THE CYBERSECURITY AND CYBERCRIME ACT 2021

Act No. 16 of 2021

I assent

MARIE CYRIL EDDY BOISSÉZON

24th November 2021 *Acting President of the Republic*

ARRANGEMENT OF SECTIONS

Section

PART I – PRELIMINARY

1. Short title
2. Interpretation

PART II – THE NATIONAL CYBERSECURITY COMMITTEE

3. Establishment of National Cybersecurity Committee
4. Functions of Committee
5. Meetings of Committee
6. Reports by Committee

PART III – OFFENCES

7. Unauthorised access to computer data
8. Unauthorised interception of computer service
9. Unauthorised interference
10. Access with intent to commit offences
11. Unauthorised modification of computer data
12. Unauthorised disclosure of password
13. Unlawful possession of devices and computer data

14. Electronic fraud
15. Computer-related forgery
16. Misuse of fake profile
17. Cyberbullying
18. Cyber extortion
19. Revenge pornography
20. Cyberterrorism
21. Infringement of copyright and related rights
22. Increased penalty for offences involving critical information infrastructure
23. Failure to moderate undesirable content
24. Disclosure of details of an investigation
25. Obstruction of investigation

PART IV – INVESTIGATION PROCEDURES

26. Expedited preservation and partial disclosure of traffic data
27. Production order
28. Powers of access, search and seizure for purpose of investigation
29. Real-time collection of traffic data
30. Interception of content data
31. Deletion order
32. Limited use of disclosed computer data and information

PART V – CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

33. Critical information infrastructure
34. Protection of critical information infrastructure
35. Reports on critical information infrastructure
36. Information sharing agreement
37. Auditing of critical information infrastructure to ensure compliance

PART VI – COMPUTER EMERGENCY RESPONSE TEAM OF MAURITIUS (CERT-MU)

38. Setting up of CERT-MU
39. Functions of CERT-MU

PART VII – INTERNATIONAL COOPERATION

40. General principles relating to international cooperation
41. Spontaneous information
42. Expedited preservation of stored computer data
43. Expedited disclosure of preserved traffic data
44. Mutual assistance regarding accessing of stored computer data

45. Transborder access to stored computer data with consent or where publicly available
46. Mutual assistance in real-time collection of traffic data
47. Mutual assistance regarding interception of content data
48. 24/7 point of contact

PART VIII – GENERAL PROVISIONS

49. Prosecution
50. Jurisdiction
51. Regulations
52. Extradition
53. Forfeiture
54. Repeal
55. Savings and transitional provisions
56. Commencement

An Act

To establish the National Cybersecurity Committee and a comprehensive legal framework to deal with cybercrime

ENACTED by the Parliament of Mauritius, as follows –

PART I – PRELIMINARY

1. Short title

This Act may be cited as the Cybersecurity and Cybercrime Act 2021.

2. Interpretation

In this Act –

"access" means gaining entry to a program or computer data stored in a computer system;

"Budapest Convention" means the Budapest Convention on Cybercrime of 2001, acceded to by Mauritius on 1 March 2014;

"Central Authority" has the same meaning as in the Mutual Legal Assistance in Criminal and Related Matters Act;

"CERT-MU" means the Computer Emergency Response Team of Mauritius set up under section 38;

"Committee" means the National Cybersecurity Committee established under section 3;

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

"Computer Emergency Response" means to –

(a) coordinate in the event of cyber security emergencies;

(b) provide help in resolving security incidents;

(c) provide information to improve cyber security;

"computer program" means a set of instructions, expressed in words, codes, schemes or any other form, which is capable of causing a computer to perform or achieve a particular task or result**;**

"computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

"content data" –

(a) means –

(i) the communication content of the communication;

(ii) the meaning or purport of the communication; or

(iii) the message or information being conveyed by the communication; and

(b) includes everything transmitted as part of communication that is not traffic data;

"critical information infrastructure" means an asset, facility, system, network or process, whose incapacity, destruction or modification would have –

(a) a debilitating impact on the availability, integrity or delivery of essential services, including those services whose integrity, if compromised, could result in significant loss of life or casualties; or

(b) a significant impact on national security, national defence, or the functioning of the State;

"cyberbullying" means any behaviour by means of information and communication technologies, which –

(a) is repetitive, persistent and intentionally harmful; or

(b) involves an imbalance of power between the perpetrator and the victim and causes feelings of distress, fear, loneliness or lack of confidence in the victim, and which results in serious physical or psychological harm to the victim, disability of the victim or death of the victim;

"cybersecurity" means protecting information, equipment, device, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction;

"cybersecurity best practices" means a set of models, frameworks, processes or technologies advised and adopted by peers of cybersecurity;

"cybersecurity incident" means –

(a) use, disclosure, breach, modification, theft, loss, corruption, or destruction of information;

(b) interference with information technology operations; or

(c) interference with system operations;

"cybersecurity policy" means a formal set of rules enforced in order to protect the information and computer system;

"cyber extortion" means a form of cybercrime which occurs when a person uses the internet to demand money or other goods or behaviour from another person by threatening to inflict harm to his person, reputation, or property;

"device" –

(a) means a unit of physical or virtual hardware or equipment that provides one or more computing functions; and

(b) includes –

(i) a computer program, code, software or an application;

(ii) a component of a computer system such as, but not limited to a graphic card, memory card, chip or processor;

(iii) computer storage component; or

(iv) an input and/or output device;

"electronic communication" means the transfer of a sign, signal or computer data of any nature, transmitted in whole or in part by an electrical, digital, magnetic, electromagnetic, optical, wire, wireless, radio, photo electronic or photo optical system or any other similar form;

"fake profile" means an untrue online representation, existent or non-existent;

"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication to, from or within a computer system;

"Global Action on Cybercrime Extended project" refers to the Council of Europe's Glacy project designed to strengthen the capacities of States worldwide on the application of cybercrime legislation and electronic evidence, and of which Mauritius is a priority country;

"harm" includes physical, sexual, psychological, emotional or moral abuse, injury, neglect, ill-treatment, degradation, discrimination, exploitation or impairment of health or development;

"information and communication technologies" has the same meaning as in the Information and Communication Technologies Act;

"intercept", in relation to a function of a computer, includes to monitor, or record a function of a computer, or acquire the substance, its meaning or purport of such function;

"interference", in relation to a computer system, means –

(a) any impairment to the confidentiality, integrity or availability of computer data;

(b) corrupting a computer system by any means;

(c) impairing, by any means, the connectivity, infrastructure or support of a computer system;

"investigatory authority" means the police or any other body lawfully empowered to investigate any offence;

"Minister" means the Minister to whom responsibility for the subject of information technology is assigned;

"Ministry" means the Ministry responsible for the subject of information technology;

"modification" means inputting, transmitting, damaging, deleting, suppressing, altering or modifying computer data;

"netflow" –

(a) means Internet Protocol network traffic data which includes Internet Protocol source address, Internet Protocol destination address, source port, destination port and protocol type; but

(b) does not include content data;

"online account" includes accounts or pages on social networking services, search engine services, internet based messaging services or video sharing services;

"password" means any form of authentication that allows access to a computer program, storage medium or computer system;

"pornography" means –

(a) the representation in a book, magazine, photograph, film, computer data or any such other media;

(b) a scene of sexual behaviour in any form,

that is erotic or lewd and is designed to arouse sexual interest;

"property" has the same meaning as in the Asset Recovery Act;

"regulatory authority" means a Government agency responsible for exercising autonomous authority over a critical sector;

"service provider" means –

(a) a public or private entity that provides to users the ability to communicate by means of a computer system; and

(b) any other entity that processes or stores computer data on behalf of such communication service or users of such service;

"sexual photograph or film" means –

(a) an image or video that depicts nudity; or

(b) a picture of someone who is engaged in sexual behaviour or posing in a sexually provocative way;

"subscriber information" means any information, contained in the form of data or any other form, that is held by a service provider, relating to subscribers, other than traffic or content data, by which can be established –

(a) the type of the communication service used, the technical provisions taken to use the communication service and the period of the service;

(b) the subscriber's identity, postal or geographical address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; or

(c) any other information on the site of installation of a communication equipment available on the basis of the service agreement or arrangement;

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

"vulnerability" means a weakness or flaw in a computer system or computer program, that can be exploited, resulting in its adverse or different functioning, other than the intended functions.

PART II – THE NATIONAL CYBERSECURITY COMMITTEE

3. Establishment of National Cybersecurity Committee

(1) There is established, for the purposes of this Act, the National Cybersecurity Committee.

(2) The Committee shall comprise –

(a) a Chairperson, to be appointed by the Prime Minister;

(b) a representative of the Prime Minister's Office;

(c) a representative of the Ministry;

(d) a representative of the Computer Emergency Response Team of Mauritius (CERT-MU);

(e) a representative of the Data Protection Office;

(f) a representative of the Mauritius Police Force;

(g) a representative of the Attorney-General's Office;

(h) a representative of the Information and Communication Technologies Authority;

(i) a representative of the Bank of Mauritius;

(j) a representative of the Financial Services Commission;

(k) a representative of the Counterterrorism Unit, Prime Minister's Office;

(l) a representative of the private sector, having experience in the field of cybersecurity and cybercrime, to be appointed by the Minister; and

(m) a representative of civil society, having experience in the field of cybersecurity and cybercrime, to be appointed by the Minister.

(3) Every member shall be paid such fees or allowances as the Minister may determine.

(4) The Committee may co-opt any person who may be of assistance in relation to any matter before it and the co-opted member shall –

(a) not have the right to vote at any meeting of the Committee; and

(b) be paid such fees or allowances as the Committee may determine.

(5) No member shall engage in any activity which may undermine the reputation, confidentiality or integrity of the Committee.

4. Functions of Committee

(1) The Committee shall –

(a) advise the Government on cybersecurity and cybercrime;

(b) implement Government policy relating to cybersecurity and cybercrime;

(c) coordinate all matters relating to cybersecurity and cybercrime;

(d) receive and act on reports relating to cybersecurity and cybercrime;

(e) coordinate and facilitate the implementation of a critical information infrastructure protection framework;

(f) coordinate the collection and analysis of internal and external cyber threats, and response to cyber incidents that threaten the Mauritian cyberspace;

(g) cooperate with computer incident response teams and other relevant bodies, locally and internationally, on response to cyber threats and cybersecurity incidents;

(h) establish cybersecurity best practices and standards for critical information infrastructures;

(i) promote capacity building on the prevention, detection and mitigation of cyber threats;

(j) perform any other relevant function conferred on it under this Act or any other law.

(2) Subject to the other provisions of this Act, the Committee shall regulate its meetings and proceedings in such manner as it may determine.

5. Meetings of Committee

(1) (a) The Committee shall meet as often as is necessary, but at least once every 2 months.

(b) A meeting of the Committee shall be held at such time and place as the Chairperson may determine.

(2) At any meeting of the Committee, 7 members shall constitute a quorum.

(3) The Chairperson shall convene a meeting on a request made by at least 5 members.

(4) (a) The Ministry shall, in consultation with the Chairperson, appoint a Secretary to the Committee.

(b) The Secretary shall –

(i) prepare and attend every meeting of the Committee;

(ii) keep minutes of proceedings of any meeting of the Committee; and

(iii) have such other duties as may be conferred upon him by the Committee.

(5) The Committee shall regulate its meetings and proceedings in such manner as it may determine.

6. Reports by Committee

(1) The Committee shall submit reports to the Minister on a quarterly basis or whenever required.

(2) The Minister may, where he considers appropriate, refer to Cabinet any matter referred to him under subsection (1).

(3) The Minister may, where he considers appropriate, refer any matter referred to him under subsection (1) to the police for enquiry.

PART III – OFFENCES

7. Unauthorised access to computer data

(1) Subject to subsection (2), any person who gains unauthorised access to any program or data held in a computer system shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to penal servitude for a term not exceeding 10 years.

(2) Access by a person to a computer system shall be unauthorised where the person –

(a) is not entitled to control access of the kind in question; and

(b) is not authorised to access of the kind in question by any person who is so entitled.

(3) For the purpose of this section, it is immaterial that the unauthorised access is not directed at –

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer system.

(4) A person shall not be liable under subsection (1) where –

(a) he is a person with a right to control the operation or use of the computer system and exercises such right in good faith;

(b) he has the express or implied consent of the person empowered to authorise him to have such an access;

(c) he has reasonable grounds to believe that he had such consent as specified in paragraph (b);

(d) he is acting pursuant to measures that can be taken under Part IV of this Act; or

(e) he is acting in reliance of any statutory power arising under any enactment for the purpose of obtaining information, or of taking possession of, any document or other property.

8. Unauthorised interception of computer service

(1) Subject to subsection (4), any person who, by any technical means, wilfully intercepts or causes to be intercepted without authorisation, any computer data, or electromagnetic emissions carrying computer data, or non-public transmissions to, from or within, a computer system shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to penal servitude for a term not exceeding 10 years.

(2) Where, as a result of the commission of an offence under subsection (1), the operation of the computer system is impaired, or transmitted computer data is suppressed or modified, a person convicted of such offence shall be liable to a fine not exceeding one million rupees and to penal servitude for a term not exceeding 20 years.

(3) For the purpose of this section, it is immaterial that the unauthorised access or interception is not directed at –

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer system.

(4) A person shall not be liable under subsection (1) where he –

(a) has obtained prior consent of both the person who sent the data and the intended recipient of such data;

(b) is acting in reliance on any statutory power;

(c) is acting in the performance of his lawful duties, contractual obligations or is discharging any legal obligation.

9. Unauthorised interference

(1) Any person who, intentionally and without authorisation, hinders the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to penal servitude for a term not exceeding 10 years.

(2) For the purpose of this section, an interference is unauthorised if the person whose act causes the interference –

(a) is not entitled to cause that interference;

(b) does not have consent to interfere from a person who is so entitled.

(3) A person who commits an offence under subsection (1) which –

(a) results in financial loss to any person or organisation;

(b) threatens national security;

(c) causes reputational damage to any person;

(d) causes physical or mental injury to, or the death of, any person;

(e) causes, directly or indirectly, degradation, failure, interruption or obstruction of the operation of a computer system; or

(f) threatens public health or public safety,

shall, on conviction, be liable to a fine not exceeding one million rupees and to penal servitude for a term not exceeding 20 years.

(4) For the purpose of this section, it is immaterial whether or not the unauthorised interference is directed at –

(a) any particular computer system, program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer system.

(5) For the purpose of this section, it is immaterial whether an unauthorised interference or any intended effect of it is permanent or temporary.

10. Access with intent to commit offences

Any person who, intentionally and without authorisation, gains access to any computer program or computer data held in a computer system with intent to commit an offence shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to penal servitude for a term not exceeding 20 years.

11. Unauthorised modification of computer data

(1) Subject to subsection (3), any person who, intentionally and without authorisation, modifies computer data shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and penal servitude for a term not exceeding 20 years.

(2) Where, as a result of the commission of an offence under this section –

(a) the operation of the computer system;

(b) access to any computer program or computer data held in any computer; or

(c) the operation of any computer program or the reliability of any such computer data,

is suppressed, modified or otherwise impaired, a person who is convicted of the offence shall be liable to a fine not exceeding one million rupees and to penal servitude for a term not exceeding 20 years.

(3) A modification is unauthorised if –

(a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and

(b) he does not have consent to the modification from any person who is so entitled.

(4) For the purpose of this section, it is immaterial whether an unauthorised modification, or any intended effect of it, is permanent or temporary.

12. Unauthorised disclosure of password

Any person who, intentionally and without authorisation, discloses any password, access code, biometric authentication, token, two-factor authentication, multi-factor authentication or any other means of gaining access to any computer program or computer data held in any computer system for its production, sale, procurement for use, import or distribution shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to penal servitude for a term not exceeding 10 years.

13. Unlawful possession of devices and computer data

(1) Any person who intentionally manufactures, sells, procures for use, imports, distributes or otherwise makes available, a computer system, computer data or any other device, designed or adapted primarily for the purpose of committing any offence under this Act shall commit an offence.

(2) Any person who intentionally and without authorisation, receives or is in possession of devices and computer data under subsection (1) shall commit an offence.

(3) Any person who commits an offence under this section shall, on conviction, be liable to a fine not exceeding one million rupees and to penal servitude for a term not exceeding 10 years.

(4) In this section –

"possession of any computer data" includes –

(a) having possession of a computer system or device that holds or contains the computer data or computer program;

(b) having possession of a document in which the computer data or computer program is recorded; or

(c) having control of computer data or computer program that is in the possession of another person.

14. Electronic fraud

Any person who, intentionally and without authorisation, causes loss of property to another person by –

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

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

to procure for himself or another person any form of advantage shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to penal servitude for a term not exceeding 20 years.

15. Computer-related forgery

(1) Any person who, intentionally and without authorisation, inputs, alters, deletes, or suppresses computer data, resulting in inauthentic data, with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible, shall commit an offence and shall, on conviction, be liable to fine not exceeding one million rupees and to penal servitude for a term not exceeding 10 years.

(2) A person who performs the acts described under subsection (1) –

(a) for wrongful gain;

(b) for wrongful loss to another person; or

(c) for any benefit for oneself or for another person,

shall, on conviction, be liable to a fine not exceeding one million rupees and to penal servitude for a term not exceeding 20 years.

16. Misuse of fake profile

Any person who individually, or with other persons, makes use of a fake profile to cause harm shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees or to penal servitude for a term not exceeding 20 years.

17. Cyberbullying

Any person who, individually or with other persons, commits cyberbullying, shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to penal servitude for a term not exceeding 20 years.

18. Cyber extortion

Any person who engages in cyber extortion shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to penal servitude for a term not exceeding 20 years.

19. Revenge pornography

Any person who, by means of a computer system, discloses or publishes a sexual photograph or film without the consent of the person who appears in the photograph or film, and with the intention of causing that person distress, shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to penal servitude for a term not exceeding 20 years.

20. Cyberterrorism

(1) Any person who intentionally accesses or causes to be accessed a computer system or network for the purpose of carrying out an act of terrorism, shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to penal servitude for a term not exceeding 20 years.

(2) In this section –

"act of terrorism" has the same meaning as in the Prevention of Terrorism Act.

21. Infringement of copyright and related rights

(1) Any person who, without the express authorisation of the author or owner of the copyright –

(a) attempts to use, publish or distribute another person's work for commercial purpose, through a computer system;

(b) downloads movies, music files or pirated software applications for gain or against remuneration; or

(c) posts a copyrighted work such as writing or graphics, online for gain or against remuneration,

shall commit an offence.

(2) Any person convicted under subsection (1) shall, on –

(a) a first conviction, be liable to a fine not exceeding 300,000 rupees and to imprisonment for a term not exceeding 2 years;

(b) a second or subsequent conviction, be liable to a fine not exceeding 500,000 rupees and to imprisonment for a term not exceeding 8 years.

22. Increased penalty for offences involving critical information infrastructure

Any person who commits an offence specified in sections 7, 8, 9, 10 and 11 on a critical information infrastructure shall, on conviction, be liable to a fine not exceeding 2 million rupees and to imprisonment for a term not exceeding 25 years.

23. Failure to moderate undesirable content

(1) It shall be the responsibility of the administrator of an online account to moderate and control undesirable content that has been brought to his attention by an investigatory authority.

(2) Any person who contravenes subsection (1) shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to penal servitude for a term not exceeding 20 years.

(3) For the purpose of this section –

"undesirable content" includes any online content that –

(a) is deceptive or inaccurate, posted with intent to defame, threaten, abuse or mislead the public;

(b) threatens public health or public safety;

(c) threatens national security; or

(d) promotes racism.

24. Disclosure of details of an investigation

(1) No person shall disclose any detail of a criminal investigation under this Act and the investigation shall be kept confidential.

(2) Any person who contravenes subsection (1) shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to penal servitude for a term not exceeding 20 years.

(3) A person shall not be liable under subsection (2) where he –

(a) is acting in reliance of any statutory power; or

(b) is acting in the performance of his lawful duties, contractual obligation or in the discharge of any legal obligation.

25. Obstruction of investigation

(1) Any person who destroys, deletes, alters, conceals, modifies or renders computer data meaningless, ineffective or useless with intent to obstruct or delay an investigation shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to penal servitude for a term not exceeding 20 years.

(2) Any person who prevents the execution of, or fails to comply with, an order issued under this Act shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to penal servitude for a term not exceeding 20 years.

(3) A person shall not be liable under subsection (1) where he –

(a) is acting in reliance of any statutory power; or

(b) is acting in the performance of his lawful duties, contractual obligation or in the discharge of any legal obligation.

PART IV – INVESTIGATION PROCEDURES

26. Expedited preservation and partial disclosure of traffic data

(1) Where an investigatory authority has reasonable grounds to believe that–

(a) any specified traffic data stored in any computer system or device, or by means of a computer system, is reasonably required for the purpose of a criminal investigation; and

(b) there is a risk that the traffic data may be modified, lost, destroyed or rendered inaccessible,

the investigatory authority shall serve a notice on the person who is in possession or control of the traffic data, requiring the person to –

(i) undertake expeditious preservation of such available traffic data regardless of whether one or more service providers were involved in the transmission of that communication; or

(ii) disclose required traffic data concerning that communication in order to identify the service providers and the path through which communication was transmitted.

(2) The data specified in the notice referred to in subsection (1) shall be preserved and its integrity shall be maintained for a period not exceeding 90 days.

(3) The period of preservation and maintenance of integrity may be extended for a period exceeding 90 days if, on an application by the investigatory authority to the Judge in Chambers, the Court is satisfied that –

(a) an extension of the period of preservation is reasonably required for the purpose of an investigation or prosecution;

(b) there is a real risk that the traffic data may be modified, lost, destroyed or rendered inaccessible.

(4) The person in possession or control of the traffic data shall be responsible to preserve the data specified –

(a) for the period specified in the notice for preservation and maintenance of integrity, or for any extension thereof permitted by the Court; and

(b) for the period specified to keep confidential any preservation ordered under this section.

27. Production order

(1) Where the disclosure of data is required for the purpose of a criminal investigation or prosecution of an offence, an investigatory authority may make an application to the Judge in Chambers for an order compelling –

(a) a person in the territory of Mauritius to submit specified data in that person's possession or control, which is stored in a computer system or device;

(b) any service provider offering its services in the territory of Mauritius to submit subscriber information in relation to such services in that service provider's possession or control.

(2) Where any material, to which an investigation relates, consists of computer data stored in a computer system, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is easily understood.

28. Powers of access, search and seizure for purpose of investigation

(1) Where an investigatory authority has reasonable grounds to believe that –

(a) stored data is relevant for the purpose of an investigation or the prosecution of an offence, it may make an application to the Judge in Chambers for the issue of a warrant to enter any premises to access, search and seize such data;

(b) data sought is stored in another computer system or part of it in Mauritian territory, and such data is lawfully accessible from or available to the initial system, the investigatory authority shall expeditiously extend the search or similar access to the other system.

(2) The investigatory authority may, in the execution of a warrant under subsection (1) –

(a) seize or secure a computer system or part of it or a computer data storage medium;

(b) make and retain a copy of those computer data;

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

(d) render inaccessible or remove those computer data from the accessed computer system.

(3) The investigatory authority may order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs (1) and (2).

29. Real-time collection of traffic data

(1) Where an investigatory authority has reasonable grounds to believe that traffic data is relevant for the purpose of investigation and prosecution of an offence, it may make an application to the Judge in Chambers for an order –

(a) authorising the collection or recording of traffic data on Mauritian territory by technical means, in real-time, associated with specified communications transmitted by means of any computer system;

(b) compelling a service provider, within its technical capabilities, to –

(i) effect such collection and recording specified in paragraph (a); or

(ii) cooperate with the investigatory authority to effect such collection and recording; or

(c) compelling a service provider to keep confidential the fact of the execution of any power provided under this section and any information relating to it.

30. Interception of content data

Where an investigatory authority has reasonable grounds to believe that any content data is relevant for the investigation and prosecution of an offence, it may make an application to the Judge in Chambers for an order to –

(a) collect or record content data in the territory of Mauritius by technical means in real-time of specified communications by means of a computer system;

(b) compel a service provider, within its existing technical capabilities, to –

(i) collect or record by technical means on the territory of Mauritius;

(ii) cooperate and assist the investigatory authority in the collection or recording of content data, in real-time, of specified communications in the territory of Mauritius, transmitted by means of a computer system; or

(c) compel a service provider to keep the confidentiality of the fact of the execution of any power provided for in this section and any information relating to it.

31. Deletion order

The Judge in Chambers may, for the purpose of this Act, upon application by an investigatory authority, and upon being satisfied that a computer system or any other device contains any unlawful material or activity, order that such computer data be –

(a) no longer stored on and made available through the computer system or any other device; or

(b) deleted or destroyed.

32. Limited use of disclosed computer data and information

(1) Computer data obtained under this Act by any person authorised, in writing, by an investigatory authority shall be used for the purpose of a criminal investigation or the prosecution of an offence, unless such computer data is sought in –

(a) accordance with any other enactment;

(b) compliance with an order from a Court;

(c) relation to the prevention of injury or other damage to the health of a person or serious loss of, or damage to, property; or

(d) the public interest.

(2) Subject to subsections (1) and (3), any person authorised by an investigatory authority shall, on receipt of a request, in writing, permit a person who had the custody or control of a computer system to access and copy computer data on the computer system.

(3) Any person authorised, in writing, by an investigatory authority, may refuse to give access to computer data or provide copies of such computer data if he has reasonable grounds to believe that –

(a) possession of the data constitutes, or may lead to, or assist in, a criminal offence; or

(b) giving access or copies prejudices the investigation in connection with which the search was carried out, another ongoing investigation, or any criminal proceedings that are pending or which may be brought in relation to any of those investigations.

PART V – CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

33. Critical information infrastructure

(1) The Committee may, after consultation with the regulatory authority in control of any information infrastructure which is identified as a potential critical information infrastructure, within 3 months of the consultation, identify the information structures which need to be declared critical information infrastructures.

(2) A system is selected as a critical information infrastructure if a disruption of the system or its data would result in –

(a) the interruption of a life sustaining service such as the supply of water, health services and energy;

(b) an important effect on the economy;

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

(d) failure or substantial disruption of the money market.

(3) Any regulatory authority shall, within a reasonable time of the declaration of any information infrastructure as a critical information infrastructure, in accordance with the critical information infrastructure framework, monitor and report to the Committee on –

(a) the classification of data held by the critical information infrastructure;

(b) the protection, storing and archiving of data held by the critical information infrastructure;

(c) cybersecurity incident management by the critical information infrastructure;

(d) disaster contingency and recovery measures, which may be put in place by the critical information infrastructure;

(e) minimum physical and technical security measures that may be implemented in order to protect the critical information infrastructure;

(f) reporting to CERT-MU cybersecurity incidents impacting national security, public safety and public interest by the owners of critical information infrastructure;

(g) the establishment of a point of contact at the level of the critical information infrastructure;

(h) any other relevant matter which is necessary or expedient in order to promote cybersecurity in respect of the critical information infrastructure.

34. Protection of critical information infrastructure

Any regulatory authority of the respective critical information infrastructure shall, in consultation with the Committee, direct the owner of a critical information infrastructure to –

(a) conduct an assessment of the threats, vulnerabilities, risks and probability of a cyber-attack of the critical information infrastructure;

(b) measure the overall preparedness against damage or unauthorised access to a critical information infrastructure;

(c) identify any other risk based factors appropriate and necessary to protect the critical information infrastructure;

(d) implement information security policy;

(e) conduct periodic IT Security Risk Assessment of a critical information infrastructure;

(f) implement an incident reporting policy;

(g) develop a Security Awareness Programme.

35. Reports on critical information infrastructure

(1) The owner of a critical information infrastructure shall report to the Committee on any cybersecurity incident impacting the national security, public safety or public interest and the action the owner intends to take to mitigate the cybersecurity incident.

(2) The Committee shall, on receipt of a report under subsection (1), direct CERT-MU to advise the owner of a critical information infrastructure on the mitigation of the cybersecurity incident.

(3) CERT-MU shall submit a report to the Committee on the reported cybersecurity incidents impacting the national security, public safety and public interest reported by the owners of critical information infrastructure.

36. Information sharing agreement

(1) A private entity may enter into an information sharing agreement with a public entity regarding a critical information infrastructure.

(2) An agreement under subsection (1) shall only be entered into for the following purposes and in accordance with the critical information infrastructure policy –

(a) to enforce cybersecurity;

(b) for the investigation and prosecution of cybercrimes; and

(c) for the protection of national security, public safety or public interest.

37. Auditing of critical information infrastructure to ensure compliance

(1) The owner of a critical information infrastructure shall, every year or where there is a major upgrade or change in the IT infrastructure, carry out an independent IT Security Audit.

(2) The report of the independent IT Security Audit shall be submitted to the National Cybersecurity Committee to evaluate compliance.

(3) The Committee may request the owner of a critical information infrastructure to provide such additional information as may be required within a specified period in order to evaluate any issues raised by the IT Security audit.

(4) Any owner of a critical information infrastructure who –

(a) fails to carry out an IT Security Audit under subsection (1);

(b) fails to submit to the Committee the report of the IT Security Audit;

(c) fails to provide to the Committee any additional information as may be required within a specified period in order to evaluate the report of the IT Security audit;

(d) hinders, obstructs or improperly attempts to influence any person or organisation authorised to carry out the IT Security audit; or

(e) hinders, obstructs or attempts to influence any member of the Committee, person or entity to monitor, evaluate and report on the adequacy and effectiveness of the findings of the IT Security audit,

shall commit an offence and shall, on conviction, be liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding 5 years.

PART VI – COMPUTER EMERGENCY RESPONSE TEAM OF MAURITIUS (CERT-MU)

38. Setting up of CERT-MU

(1) There is set up, within the Ministry, for the purposes of this Act, the Computer Emergency Response Team of Mauritius (CERT-MU) which shall be the national agency for coordinating cybersecurity response activities and promoting cybersecurity at national level.

(2) The head of CERT-MU shall be the Director of CERT-MU.

(3) The Director of CERT-MU shall be assisted by a team of officers with such qualifications and experience as may be prescribed.

39. Functions of CERT-MU

The functions of CERT-MU shall be to –

(a) advise and assist the Government on the development and implementation of cybersecurity policies, strategies and best practices;

(b) coordinate cybersecurity incident response activities;

(c) provide technical assistance to law enforcement agencies in the resolution of cybersecurity incidents;

(d) disseminate cybersecurity alerts, advisories, vulnerability notes to organisations and the public;

(e) issue publications related to cybersecurity best practices;

(f) screen netflow data for detecting potential cyber threats at the level of Internet Service Providers;

(g) collect information from organisations for identifying, assessing, monitoring, and responding to cyber threats;

(h) promote cybersecurity awareness and cyber hygiene at national level;

(i) collaborate with the international CERT community, industry and regional, sectorial and international security forums for sharing information on cyber threats and related information;

(j) promote research and development in cybersecurity;

(k) participate and advise on the Council of Europe's Global Action on Cybercrime Extended project.

PART VII – INTERNATIONAL COOPERATION

40. General principles relating to international cooperation

(1) This Part shall apply in addition to, and not in derogation from, the Extradition Act and the Mutual Assistance in Criminal and Related Matters Act.

(2) The Central Authority may make a request for mutual legal assistance in any criminal matter to a foreign State for the purpose of –

(a) undertaking investigations or proceedings concerning offences related to computer systems, electronic communications or computer data;

(b) collecting evidence of an offence in electronic form;

(c) collecting evidence in electronic form of any criminal offence not limited to offences under this Act; or

(d) obtaining expeditious preservation and disclosure of data, including traffic data, real-time collection of traffic data associated with specified communications or interception of computer data or any other means, power, function or provisions under this Act.

(3) For any of the purposes listed in subsection (2)(a) to (d), a requesting State may make a request for mutual legal assistance to the Central Authority in any criminal matter.

(4) Where a request is received under subsection (3), the Central Authority may, subject to this Act and the provisions of the Extradition Act and the Mutual Assistance in Criminal and Related Matters Act and any other relevant law –

(a) grant the legal assistance requested; or

(b) refuse to grant the legal assistance requested solely on the ground that the request concerns an offence which it considers to be a tax offence in relation to the offences referred to in sections 7 to 11, 14, 15 and 20.

(5) The Central Authority may require a requesting State to –

(a) keep the contents, information and materials provided in a confidential manner;

(b) only use the contents, information and materials provided for the purpose of the criminal matter specified in the request; and

(c) use the contents, information and materials subject to such conditions as may be specified.

(6) Prior to providing any information, the Central Authority may request that it be kept confidential or only used subject to such conditions as may be specified.

(7) If the receiving Party cannot comply with such a request, it shall notify the Central Authority accordingly, which shall then determine whether the information should nevertheless be provided.

(8) Where, subject to subsections (6) and (7), a receiving party accepts the information, it shall comply with the conditions specified.

41. Spontaneous information

(1) The Central Authority may, subject to this Act and any other relevant law, without a prior request, forward to a foreign State information obtained within the framework of a Mauritian investigation where it considers that the disclosure of such information may –

(a) assist the foreign State in initiating or carrying out investigations or proceedings concerning criminal offences related to cybercrime and cybersecurity; or

(b) lead to a request for cooperation by the foreign State under this Act.

(2) Prior to providing the information under subsection (1), the Central Authority may request that such information be kept confidential or disclosed only subject to such conditions as may be specified.

(3) Where a foreign State does not comply with the conditions specified under subsection (2), the State shall forthwith notify the Central Authority.

(4) The Central Authority shall, on receipt of a notice under subsection (3), determine whether the foreign State should be provided the information requested for.

(5) The Central Authority may refuse to provide the information where the foreign State does not take the commitment to respect the conditions specified by the Central Authority.

42. Expedited preservation of stored computer data

(1) A requesting State which intends to make a request for mutual legal assistance for the search or similar access, seizure or similar securing or the disclosure of computer data, may request the Central Authority to obtain the expeditious preservation of stored computer data located within the territory of Mauritius.

(2) The requesting State shall, in its request under subsection (1), specify –

(a) the name of the authority seeking the preservation;

(b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

(c) the stored computer data to be preserved and its connection to the offence;

(d) any available information identifying the custodian of the stored computer data or the location of the computer system;

(e) the necessity of the preservation; and

(f) the intention to submit a request for mutual assistance for the search or similar access, seizure or similar securing or the disclosure of the stored computer data.

(3) (a) The Central Authority shall, on receipt of the request under this section, take appropriate measures to preserve the specified data in accordance with the procedures set out in, and powers conferred under, this Act and any other relevant legislation.

(b) The purpose of the preservation of stored computer data effected under this section shall be to enable the State to submit a request for the search or access, seizure or securing, or the disclosure of the data.

(c) The stored computer data shall be preserved for a period not exceeding 120 days.

(4) The data shall, on receipt for a request under this section, continue to be preserved pending the final decision being made with regard to that request.

43. Expedited disclosure of preserved traffic data

(1) Where, in the course of executing a request under section 41 with respect to a specified communication, the investigating agency discovers that a service provider in another State was involved in the transmission of the communication, the Central Authority shall expeditiously disclose to the requesting State a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

(2) Disclosure of traffic data under subsection (1) may only be withheld if the Central Authority considers that the execution of the request is likely to prejudice Mauritius' sovereignty, security, public order or public interest.

44. Mutual assistance regarding accessing of stored computer data

(1) A requesting State may request the Commissioner of Police, through the Central Authority, to search or similarly access, seize or similarly secure, and disclose stored computer data located within the territory of Mauritius, including computer data that are specified in section 40.

(2) For the purpose of subsection (1), the requesting State shall –

(a) provide the name of the authority conducting the investigation or proceedings to which the request relates;

(b) give a description of the nature of the criminal matter and a statement setting out a summary of the relevant facts and laws;

(c) give a description of the purpose of the request and the nature of the assistance being sought;

(d) in the case of a request to restrain or confiscate assets believed, on reasonable grounds, to be located in Mauritius, give details of the offence, particulars of the investigation or proceedings commenced in respect of the offence, and be accompanied by a copy of any relevant restraining or confiscation order;

(e) give details of any procedure that the requesting State wishes to be followed by Mauritius in giving effect to the request, particularly in the case of a request to take evidence;

(f) include a statement setting out any demands of the requesting State concerning any confidentiality relating to the request and the reasons for those demands;

(g) give details of the period within which the requesting State wishes the request to be complied with;

(h) where applicable, give details of the property, computer system or device to be traced, restrained, seized or confiscated, and of the grounds for believing that the property is believed to be in Mauritius;

(i) give details of the stored computer data, or program to be seized and its relationship to the offence;

(j) give any available information that may identify the custodian of the stored computer data or the location of the computer system or device;

(k) include an agreement on the question of the payment of the damages or costs of fulfilling the request; and

(l) give any other information that may assist in giving effect to the request.

(3) The Central Authority shall, on receiving the request under this section, take such appropriate measures as may be required to obtain necessary authorisation, including any warrants, to execute the request in accordance with this Act and any other relevant law.

(4) Where the Central Authority obtains the necessary authorisation in accordance with subsection (3), including any warrants, to execute the request, the Central Authority may seek the support and cooperation of the requesting State during such search and seizure.

(5) For the purpose of conducting the search and seizure request, the Central Authority shall, subject to section 40, provide, to the requesting State, the results of the search and details in respect of any electronic or physical evidence seized.

(6) The request shall be responded to on an expedited basis where –

(a) there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

(b) any relevant laws so require.

45. Transborder access to stored computer data with consent or where publicly available

The investigatory authority may, without the authorisation of another State, and subject to this Act –

(a) access publicly available stored computer data, regardless of where the data is located geographically; or

(b) access or receive, through a computer system in Mauritius, stored computer data located in another State, if a police officer or authorised person obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to Mauritius through that computer system.

46. Mutual assistance in real-time collection of traffic data

(1) A requesting State may request the Central Authority to provide assistance in real-time collection of traffic data associated with specified communications in Mauritius, transmitted by means of a computer system.

(2) For the purpose of subsection (1), the requesting State shall specify –

(a) the authority seeking the use of powers under this section;

(b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

(c) the name of the authority which has access to the relevant traffic data;

(d) the location at which the traffic data may be held;

(e) the intended purpose of requiring the traffic data;

(f) such information as may be required to identify the traffic data;

(g) any further details relevant to the traffic data;

(h) the reason for using powers under this section; and

(i) the terms and conditions for the use and disclosure of the traffic data to third parties.

(3) The Central Authority shall, on receipt of the request under this section, take all appropriate measures to obtain necessary authorisation, including any warrant to execute upon the request in accordance with the procedures and powers provided under this Act and any other relevant law.

(4) Where the Central Authority obtains the necessary authorisation, including any warrant to execute upon the request, the Central Authority may seek the support and cooperation of the requesting State during the collection.

(5) The Central Authority shall, upon conducting the measures under this section, and subject to section 47, provide the results to the requesting State.

47. Mutual assistance regarding interception of content data

(1) A requesting State may request the Central Authority to provide assistance in the real-time collection or recording of content data of specified communications in the territory of Mauritius transmitted by means of a computer system.

(2) When making a request under subsection (1), a requesting State shall specify –

(a) the authority seeking the use of powers under this section;

(b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

(c) the name of the authority with access to the relevant communication;

(d) the intended duration of the interception;

(e) the reason for using powers under this section; and

(f) the terms and conditions of the use and disclosure of the communication to third parties.

(3) The Central Authority shall, on receipt of the request under this section, take such appropriate measures as may be required to obtain necessary authorisation, including any warrant to execute the request in accordance with this Act and any other relevant legislation.

(4) Where the Central Authority obtains the necessary authorisation, including any warrant to execute upon the request, the Central Authority may seek the support and cooperation of the requesting State during the interception.

(5) The Central Authority shall, upon conducting the measures under this section, provide the results to the requesting State.

48. 24/7 point of contact

(1) The Commissioner of Police shall designate a 24/7 point of contact available on twenty-four-hour, seven-day-a-week basis in order to provide immediate assistance to the point of contact of another Party on an expedited basis, for the purpose of investigations or proceedings concerning criminal offences related to computer systems and computer data, or for the collection of evidence in electronic form of a criminal offence.

(2) Such assistance shall include the following measures –

(a) providing technical advice;

(b) preserving data pursuant to sections 42 and 43;

(c) collecting evidence, the provision of legal information, and locating suspects, within expeditious timelines to be defined by regulations under this Act;

(d) acquiring trained and equipped personnel in order to facilitate the operation of this Act.

(3) The 24/7 point of contact shall –

(a) facilitate or directly carry out the provision of technical advice, preservation of data, collection of evidence, giving of legal information and locating of suspects;

(b) provide technical advice in respect of stopping or tracing any cyberattack;

(c) facilitate international extradition or mutual assistance;

(d) carry out communications with other parties to the Budapest Convention on an expedited basis.

PART VIII – GENERAL PROVISIONS

49. Prosecution

No prosecution shall be instituted under this Act except on an information filed by, or with the consent of, the Director of Public Prosecutions.

50. Jurisdiction

(1) Notwithstanding any other enactment, the Intermediate Court shall have jurisdiction to try any offence under this Act or any regulations made under it and may, on conviction, impose any penalty or forfeiture provided under this Act.

(2) The Intermediate Court shall also have jurisdiction where an offence under this Act has been committed outside Mauritius –

(a) on board a Mauritian ship; or

(b) on board an aircraft registered in Mauritius.

51. Regulations

The Minister may make such regulations as he thinks fit for the purposes of this Act.

52. Extradition

Any offence under this Act shall be considered to be an extraditable crime for which extradition may be granted or obtained under the Extradition Act.

53. Forfeiture

The Court before which a person is convicted of an offence may, in addition to any other penalty imposed, order the forfeiture of any apparatus, article or device which is the subject matter of the offence or is used in connection with the commission of the offence.

54. Repeal

The Computer Misuse and Cybercrime Act is repealed.

55. Savings and transitional provisions

(1) Any order made under the repealed Computer Misuse and Cybercrime Act and which is valid before the commencement of this Act shall, on the commencement of this Act, be deemed to have been made under this Act and shall be dealt with in accordance with the relevant provisions of this Act.

(2) Any application made under the repealed Computer Misuse and Cybercrime Act and which is still pending before the commencement of this Act shall, on the commencement of this Act, be deemed to have been made under this Act and shall be dealt with in accordance with the relevant provisions of this Act.

(3) Where this section does not make any provision for any transition, the Minister may make such regulations as may be necessary for such transition.

56. Commencement

(1) Subject to subsection (2), this Act shall come into operation on a date to be fixed by Proclamation.

(2) Different dates may be fixed for the coming into operation of different sections of this Act.

Passed by the National Assembly on the nineteenth day of November two thousand and twenty one.

Bibi Safeena Lotun (Mrs)
Clerk of the National Assembly

By Authority: Government Printing Department, La Tour Koenig 173/11/2021 – 928