2023-11-17

OBJECTS AND REASONS

This Bill would provide for

(a) the combatting of cybercrime;

(b) the protection of legitimate interests in the use and development of information technologies;

(c) the facilitation of international co-operation in computer related crimes;

(d) the repeal of the *Computer Misuse Act*, Cap. 124B; and

(e) related matters.

Arrangement of Sections

PART I

PRELIMINARY

1. Short title

2. Interpretation

3. Application

PART II

PROHIBITED CONDUCT

4. Illegal access

5. Modification of programme or data

6. Interfering with programme or data

7. Interfering with computer system

8. Illegal interception of data

9. Misuse of devices

10. Access with intent to commit further offence

11. Disclosure of access code

12. Critical information infrastructure system

13. Receiving or giving of access to computer programme or data

14. Computer-related forgery

15. Computer-related fraud

16. Child pornography

17. Child grooming

18. Online child sexual abuse

19. Malicious communications

20. Cyber bullying

21. Cyber terrorism

22. Aiding or abetting

PART III

INVESTIGATION AND ENFORCEMENT

23. Search and seizure

24. Assisting a police officer

25. Record of seized data to be provided to owner

26. Production of data for criminal proceedings

27. Expedited preservation and partial disclosure of traffic data

28. Preservation of data for criminal proceedings

29. Order for payment of compensation

30. Regulations.

31. Consequential amendments

32. Repeal

33. Commencement

SCHEDULE

CONSEQUENTIAL AMENDMENTS

BARBADOS

A Bill entitled

An Act to provide for the combatting of cybercrime, protection of legitimate interests in the use and development of information technologies, the facilitation of international co-operation in computer related crimes and related matters.

ENACTED by the Parliament of Barbados as follows:

PART I

PRELIMINARY

Short title

1. This Act may be cited as the *Cybercrime Act, 2023.*

Interpretation

2.(1) In this Act,

"approved person" means a person who has the relevant training and skill in computer systems and technology, who has knowledge about the functioning of the computer system and is identified, in writing, by the Commissioner of Police or other gazetted officer designated by the Commissioner, to assist the police;

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

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

"computer programme" or "programme" means data or a portion of data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

"computer system" means a device or a group of inter-connected or related devices, one or more of which, pursuant to a programme, facilitates communication, performs automatic processing of data or any other function;

"damage" includes

(a) any impairment to the integrity of a computer system or the integrity or availability of any data or programme held in a computer system; and

(b) the impairment of the confidentiality of data or programme held in a computer system;

"intercept" includes, in relation to a computer system, listening to, monitoring or surveillance of or recording a function of a computer system, or acquiring the substance, meaning or purport of the function;

"service provider" means

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

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

"ship" means a vessel which is designed, used or capable of being used solely or partly for navigation in, on, through, or immediately above the water, without regard to method or lack of propulsion and includes a maritime autonomous surface ship;

"traffic data" means computer data that

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

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

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

(2) For the purposes of this Act, access of any kind by a person to any computer system, programme or data is obtained without authority if he knows that he is

not entitled to access of the kind in question relating to the computer system, programme or data and

(a) he accesses the computer system, programme or data; or

(b) he exceeds any right or permission to access the computer system, programme or data from any person who may permit such access.

(3) A reference in this Act to any "programme or data" held in a computer system includes a reference to

(a) any programme or data held in any removable storage medium which is for the time being in the computer system; or

(b) any programme or data held in any storage medium which is external to the computer system, but which is connected to it.

(4) For the purposes of this Act, a modification of the contents of any computer system takes place if, by the operation of any function of the computer system concerned or of any other computer system

(a) any programme or data held in the computer system is altered or erased;

(b) any programme or data is added to any programme or data held in the computer system; or

(c) any act occurs which impairs the normal operation of any computer system,

and any act which contributes towards such a modification shall be regarded as causing it.

(5) Any modification referred to in subsection (4) is without authority if the person whose act causes the modification

(a) knows that he is not entitled to determine whether the modification should be made; and

(b) has not obtained the consent of the person who is entitled to consent to the modification.

(6) A reference in this Act to a programme includes a reference to a part of a programme.

Application

3.(1) This Act applies to an act done or an omission made

(a) in Barbados;

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

(c) by a national of Barbados outside the territory of Barbados, if the person's conduct would also constitute an offence under the law of a country where the offence was committed.

(2) For the purpose of paragraph *(a)* of subsection (1), an act is carried out in Barbados if

(a) the person is in Barbados when the act is committed; or

(b) the person is outside Barbados at the time when the act is committed but

(i) a computer system located in Barbados or electronic data storage medium located in Barbados is affected by, or contains information about the act; or

(ii) transmission or effect of the act, or the damage resulting from the act, occurs in whole or in part within Barbados.

(3) The *Mutual Assistance in Criminal Matters Act*, Cap. 140A shall apply to this Act in relation to an offence under this Act as if the offence were a serious offence within the meaning of section 2 of that Act.

PART II

PROHIBITED CONDUCT

Illegal access

4.(1) A person who intentionally or recklessly and without authority,

(a) gains access to the whole or any part of a computer system;

(b) causes a programme to be executed; or

(c) uses a programme to gain access to any data,

is guilty of an offence and is liable on conviction on indictment to a fine of $50 000 or to imprisonment for a term of 5 years or to both.

(2) For the purposes of subsection (1), the form in which any programme or data is accessed or obtained and, in particular, whether or not it represents a form in which it is capable of being executed is immaterial.

Modification of programme or data

5.(1) A person who intentionally or recklessly and without authority causes any modification to a programme or data is guilty of an offence and is liable on conviction on indictment to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

(2) For the purposes of subsection (1), the act in question need not be directed at

(a) any specifically identifiable programme or data or type of programme or data; or

(b) any programme or data that is held in a specifically identifiable computer system.

(3) For the purposes of subsection (1), it is immaterial whether the modification is or is intended to be permanent or temporary.

Interfering with programme or data

6.(1) A person who intentionally or recklessly and without authority,

(a) copies or moves a programme or data

(i) to any storage medium other than that in which that programme or data is held; or

(ii) to a different location in the storage medium in which that programme or data is held;

(b) destroys or erases a programme or data;

(c) damages a programme or data;

(d) suppress a programme or data;

(e) adds, deletes or alters a programme or data;

(f) renders a programme or data meaningless, useless or ineffective;

(g) obstructs, interrupts or interferes with the lawful use of a programme or data; or

(h) denies access to a programme or data,

is guilty of an offence and is liable on conviction on indictment to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

(2) Subsection (1) applies whether the person's act is of temporary or permanent effect.

(3) For the purposes of subsection (1), the form in which a programme or data is copied and, in particular, whether or not it represents a form in which it is capable of being executed is immaterial.

Interfering with computer system

7. A person who intentionally or recklessly and without authority,

(a) hinders the functioning of a computer system by

(i) causing electromagnetic interference to a computer system;

(ii) accessing or causing access to a computer system; or

(iii) corrupting a computer system by any means; or

(b) interferes with the functioning of a computer system,

is guilty of an offence and is liable on conviction on indictment to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

Illegal interception of data

8. A person who intentionally and without authority, undertakes an act to intercept by technical means any non-public transmission to, from or within a computer system, including electromagnetic emissions from a computer system carrying computer data, is guilty of an offence and is liable on conviction on indictment to a fine of $100 000 or to imprisonment for a term of 10 years or to both.

Misuse of devices

9. A person who intentionally or recklessly and without authority,

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

(i) a device, including a computer programme, that is primarily designed or adapted for the purpose of committing an offence; or

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

accessed, with the intent that it be used by any person for the purpose of committing an offence; or

(b) has an item mentioned in paragraph (*a*)(i) or (ii) in his possession with the intent that it be used by himself or any other person for the purpose of committing an offence,

is guilty of an offence and is liable on conviction on indictment to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

Access with intent to commit further offence

10. A person who intentionally and without authority uses a computer system to perform any function in order to secure access to any programme or data held in that computer system or in any other computer system with the intention to commit a further offence is guilty of an offence and is liable on conviction on indictment to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

Disclosure of access code

11.(1) A person who intentionally or recklessly and without authority discloses any password, access code or any other means of gaining access to any programme or data held in a computer system is guilty of an offence and is liable on summary conviction to a fine of $25 000 or to imprisonment for a term of 3 years or to both.

(2) A person who intentionally or recklessly and without authority discloses any password, access code or any other means of gaining access to any programme or data held in a computer system for any unlawful gain, whether to himself or to another person, knowing that it is likely to cause unlawful damage, is guilty of an offence and is liable on conviction on indictment to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

Critical information infrastructure system

12.(1) For the purposes of this section "critical information infrastructure system" means any computer system, programme or data that supports or performs a function that relates to

(a) electricity generation or distribution**;**

(b) telecommunications;

(c) government services;

(d) emergency services;

(e) law enforcement, security or intelligence agencies;

(f) public works; or

(g) any computer system, programme or data that may be designated as a critical information infrastructure system by the Minister responsible for the prevention of cybercrime, published in the *Official Gazette*,

that is so vital that the incapacity or destruction of such computer system, programme or data would have a debilitating impact on the security, national economic security, national public health or safety or any combination of those matters, in Barbados.

(2) A person who without authority,

(a) gains access to; or

(b) interferes with

a critical information infrastructure system is guilty of an offence and is liable on conviction on indictment to a fine of $100 000 or to imprisonment for a term of 10 years or to both.

(3) A person who without authority gains access to or interferes with a critical information infrastructure system in the course of the commission of any offence

is liable on conviction on indictment to a fine of $150 000 or to imprisonment for a term of 12 years or to both.

(4) It shall be a defence to a charge brought under subsection (2) or (3) to prove that access to or interference with a critical information infrastructure system was obtained inadvertently and with no intent to commit an offence.

Receiving or giving of access to computer programme or data

13.(1) A person who

(a) intentionally or recklessly and without authority receives or is given access to any programme or data; and

(b) knows or believes that

(i) the programme or data was obtained without authority; or

(ii) access to the programme or data was obtained without authority,

is guilty of an offence and is liable on conviction on indictment to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

(2) It shall be a defence to a charge brought under subsection (1) to prove that the programme or data or access to the programme or data

(a) was received inadvertently and with no intent to commit an offence;

(b) was subject to legal privilege; and

(c) was received by a law enforcement officer in the course of an investigation.

Computer-related forgery

14. A person who intentionally and without authority, inputs, alters, deletes or suppresses a programme or data that results in inauthentic data being considered or acted on for any legal purpose as if it were authentic, whether or not the data is directly readable and intelligible, is guilty of an offence and liable

on conviction on indictment to a fine of $100 000 or to imprisonment for a term of 10 years or to both.

Computer-related fraud

15. A person who intentionally, fraudulently or dishonestly and without authority, inputs, alters, deletes or suppresses any computer data or interferes with the functioning of a computer system for the purpose of

(a) procuring an economic benefit for himself or another person;

(b) causing loss of property to a person;

is guilty of an offence and is liable on conviction on indictment to a fine of $100 000 or to imprisonment for a term of 10 years or to both.

Child pornography

16.(1) A person who intentionally or recklessly

(a) publishes child pornography through a computer system;

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

(c) possesses child pornography in a computer system or on a computer data storage medium for the purpose of publication; or

(d) procures child pornography through a computer system for himself or for another person,

is guilty of an offence and is liable on conviction on indictment

(i) in the case of an individual to a fine of $100 000 or to imprisonment for a term of 10 years or to both; or

(ii) in the case of a corporation, to a fine of $250 000.

(2) It shall be a defence to a charge brought under subsection (1) if the person establishes that the child pornography was for a *bona fide* research, medical or law enforcement purpose.

(3) For the purposes of subsection (1),

(a) “child” means a person under the age of 18 years;

(b) "child pornography" includes material that visually 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) "publish" includes

(i) distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way;

(ii) have in possession or custody, or under control, for the purpose of doing an act referred to in paragraph *(b)*; or

(iii) print, photograph, copy or make in any other manner, whether of the same or of a different kind or nature, for the purpose of doing an act referred to in paragraph *(b)*.

Child grooming

17. A person who intentionally or recklessly uses a computer system to befriend, manipulate, communicate with or establish a connection with a child in order to abuse the child, whether sexually or otherwise, is guilty of an offence and is liable on conviction on indictment

(a) in the case of an individual to a fine of $100 000 or to imprisonment for a term of 10 years or to both; or

(b) in the case of a corporation, to a fine of $250 000.

Online child sexual abuse

18.(1) A person who intentionally or recklessly uses a computer system to meet a child for the purpose of

(a) engaging in sexual activity with a child;

(b) engaging in sexual activity with the child where

(i) coercion, inducement, force or threat is used;

(ii) a recognised position of trust, authority or influence over the child, including within the family is abused; or

(iii) a child's mental or physical disability or situation of dependence is abused

is guilty of an offence.

(2) A person who is guilty of an offence under subsection (1) is liable on conviction on indictment

(a) in the case of an individual to a fine of $100 000 or to imprisonment for a term of 10 years or to both; or

(b) in the case of a corporation to a fine of $250 000.

Malicious communications

19.(1) A person who intentionally or recklessly uses a computer system to publish, broadcast or transmit computer data that

(a) intimidates a person; or

(b) threatens to

(i) use violence towards a person or a member of his family; or

(ii) damage the property of a person or the property of his family,

is guilty of an offence and is liable on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

(2) A person who intentionally or recklessly uses a computer system

(a) to publish, broadcast or transmit data that includes private sexual photographs and videos without the consent of a person who appears in them, with intent to humiliate, harass or cause substantial emotional distress to that person; or

(b) to send repeatedly to another person data that is obscene, vulgar, profane, lewd or indecent with intent to humiliate or harass the other person to the detriment of that person's health, emotional well-being, self-esteem or reputation,

is guilty of an offence and is liable on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

(3) A person who intentionally uses a computer system to disseminate any image or words, not caring whether they are true or false, and causes or is likely to cause or subject a person to ridicule, contempt or embarrassment, is guilty of an offence and is liable on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

(4) For the purposes of subsection (1),

(a) "intimidate" means to cause

(i) in the mind of a reasonable person injury to himself, any member of his family or any of his dependants;

(ii) in the mind of a reasonable person an apprehension of violence or damage to any person or property; or

(iii) a person substantial emotional distress;

(b) "injury" includes injury or damage to a person in respect of his business, occupation, profession, employment or other source of income.

(5) The defences of truth, comment, triviality and privilege, whether absolute or qualified, provided for under the *Defamation Act*, Cap. 199 shall extend to a prosecution under subsection (3).

Cyber bullying

20.(1) A person who intentionally uses a computer system

(a) to publish, broadcast or transmit data that is offensive, pornographic, indecent, vulgar, profane, obscene or of a menacing character or causes any such data to be so sent;

(b) for the purpose of causing annoyance, inconvenience, danger, obstruction, embarrassment, insult, injury, humiliation, intimidation, hatred, anxiety or causes substantial emotional distress to that person,

is guilty of an offence and is liable on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

(2) Notwithstanding subsection (1) a person shall not be deemed to have committed an offence if he does an act

(a) for a *bona fide* scientific or medical research or law enforcement; or

(b) in compliance of and in accordance with the terms of a court order issued in exercise of any power under this Act or any law.

Cyber terrorism

21.(1) A person who intentionally uses or causes to be accessed a computer system for the purpose of terrorism is guilty of an offence and is liable on conviction on indictment to imprisonment for a term of 25 years.

(2) For the purposes of this section, “terrorism” has the meaning assigned to it in section 3 of the *Anti-Terrorism Act*, Cap. 158.

Aiding or abetting

22. A person who aids or abets the commission of an offence under this Act is guilty of that offence and is liable to the penalty of that offence.

PART III

INVESTIGATION AND ENFORCEMENT

Search and seizure

23.(1) Where a Judge or magistrate is satisfied, on information on oath given by a police officer, that there are reasonable grounds for suspecting that an offence has been, is being or is about to be committed in any place and that there is evidence that such an offence has been, is being or is about to be committed in that place, the magistrate may issue a warrant authorising any police officer to enter and search that place, including any computer system, using such reasonable force as is necessary.

(2) A warrant issued under this section may authorise a police officer to

(a) seize or similarly secure any computer system, data, programme, information, document or thing if he reasonably believes that it is evidence that an offence has been or is about to be committed;

(b) inspect and check the operation of any computer system referred to in paragraph *(a)*;

(c) use or cause to be used any computer system referred to in paragraph *(a)* to search any programme or data held in or available to such computer system;

(d) have access to any information, code or technology which has the capability of transforming or converting an encrypted programme or data held in or available to the computer system into readable and

comprehensible format or text, for the purpose of investigating any offence;

(e) convert an encrypted programme or data held in another computer system at the place specified in the warrant, where there are reasonable grounds for believing that computer data connected with the commission of the offence may be stored in that other system;

(f) make and retain a copy of any programme or data held in the computer system referred to in paragraph *(a)* or *(e)* and any other programme or data held in the computer system;

(g) maintain the integrity of the relevant stored computer data; and

(h) render inaccessible or remove computer data from the computer system.

(3) Where a Judge or magistrate is satisfied on the basis of an application by the Commissioner of Police or other gazetted officer that specified computer data or other information is required for the purpose of a criminal investigation or criminal proceedings, the Judge or magistrate may order a person who has knowledge about the functioning of a 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 in subsections (1) and (2).

(4) A warrant issued under this section shall authorise an approved person or a person who has knowledge about the functioning of a computer system or measures applied to protect the computer data to assist a police officer in the execution of the warrant.

(5) A person who obstructs a police officer in the execution of his duty under this section or who fails to comply with a request under this section is guilty of an offence and is liable on summary conviction to a fine of $25 000 or to imprisonment for a term of 2 years or to both.

(6) For the purposes of this section,

"encrypted programme or data" means a programme or data which has been transformed from its plain text version to an unreadable or incomprehensible format, regardless of the technique utilised for such transformation and irrespective of the medium in which such programme or data occurs or can be found, for the purpose of protecting the content of such programme or data;

"plain text version" means a programme or original data before it has been transformed to an unreadable or incomprehensible format.

Assisting a police officer

24.(1) A person who

(a) is in possession or control of a computer data storage medium or computer system; or

(b) has knowledge about the functioning of a computer system or measures applied to protect the computer data therein,

that is the subject of a search or a seizure, shall assist a police officer in the execution of a warrant issued under section 23.

(2) The assistance referred to in subsection (1) may include the following:

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

(b) obtaining and copying computer data referred to in paragraph *(a)*;

(c) using equipment to make copies;

(d) obtaining access to decryption information necessary to decrypt computer data required for the purpose of investigating the commission of the offence;

(e) obtaining an intelligible output from a computer system in a plain text format that can be read by a person;

(f) maintaining the integrity of the computer data; and

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

(3) A person who fails without lawful excuse or justification to assist a police officer in accordance with subsection (1) is guilty of an offence and is liable on summary conviction to a fine of $25 000 or to imprisonment for a term of 2 years or to both.

(4) A person who seeks to prevent or prevents another person from assisting a police officer in the execution of a warrant issued under section 23 is guilty of an offence and is liable on summary conviction to a fine of $25 000 or to imprisonment for a term of 2 years or to both.

(5) For the purposes of this section, "decryption information" means information or technology that enables a person to readily transform an encrypted programme or data from its unreadable and incomprehensible format to its plain text version.

Record of seized data to be provided to owner

25.(1) Where a computer system or computer data has been removed or rendered inaccessible to the owner or person who has control of the system following a search or a seizure under section 23, the person who made the search shall, at the time of the search or as soon as practicable after the search,

(a) make a list of what has been seized or rendered inaccessible, with the date and time of the seizure; and

(b) give a copy of that list to

(i) the owner of the computer system or computer data;

(ii) the occupier of the premises; or

(iii) the person in control of the computer system or computer data.

(2) Subject to subsection (3), a police officer or an approved person shall, on request,

(a) permit a person who had the custody or control of the computer system, or someone acting on behalf of that person, to gain access to and copy computer data on the system; or

(b) give the person referred to in paragraph *(a)*, a copy of the computer data.

(3) A police officer or an approved person may refuse to give access to or provide copies of computer data referred to in subsection (2) if he has reasonable grounds for believing that giving the access or providing the copies

(a) would constitute a criminal offence; or

(b) would prejudice

(i) the investigation in connection with which the search and seizure was carried out;

(ii) another investigation connected to the one in respect of which the search and seizure was carried out; or

(iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations.

Production of data for criminal proceedings

26.(1) Where a Judge or magistrate is satisfied on the basis of an application by a police officer that specified computer data or other information is required for the purpose of a criminal investigation or criminal proceedings, the Judge or magistrate may order that

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

(b) a service provider offering services in Barbados produce subscriber information relating to such services that is in the service provider's possession or control.

(2) A person referred to in subsection (1) who discloses without authority any information in his possession or under his control is guilty of an offence and is liable on conviction on indictment,

(a) in the case of an individual, to a fine of $70 000 or to imprisonment for a term of 7 years or to both; or

(b) in the case of a corporation, to a fine of $250 000.

(3) For the purposes of subsection (1), "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services, other than traffic or content data, which can establish

(a) the type of communication service used;

(b) the technical provisions taken relating to the communication service;

(c) the period of service;

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

(e) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Expedited preservation and partial disclosure of traffic data

27. Where a Judge or magistrate is satisfied on the basis of an *ex parte* application by the Commissioner of Police or other gazetted officer that specified data stored in a computer system is required for the purpose of a criminal

investigation or criminal proceedings, the Judge or magistrate may make an order to ensure that expeditious

(a) preservation of traffic data is available regardless of whether one or more service providers was involved in the transmission of that communication; and

(b) disclosure of a sufficient amount of traffic data is given to enable the identification of

(i) the service providers; and

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

Preservation of data for criminal proceedings

28.(1) The Commissioner of Police or any other gazetted officer may make an *ex parte* application for a preservation order to a Judge or magistrate where

(a) computer data, including traffic data, stored in a computer system is required for the purposes of a criminal investigation; and

(b) there are grounds to believe that the computer data, including traffic data, stored in a computer system is particularly vulnerable to loss or modification.

(2) Where the Commissioner of Police or any other gazetted officer satisfies a Judge or magistrate on the basis of an *ex parte* application made under subsection (1), the Judge or magistrate may make an order requiring the person in control of the computer system to

(a) ensure that the computer data specified in the order is preserved for a period of up to 90 days;

(b) maintain the integrity of the computer data for a period of up to 90 days; and

(c) keep confidential any information or action relating to the preservation order.

(3) Where the Commissioner of Police or other gazetted officer makes an *ex parte* application for an extension of a preservation order, a Judge or magistrate may extend the preservation order beyond the 90 day period for a further period of up to 90 days.

Order for payment of compensation

29.(1) The Court may make an order for the payment of compensation where a person is convicted of any offence and he causes damage to another person's computer system, programme or data.

(2) A claim by a person for damages sustained by reason of the offence is deemed to have been satisfied to the extent of any amount which has been paid to that person under an order for compensation.

(3) An order made under subsection (1) shall not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order.

(4) An order for compensation under this section is recoverable as a civil debt.

(5) For the purposes of this section, a programme or data held in a computer system is deemed to be the property of the owner of the computer system.

Regulations.

30. The Minister may make regulations generally for the purpose of giving effect to this Act.

Consequential amendments

31. The enactments set out in the first column of the *Schedule* are amended in the manner set out opposite thereto in the second column.

Repeal

32. The *Computer Misuse Act*, Cap. 124B is repealed.

Commencement

33. This Act shall come into operation on a date to be fixed by Proclamation.

SCHEDULE

(Section 31)

CONSEQUENTIAL AMENDMENTS

Column 1	Column 2
Enactment	*Amendment*
Copyright Act, Cap. 300	In section 31
	(a) delete subsection (5) and substitute the following: "(5) Copyright in a work is infringed by a person who, without the licence of the copyright owner, transmits the work by means of a computer system or telecommunications system (otherwise than by broadcasting or inclusion in a cable programme service) knowing or having reason to believe that infringing copies of the work will be made by means of the reception of the transmission in Barbados or elsewhere.".
	(b) insert immediately after subsection (5) the following new subsection: "(5A) For the purposes of subsection (5) "computer system" means a device or a group of interconnected or related devices, one or more of which, pursuant to a programme, facilititates communication, performs automatic processing of data or any other function.".

Schedule - (Concl'd)

CONSEQUENTIAL AMENDMENTS - *(Concl'd)*

Column 1 *Enactment*	Column 2 *Amendment*
Defamation Act, Cap. 199	Section 34 is deleted.
Extradition Act, Cap. 189	*(a)* In section 4, insert immediately after subsection (2) the following new subsection: "(3) An order made under subsection (2) shall be subject to affirmative resolution.". *(b)* In the *Schedule* insert immediately after paragraph 40 the following new paragraph: "41. Any offence under the *Cybercrime Act*, 2023 (2023-).".

Read three times and passed the House of Assembly this day of , 2023.

Speaker

Read three times and passed the Senate this day of , 2023.

President