THE CYBER SECURITY AND CYBER CRIMES ACT, 2021

ARRANGEMENT OF SECTIONS

Single copies of this Act may be obtained from the Government Printer, P.O. Box 30136, 10101 Lusaka, Price K96.00 each.

PART VIII

INTERNATIONAL COOPERATION IN MAINTAINING CYBER SECURITY

PART IX

CYBER CRIME

PART X

ELECTRONIC EVIDENCE

PART XI

GENERAL PROVISIONS

GOVERNMENT OF ZAMBIA

ACT

No. 2 of 2021

Date of Assent: 23rd March, 2021

An Act to provide for cyber security in the Republic; provide for the constitution of the Zambia Computer Incidence Response Team and provide for its functions; provide for the constitution of the National Cyber Security Advisory and Coordinating Council and provide for its functions; provide for the continuation of the Central Monitoring and Co-ordination Centre; provide for the protection of persons against cyber crime; provide for child online protection; facilitate identification, declaration and protection of critical information infrastructure; provide for the collection of and preservation of evidence of computer and network related crime; provide for the admission; in criminal matters, of electronic evidence; provide for registration of cyber security service providers; and provide for matters connected with, or incidental to, the foregoing.

[24th March,2021

ENACTED by the Parliament of Zambia. Enactment

PART I

PRELIMINARY PROVISIONS

1. This Act may be cited as the Cyber Security and Cyber Crimes Act, 2021, and shall come into operation on the date appointed by the Minister by statutory instrument. Short title and commence-ment

2. In this Act, unless the context otherwise requires— Interpretation

"access" has the meaning assigned to the word in the Electronic Communications and Transactions Act, 2021; Act No. 4 of 2021

"advanced electronic signature" has the meaning assigned to the words in the Electronic Communications and Transactions Act, 2021; Act No. 4 of 2021

"article" means any data computer program, computer data storage medium or computer system which—

(a) is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission of a crime or suspected commission of a crime;

(b) may afford evidence of the commission or suspected commission of a crime; and

(c) is intended to be used or is, on reasonable grounds, believed to be intended to be used in the commission of a crime;

Act No. 15 of 2009

"Authority" has the meaning assigned to the word in the Information and Communications Technologies Act, 2009;

"cache" means the storing of data in a transmission system in order to speed up data transmission or processing";

Act No. 4 of 2021

"caching" has the meaning assigned to the word in the Electronic Communications and Transactions Act, 2021;

Cap. 1

"child" has the meaning assigned to the word in the Constitution;

"child pornography" means pornography in audio, visual, text or other digital format that depicts or represents a child engaged in sexually explicit conduct;

"child solicitation" means persuading, luring, or attempting to persuade or lure a child into sexual activity through the use of a computer system or device, regardless of the outcome;

Act No. 4 of 2021

"computer" has the meaning assigned to the word in the Electronic Communications and Transactions Act, 2021;

"computer data" means a representation of facts, concepts or information in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

"computer data storage medium" means an apparatus or object from which electronic information is capable of being reproduced, with or without the aid of an article or device;

"computer system" means a set of integrated devices that input, output, process, and store data and information including internet;

"controller" means a person, either alone or in common with other persons, who controls and is responsible for critical information infrastructure;

"Council" means the National Cyber Security Advisory and Coordinating Council constituted under section 7;

"critical information" means information that is declared by the Minister to be critical for the purposes of national security or the economic and social wellbeing of the Republic;

"critical information infrastructure" means the cyber infrastructure that is essential to vital services for public safety, economic stability, national security, international stability and for the sustainability and restoration of critical cyberspace;

"cyber" means the—

(a) computer simulated environment; or

(b) state of connection or association with electronic communications systems or networks including the internet;

"cyber crime" means a crime committed in, by or with the assistance of the simulated environment or state of connection or association with electronic communications or networks including the internet;

"cyber ecosystem" means the interconnected information infrastructure of interactions among persons, processes, data, and information and communication technologies, along with the environment and the conditions that influence those interactions;

"cyber inspector" means a person appointed as cyber inspector under section 8;

"cyber security" means tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber environment, organisation and user assets;

"cyber security incident" means an act or activity on or through a computer or computer system, that jeopardises or adversely impacts, without lawful authority, the security, availability or integrity of a computer or computer system, or the availability, confidentiality or integrity of information stored on, processed by, or transiting a computer or computer system;

"damage" means the impairment to the intergrity or availability of data, a program, a system or information;

"device" includes—

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

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

(c) input devices such as keyboards, mouse, trackpad, scanner and digital cameras;

(d) output devices such as printer and screens; and

(e) an apparatus which can be used to intercept a wire, oral or electronic communications;

"denial of service" means rendering a computer system incapable of providing a normal service to its legitimate user;

"digital forensics" means the application of scientific investigatory techniques to cyber crimes by collecting, identifying and validating the digital information for purposes of reconstructing past events;

"digital forensic tool" means hardware or software used for conducting digital forensics;

"Director-General" means a person appointed as Director-General under the Information and Communication, Technologies Act, 2009;

Act No. of 15 2009

"electronic communications" has the meaning assigned to the words in the Electronics Communications and Transactions Act, 2021;

Act No. 4 of 2021

"electronic communications service" means any service which provides the ability to send, receive, process or store electronic communications;

"electronic signature" has the meaning assigned to the words in the Electronic Communications and Transactions Act, 2021;

Act No. 4 of 2021

"explicit sexual conduct" includes sexual intercourse, or other sexual conduct whether between persons or between a person and an animal, masturbation, sexual sadistic or masochistic abuse, or the lascivious exhibition of the genitals or pubic area of any person;

"Genocide" has the meaning assigned to the word in the United Nations Convention on the Prevention and Punishment of the Crime of Genocide;

"hate speech and conduct" means verbal or non verbal communication, action, material whether video, audio, streaming or written, that involves hostility or segregation directed towards an individual or particular social groups on grounds of race, ethnicity, antisemitism, tribalism, sex, age, disability, colour, marital status, pregnancy, health status and economic status, culture, religion, belief, conscience, origin;

"hosting" has the meaning assigned to the word in the Electronic Communications and Transactions Act, 2021;

Act No. 4 of 2021

"hyperlink" means a clickable electronic reference or link of a data message that contains information about another source and when clicked points to and causes to display another data message;

"interception" means an act, by a person who is not a party to a conversation, of wiretapping subscribers or aural or other acquisition of conversation of any wire, electronic or oral communication through the use of an electronic, mechanical or other device;

"internet connection record" shall include—

(a) connections which are made automatically by a person, browser or device;

(b) a customer account reference such as an account number or identifier of the customer's device or internet connection;

(c) the time stamp of the session log;

(d) the source and destination IP addresses and their associated identity information;

(e) the volume of data transferred in either, or both, directions;

(f) the name of the internet service or server connected to;

(g) those elements of a URL which constitutes communications data; or

(h) any other related meta data.

"information infrastructure" means the communication networks and associated software that support interaction among people and organisations;

"Information Technology Auditor" means a person who possesses the expertise to examine and evaluate an information security management system as it relates to information technology infrastructure;

"Judge" means a Judge of the High Court;

"law enforcement officer" means—

(a) a police officer above the rank of subinspector;

(b) an officer of the Anti-Corruption Commission;

(c) an officer of the Drug Enforcement Commission;

(d) an officer of the Zambia Security Intelligence Service; and

(e) any other person appointed as such by the Minister for purposes of this Act;

"malicious software" means a computer program written to allow access to a computer system, whether with or without user intervention for purposes of negatively affecting normal computer system usage or modifying data or transmitting data to another computer system;

"meta data" means data that describes other data;

"multiple electronic mail message" means a mail message including email and instant messaging sent more than once to a recipient;

"penetration testing service" means a service for assessing, testing or evaluating the cyber security of a computer or computer system and the integrity of any information stored in or processed by the computer or computer system, by searching for vulnerabilities in, and compromising, the cyber security defences of the computer or computer system with express permission of the system owner;

"pornography" means audio or visual material that depicts images of a person engaged in explicit sexual conduct;

"premises" includes a computer and data messages;

"racist and xenophobic material" includes any image, video, audio recording or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin;

"service provider" means a public or private entity authorised to—

(a) provide or offer an electronic communication system;

(b) process or store computer data on behalf of a communication service or user of such service; or

(c) own an electronic communication system to provide or offer an electronic communication service;

"traffic data" means digital data that—

(a) relates to a communication by means of a computer system;

(b) is generated by a computer system that is part of the chain of communication; and

(c) shows the communication's origin, destination, route, time, date, size, duration or the type of underlying services;

"Uniform Resource Locator (URL)" means the unique address of the world wide web page; and

"Zambia Computer Incidence Response Team" means the Zambia Computer Incidence Response Team constituted under section 6.

Supremacy of Act Cap.1

3. Subject to the Constitution, where there is an inconsistency between the provisions of this Act and the provisions of any other written law relating to the regulation of cyber security, cyber crimes and digital forensics, the provisions of this Act shall prevail to the extent of the inconsistency.

PART II
Regulation of Cyber Security Services

Cyber security regulator

4. The Authority is responsible for the implementation of this Act.

Functions of Authority

5. (1) The functions of the Authority are to—

(a) co-ordinate and oversee activities relating to cyber security and the combatting of cyber crime;

(b) provide quarterly reports to the Council;

(c) assess the work of the incident response teams within the public and private sectors;

(d) disseminate information on emerging cyber threats and vulnerabilities as presented;

(e) develop and promote an all inclusive secure cyber ecosystem;

(f) create a safe cyber space in critical information infrastructure;

(g) issue guidelines, cyber security codes of practice and standards of performance for implementation by owners of critical information infrastructure;

(h) promote, develop, maintain and improve competencies, expertise and professional standards in the cyber security community;

(i) promote research and development in the use of new and appropriate technologies and techniques in cybercrimes;

(j) promote education and awareness of the need for and importance of cyber security;

(k) establish international cooperation with foreign states and cyber security entities and strengthen partnerships in combatting cyber crime;

(l) undertake information security audits and penetration testing services on all critical information infrastructure.

(m) maintain a register of cyber security service providers;

(n) coordinate with law enforcement agencies to ensure safe cyber space and investigations of cyber incidences; and

(o) issue guidelines relating to digital forensics.

(2) The Authority shall in performing it's functions, collaborate with the Ministry responsible for security, defence, and other relevant agencies on matters relating to cyber security.

Constitution of Zambia Computer Incidence Response Team

6. (1) The Authority shall constitute the Zambia Computer Incidence Response Team which shall—

(a) be the first point of contact with reference to the handling of cyber incidents and communication between local, regional and international cyber security emergency response teams or cyber security incident response teams;

(b) provide incident response and management services in a coordinated manner through established industry standard policies and procedures to manage threats associated with cyber incidents;

(c) provide alerts and warnings on the latest cyber threats and vulnerabilities which may impact the national community;

(d) assess and analyse the impact of incidents such as network security breaches, website hackings, virus and network attacks;

(e) assess and coordinate the work of sectorial cyber incidence response teams within the public and private sector;

(f) participate in information sharing and disseminate information with international cyber security incidence response teams and computer emergency response teams on the emerging threats to critical information infrastructure and internet resources;

(g) participate in and be a member of regional and international computer emergency response team groups; and

(h) perform any other functions conferred on it by the Authority for purposes of this Act.

(2) The Authority shall determine the composition, tenure and procedures of the Zambia Computer Incidence Response Team.

Constitution of National Cyber Security Advisory and Co-ordinating Council

7. (1) The Minister shall constitute the National Cyber Security Advisory Coordinating Council which shall consist of part-time members who are experts in cyber security and cyber crime and in matters related to the Act.

(2) The Council constituted under subsection (1) shall—

(a) coordinate and strengthen collaboration between security wings on matters to do with cyber security;

(b) oversee the implementation of cyber security related functions of the Authority;

(c) monitor and evaluate the performance of the Authority in relation to cyber security;

(d) provide periodic reports to the Minister on cyber security matters;

(e) provide advice to the Minister and the Authority on matters relating to cyber security;

(f) provide guidance in the issuance of cyber security linked advisories affecting the Republic; and

(g) any other functions as the Minister may delegate.

(3) Subject to any specific or general directive of the Minister, the Council may regulate its own procedure.

(4) The members of the Council shall elect a Chairperson and Vice-Chairperson from among themselves.

(5) The Minister may, by statutory instrument, make regulations to provide for the composition and tenure of the Council.

(6) There shall be paid to the members of the Council allowances that the Emoluments Commission may, on the recommendation of the Minister, determine.

PART III

INSPECTORATE

Appointment of cyber inspector

8. (1) The Authority may appoint a suitably qualified person as a cyber inspector for the purposes of ensuring compliance with this Act.

(2) The Authority shall, issue a certificate of appointment to a person appointed as a cyber inspector.

(3) The certificate of appointment referred to in subsection (2), shall be in a prescribed form and shall be *prima facie* evidence of the cyber inspector's appointment.

(4) A cyber inspector shall in performing any function under this part—

(a) be in possession of a certificate of appointment referred to in subsection (2); and

(b) show the certificate of appointment to a person who requests to see the certificate.

(5) A person commits an offence if that person falsely holds oneself out as a cyber inspector.

(6) A person convicted of an offence under subsection (5) is liable, on conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a term not exceeding two years, or to both.

Power to inspect and monitor

9. A cyber inspector may in the performance of the inspector's functions, with a warrant—

(a) monitor and inspect a computer system or activity on an information system, where such activity or information is not in public domain or is not accessible to the public;

(b) enter and inspect the premises of a cyber security service provider if there is reasonable ground to believe that the licensee has contravened the provisions of this Act; and

(c) audit critical information infrastructure.

Data retention notice

10. (1) Where a data retention notice is issued requiring an electronic communications service provider to retain internet connection records the specific data that the electronic communications service provider may be required to retain shall be specified in the retention notice.

(2) An electronic communication service provider shall not be required to retain data as part of an internet connection record.

Power to access, search and seize

11. (1) A cyber inspector may, in the performance of the cyber inspector's functions, with a warrant, at any reasonable time and without prior notice, enter any premises or access an information system and—

(a) search the premises or that information system;

(b) search any person on the premises if there are reasonable grounds to believe that the person has possession of an article, document or record that has a bearing on an investigation;

(c) take extracts from, or make copies of any book, document or record that is on or in the premises or in the information system and that has a bearing on an investigation;

(d) demand the production of, and inspect, relevant licences and registration certificates;

(e) inspect any facilities on the premises which are linked or associated with the information system;

(f) access and inspect the operation of any computer or equipment forming part of an information system and any associated apparatus or material which the cyber inspector has reasonable cause to believe is, or has been used in, connection with any offence;

(g) use or cause to be used any information system or part thereof to search any data contained in or available to such information system;

(h) require the person by whom, or on whose behalf, the cyber inspector has reasonable cause to suspect the computer or information system is or has been used, or require any person in control of, or otherwise involved with the operation of the computer or information system, to provide the cyber inspector with such reasonable technical and other assistance as the cyber inspector may require for the purposes of this Part; or

(i) make such inquiries as may be necessary to ascertain whether the provisions of this Act or any other law on which an investigation is based, have been complied with.

(2) A person shall be searched with decency by a designated person of the same sex.

Obstruction of cyber inspector

12. (1) A person commits an offence if that person obstructs a cyber inspector from conducting a lawful search or seizure under this Act.

(2) A person convicted of an offence under subsection (1) is liable, on conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a period not exceeding two years, or to both.

Appointment of cyber security technical expert

13. (1) The Director-General may, appoint in a prescribed manner and form, any person as a cyber security technical expert for a specified period to assist a cyber inspector in the cyber inspector's exercise of any powers under this Act.

(2) The Director-General shall issue an identification card, which shall be carried at all times by the cyber security technical expert when performing the functions of a cyber security technical expert under in this Act.

Emergency cyber security measures and requirements

14. (1) The Minister may, in consultation with other relevant agencies, issue regulations authorising or directing a person or organisation specified in the regulations to take such measures or comply with such requirements, where the Minister considers it necessary for the purposes of preventing, detecting or countering a threat to—

(a) the essential services;

(b) national security and defence;

(c) foreign relations;

(d) economy;

(e) public health and public safety;

(f) public order of the Republic; or

(g) an electronic communication system, computer system and information system.

(2) A person who fails to take any measure or comply with any requirement directed by the Minister under subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand penalty units or to imprisonment for a term not exceeding three months or to both.

PART IV

Investigation of Cyber Security Incidents

Power to investigate

15. (1) Where the Authority receives information regarding an alleged cyber security threat or an alleged cyber security incident a cyber inspector appointed under section 8 may, having regard to the impact or potential impact of the alleged cyber security threat or alleged cyber security incident—

(a) require, by written notice, a person to attend at such reasonable time and place as may be specified in the notice to answer any question or to provide a signed statement in writing concerning the alleged cyber security incident or alleged cyber security threat;

(b) require, by written notice, a person to produce a physical or electronic record, document or copy thereof in the possession of that person;

(c) require, by written notice, a person to provide the cyber inspector with information, which the cyber inspector considers to be relevant to the investigation;

(d) copy or take extracts from any physical or electronic record or document; or

(e) examine orally a person who appears to be acquainted with the facts and circumstances relating to the alleged cyber security incident or cyber security threat and to reduce to writing a statement made by the person so examined.

(2) The cyber inspector may specify in the notice mentioned in subsection (1)*(b)*—

(a) the time and place at which any record or document is to be produced or any information is to be provided; and

(b) the manner and form in which it is or be produced or provided.

(3) A person examined under this section who, in good faith, discloses any information to a cyber inspector shall not be treated as being in breach of any restriction on the disclosure of information imposed by law, contract or rules of professional conduct.

(4) A person commits an offence if that person—

(a) willfully gives false information or without lawful excuse refuses to give any information or produce any record, document or copy thereof required of that person by a cyber inspector under subsection (1); or

(b) refuses to cooperate with or hinders a cyber inspector from conducting a lawful search or seizure.

(5) A person convicted of an offence under subsection (4) is liable to a fine not exceeding two hundred thousand penalty units or to imprisonment for a term not exceeding two years or to both.

PART V

PROTECTION OF CRITICAL INFORMATION AND CRITRICAL INFORMATION INFRASCTRUCTURE

Scope of protecting critical information infrastructure

16. The provisions of this Part apply to a critical information infrastructure or parts thereof and to the controllers of critical information infrastructure.

Declaration of critical information

17. (1) The Minister may by statutory instrument declare information which is of importance to the protection of national security, economic or social well being of the Republic, to be critical information for the purposes of this part.

(2) Infrastructure containing critical information shall be declared critical information infrastructure.

Localisation of critical information

18. (1) A controller of critical information shall store all critical information on a server or data center located within the Republic.

(2) Despite subsection (1), the Minister may authorise a controller of critical information to externalise the critical information outside the Republic as prescribed.

(3) In an event where the purpose for which critical information collected expires or the data controller ceases to exist, such critical information shall be surrendered to the Authority.

Registration of critical information infrastructure

19. (1) The Minister may by statutory instrument prescribe—

(a) the requirements for the registration of critical information infrastructure with the Authority;

(b) the procedure to be followed for the registration of critical information infrastructure; and

(c) any other matter relating to the registration of critical information infrastructure.

Change in ownership of critical information infrastructure

20. (1) A person who owns a critical information infrastructure and intends to change ownership of the critical information infrastructure shall apply to the Authority in the prescribed manner and form on payment of the prescribed fee.

(2) A person who contravenes subsection (1), commits an offence.

Register of critical information infrastructure

21. The Authority shall maintain a register of critical information infrastructure which shall contain such information as may be prescribed.

Auditing of critical information infrastructure to ensure compliance

22. (1) A controller of a critical information infrastructure shall, annually appoint an information technology auditor to audit the critical information infrastructure as prescribed.

(2) Despite subsection (1), the Authority may at anytime require a controller of a critical information infrastructure to perform an audit.

(3) A controller of a critical information infrastructure who contravenes subsection (2) commits an offence and is liable on conviction to a fine not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding one year or to both.

Duty to report cyber security incident in respect of critical information infrastructure

23. (1) A controller of a critical information infrastructure shall report to the Authority on or after the occurrence of any of the following events:

(a) a cyber security incident in respect of the critical information infrastructure;

(b) a cyber security incident in respect of any computer or computer system under the controller's control that is interconnected with or communicates with the critical information infrastructure; and

(c) any other type of cyber security incident in respect of the critical information infrastructure that the Authority may specify by written direction.

(2) A report under subsection (1) shall be in the prescribed manner and form.

(3) The controller of critical information infrastructure shall submit a monthly cyber security incident and threat report to the Authority.

(4) A controller of a critical information infrastructure shall establish mechanisms and processes, in accordance with information security standards published in the *Gazette*, as may be necessary for the detection of a cyber security threat in respect of its critical information infrastructure.

(5) A controller of a critical information infrastructure who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding five years or to both.

National cyber security exercises

24. (1) The Authority shall conduct cyber security exercises for the purposes of testing the state of readiness of owners of different critical information infrastructure in responding to significant cyber security incidents at the national level.

(2) A controller of a critical information infrastructure shall participate in a national cyber security exercise as directed in writing by the Authority.

(3) A person who fails to comply with a written direction issued under subsection (2) commits an offence and is liable on conviction—

(a) to a fine not exceeding one hundred thousand penalty units or to imprisonment for a term not exceeding one year or to both; and

(b) in the case of a continuing offence, a further fine not exceeding one hundred thousand penalty units for every day and part thereof during which the offence continues.

Non-compliance with Part V

25. (1) The Authority shall, where an audit reveals that a controller of a critical information infrastructure has contravened a provision of this Part, notify the said controller in writing, stating the—

(a) finding of the audit report;

(b) action required to remedy the noncompliance; and

(c) period within which the controller shall take the remedial action.

(2) A controller that fails to take any remedial action within the period stipulated under subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding five years, or to both.

PART VI

INTERCEPTION OF COMMUNICATIONS

Prohibition of interception of communication

26. (1) A person commits an offence, if that person—

(a) intercepts, attempts to intercept or procures another person to intercept or attempt to intercept any communication; or

(b) use, attempt to use or procure another person to use or attempt to use any electronic, software, mechanical or other device to intercept any communication.

(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding one million penalty units or to imprisonment for a term not exceeding ten years or to both.

Central Monitoring and Co-ordination Centre

27. (1) There is established the Central Monitoring and Co-ordination Centre.

(2) The Central Monitoring and Co-ordination Centre is the sole facility through which authorised interceptions in terms of this Act shall be effected and all the intercepted communication and call related information of any particular interception target forwarded.

(3) The Central Monitoring and Co-ordination Centre shall be managed, controlled and operated by the department responsible for Government communications in liaison with the Authority.

Lawful interception

28. (1) Subject to subsection (2), a law enforcement officer may, where the law enforcement officer has reasonable grounds to believe that an offence has been committed, is likely to be committed or is being committed and for the purpose of obtaining evidence of the commission of an offence under this Act, apply, *ex-parte*, to a Judge, for an interception of communications order.

(2) A law enforcement officer shall, apply for a written consent of the Attorney-General in a prescribed manner and form, before making an application under subsection (1).

(3) A Judge to whom an application is made under subsection (1) may make an order—

(a) requiring a service provider to intercept and retain a specified communication or communications of a specified description received or transmitted, or about to be received or transmitted by that service provider;

(b) authorising the law enforcement officer to enter specified premises with a warrant and to install on such premises any device for the interception and retention of a specified communication or communications of a specified description and to remove and retain such device;

(c) requiring any person to furnish the law enforcement officer with such information, facilities and assistance as the Judge considers necessary for the purpose of the installation of the interception device; or

(d) imposing the terms and conditions for the protection of the interests of the persons specified in the order or any third parties or to facilitate any investigation.

(4) A Judge may grant an order under subsection (3) where the Judge is satisfied that—

(a) the written consent of the Attorney General has been obtained as required by subsection (2); and

(b) there are reasonable grounds to believe that material information relating to the—

(i) commission of an offence under this Act or any other law; or

(ii) whereabouts of the person suspected by the law enforcement officer to have committed the offence; is contained in that communication or communications of that description.

(5) Any information contained in a communication—

(a) intercepted and retained pursuant to an order under subsection (3); or

(b) intercepted and retained in a foreign State in accordance with the law of that foreign State and certified by a Judge of that foreign State to have been so intercepted and retained, shall be admissible in proceedings for an offence under this Act, as evidence of the truth of its contents despite the fact that it contains hearsay.

(6) An interception of communications order referred to in this section shall be valid for a period of three months and may, on application by a law enforcement officer, be renewed for such period as the Judge may determine.

(7) An action does not lie in any court against a service provider, any officer, employee or agent of the service provider or other specified person, for providing information, facilities or assistance in accordance with the terms of a court order under this Act or any other law.

Interception of communication to prevent bodily harm, loss of life or damage to property

29. (1) A law enforcement officer may, intercept any communication and orally request a service provider to route duplicate signals of indirect communications specified in that request to the Central Monitoring and Coordination Centre where the law enforcement officer has reasonable grounds to believe that—

(a) a person who is a part of any communication—

(i) has caused, or may cause, the infliction of bodily harm to another person;

(ii) threatens, or has threatened, to cause the infliction of bodily harm to another person;

(iii) threatens, or has threatened, to kill oneself or another person, or to perform an act which would or may endanger that party's own life or that of another person, would or may cause the infliction of bodily harm to that party or another person;

(iv) has caused or may cause damage to property; or

(v) has caused or may cause financial loss to banks, financial institutions, account holders or beneficiaries of funds being remitted or received by such account holders or beneficiaries;

(b) it is not reasonable or practical to make an application under section 28 for an interception of communication order because the delay to intercept a specified communication would result in the actual infliction of bodily harm, the death of another person or damage to property; or

(c) the sole purpose of the interception is to prevent bodily harm to, or loss of life of, any person or damage to property.

(2) An electronic communication service provider shall, on receipt of a request made under subsection (1) by a law enforcement officer, route the duplicate signals of the indirect communication to the Central Monitoring and Coordination Centre.

(3) A law enforcement officer who makes a request to a service provider under subsection (1) shall, immediately after making that request, furnish the service provider with a written confirmation of the request setting out the information given by that law enforcement officer to that service provider in connection with the request.

(4) A law enforcement officer who intercepts any communication under this section, shall immediately after the interception of the communication, submit to a Judge—

(a) a copy of the written confirmation referred to in subsection (3);

(b) an affidavit setting out the results and information obtained from that interception; and

(c) a recording of the communication that has been obtained by means of that interception, a full or partial transcript of the recording of the communication and any notes made by the law enforcement officer.

(5) An electronic communications service provider who, in accordance with subsection (2), routes duplicate signals of indirect communications to the Central Monitoring and Coordination Centre shall, as soon as practicable thereafter, submit an affidavit to a Judge setting out the steps taken by that service provider in giving effect to the request and the results obtained from such steps.

(6) A Judge shall cause to be kept all written confirmations and affidavits, recording, transcripts or notes submitted under this section for a period of at least five years.

(7) Where a Judge, on receipt of a written confirmation and affidavit under this section, determines that the interception was effected or used for purposes contrary to, or in contravention of the provisions of this Act or any other law, the Judge may make an order as the Judge considers appropriate in relation to the service provider, or the person whose communication has been intercepted or law enforcement officer.

Interception of communication for purposes of determining location

30. (1) Where a person is a party to a communication and that person, as a result of information received from another party to the communication, in this section referred to as the "sender", has reasonable grounds to believe that an emergency exists by reason of the fact that—

(a) theft of finances from a bank or a financial institution is likely to occur;

(b) the life of another person, whether or not the sender, is being endangered;

(c) a person is dying, or is being or has been injured;

(d) a person's life is likely to be endangered;

(e) a person is likely to die or to be injured; or

(f) property is likely to be damaged, is being damaged or has been damaged.

(2) The location of the sender is unknown to the person, that person may, if that person is—

(a) a law enforcement officer, and has reasonable grounds to believe that determining the location of the sender is likely to be of assistance in dealing with the emergency, orally request, or cause another law enforcement officer to orally request, an electronic communications service provider to—

(i) intercept any communication to or from the sender, for purposes of determining the sender's location; or

(ii) determine the location of the sender; or

(b) not a law enforcement officer, inform or cause another person to inform, any law enforcement officer of the matter referred to in subsection (1)*(a), (b), (c), (d)* and *(e)*.

(3) A law enforcement officer who receives information under subsection (1) may, orally request, or cause another law enforcement officer to orally request, an electronic communication service provider to determine the location of the sender, where the law enforcement officer has reasonable grounds to believe that determining the location of the sender is likely to be of assistance in dealing with an emergency.

(4) An electronic communication service provider shall, on receipt of a request made under subsections (1) or (2)—

(a) intercept any communication to, or from, the sender for purposes of determining the sender's location; or

(b) use its best efforts to determine the location of the sender in any other manner which the service provider considers appropriate.

(5) Where the location of the sender has been determined, the electronic communication service provider shall, immediately after determining that location, provide the law enforcement officer who made the request with the location of the sender and any other information obtained which is likely to assist in the investigation.

(6) A law enforcement officer who makes a request to an electronic communication service provider under subsections (1) or (2) shall—

(a) immediately after making that request, furnish—

(i) the electronic communication service provider with a written confirmation and affidavit of the request setting out the information given by that law enforcement officer to that electronic communications service provider in connection with the request; and

(ii) a judge with a copy of the written confirmation; and

(b) where the location of the sender and any other information has been provided to the law enforcement officer under subsection (3), immediately after receipt thereof, submit to a judge an affidavit setting out the results and information obtained from that interception.

(7) An electronic communication service provider who has taken any of the steps referred to in subsection (3), shall, immediately submit to a judge—

(a) an affidavit setting out the steps taken by the electronic communication service provider in giving effect to the request of a law enforcement officer and the results and information obtained from such steps; and

(b) where the steps included the interception of an indirect communication, any recording of that indirect communication obtained by means of the interception, a full or partial transcript of the recording and any notes made by that service provider of the indirect communication.

(8) A judge shall keep written confirmation and affidavit and any recordings, transcripts or notes submitted under subsections (6) and (7) or cause it to be kept, for a period of at least five years.

(9) Where a judge, on receipt of any written confirmation and affidavits under this section, determines that the interception was effected or used for purposes contrary to, or in contravention of the provisions of this Act or any other written law, the Judge may make an order that the judge considers appropriate in relation to the electronic communications service provider, the person whose communication has been intercepted or the law enforcement officer.

Prohibition of disclosure of intercepted communi-cation

31. (1) Subject to section 32, a law enforcement officer who intercepts any communication pursuant to an interception of communication order shall not disclose the communication or use the communication in any manner other than in accordance with the provisions of this Act.

(2) A person commits an offence if that person without authorisation—

(a) accesses, discloses or attempts to disclose to another person, the contents of any intercepted communication; or

(b) uses or attempts to use, the contents of any intercepted communication.

(3) A person who contravenes subsection (2), commits an offence and is liable, on conviction, to a fine not exceeding one million penalty units or to imprisonment not exceeding ten years, or to both.

Disclosure of intercepted communication by law enforcement officer

32. (1) A law enforcement officer who intercepts a communication pursuant to an interception of communication order may disclose the information to another law enforcement officer where the disclosure is necessary for the determination of the commission of an offence or the whereabouts of a person suspected to have committed an offence.

(2) Where a law enforcement officer, in the performance of any functions under this Act, intercepts a communication relating to the commission of an offence under any other law, the law enforcement officer shall disclose or use the communication in accordance with the provisions of this Act or that other law.

Privileged communication to retain privileged character

33. A privileged communication, oral or electronic communication intercepted in accordance with the provisions of this Act does not lose its privileged character.

Prohibition of random monitoring

34. (1) An electronic communication service provider shall not utilise the service for observing or random monitoring except for mechanical or service quality control checks.

(2) An electronic communications service provider who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units, or to imprisonment for a period not exceeding five years, or to both.

(3) In this section "monitoring" includes listening to or recording communication by means of a monitoring device; and

"monitoring device" means any electronic, software, mechanical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to listen to or record any communication.

Protection of user from fraudulent or other unlawful use of service

35. (1) An electronic communication service provider shall record that a wire or electronic communication was initiated or completed in order to protect the service provider, another service provider giving a service for the completion of a wire or electronic communication or a user of the service, from fraudulent, unlawful or abusive use of the service.

(2) An electronic communication service provider who records an electronic communication under subsection (1) shall immediately inform a law enforcement officer.

(3) An electronic communication service provider may disclose the contents of a communication referred to under subsection (1)—

(a) with the consent of the originator, to the addressee or intended recipient of the communication;

(b) to a person employed or authorised, or whose facilities are used, to forward the communication to its destination; or

(c) to a law enforcement officer, where the information relates to the commission of an offence.

(4) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

Interception of satelite transmission

36. (1) An interception of satellite transmission that is not encrypted or scrambled and that is transmitted to a broadcasting station for purposes of transmission to the public or as an audio subcarrier intended for redistribution to facilities open to the public is not an offence under this section unless the interception is for the purpose of a direct or indirect commercial advantage or private financial gain.

(2) Subsection (1) does not apply to any data transmission or a telephone call.

Prohibition of use of interception device

37. (1) Subject to subsection (3), a person shall not use an interception device or system software or hardware or other instrument, equipment or apparatus whether electronic or mechanical.

(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding three million penalty units or to imprisonment for a term not exceeding twenty-five years, or to both.

(3) Subsection (1) does not apply to the use of an interception device by an electronic communication service provider or law enforcement officer as the case may be—

(a) for the operation, maintenance and testing of a communication service;

(b) to protect the rights or property of the electronic communication service provider or the users of the service from abuse of service or any other unlawful use of the service;

(c) to record that the communication was initiated or completed in order to protect the electronic communications service provider or another electronic communication service provider in the completion of the communication, or a user of the service from fraudulent, unlawful or abusive use of the service; or

(d) where the consent of the user of the service has been obtained.

Assistance by service provider

38. (1) An electronic communication service provider shall ensure that the electronic communication service provider—

(a) uses an electronic communication system that is technically capable of supporting lawful interceptions in accordance with this Act;

(b) installs hardware and software facilities and devices to enable the interception of communications when so required by a law enforcement officer or under a court order;

(c) provides services that are capable of rendering real time and fulltime monitoring facilities for the interception of communications;

(d) provides all call-related information in realtime or as soon as possible upon call termination;

(e) provides one or more interfaces from which any intercepted communication shall be transmitted to the Central Monitoring and Coordination Centre;

(f) transmits intercepted communication to the Central Monitoring and Coordination Centre through fixed or switched connections, as the case may be; and

(g) provides access to all intercepted subjects operating temporarily or permanently within the service provider's communications systems, and where the interception subject is using features to divert calls to other service providers or terminal equipment, access to such other providers or equipment.

(2) An electronic communication service provider who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

Duties of service provider in relation to customers

39. (1) An electronic communication service provider shall, before entering into a contract with a person for the provision of any service, obtain—

(a) the person's full name, residential address and identity number contained in the person's identity document;

(b) in the case of a corporate body, its business name and address and the manner in which it is incorporated or registered; and

(c) any other information which the electronic communication service provider considers necessary for the purpose of enabling it to comply with the requirements of this Act.

(2) An electronic communication service provider shall ensure that proper records are kept of the information referred to in subsection (1) and any change in that information.

Interception capability of service provider

40. (1) Despite any other written law, an electronic communication service provider shall—

(a) provide a service which has the capability to be intercepted; and

(b) store call-related information in accordance with the provisions of this Act.

(2) The Minister may, in consultation with the Authority, by statutory instrument, make regulations to provide for the—

(a) manner in which effect is to be given to subsection (1)*(a)* by every service provider;

(b) security, technical and functional features of the facilities and devices to be acquired by every service provider to enable the—

(i) interception of communication under this Act; and

(ii) storing of call-related information; and

(c) period within which the requirements shall be complied with.

(3) The Regulations made under subsection (2) shall specify—

(a) the capacity and technical features of the devices or systems to be used for interception purposes;

(b) the connectivity of the devices or systems to be used for interception purposes with the Central Monitoring and Coordination Centre;

(c) the manner of routing intercepted information to the Central Monitoring and Coordination Centre; and

(d) any other matter which is necessary to give effect to the provisions of this Part.

(4) An electronic communication service provider shall, at the provider's own expense, acquire the facilities and devices specified in the regulations made under subsection (2).

(5) Subject to this Act a cost incurred by a service provider for the purpose of—

(a) enabling—

(i) any electronic communication to be intercepted; and

(ii) call-related information to be stored; and

(b) complying with this Part; shall be borne by the electronic communications service provider.

PART VII

LICENSING OF CYBER SECURITY SERVICE PROVIDERS

Prohibition from providing cyber security services without licence

41. (1) A person shall not, without a licence—

(a) engage in the business of providing, for reward or otherwise, cyber security service to other persons; or

(b) advertise, or in any way hold out, that the person is in the business of providing a licensable cyber security service, provides for reward or otherwise, or is willing to provide for reward or otherwise, the licensable cyber security service, except under and in accordance with a cyber security service provider's license granted under this Act.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand penalty units or to imprisonment for a term not exceeding one year or to both.

(3) This section does not apply to a person employed under a contract of service by another person to carry out a cyber security service for a computer or computer system belonging to that other person.

Application for licence

42. (1) A person who intends to engage in a cyber security service shall apply to the Authority in a prescribed form and manner on payment of a prescribed fee.

(2) The Authority shall within thirty days of receipt of an application, grant or reject the application on terms and conditions the Authority may determine.

(3) Where the Authority fails to make a decision within the period referred to under subsection (2), except as otherwise provided, the application shall be deemed to have been granted.

(4) The Authority shall, where it rejects an application for a licence, inform the applicant and give the reasons for the rejection.

(5) The Authority may request for further particulars or information in respect of an application under this section in a prescribed manner and form.

(6) Where the Authority requests for further particulars, the Period under subsection (2), shall stop running

Renewal of licence

43. (1) A person may apply for the renewal of a licence to the Authority in a prescribed manner and form on payment of a prescribed fee.

(2) The Authority may on receipt of an application under subsection (1), within thirty days—

(a) renew the licence applied for, with or without conditions; or

(b) reject the application.

Refusal to grant or renew licence

44. (1) The Authority may refuse to grant or to renew a licence where the Authority determines that—

(a) in the case of an individual, that individual is not a fit or proper person to hold or to continue to hold the licence;

(b) in the case of a business entity, an officer of the business entity is not a fit or proper person;

(c) it is not in the public interest to grant or renew the licence, or the grant or renewal of the licence may pose a threat to national security; or

(d) the applicant has not met the prescribed criteria.

(2) A person commits an offence if that person, in making an application for a licence—

(a) makes any statement or furnishes any particulars, information or document which the person knows to be false or does not believe to be true; or

(b) intentionally suppresses any material fact, or furnishes any information which is misleading in a material particular.

(3) A person convicted of an offence under subsection (3) is liable to a fine not exceeding one hundred thousand penalty units or to imprisonment for a term not exceeding one year or to both.

(4) The Authority may consider any of the following matters as applicable in deciding for the purposes of this section whether a person or an officer of a business entity or the business entity is a fit and proper person:

(a) that the person or officer associates with a person in a way that indicates involvement in an unlawful activity;

(b) that in dealings in which the person or officer has been involved, the person or officer has shown dishonesty or lack of integrity;

(c) that the person or officer is or was suffering from a mental disorder;

(d) that the person or officer is an undischarged bankrupt or has entered into a composition with the creditor of the person or officer;

(e) that the person or officer has had a license revoked by the Authority previously;

(f) any other criteria prescribed by the Authority.

(5) Subsection (4) does not limit the circumstances in which a person or an officer of a business entity may be considered by the Authority not to be a fit and proper person.

Validity of licence

45. A licence is valid for the period prescribed by statutory instrument.

Revocation or suspension of licence

46. (1) Subject to subsection (3), the Authority may by order revoke any license if the Authority is satisfied that—

(a) the licensee has failed to comply with any condition imposed by the Authority on the license;

(b) the license had been obtained by fraud or misrepresentation;

(c) a circumstance which the Authority becomes aware of would have required or permitted the Authority to refuse to grant or renew the licensee's license, had the Authority been aware of the circumstance immediately before the license was granted or renewed;

(d) the licensee has ceased to carry on in the Republic the business or activity for which the licensee is licensed;

(e) the licensee has been declared bankrupt or has gone into compulsory or voluntary liquidation other than for the purpose of amalgamation or reconstruction;

(f) the licensee has been convicted of an offence under this Act, or an offence involving dishonesty;

(g) where the licensee is an individual the licensee is no longer a fit and proper person to continue to hold the license;

(h) where the licensee is a business entity an officer of the business entity or the business is no longer a fit and proper person; or

(i) it is in the public interest to do so.

(2) Subject to subsection (3), the Authority may, in any case in which the Authority considers that no cause of sufficient gravity for revoking any license exists, by order—

(a) suspend the license for a period not exceeding six months;

(b) censure the licensee concerned; or

(c) impose such other directions or restrictions as the Authority considers appropriate.

(3) The Authority shall not exercise its powers under subsections (1) or (2) except where an opportunity to be heard whether in person or by a representative and whether in writing or otherwise, had been given to the licensee against whom the Authority intends to exercise the licensing officer's powers, being a period of not more than fourteen days after the Authority informs the licensee of such intention.

(4) Where the Authority has by order revoked a licence under subsection (1) or made any order under subsection (2) in respect of a licensee, the Authority shall serve on the licensee concerned a notice of the order made under those subsections.

(5) Despite subsection (3), where a licensee has been charged with or convicted of a prescribed offence, being an offence which would make it undesirable in the public interest for the licensee to continue to carry out the functions of a licensee—

(a) the Authority may serve on the licensee a notice of immediate suspension of the licence; and

(b) the licensee shall, upon a notice being served under paragraph *(a)* but subject to subsection (7), immediately cease to carry out any function of a licensee to which the licence refers.

(6) A licensee whose licence has been suspended under subsection (5) may, within fourteen days after the Authority has served the notice of suspension, apply to the Authority for review of the Authority's decision.

(7) The Authority may, on review of its decision, by order—

(a) revoke the licence in question;

(b) suspend that licence for a period not exceeding six months starting from the date of immediate suspension of that licence; or

(c) rescind the immediate suspension of that licence.

(8) Where the Authority has by order revoked or suspended a licence under subsection (7), the Authority shall serve on the licensee concerned a copy of the order.

(9) An order under this section shall not take effect until the expiration of fourteen days after the order has been served on the licensee.

PART VIII

INTERNATIONAL COOPERATION IN MAINTAINING CYBER SECURITY

Identifying areas of cooperation

47. The Authority shall identify and ensure that it cooperates with private, international organisations and other government entities involved in cyber security matters at international level.

Entering into agreement

48. The Republic may enter into any agreement with any foreign State and international body regarding—

(a) the provision of mutual assistance and cooperation relating to the investigation and prosecution of—

(i) an offence committed under this Act;

(ii) any other offence in terms of the laws of the Republic which is or was committed by means or facilitated by the use of an article; or

(iii) any other offence substantially similar to an offence recognised in the Republic which is or was committed by means of, or facilitated by the use of an article, in that foreign State.

PART IX
CYBER CRIME

Unauthorised access to, interception of or interference with computer system and data

49. (1) A person who intentionally accesses or intercepts any data without authority or permission to do so or who exceeds the authorised access, commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment not exceeding five years, or to both.

(2) A person who intentionally and without authority to do so, interferes with or deviates data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, commits an offence and is liable, on conviction to a fine not exceeding five hundred thousand penalty units or, to imprisonment for a period not exceeding five years, or to both.

(3) Where an offence under this section is committed in relation to data that is in a critical information infrastructure or that is concerned with national security or the provision of an essential service, the penalty is a fine not exceeding two million five hundred thousand penalty units or to imprisonment not exceeding twenty five years, or to both.

(4) A person commits an offence if that person—

(a) without authority to do so, communicates, discloses or transmits any data, information, program, access code or command to any person not entitled or authorised to access the data, information, program, code or command;

(b) without authority to do so, introduces or spreads a software code that damages a computer, computer system or network;

(c) accesses or destroys any files, information, computer system or device without authorisation, or for purposes of concealing information necessary for an investigation into the commission, or otherwise, of an offence; or

(d) damages, deletes, alters or suppresses any communication or data without authorisation.

(5) A person who commits an offence under subsection (4) is liable, on conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a period not exceeding two years, or to both.

Act No. 4 of 2010

(6) Subject to the Public Interest Disclosure (Protection of Whistleblowers) Act, 2010 or any other relevant law, a person who knowingly possesses unauthorised data, commits an offence and is liable, on conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a term not exceeding two years, or to both.

Illegal devices and software

50. (1) A person commits an offence if that person—

(a) unlawfully produces, sells, procures for use, imports, exports, distributes or otherwise makes available—

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

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

(iii) introduces or spreads a software code that damages a computer or computer system with the intent that it be used by any person for the purpose of committing an offence defined by other provisions under this Part; or

(b) knowingly has an item mentioned in subparagraph *(a)*(i) or (ii) in that person's possession with the intent that it be used by any person for the purpose of committing any offence under this Part.

(2) A person convicted of an offence under subsection (1), is liable to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

(3) This provision shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in subsection (1)*(a)* is not for the purpose of committing an offence established in accordance with other provisions of this Part, such as for the authorised testing or protection of a computer system.

Computer related misrepresentation

51. (1) A person who knowingly, without lawful excuse, inputs, alters, deletes, or suppresses computer data, resulting in unauthentic data with the intent that it be considered or acted on as if it were authentic, regardless whether or not the data is directly readable and intelligible commits an offence and is liable, on conviction, to a fine not exceeding seven hundred thousand penalty units or to imprisonment for a period not exceeding seven years or to both.

(2) Where the offence in subsection (1) is committed by sending out multiple electronic mail messages from or through computer systems, the penalty is one million five hundred thousand penalty units or imprisonment for a period not exceeding fifteen years, or to both.

Cyber extortion

52. (1) A person commits an offence if that person, through a computer system with intent to extort or gain anything from any person—

(a) accuses or threatens to accuse any person of committing a crime or offering or making any solicitation or threat to any person as an inducement to commit or permit the commission of a crime;

(b) threatens that any person shall be accused by any other person of commission of an offence;

(c) knowing the contents of the writing, causes any person to receive any writing containing such accusation or threat;

(d) knowingly transmits any communication containing any threat to cause damage to a computer system with the intent to extort from any person any money or other thing of value;

(e) obtains any advantage from another person; or

(f) compels another person to perform or to abstain from performing any act.

(2) A person convicted of an offence under subsection (1), is liable to a fine not exceeding seven hundred thousand penalty units or imprisonment for a period not exceeding seven years, or to both.

Identity related crimes

53. A person who, knowingly without lawful excuse by using a computer system transfers, possesses, or uses, a means of identification of another person, commits an offence and is liable, on conviction, to a fine not exceeding one million penalty units or to imprisonment for a term not exceeding ten years, or to both.

Publication of information

54. A person who, with intent to compromise the safety and security of any other person, publishes information or data presented in a picture, image, text, symbol, voice or any other form in a computer system commits an offence and is liable, on conviction, to a fine of not less than five hundred thousand penalty units or to imprisonment for a term exceeding five years or to both.

Aiding, abetting, counselling etc.,

55. (1) A person who aids, abets, counsels, procures, incites or solicits another person to commit or conspires to commit any offence under this Act, commits an offence and is liable, on conviction, to the penalty specified for that offence.

(2) A person who attempts to commit any of the offences under this Act, commits an offence and is liable, on conviction, to the penalty specified for that offence.

Prohibition of pornography

56. (1) A person shall not produce or participate in the production of pornography using a computer system.

(2) A person convicted of an offence under subsection (1) is liable, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or both.

(3) A person who knowingly—

(a) produces pornography for the purpose of its distribution for profit through a computer system commits an offence and is liable on conviction to a fine not exceeding one million penalty units or to imprisonment for a period not exceeding ten years, or to both; or

(b) offers, circulates or makes available, pornography through a computer system commits an offence and is liable on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

Child pornography

57. (1) A person commits an offence if that person knowingly—

(a) produces child pornography for the purpose of its distribution through a computer system;

(b) sells or makes available any pornography to a child through a computer system;

(c) compels, invites or allows a child to view pornography through a computer system intended to corrupt a child's morals;

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

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

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

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

(h) obtains access, through information and communication technologies, to child pornography.

(2) A person convicted of an offence under subsection (1) is liable to imprisonment for a period not less than fifteen years.

(3) Subsections (1)*(d)* to *(h)* do not apply to a person performing a *bona fide* law enforcement function.

Child solicitation

58. (1) A person commits an offence if that person—

(a) uses computer system to meet a child for the purpose of committing a sexual related crime;

(b) communicates with a child through a computer system for the purpose of making it easier to procure the child to engage in sexual activity with that person;

(c) attracts a child for the purpose of making it easier to procure the child to engage in sexual activity with that person;

(d) attracts a child for the purpose of making it easier to procure the child to engage in sexual activity with another person; or

(e) recruits a child to participate in pornographic performances that is intended to be produced or recorded with or without the intent to distribute such material through a computer system or computer network;

(2) A person convicted of an offence under subsection (1) is liable to imprisonment for a period not exceeding fifteen years.

Obscene matters or things

59. (1) A person commits an offence under subsection (1) is liable to imprisonment for a period not exceeding fifteen years—

(a) makes, produces or has in the persons possession any one or more obscene, drawings, paintings, pictures, images, posters, emblems, photographs, videos or any other object tending to corrupt morals; or

(b) imports, conveys or exports, or causes to be imported conveyed or exported, any such matters or things, or in any manner whatsoever puts any of them in circulation; or

(c) carries on or takes part in any business, whether public or private, concerned with any such matters or things, or deals in any such matters or things in any manner whatsoever, or distributes any of them, or exhibits any of them publicly, or makes a business of lending any of them;

(d) advertises or makes known by any means whatsoever with a view to assisting the circulation of, or traffic in, any such matters or things, that a person is engaged in any of the acts referred to in this section, or advertises or makes known how, or from whom, any such matters or things can be procured either directly or indirectly through a computer system; or

(e) publicly exhibits any indecent show or performance or any show or performance tending to corrupt morals through a computer system.

(2) A person convicted of an offence under subsection (1) is liable to a fine not exceeding ten thousand penalty units.

(3) A prosecution for an offence under this section shall not be instituted without the written consent of the Director of Public Prosecutions.

Introduction of malicious software into computer system

60. A person who intentionally introduces or spreads malicious software into a computer system commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

Denial of service attacks

61. A person who intentionally renders a computer system incapable of providing normal services to its legitimate users commits an offence and is liable, on conviction, to a fine not exceeding one million penalty units or to imprisonment for a term not exceeding ten years, or to both.

Unsolicited electronic messages

62. (1) A person commits an offence if that person, knowingly and without lawful excuse or justification—

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

(b) uses a computer system to relay or retransmit multiple electronic communications, with the intent to deceive or mislead users, or any electronic mail of licensee, as to the origin of such messages, or

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

(2) A person convicted of an offence under subsection (1), is liable, on conviction, to imprisonment for a period not exceeding two years, or a fine not exceeding two hundred thousand penalty units, or to both.

(3) Despite subsection (1), it shall not be an offence under this Act where—

(a) the transmission of multiple electronic communications from or through such computer system is done within customer, business or any other relationships where a person would reasonably be expected to transmit multiple electronic mail messages;

(b) the recipient of such electronic communications has not opted out of the business, customer or other relationship; and

(c) the transmission is by public institutions and is for purposes of raising awareness or collecting information with regard to education, health, security, safety outages and emergencies.

Prohibition of use of computer system for offences

63. (1) A person shall not use a computer system for any activity which constitutes an offence under any written law which is not provided under this Act.

(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to the penalty specified for that offence in the applicable written law.

Application of offences under Act

64. (1) Subject to subsection (2), this Act has effect in relation to a person, whatever the person's nationality or citizenship, outside as well as within the Republic, and where an offence under this Act is committed by a person in a place outside the Republic, the person shall be dealt with as if the offence had been committed within the Republic.

(2) For the purposes of subsection (1), this Act shall apply if, for the offence in question—

(a) the accused was in the Republic at the material time;

(b) the computer, program or data was in the Republic at the material time; or

(c) the damage occurred within the Republic whether or not paragraph *(a)* or *(b)* applies.

Hate speech

65. A person who, using a computer system, knowingly without lawful excuse, uses hate speech commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding two years, or to both.

Minimisation, etc., of genocide and crimes against humanity

66. A person who, knowingly without lawful excuse distributes or otherwise makes available, through a computer system to the public or another person, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity commits an offence and is liable, on conviction, to a fine not exceeding two million penalty units, or to imprisonment for a period not exceeding twenty years, or to both.

Unlawful disclosure of details of investigation

67. (1) A person commits an offence if that person receives an order related to a criminal investigation and without lawful excuse discloses—

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

(b) anything done under the order; or

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

(2) A person convicted of an offence under subsection (1) is liable to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

Obstruction of law enforcement officer or cyber inspection officer

68. A person who obstructs or hinders a law enforcement officer, cyber inspector or any person in the exercise of any powers under this Act or who neglects or fails to comply with an order commits an offence and is liable, on conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a period not exceeding two years, or to both.

Harassment utilising means of electronic communic-ation

69. A person who using a computer system intentionally initiates any electronic communication, with the intent to coerce, intimidate, harass, or cause emotional distress to a person commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

Cyber terrorism

70. (1) A person who uses or causes to be used a computer system for the purposes of cyber terrorism commits an offence and is liable on conviction to life imprisonment.

(2) In this section "cyber terrorism" means the unlawful use of computers and information technology to unlawfully attack or threaten to attack computers, networks and the information stored therein done to intimidate or coerce a government or its people in furtherance of political or social objectives and to cause severe disruption or widespread fear in society.

Cyber attack

71. A person who carries out a cyber attack commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

Cognizable offences Cap. 88

72. An offence under this Act shall be deemed to be a cognizable offence for the purposes of the Criminal Procedure Code.

PART X
ELECTRONIC EVIDENCE

Admissibility of electronic evidence

73. (1) In any legal proceedings, the rules of evidence shall not be applied so as to deny the admissibility of a data message in evidence—

(a) on the mere grounds that it is constituted by a data message; or

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message shall be given due evidential weight.

(3) In assessing the evidential weight of a data message, regard shall be had to—

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

(b) the reliability of the manner in which the integrity of the data message was maintained;

(c) the manner in which its originator was identified; and

(d) any other relevant factor.

PART XI
GENERAL PROVISIONS

Appeals

74. (1) A person aggrieved by a decision made by the Authority may appeal to the Minister.

(2) A person aggrieved by the decision made by the Minister may appeal to the High Court.

Search and seizure Cap. 88

75. (1) The provisions of the Criminal Procedure Code relating to warrants shall apply to this Part.

(2) A law enforcement officer may with warrant, where the law enforcement officer or an authorised officer has reasonable grounds to believe that there may be in a specified computer system or part of it—

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

(b) material that has been acquired by a person as a result of an offence, enter the place where the computer system is to search and seize the computer system including search or similarly access—

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

(ii) a computer data storage medium in which computer data may be stored within or outside the Republic.

(3) A law enforcement officer that is undertaking a search under this Act may, where the law enforcement officer has reasonable grounds to believe that the data sought is stored in another device or computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial device or system, extend the search or similar accessing to the other device or system.

(4) A law enforcement officer or an authorised officer that is undertaking a search is empowered to seize or similarly secure computer data accessed according to subsections (1) or (2).

Prohibition of disclosure of information to unauthorised persons

76. (1) A person shall not without the consent in writing given by, or on behalf of the Authority, publish or disclose to any person otherwise than in the cause of such person's duties, the contents of any documents, communication, or information which relates to, and which has come to that person's knowledge in the course of that person's duties under this Act.

(2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to a fine not exceeding three hundred thousand penalty units or to imprisonment for a term not exceeding three years, or to both.

77. (1) A person, who is not a suspect of a crime or otherwise excluded from an obligation to follow such order, but who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein that is the subject of a search under this Act shall permit, and assist if reasonably required and requested by the person authorised to make the search by—

(a) providing information that enables the undertaking of necessary measures in the circumstances;

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

(c) obtaining and copying such computer data; or

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

Production order

78. Where a judge is satisfied on the basis of an *ex-parte* application by a law enforcement officer that specified computer data, or a printout or otherinformation, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the Judge may order that—

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

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

Expedited preservation

79. (1) A law enforcement officer may, where the law enforcement officer has grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, by written notice given to a person in control of the computer data, require the person to ensure that the data specified in the notice be preserved for a period of up to seven days as specified in the notice.

(2) The law enforcement officer may apply to a Judge for the extension of the period referred to under subsection (1).

Partial disclosure of traffic data

80. A law enforcement officer may, where the law enforcement officer is satisfied computer data is reasonably required for the purposes of a criminal investigation, by written notice given to a person in control of the computer system, require the person to disclose relevant traffic data about a specified communication to identify—

(a) the electronic communications service providers; or

(b) the path through which a communication was transmitted.

Collection of traffic data

81. (1) Where a judge is satisfied on the basis of an *ex-parte* application by a law enforcement officer, supported by affidavit that there are reasonable grounds to suspect or believe that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the Judge may order a person in control of such data to—

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

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

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

No monitoring obligation

82. (1) An electronic communication service provider shall not have a general obligation to monitor the data which it transmits or stores; or actively seek facts or circumstances indicating an unlawful activity.

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

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

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

Limitation of Liability

83. An electronic communications service provider shall not be criminally liable for providing access and transmitting information on condition that it meets the limitation of liability criteria stipulated in the Electronic Communications and Transactions Act, 2021.

Act No. 4 of 2021

Extradition Cap. 94

84. An offence under the provisions of this Act is an extraditable offence for the purposes of the Extradition Act.

Evidence obtained by unlawful interception not admissible in criminal proceedings

85. Despite any other law, evidence which is obtained by means of any interception effected in contravention of this Act, shall not be admissible in any criminal proceedings except with the leave of the court, and in granting or refusing such leave, the court shall have regard, among other things, to the circumstances in which it was obtained, the potential effect of its admission or exclusion on issues of national security and the unfairness to the accused person that may be occasioned by its admission or exclusion.

General penalty

86. A person who commits an offence under this Act for which no penalty is provided is liable, on conviction—

(a) in the case of an individual, to a penalty not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both; or

(b) in the case of a body corporate or unincorporate body to a penalty not exceeding one million penalty units.

Power of court to order cancellation of licence, forfeiture etc.,

87. (1) The court may on conviction of a person of an offence under this Act order—

(a) forfeiture of any—

(i) property constituting proceeds of such offence; or

(ii) device or property used or intended to be used to commit or facilitate the commission of the offence; or

(b) the cancellation of a licence issued under this Act.

Act No. 19 of 2010

(2) The Forfeiture of Proceeds of Crime Act, 2010 applies in relation to an order of forfeiture made by the court under subsection (1).

Guidelines

88. (1) The Authority may issue guidelines as are necessary for the better carrying out of the provisions of this Act.

(2) The guidelines issued by the Authority under this Act shall bind all persons regulated under this Act.

(3) The Authority shall publish the guidelines on the website, in a daily newspaper of general circulation in the Republic or the *Gazette*.

Exemptions

89. (1) The Authority may, by declaration, exempt a person or class of persons, for a limited or unlimited period of time, from the requirement to abide by the provisions of this Act.

(2) The Authority may, where it issues a declaration under subsection (1), reverse its decision where it considers necessary.

(3) The Authority shall, where it reverses its decision under subsection (2), notify by declaration, the affected persons.

Regulations

90. (1) The Minister may, on the recommendation of the Authority, by statutory instrument, make regulations for the better carrying out of the provisions of this Act.

(2) Despite the generality of subsection (1), the regulations may make provisions for—

(a) the form and manner of making applications for registration, licences duration of licences and the fees payable on that application; and

(b) fees payable under this Act.