THE CYBERCRIMES AND OTHER RELATED CRIMES BILL, 2021

(Bill No. 49 of 2021)

OBJECTS AND REASONS

The object of this Bill is to repeal the Computer Misuse Act, CAP 254 and substitute it with a modern cybercrimes law that is effective, more up-to-date, and which is aligned to international best practice.

The Bill seeks to address and close the gaps in the types of offences relating to interference with computer data and computer system operation, unlawful possession of illegal devices, electronic fraud, computer related forgery, unauthorized disclosure of access credentials and unlawful disclosure by electronic service provider among others.

In terms of investigations and procedural powers of the investigatory authority, the Bill seeks to address the following missing components to ensure thorough analysis of the offences for better prosecution —

(a) procedures regarding the preservation of computer data for investigatory purposes and the need for a preservation order from the court;

(b) provisions for the disclosure of preserved computer data for investigations and prosecution purposes;

(c) provisions about the production of computer data for the prosecution of an offence as well as for investigation;

(d) procedures relating to the powers of the Investigatory Authority to access search and seize stored computer data for the purposes of an investigation;

(e) provisions on real- time collection of traffic data;

(f) procedures relating to orders from the court, following a request from the Investigatory Authority to remove indecent material of a

child from a computer system or any other information and communication technologies medium; and

(g) provisions regarding limited use of disclosed computer data and information, solely for the purposes of investigations and prosecution of criminal offences.

Regarding other mechanisms to ensure smooth proceedings with investigations and prosecution as well as collaboration with other authorities, the following provisions have been introduced in the Bill, and that is to say —

(a) the granting of extradition by the court for offences committed under the Bill;

(b) forfeiture of property or apparatus which is a subject matter, or was used in connection with committing an offence;

(c) spontaneous provision of information by an authority to assist with investigations;

(d) orders by the Investigatory Authority to preserve computer data obtained from another Investigatory Authority;

(e) expeditious disclosure of preserved traffic data by the requested Investigatory Authority from an electronic service provider in another country;

(f) mutual assistance regarding accessing stored computer data, subject to Article 29 of the Budapest Convention;

(g) provision for transborder access to stored computer data with consent or where publically available;

(h) mechanisms for mutual assistance in the real-time collection of traffic data and interception of content computer data;

(i) mechanisms for mutual assistance in relation to the interception of content computer data;

(j) the setting up of a network to facilitate investigation and proceedings concerning criminal offences;

(k) non-liability of electronic service providers to monitor computer data that it transmits or stores;

(l) non-criminal liability on electronic service providers for providing access to and transmitting information, based on certain conditions; and

(m) non-criminal liability on electronic service providers, based on certain conditions, for the information they store at the request of users.

Finally, the legal and regulatory impacts of this Bill once enacted will be in relation to the implementation of the targeted projects and initiatives specified in the strategic action-plan corresponding to the strategic objective pertaining to the "Legal and Regulatory Framework on Cyber Security". This includes the review and formulation of new laws as well as alignment of the different legal instruments in Seychelles to the provisions of the Budapest Convention.

Dated this 5th day of October, 2021.

FRANK D.R. ALLY
ATTORNEY-GENERAL

THE CYBERCRIMES AND OTHER RELATED CRIMES BILL, 2021

(Bill No. 49 of 2021)

ARRANGEMENT OF SECTIONS

PART I - PRELIMINARY

Sections

PART II - OFFENCES

PART III - INVESTIGATIONS AND PROCEDURES

PART IV - MISCELLANEOUS

THE CYBERCRIMES AND OTHER RELATED CRIMES BILL, 2021

(Bill No. 49 of 2021)

A BILL

FOR

AN ACT to combat criminal activities perpetrated using computer systems and for matters connected therewith or incidental thereto.

ENACTED by the President and the National Assembly.

PART I - PRELIMINARY

Short title and commencement

1. This Act may be cited as the Cybercrimes and other Related Crimes Act, 2021 and shall come into operation on such a date as the Minister may, by Notice in the Gazette, appoint.

Interpretation

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

"access" in relation to a computer system means to instruct, communicate with, store data in, retrieve data from or otherwise make use of any of the resources of a computer system;

"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 system" means any computer data processing device, or a group of such interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, performing logical, arithmetic, or storage functions, and —

(a) includes any computer data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, whether available in a single or distributed or decentralised form;

(b) any reference in this Act to any program or computer data held in a computer system includes a reference to any program or computer data held in any removable storage medium which is for the time being in the computer system; and a computer system is to be regarded as containing any program or computer data held in any such medium;

"Convention" means the Budapest Convention on Cybercrime adopted by the Committee of Ministers of the Council of Europe and entered into force on 1st July 2004;

"electronic service provider" means any public or private entity that provides to users of its service the ability to communicate by

means of a computer system, and any other entity that processes or stores computer data on behalf of such communication service or users of such service;

"investigatory authority" means the Police Force of Seychelles or any other body empowered to investigate any offence;

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

"message" means a verbal, written, recorded, drawn or picture communication sent to or left for a recipient;

"Minister" means the Minister responsible for internal Affairs;

"seize" includes —

(a) make and retain a copy of computer data, including by using on-site equipment; and

(b) render inaccessible, or remove, computer data in the accessed computer system; and

(c) take a printout of output of computer data;

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

Application of the Act

3. This Act applies to an act —

(a) that occurs wholly or partly in the territory of Seychelles;

(b) that occurs wholly or partly on a ship flying the flag of Seychelles;

(c) that occurs wholly or partly on board an aircraft registered under the laws of Seychelles; and

(d) directly or indirectly connected to, or affecting, a person, computer system or event within Seychelles.

PART II - OFFENCES

Unauthorised access to computer system

4.(1) A person who causes a computer system to perform a function with the intent to secure unauthorised access to any computer data held in a computer system, commits an offence and shall, on conviction, be liable to a fine of level 4 on the standard scale or to imprisonment for a term not exceeding 5 years or to both.

(2) For the purpose of subsection (1) —

(a) an access by a person to a computer system is unauthorised, where the person —

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

(ii) does not have consent to access of the kind in question from any person who is so entitled.

(b) for the purposes of this section, it is immaterial that the unauthorised access is not directed at —

(i) any particular program or computer data;

(ii) a program or computer data of any kind; or

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

Access with criminal intent

5.(1) A person who causes a computer system to perform any function for the purpose of securing access to any computer data held in any computer system, with criminal intent, commits an offence and shall, on conviction, be liable to a fine of level 5 on the standard scale or to imprisonment for a term not exceeding 20 years or to both.

(2) For the purposes of subsection (1), it is immaterial that —

(a) the access referred to in subsection (1) is authorised or unauthorised;

(b) the further offence to which this section applies is committed at the same time when the access is secured or at any other time.

Unauthorised interception

6.(1) A person who —

(a) intentionally intercepts or causes to be intercepted any function or non-public transmissions to, from or within, a computer system and —

(i) does so by technical means; and

(ii) does not have authority to intercept the function or transmission or to cause the interception;

(b) intentionally uses or causes to be used, directly or indirectly, a computer system for the purpose of committing an offence,

commits an offence and shall, on conviction, be liable to a fine of level 4 on the standard scale or to imprisonment for a term not exceeding 5 years or both.

(2) For the purposes of subsection (1), intercepting includes listening to or viewing, by use of technical means, or recording, a function of a computer system or acquiring the substance, meaning or purport of any such function.

Unauthorised interference with computer data

7.(1) A person who, without authority intentionally, does any of the following acts —

(a) destroys or alters computer data;

(b) renders computer data meaningless, useless, inaccessible, ineffective, unreliable, impaired;

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

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

(e) denies access to computer data to any person entitled to it; or

(f) accesses or intercepts any computer data without authority,

commits an offence shall, on conviction, be liable to a fine of level 5 on the standard scale or to imprisonment for a term not exceeding 20 years or to both.

Unauthorised interference of computer system operation

8.(1) A person who intentionally, whether directly or indirectly, and without authority —

(a) interferes with, or interrupts or obstructs the use of, a computer system; or

(b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any computer data in a computer system,

commits an offence and shall, on conviction, be liable to a fine of level 5 on the standard scale or to imprisonment for a term not exceeding 20 years or to both.

(2) For the purposes of subsection (1), interference, interruption, obstruction or impendence in relation to a computer system, includes —

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

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

(c) inputting, deleting or altering computer data.

Unlawful possession of illegal devices

9. A person who —

(a) intentionally, without justification produces, sells, procures for use, imports, exports, distributes or otherwise make available —

(i) a device, including a computer data, that is designed or adapted for the purpose of committing an offence against section 6, 7, or 8 ; or

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

(b) has any item mentioned in subparagraph (i) or (ii) of paragraph (a) in his or her possession with the intent that it be used by any person for the purpose of committing an offence against section 6, 7, or 8,

commits an offence and shall, on conviction, be liable to a fine of level 4 on the standard scale or to imprisonment for a term not exceeding 5 years or to both.

Electronic fraud

10. A person who intentionally and without right causes loss of property to another person by —

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

(b) any interference with the functioning of a computer system, with intent to procure for himself or herself or another person, an advantage or economic benefit,

commits an offence and shall, on conviction, be liable to a fine of level 4 on the standard scale or to imprisonment for a term not exceeding 10 years or to both.

Computer system related forgery

11. A person who causes loss of property to another person by any input, alteration, deletion or suppression of computer data resulting in inauthentic computer data with the intent to be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the computer data is directly readable and intelligible, commits an offence and shall, on conviction, be liable to a fine of level 5 on the standard scale or to imprisonment for a term not exceeding 20 years or to both.

Unauthorised disclosure of access credentials

12. A person who, without lawful excuse or justification, discloses, sells, procures for use, distributes or otherwise makes available, any password, access code or other means of gaining access to a computer system or computer data —

(a) for wrongful gain;

(b) for any unlawful purpose;

(c) to overcome security measures for the protection of computer data; or

(d) with the knowledge that it is likely to cause prejudice to any person,

commits an offence and shall, on conviction, be liable to a fine of level 4 on the standard scale or to imprisonment for a term not exceeding 5 years, or to both.

Cyber extortion

13. A person who performs or threatens to perform any of the acts described under this Part, for the purposes of obtaining any unlawful advantage by —

(a) undertaking to cease or desist from such actions; or

(b) undertaking to restore any damage caused as a result of those actions,

commits an offence and shall be liable, on conviction to a fine of level 4 on the standard scale or to imprisonment for a term not exceeding 5 years or to both.

Cyber harassment

14. A person who uses a computer system or who knowingly permits a device to be used, for any of the following purposes —

(a) making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent; or

(b) threatening to inflict injury or physical harm to the person or property of any person; or

(c) sending, delivering or showing a message, visual or otherwise, which is abusive, obscene, indecent, threatening, false or misleading, causing annoyance, inconvenience or is likely to cause distress or needless anxiety to any person,

commits an offence and shall, on conviction, be liable to a fine of level 4 on the standard scale or to imprisonment for a term not exceeding 5 years, or to both.

Cyber stalking

15. A person who willfully, maliciously or repeatedly uses electronic communication to harass another person, or makes a threat with the intent to place that person in reasonable fear for his or her safety or for the safety of his or her immediate family, commits an offence and shall, on conviction, be liable to a fine of level 4 on the standard scale or to imprisonment for a term not exceeding 5 years, or to both.

Offensive electronic communications

16. A person who wilfully, maliciously or repeatedly uses electronic communication of an offensive nature to disturb or attempt to disturb the peace, quiet or privacy of any person with no purpose to legitimate communication, whether or not a conversation ensues, commits an offence and shall, on conviction, be liable to a fine of level 4 on the standard scale or to imprisonment for a term not exceeding 5years, or to both.

Pornographic or obscene material

17.(1) In this section —

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

(b) "child pornography" includes material that visually or otherwise depicts —

(i) a child engaged in sexually explicit conduct,

(ii) a person who appears to be a child engaged in sexually explicit conduct, or

(iii) realistic images representing a child engaged in sexually explicit conduct; and

(c) "sexually explicit conduct" means any conduct, whether real or simulated, which involves —

(i) sexual intercourse, including genital-genital, oral-genital, anal genital or oral-anal, between children, or between an adult and a child, of the same or opposite sex,

(ii) bestiality,

(iii) masturbation,

(iv) sadistic or masochistic sexual abuse, or

(v) the exhibition of the genitals or pubic area of a child.

(2) A person who —

(a) publishes child pornography or obscene material relating to children through a computer system;

(b) produces child pornography or obscene material relating to children for the purpose of its publication through a computer system;

(c) possesses child pornography or obscene material relating to children in a computer system or on a computer data storage medium;

(d) publishes or causes to be published an advertisement likely to be understood as conveying that the advertiser distributes or shows child pornography or obscene material relating to children; or

(e) accesses child pornography or obscene material relating to children through a computer system,

commits an offence and shall, on conviction, be liable to a fine of level 4 on the standard scale or to imprisonment for a term not exceeding 5years, or to both.

(3) A person who, by means of a computer system, communicates with a person who is, or who the accused believes is —

(a) under the age of 18 years, for the purpose of facilitating the commission of the offence of child pornography under this Act, or the offences of prostitution, rape or indecent assault under the Penal Code;

(b) under the age of 16 years, for the purpose of facilitating the commission of the offences of abduction or kidnapping of that person under the Penal Code; or

(c) under the age of 16 years, for the purpose of facilitating the commission of any sexual offence with that person under the Penal Code,

commits an offence and shall, on conviction, be liable to a fine of level 4 on the standard scale or to imprisonment for a term not exceeding 5 years, or to both.

(4) Evidence that the person in subsection (3)(*a*), (*b*) or (*c*) was represented to the accused as being under the age of 18 years or 16 years shall be, in absence of evidence to the contrary, proof that the accused believed that the person was under that age.

(5) It shall not be a defence to a charge under subsection (3) that the accused believed that the person he or she was communicating with was at least 16 or 18 years of age, as the case may be, unless the accused took reasonable steps to ascertain the age of the person.

(6) For the purposes of subsection (3), it does not matter that the person in subsection (3)(*a*), (*b*) or (*c*) is a fictitious person, represented to the accused as a real person.

Pornographic publication

18. A person who, by means of a computer system, discloses or publishes a private sexual photograph or film without the consent of the person who appears in the photograph or film commits an offence and shall, on conviction, be liable to a fine of level 4 on the standard scale or to imprisonment for a term not exceeding 5 years, or to both.

Unlawful disclosure by electronic service provider

19. An electronic service provider who, without lawful authority, discloses —

(a) that an order under this Act has been made;

(b) any act done under an order; or

(c) any computer data collected or recorded under an order,

commits an offence and shall, on conviction, be liable to a fine of level 4 on the standard scale or to imprisonment for a term not exceeding 5 years, or to both.

PART III - INVESTIGATIONS AND PROCEDURES

Preservation order

20.(1) An investigatory authority may order for the expeditious preservation of computer data that has been stored by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such computer data is vulnerable to loss or modification.

(2) For the purposes of subsection (1), computer data includes traffic data.

(3) An order made under subsection (1) shall remain in force for a period not exceeding 90 days.

(4) Where the computer data is required to be preserved beyond 90 days, the investigatory authority shall make an application to the Court and the Court may make such order for preservation of the computer data as it may deem fit.

(5) The powers and procedures for the purposes of subsections (1), (2) and (3) shall apply to all offences under this Act.

Disclosure of preserved computer data

21.(1) The investigatory authority may, for the purposes of an investigation or the prosecution of an offence order for the disclosure of —

(a) all preserved traffic computer data, irrespective of whether one or more electronic service providers were involved in the transmission of such computer data;

(b) sufficient traffic computer data to identify the electronic service providers and the path through which the computer data was transmitted.

(2) The powers and procedures for the purposes of subsection (1) apply to all offences under this Act.

Production Order

22.(1) Where the disclosure of computer data is required for the purposes of an investigation or the prosecution of an offence, an investigatory authority may apply to the court for a Production Order compelling —

(a) any person to submit specified computer data in that person's possession or control, which is stored in a computer system or computer data storage medium;

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

(2) Where any material to which an investigation relates consists of computer data stored in a computer system, disc, cassette, or on microfilm, or preserved by any mechanical or electronic device, 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 visible and legible.

Powers of access, search and seizure for purposes of investigation

23.(1) Where an investigatory authority has reasonable grounds to believe that stored computer data would be relevant for the purposes of an investigation or the prosecution of an offence, it may apply to the court for the issue of a warrant to search or access, search or secure computer data —

(a) to secure computer data under subsection (1), the powers of the investigatory authority shall include the power to —

(i) search, seize or secure a computer system or any information and communication technologies medium;

(ii) make and retain a copy of such computer data or information;

(iii) maintain the integrity of the relevant stored computer data or information; or

(b) render inaccessible or remove the stored computer data or information from the computer system, or any information and communication technologies medium.

Real time collection of traffic data

24. Where the investigatory authority has reasonable grounds to believe that any computer data would be relevant for the purposes of an investigation or the prosecution of an offence, it may apply to the court for an order —

(a) allowing the collection or recording of traffic data, in real time, associated with specified communications transmitted by means of any computer system; or

(b) compelling an electronic service provider, within its technical capabilities, to effect such collection and recording referred to in paragraph (a), or assist the investigatory authority to effect such collection and recording.

Deletion order

25.(1) The court may, upon application by an investigatory authority, and being satisfied that a computer system or any other information and communication technologies medium contains an indecent material of a child, order that such computer data be —

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

(b) deleted or destroyed.

(2) For the purposes of this section, "indecent material" means —

(a) any indecent or obscene writing, photograph, sketch, drawing or picture including whether partly or wholly generated by computer;

(b) any indecent or obscene printed matter, print, painting, poster drawing, model or cinematographic film or video film, cassette or disc; or

(c) any other indecent or obscene object.

Limited use of disclosed computer data and information

26. No information on computer data under sections 21 to 24 shall be used for any purpose other than that for which the computer data was originally sought, except —

(a) in accordance with any other written law;

(b) in compliance with an order of court;

(c) where such computer data is required for the purpose of preventing detecting or investigating offences, apprehending or prosecuting offenders, assessing or collecting tax, duties or other monies owed or payable to the Government; or

(d) for the prevention of injury or other damage to the health of a person or serious loss of or damage to property.

PART IV - MISCELLANEOUS

Punishment for non compliance of an order section 20, 21, 22 or 25 or contravention of section 26

27. A person who —

(a) fails to comply with a preservation order under section 20 or an order for the disclosure under section 21, a protection order under section 22; or a deletion order under section 25; or

(b) uses any computer data in contravention of section 26,

commits an offence and shall, on conviction, be liable to a fine of level 4 on the standard scale or to imprisonment for a term not exceeding 5 years, or to both.

Jurisdiction

28.(1) Notwithstanding any other written law, the Supreme Court shall have jurisdiction to try an offence under this Act or any regulations made thereunder and may, on conviction, impose any penalty or forfeiture provided for under this Act.

(2) The Supreme Court shall have jurisdiction where the act constituting an offence under this Act has been committed outside Seychelles —

(a) on board a Seychelles ship; or

(b) on board an aircraft registered in Seychelles.

Extradition

29. Any offence under this Act may, with the consent of the Attorney General, be an extraditable crime for which extradition may be granted or obtained under the Extradition Act (*Cap 78*)

Forfeiture

30. A 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 thing which is the subject matter of the offence or is used in connection with the commission of the offence.

Spontaneous information

31.(1) An authority may without prior request, forward to the investigatory authority information obtained within the framework of its own investigation when it considers that the disclosure of such information might assist in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Act.

(2) Prior to the disclosure of computer data under subsection (1) —

(a) the authority may request the investigatory authority to maintain the confidentiality of the information provided; and

(b) where the investigatory authority cannot comply with such request, it shall notify the authority, which may then determine whether the information should nevertheless be provided.

(3) For the purposes of this section, "authority" means any public body, agency, organ or department established by law.

Expedited preservation of stored computer data

32.(1) An investigatory authority may order for the expeditious preservation of computer data that has been stored by means of a computer system, located within or outside its territory where a mutual assistance request has been obtained from another investigatory authority for the search

or similar access, seizure or similar securing, or disclosure of the computer data.

(2) A request for preservation made under subsection (1) shall specify —

(a) the investigatory authority seeking the preservation;

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

(c) the stored computer data to be preserved and its relationship 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) that the investigatory authority intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

(3) Upon receiving the request from another investigatory authority, the requested authority shall take all appropriate measures to preserve expeditiously the specified computer data in accordance with its domestic law.

(4) For the purposes of responding to a request under this section, dual criminality shall not be required as a condition for providing such preservation.

(5) An investigatory authority that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored computer data may, in respect of offences, reserve the right to refuse the request for preservation under this Act in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

(6) A request for preservation may be refused where —

(a) the compliance with the request would be contrary to the Constitution;

(b) it is of prejudice to the sovereignty, international relations, security, public order, or other public interest of Seychelles;

(c) in the reasonable belief the request for assistance has been made for the purpose of prosecuting a person on account of that person's race, sex, religion, nationality, ethnic origin or political opinions, or that a person's position may be prejudiced for any of those reasons;

(d) in absence of dual criminality, where granting the request would require a court in Seychelles to make an order in respect of any person or property, in respect of conduct which does not constitute an offence, nor gives rise to a confiscation or restraining order, in Seychelles;

(e) the request relates to an offence under military law, or a law relating to military obligations, which would not be an offence under ordinary criminal law;

(f) the request relates to a political offence or an offence of a political character;

(g) the request relates to an offence, the prosecution of which, in the foreign State, would be incompatible with laws of Seychelles on double jeopardy;

(h) the request requires Seychelles to carry out measures that are inconsistent with its laws and practice, or that cannot be taken in respect of criminal matters arising in Seychelles; or granting the request in whole or in part, on the ground that granting the request immediately would be likely to prejudice the conduct of proceedings in Seychelles.

(7) Any preservation effected in response to the request referred to in subsection (1) shall be for a period of not less than sixty days, in order to enable

the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the computer data, following the receipt of such request, the computer data shall continue to be preserved pending a decision on that request.

Expeditious disclosure of preserved traffic data

33.(1) Where, in the course of the execution of a request made to subject to Article 29 of the Convention to preserve traffic data concerning a specific communication, the requested investigatory authority discovers that an electronic service provider in another State was involved in the transmission of the communication, the requested investigatory authority shall expeditiously disclose to the requesting investigatory authority a sufficient amount of traffic data to identify that electronic service provider and the path through which the communication was transmitted.

(2) The disclosure of traffic data under subsection (1) may be withheld where —

(a) the compliance with the request would be contrary to the Constitution;

(b) it is of prejudice to the sovereignty, international relations, security, public order, or other public interest of Seychelles;

(c) in the reasonable belief that the request for assistance has been made for the purpose of prosecuting a person on account of that person's race, sex, religion, nationality, ethnic origin or political opinions, or that a person's position may be prejudiced for any of those reasons;

(d) in the absence of dual, criminality, accepting the request would require a court in Seychelles to make an order in respect of any person or property in respect of conduct which does not constitute an offence, nor gives rise to a confiscation or restraining order, in Seychelles;

(e) the request relates to an offence under military law, or a law relating to military obligations, which would not be an offence under ordinary criminal law;

(f) the request relates to a political offence or an offence of a political character;

(g) the request relates to an offence, the prosecution of which, in the foreign State, would be incompatible with laws of Seychelles on double jeopardy;

(h) the request requires Seychelles to carry out measures that are inconsistent with its laws and practice, or that cannot be taken in respect of criminal matters arising in Seychelles; or granting the request in whole or in part, on the ground that granting the request immediately would be likely to prejudice the conduct of proceedings in Seychelles.

Mutual assistance regarding accessing of stored computer data

34.(1) An investigatory authority may request another investigative authority to search or similarly access, seize or similarly secure, and disclose computer data stored by means of a computer system located within the territory of the requested Party, including computer data that has been preserved subject to Article 29 of the Convention.

(2) The requested investigatory authority may respond to the request through the application of international instruments, arrangements and laws subject to Article 23 of the Convention, and in accordance with other relevant provisions of this Act.

(3) The request shall be responded to on an expedited basis where —

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

(b) the instruments, arrangements and laws referred to in subsection (2) otherwise provide for expedited co-operation.

Trans-border access to stored computer data with consent or where publicly available

35. An investigatory authority may, without the authorisation of another authority —

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

(b) access or receive, through a computer system in its territory, stored computer data located in another investigatory authority,

where the investigation authority obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the computer data to the investigation authority through that computer system.

Mutual assistance in the real-time collection of traffic data

36.(1) The investigatory authorities shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system, subject to the provisions of subsection (2), this assistance shall be governed by the conditions and procedures provided for under the laws of Seychelles.

(2) The assistance under subsection (1) shall be governed by the conditions and procedures provided for under the laws of Seychelles.

(3) Each investigatory authority shall provide such assistance at least with respect to offences for which real-time collection of traffic data would be available in a similar domestic case.

Mutual assistance regarding the interception of content computer data

37. The investigatory authority shall provide mutual assistance to each other in the real-time collection or recording of content computer data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and the laws of Seychelles.

Networking

38.(1) A point of contact shall be established on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate

assistance 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 and such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the measures for —

(a) the provision of technical advice;

(b) the preservation of computer data pursuant to Articles 29 and 30 of the Convention;

(c) the collection of evidence, the provision of legal information, and locating of suspects.

(2) An investigatory authority's point of contact shall have the capacity to carry out communications with the point of contact of another authority on an expedited basis.

(3) Where the point of contact designated by an investigatory authority is not responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

(4) An investigatory authority shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Obligation to monitor transmitted or stored computer data

39.(1) When providing the services there is no general obligation on an electronic service provider to monitor that computer data which it transmits or stores; or actively seek facts or circumstances indicating an unlawful activity.

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

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

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

Criminal liability for providing access and transmitting information

40.(1) An electronic service provider is not criminally liable for providing access and transmitting information on condition that the provider —

(a) does not initiate the transmission;

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

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

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

Criminal liability for storing at the request of user

41.(1) An electronic service provider is not criminally liable for the information stored at the request of a user of the service, on condition that —

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

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

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

(3) If the electronic service provider is removing the content after receiving an order pursuant to subsection (1), the provider is exempted from contractual obligations with his customer to ensure the availability of the service.

(4) An electronic service provider is not criminally liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other users of the service upon their request, on condition that —

(a) the electronic service provider does not modify the information;

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

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

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

(e) the electronic service provider acts expeditiously to remove or to disable access to the information it has stored upon knowledge of the fact that the information at the initial sources of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

(5) An electronic service provider who enables the access to

information provided by third person by providing an electronic hyperlink is not liable for the information if the electronic service provider —

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

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

(6) An electronic service provider who makes or operates a search engine that either automatically or based on entries by others creates and index of internet-related content or make available electronic tools to search for information provided by third party is not liable for search results on condition that the provider —

(a) does not initiate the transmission;

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

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

Application of certain provisions of the Penal Code

42. Sections 25, 30 and 30A of the Penal Code shall, unless the court determines otherwise, apply to a person convicted of an offence under this Act.

Regulations

43. The Minister may make regulations for carrying into effect the purposes and provisions of this Act.

Repeal of Cap 254

44. The Computer Misuse Act Cap 254 is hereby repealed.

Savings provisions

45. Notwithstanding the repeal under section 43 —

(a) anything made, given, issued or done under the repealed Act shall have the same effect as if it was made, given, done or issued under this Act;

(b) any application made to a court under the repealed Act shall continue to be dealt with and determined as if it was made under this Act; and

(c) any legal proceedings which, before the coming into force of this Act were pending, shall be continued or enforced I the same manner as they would have continued or enforced before the coming into force of this Act.