data to a country outside Zimbabwe which does not assure an adequate level of protection may take place in one of the following cases—

(a) the data subject has unambiguously given his or her consent to the proposed transfer;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request;

(c) the transfer is necessary for the conclusion or performance of a contract concluded or to be concluded between the controller and a third party in the interest of the data subject;

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims;

(e) the transfer is necessary in order to protect the vital interests of the data subject;

(f) the transfer is made from a register which, according to acts or regulations, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the case at hand.

PART VIII

CODE OF CONDUCT

30 Code of Conduct

(1) The Authority shall provide guidelines and approve codes of conduct and ethics governing the rules of conduct to be observed by data controllers and categories of data controllers.

(2) In effecting (1) above, the Authority shall consider trade associations and other bodies representing other categories of controllers who have national codes or have the intention of amending or extending existing national codes and allow them to submit such codes for the approval of the Authority.

(3) The Authority in considering codes of conduct for approval, shall ascertain, among other things, whether the Codes submitted comply with the provisions of this Act.

(4) If it deems it fit, the Authority shall seek the views of affected data subjects or their representatives.

PART IX

WHISTLEBLOWING

31 Whistleblower

(1) The Authority shall establish rules giving the authorisation for and governing the whistleblowing system.

(2) Rules established in terms of subsection (1) must preserve—

(a) the principles of fairness, lawfulness and purpose of the processing;

(b) the principles related to the proportionality on the limitation of the scope, accuracy of the data which will be processed;

(c) the principle of openness and delivering an adequate system for the collection of personal information shall address—

(i) the scope and purpose of the whistleblowing;

(ii) the processing of reporting;

(iii) the consequences of the justified and unjustified reporting;

(iv) the way of exercising the rights of access, correction, deletion as well as the competent authority to which a request can be made; and

(v) the third party who may receive data concerning the informer and the person who is implicated in the scope of the processing of the report;

(vi) the technical and organisational rules;

(vii) rules concerning the rights of the data subject by making clear that the right of access doesn't allow to access to data linked to a third person without his or her express and written consent; and

(viii) the method of notifying the Authority.

(3) The person who is implicated shall be informed as soon as possible of the existence of the report and about the facts which he or she is accused of in order to exercise the rights established in this Act.

(4) The release of information to the person who is implicated may be withheld in exceptional circumstances.

PART X

GENERAL PROVISIONS

32 Regulations

(1) The Minister may, in consultation with the Authority, 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 prescribed for carrying out or giving effect to this Act.

(2) Regulations referred to in subsection (1) may provide for the exercise of the rights referred to in sections 25 to 27 of this Act.

33 Offences and penalties

(1) Any member of staff of the Authority or any expert, contractor, sub-contractor who violates the provisions of this Act shall be guilty of an offence and liable to a fine not exceeding level 7 or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment.

(2) Any data controller, his or her representative, agent or assignee who contravenes section 11, 13, 18(4), 24 and 28 shall be guilty of an offence and liable to a fine not exceeding level 11 or to imprisonment for a period not exceeding seven years or to both such fine and such imprisonment.

(3) Upon conviction by a Court of competent jurisdiction the Court may order the seizure of the media containing the data to which the offence relates, such as manual filing systems, magnetic discs or magnetic tapes, except for computers or any other equipment, or the deletion of the data.

(4) Seizure or deletion may be ordered where the media containing the data does not belong to the person convicted.

(5) The objects seized in terms of this section shall be destroyed.

(6) The controller or his or her representative shall be liable for the payment of the fines incurred by his or her agent or assignee.

34 Appeals

Any person aggrieved by the decision of the Authority may appeal to the Administrative Court.

PART XI

CONSEQUENTIAL AMENDMENTS

35 Amendment of Chapter VIII of Cap. 9:23

(1) The Criminal Law (Codification and Reform) Act [*Chapter 9:23*] (hereinafter called the "principal Act") is amended in section 162 by the repeal of the definitions of "computer virus", "data", "essential service" and "owner" and the substitution of the following definitions—

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

"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) in an aggravating circumstance certified by the Cyber Security and Monitoring Interception of Communications Centre to be a breach of State Security to a fine not exceeding level 14 or to imprisonment for a period not exceeding ten years or to both such fine and such imprisonment;

(f) programmes; and

(g) 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;

"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;

"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;

"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" means a device or inter-connected or related devices that are used or that are responsible for the creation, transmission, receiving, processing 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;

"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;

"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.

(2) The principal Act is amended by the repeal of sections 163 to 166 and the substitution of the following—

"PART I

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

163 Hacking

(1) A person who—

(a) knowing or suspecting that he or she must obtain prior authority to access the data, computer programme, computer data storage medium, or the whole or any part of a computer system in question; and

(b) intentionally, unlawfully and without such authority, secures access to such data, programme, medium or system;

shall be guilty of hacking and liable—

(c) in any of the aggravating circumstances described in section 13 to a fine not exceeding level 14 or to imprisonment for a period not exceeding ten years or both such fine and such imprisonment;

(d) in any other case, to a fine not exceeding level 10 or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

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

(a) to obtain, to make use of, gain entry into, view, display, instruct or communicate with, or store data in or retrieve data from;

(b) 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.

163A Unlawful acquisition of data

(1) Any person who unlawfully and intentionally—

(a) intercepts by technical or any other means any private transmission of computer data to, from or within a computer network, computer device, database or information system or electromagnetic emissions from a computer or information system carrying such computer data;

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

(c) 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 14 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 14 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 14 or to imprisonment for a period not exceeding ten years or to both such fine and such imprisonment.

163B 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 authorised 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 10 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 14 or to imprisonment for a period not exceeding ten years or to both such fine and such imprisonment.

163C 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 14 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 14 or to imprisonment for a period not exceeding twenty years or to both such fine and such imprisonment.

163D 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 authorised 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 12 or imprisonment for a period not exceeding ten years or both such fine and 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.

163E 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 12 or imprisonment for a period not exceeding ten years or both such fine and 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 10 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 12 or imprisonment for a period not exceeding ten years or to both such fine and such imprisonment.

163F 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 an organised criminal gang.

PART II

OFFENCES RELATING TO ELECTRONIC COMMUNICATIONS AND MATERIALS

164 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 intent 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 10 or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

164A Sending threatening data message

(1) 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 10 or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

(2) Any person who up skirts and records nude images or videos of a citizen or a foreigner who is resident in Zimbabwe without consent shall be guilty of an offence and liable to a fine not exceeding level 10 or imprisonment for a period not exceeding 5 years or both such fine or such imprisonment.

164B 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 10 or to imprisonment for a period not exceeding ten years or to both such fine and such imprisonment.

164C 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 10 or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

164D Spam

Any person who intentionally and without lawful excuse—

(a) 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

(b) 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 5 or to imprisonment for a period not exceeding one year or to both such fine and such imprisonment.

164E 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 or video of an identifiable person without the consent of the person concerned or with recklessness as to the lack of consent of the person concerned, with the aim of causing the humiliation or embarrassment of such person shall be guilty of an offence and liable to a fine not exceeding level 10 or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.".

(2) For the purposes of subsection (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.

164F 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 14 or to imprisonment for a period not exceeding ten years or to both such fine and such imprisonment.

164G Identity-related offence

(1) Any person who unlawfully and intentionally by means of information and communication technologies 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 10 or to imprisonment for a period not exceeding ten years or to both such fine and such imprisonment

(2) Special consideration shall be given when a child is found guilty of any of the offences set out in (1), in line with the law of Zimbabwe:

Provided that the penalty shall not give the child a criminal record nor shall the child be imprisoned for this offence.

PART III

OFFENCES AGAINST CHILDREN AND PROCEDURAL LAW

165 Recording of genitalia and buttocks beneath closing without consent

(1) Any person who unlawfully and intentionally records an image or video beneath the clothing of another person which depicts this person's genitalia or buttocks, whether covered by underwear or not, without the consent of the depicted person or with recklessness as to the lack of consent of the person concerned, as far as these are to be protected against sight according to the recognizable will of the depicted person, shall be guilty of an offence and liable to a fine not exceeding level 10 or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

(2) Section 164E shall apply *mutatis mutandis* to any person who makes available, broadcasts or distributes a data message containing an image or video as described in (1).

165A Child sexual abuse material

(1) In this Act—

"Child sexual abuse material" means any representation through publication, exhibition, cinematography, electronic means or any other means whatsoever, of a child, a person made to appear as a child or realistic material representing a child, engaged in real or simulated explicit sexual activity, or any representation of the sexual parts of a child for primarily sexual purposes.

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

(a) produces child sexual abuse material;

(b) offers or makes available child sexual abuse material;

(c) distributes or transmits child sexual abuse material;

(d) procures or obtains child sexual abuse material for oneself or for another person;

(e) possesses child sexual abuse material on a computer system or a computer-data storage medium;

(f) knowingly obtains, accesses or procures child sexual abuse material;

(g) baits a child into the production or distribution of child sexual abuse material;

shall be guilty of an offence and liable to a fine not exceeding level 14 or to imprisonment for a period not exceeding ten years, or both such fine and such imprisonment.

(3) Any person of 18 years or above, who unlawfully and intentionally through information and communication technologies, proposes to meet a child who has not reached the age of consent to sexual activity as set by the Criminal Law (Codification and Reform Act) [*Chapter 9:23*] for the purpose of engaging in sexual activity with him or her, where this proposal has been followed by material acts leading to such a meeting, shall be guilty of an offence and liable to a fine not exceeding level 14 or to imprisonment for a period not exceeding ten years, or both such fine and such imprisonment.

165B 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 14 or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

166 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;

(f) against citizens or permanent residents of Zimbabwe.

36 Amendment of Cap. 9:07

The Criminal Procedure and Evidence Act [*Chapter 9:07*] is amended by the insertion after Part XX of the following Part—

"PART XXA

PROVISIONS RELATING TO CYBER CRIME

379A 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 be 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.

(5) Any person who does not comply with the order given in terms of this section shall be guilty of an offence and liable to a fine.

379B 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) authorise 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) Section 33(3) of the Data Protection Act [*Chapter 11:22*] shall apply *mutatis mutandis* to an application in terms of this section.

379C Obligations and immunity 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 8 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 8 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 8 or to imprisonment for a period not exceeding two years or both such fine and such imprisonment.

(11) Any service provider who knowingly enablesaccess 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 14 or to imprisonment not exceeding a period of ten years or to both such fine and such imprisonment.

379D 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 directed against a computer or information system or

(ii) device, software or data located in Zimbabwe.

379E 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.

(3) 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.

(4) 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.

379F 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.".

37 Amendment of Cap.11:20

(1) The Interception of Communications Act [*Chapter 11:20*] (hereinafter called the "principal Act") is amended in section 2—

(a) by the repeal of the definition of "monitoring centre" and substitution of—

""cyber security and monitoring centre" means the Cyber Security and Monitoring of Interception of Communications Centre being unit central monitoring apparatus designated to be the monitoring facility through which all the intercepted communications and call-related information of a particular interception target are forwarded to an authorised person;".

(2) The principal Act is amended in by the repeal of section 4 and the following is substituted—

"4 Cyber Security and Monitoring of Interceptions of Communications Centre

(1) There shall be established a unit in the Office of the President, which shall be called the Cyber Security and Monitoring of Interception of Communications Centre.

(2) The cyber security and monitoring centre shall be advised by a committee which shall give advice to the director of the centre on whether or not a warrant should be issued.

(3) The cyber security and monitoring centre shall be manned, controlled and operated by technical experts designated by the agency.

(4) The cyber security and monitoring centre shall give technical advice to—

(a) authorised persons; and

(b) service providers;

on cyber security and the interception of communications in terms of this Act.".

(3) The principal Act is amended by the insertion after section 4 of the following sections—

"4A Functions of Cyber Security and Monitoring of Interceptions of Communications Centre

The functions of the Cyber Security and Monitoring Centre shall be to—

(a) be the sole facility through which authorised interceptions shall be effected;

(b) advise Government and implement Government policy on cybercrime and cyber security;

(c) identify areas for intervention to prevent cybercrime;

(d) coordinate cyber security and establish a national contact point available daily around-the-clock;

(e) 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;

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

(g) provide guidelines to public and private sector interested parties on matters relating to awareness, training,

enhancement, investigation, prosecution and combating cybercrime and managing cyber security threats;

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

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

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

4B Establishment of Cyber Security Committee

(1) There is hereby established a committee to be known as the Cyber Security Committee which will shall be an *ad hoc* advisory body to the Minister.

(2) The Cyber Security Committee shall consist of eleven members appointed by the Minister for their knowledge in computer and telecommunications, law and policy 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 from the cyber security and monitoring centre;

(c) any representative from any sector of the economy or any other person who may be necessary to the deliberations in respect of a particular warrant, appointed on an ad hoc basis.

(3) From among the appointed members, the Minister shall appoint the Chairperson of the Cyber Security Committee.

(4) The Committee shall, at its first meeting, elect a Vice-Chairperson of the Committee from among its members:

Provided that the Chairperson and the Vice Chairperson shall be of different genders.

(5) The provisions of the Schedule apply to the Cyber Security Committee.

(6) The Cyber Security 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.

(7) The principal Act is amended in section 5 by the insertion after subsection (3) of the following subsection—

"(4) The Minister, upon receiving an application for a warrant in terms of this section, shall refer the application to the Cyber security committee, who shall advise the Minister on whether or not any of the reasonable grounds to issue a warrant referred to in section 6 are present:

Provided that the Minister may issue a provisional warrant if in his or her opinion any of the reasonable grounds referred to in section 6 are present.

(8) The Minister may withdraw a warrant issued provisionally upon the advice of the Committee that no reasonable grounds to issue to the warrant existed, without prejudice to anything that may be done by virtue of the warrant issued by the Minister between the time he or she issued it provisionally and the time it was referred to the committee and withdrawn.".

(9) The principal Act is amended by the insertion of the following Schedule—

"SCHEDULE (Section 4B (5))

PROVISIONS APPLICABLE TO CYBER SECURITY COMMITTEE

Terms and conditions of office of members

1. (1) Subject to this Schedule, a member shall hold office for such period, not exceeding five years, as the Minister may fix on his or her appointment.

(2) Subject to paragraph 8, a member shall hold office on such conditions as the Minister may fix in relation to members generally.

(3) A retiring member shall be eligible for re-appointment as a member.

Disqualification for appointment as member

2. (1) The Minister shall not appoint a person as a member and no person shall be qualified to hold office as a member if he or she—

(a) is married to a person who is engaged in any activity connected with any business, if in the opinion of the Minister such financial interest or activity is likely to interfere with the impartial discharge by that person of his or her duties as a member; or

(b) has, in terms of a law in force in any country—

(i) been adjudged or otherwise declared insolvent or bankrupt and has not been rehabilitated or discharged; or

(ii) made an assignment to, or arrangement or composition with, his or her creditors which has not been rescinded or set aside; or

(c) has, within the period of five years immediately preceding the date of his or her proposed appointment, been convicted—

(i) in Zimbabwe, of an offence; or

(ii) outside Zimbabwe, in respect of conduct which if committed in Zimbabwe would constitute an offence; and sentenced to a term of imprisonment imposed without the option of a fine, whether or not any portion has been suspended, and has not received a free pardon.

(2) A person who is—

(a) a member of Parliament; or

(b) a member of two or more other statutory bodies;

shall not be appointed as a member, nor shall he or she be qualified to hold office as a member.

(3) For the purpose of subparagraph (2)(b)—

(a) a person who is appointed to a council, board or other authority which is a statutory body or which is responsible for the administration of the affairs of a statutory body, shall be regarded as a member of that statutory body;

(b) "statutory body" means—

(i) any Commission established by the Constitution; or

(ii) any body corporate established-directly by or under an Act for special purposes specified in that Act, the membership of which consists wholly or mainly of persons appointed by the President, Vice President, a Minister or a statutory body or by a Commission established by the Constitution.

Vacation of office by member

3. A member shall vacate his or her office and the member's office shall become vacant—

(a) one month after the date upon which he or she gives notice in writing to the Minister of his or her intention to resign or on the expiry of such other period of notice as the member and the Minister may agree; or

(b) on the date he or she begins to serve a sentence of imprisonment imposed in Zimbabwe without the option of a fine—

(i) in Zimbabwe, in respect of an offence; or

(ii) outside Zimbabwe, in respect of conduct which if committed in Zimbabwe, would constitute an offence; or

(c) if he or she becomes disqualified in terms of paragraph 2(1)(a), (b) or (c) to hold office as a member; or

(d) if he or she is required in terms of paragraph 4 to vacate his or her office.

Dismissal or suspension of members

4. (1) The Minister may require a member to vacate his or her office if the member—

(a) has been guilty of any conduct that renders him or her unsuitable as a member; or

(b) has failed to comply with the conditions of his or her office fixed by the Minister in terms of paragraph 1(2); or

(c) is mentally or physically incapable of efficiently carrying out his or her functions as a member.

(2) The Minister, on the recommendation of the Committee, may require a member to vacate his or her office if the member has been absent without the permission of the Committee from two consecutive meetings of the Committee of which he or she was given at least seven days' notice and there was no just cause for the member's absence.

(3) The Minister may suspend a member—

(a) whom he or she suspects on reasonable grounds of having been guilty of conduct referred to in subparagraph (1)(a); or

(b) against whom criminal proceedings have been instituted for an offence in respect of which a sentence of imprisonment without the option of

a fine may be imposed; and while that member is so suspended he or she shall not carry out any functions as a member.

Filling of vacancies in Committee

5. On the death of or the vacation of office by a member the Minister shall appoint a person to fill the vacancy.

Meetings and procedure of Committee

6. (1) The Cybersecurity Committee shall hold its meetings on an ad hoc basis on such date and at such place as the Minister may fix.

(2) The chairperson or, in his or her absence, the vice-chairperson shall preside at all meetings of the Committee:

Provided that, if the chairperson and the vice-chairperson are absent from a meeting of the Committee, the members present may elect one of their members to preside at that meeting as chairperson.

(3) Five members shall form a quorum at any meeting of the Committee.

(4) All acts, matters or things authorised or required to be done by the Committee may be decided by a majority vote at a meeting of the Committee at which a quorum is present.

(5) Subject to subparagraph (9), at all meetings of the Committee each member present shall have one vote on each question before the Committee and, in the event of an equality of votes, the chairperson shall have a casting vote in addition to a deliberative vote.

Validity of decisions and acts of Committee

7. No decision or act of the Committee or act done under the authority of the Committee shall be invalid by reason only of the fact that a disqualified person acted as a member of the Committee at the time the decision was taken or act was done or authorised.

Minutes of proceedings of Committee and committees

8. (1) The Committee shall cause minutes of all proceedings of and decisions taken at every meeting of the Committee to be entered in books kept for the purpose in a confidential manner.".