ST. CHRISTOPHER AND NEVIS

CHAPTER 4.41

ELECTRONIC CRIMES ACT

Revised Edition
showing the law as at 31 December 2017

This is a revised edition of the law, prepared by the Law Commission under the authority of the Law Commission Act, Cap. 1.03.

This edition contains a consolidation of the following laws—

Printed under Authority by
The Regional Law Revision Centre Inc.
ANGUILLA

Published in
2019
Consolidated, Revised and Prepared under the Authority of the Law Commission Act,
on behalf of the Government of Saint Christopher and Nevis
by
The Regional Law Revision Centre Inc.,
P.O. Box 1626, 5 Mar Building,
The Valley, AI-2640, Anguilla,
West Indies.

Available for purchase from—

Attorney General's Chambers,
Government Headquarters, P.O. Box 164,
Church Street, Basseterre, St. Kitts,
West Indies

Tel: (869) 465-2521
Ext. 1013
Tel: (869) 465-2127
Fax: (869) 465-5040
Email: attorneygeneral@gov.kn

CHAPTER 4.41

ELECTRONIC CRIMES ACT

ARRANGEMENT OF SECTIONS

CHAPTER 4.41

ELECTRONIC CRIMES ACT

AN ACT TO PROHIBIT UNAUTHORISED ACCESS TO AND ABUSE OF COMPUTERS, COMPUTER SYSTEMS AS WELL AS THE INFORMATION CONTAINED ON THOSE SYSTEMS; AND TO PROVIDE FOR RELATED OR INCIDENTAL MATTERS.

PART I

PRELIMINARY

Short title.

1. This Act may be cited as the Electronic Crimes Act.

Interpretation.

2. (1) In this Act, unless the contrary intention appears—

"Chief of Police" means the Commissioner of Police appointed pursuant to section 11 of the Police Act, Cap. 19.07;

"computer" means a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a program or electronic instructions, performs automatic processing of data or any other function but does not include—

(a) a portable hand held calculator;

(b) an automated typewriter or typesetter;

(c) a device which is non-programmable or which does not contain any data storage facility; or

(d) such other device as the Minister may prescribe by Order;

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

"computer network" means any system that provides communications between one or more computer systems and its input or output devices, including, but not limited to, display terminals and printers that are connected by telecommunication facilities;

"computer system" means a device or collection of devices, including support devices, one or more of which contain computer programs, electronic instructions, or input data and output data, and which perform functions, including, but not limited to, logic, arithmetic, data storage, retrieval, communication, or control but the term does not include calculators that are not programmable or are incapable of being used in conjunction with external files;

"damage" includes any impairment to a computer system, the integrity or availability of any data or program held in a computer system or of the confidentiality of information held in a computer system;

"device" includes any electronic, electro-magnetic, acoustic or mechanical equipment or apparatus that is used or capable of being used to intercept any function of a computer;

"intercept" includes, but is not limited to, acquiring, viewing and capturing of any computer data communication, whether by wire, wireless, electronic, optical, magnetic, oral, or other means, during transmission through the use of any technical advice;

(Substituted by Act 26 of 2012)

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

"seize" includes—

(a) the making and retaining a copy of computer data, including by using on-site equipment;

(b) rendering inaccessible, or removing computer data from the accessed computer system; and

(c) taking a printout of output of computer data.

"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; or

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

"storage medium" means any type of any device or material on which data can be electronically placed, kept, and retrieved.

"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 used to generate the data.

(2) In this Act, access of any kind by a person to any program or data held in a computer is "unauthorised" or "obtained" without authority if the person is not entitled to access of the kind in question to the particular program or data.

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

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

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

(4) In this Act, a "modification of the contents of any computer" occurs if, by the operation of any function of the computer concerned or of any other computer—

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

(b) any program or data is added to any existing program or data held in the computer; or

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

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

(5) Any modification referred to in subsection (4) is unauthorised if the person whose act causes the modification—

(a) 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.

Application of Act.

3. This Act applies to an act done or an omission made—

(a) in Saint Christopher and Nevis;

(b) on a ship or aircraft registered in Saint Christopher and Nevis; or

(c) by a national of Saint Christopher and Nevis outside Saint Christopher and Nevis, if the person's conduct would also constitute an offence under the laws of the country where the offence was committed.

(Substituted by Act 26 of 2012)

PART II

OFFENCES

Illegal access and illegal remaining.

4. (1) A person who, without lawful excuse or justification or in excess of a lawful excuse or justification, knowingly accesses the whole or any part of a computer system, commits an offence, and shall be liable, on summary conviction, to a fine not exceeding five thousand dollars or to imprisonment for a term not exceeding one year in the case of a first conviction, and in case of any subsequent conviction to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding two years or both.

(2) If any damage results from an offence committed under subsection (1), notwithstanding the penalties referred to in that subsection, a person who is convicted of that offence shall be liable to a fine not exceeding twenty thousand dollars or to imprisonment for a term not exceeding three years or both.

(3) Where a person who is not authorised—

(a) to have a program or computer data; or

(b) to have access to any program or computer data,

has in his or her custody or control any program or computer data or other information which is held in any computer or retrieved from any computer, with the intent to commit an offence, the person shall be deemed to have committed the

offence of illegally accessing the program or computer data unless the contrary is proved.

(4) A person who commits an offence under subsection (3) shall be liable, on conviction on indictment, to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding five years or both.

(5) A person who has a right of access to a computer system or part of a computer system by virtue of the nature of that person's work commits an offence if that person accesses the computer system in accordance with the authorisation and remains logged in the computer system contrary to the authorisation with intent to commit an ulterior offence to the detriment of his or her employer.

(6) A person who is convicted of an offence under the provisions of subsection (5) shall be liable, on summary conviction, to a fine not exceeding five thousand dollars or to imprisonment for a term not exceeding one year, in the case of a first conviction and, in case of any subsequent conviction, to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding two years or both.

(Substituted by Act 26 of 2012)

Interfering with data.

5. (1) A person who, knowingly and without lawful excuse or justification, does any of the following acts—

(a) destroys or alters computer data;

(b) renders computer data meaningless, useless or ineffective;

(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,

commits an offence and is liable upon conviction on indictment to a fine of one hundred thousand dollars, or to imprisonment for a term of seven years or to both such fine and imprisonment.

(Amended by Act 26 of 2012)

(2) The provisions of subsection (1) are applicable whether the person's act is of temporary or permanent effect.

Interfering with computer system.

6. (1) A person who, knowingly and without lawful excuse or justification—

(a) impairs the functioning of a computer system by—

(i) preventing the supply of electricity to a computer system;

(ii) causing electromagnetic interference to a computer system;

(iii) corrupting the computer system by any means;

(iv) adding, deleting or altering computer data;

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

commits an offence and is liable on conviction on indictment, to a fine of fifty thousand dollars or to imprisonment for a term of five years or both such fine and imprisonment.

(2) The provisions of subsection (1) shall be applicable whether the person's act is of temporary or permanent effect.

(3) A person who knowingly, without lawful excuse or justification or in excess of a lawful excuse or justification, hinders or interferes with a computer system—

(a) which is exclusively for the use of critical infrastructure operations; or

(b) which is not exclusively for the use of critical infrastructure operations, but which is used in critical infrastructure operations,

and the conduct of the person affects the use or impacts the operations of critical infrastructure commits an offence and shall be liable, on conviction on indictment, to a fine of one hundred thousand dollars or to imprisonment for a term of ten years or both.

(Inserted by Act 26 of 2012)

Illegal interception.

7. A person who, knowingly and without lawful excuse or justification, intercepts by technical means—

(a) any non-public transmission to, from or within a computer system; or

(b) electromagnetic emissions that are carrying computer data from a computer system,

commits an offence and is liable on conviction on indictment, to a fine of fifty thousand dollars or to imprisonment for a term of five years or to both such fine and imprisonment.

Possession, sale, etc. of illegal devices.

8. A person who—

(a) knowingly, without lawful excuse or justification or in excess of a lawful excuse or justification, produces, sells, procures for use, imports, exports, distributes or otherwise makes available—

(i) a device, including a computer program, that is designed or adapted for the purpose of committing an offence defined by the other provisions of Part II of this Act; 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 defined by the other provisions of Part II of this Act; or

(b) has an item mentioned in subparagraph (i) or (ii) in his or her possession with the intent that it be used by any person for the purpose of committing an offence defined by the other provisions of Part II of this Act,

commits an offence and shall be liable, on conviction on indictment, to a fine of fifty thousand dollars or to imprisonment for a term of five years or both.

(Substituted by Act 26 of 2012)

Computer-related fraud.

9. A person who knowingly, without lawful excuse or justification or in excess of a lawful excuse or justification, causes loss of property to another person by—

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

(b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person,

commits an offence and shall be liable on conviction on indictment, to a fine of fifty thousand dollars or to imprisonment for a term of five years or both.

(Substituted by Act 26 of 2012)

Unlawful disclosure of access code.

10. (1) A person who knowingly and without authority discloses any password, access code or any other means of gaining access to any program or data held in a computer commits an offence and is liable on summary conviction to a fine of ten thousand dollars or to imprisonment for a term of twelve months or to both such fine and imprisonment, and in the case of a second or subsequent conviction, to a fine of twenty thousand dollars or to imprisonment for a term of two years or to both such fine and imprisonment.

(2) A person who knowingly and without authority discloses any password, access code or any other means of gaining access to any program or data held in a computer—

(a) for any unlawful gain, whether to himself or to another person;

(b) for an unlawful purpose; or

(c) knowing that it is likely to cause unlawful damage,

commits an offence and is liable on conviction on indictment to a fine of fifty thousand dollars or to imprisonment for a term of five years or to both such fine and imprisonment and, in the case of a second or subsequent conviction, to a fine of one hundred thousand dollars or to imprisonment for a term of seven years or to both such fine and imprisonment.

Unauthorised access to restricted computer system.

11. (1) Where a person who does not possess the relevant authorisation for gaining access to a restricted computer system—

(a) gains access to the system, that person commits an offence and is liable on conviction on indictment to a fine of seventy-five thousand dollars or to imprisonment for a term of five years or to both such fine and imprisonment;

(b) gains access to a restricted computer system in the course of the commission of an offence under section 4, 5, 6 or 7, the person convicted of that offence is, *in lieu* of the penalty prescribed in those sections, is liable, on conviction on indictment, to a fine of one hundred thousand dollars or to imprisonment for a term of seven years or to both such fine and imprisonment.

(2) For the purposes of subsection (1), a "restricted computer system" shall be treated as such if the person committing the offence knew, or ought reasonably to

have known that the computer, program or data is used directly in connection with or necessary for—

(a) the security, defence or international relations of St. Christopher and Nevis;

(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;

(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure;

(d) the protection of public safety and public health, including systems related to essential emergency services such as police, civil defence and medical services;

(e) any other service so designated by the Minister by Order to be restricted.

(3) For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in subsection (2) if there is, in respect of the computer or program or data, an electronic or other warning exhibited to the accused stating that unauthorised access to that computer or program or data attracts an enhanced penalty under this section.

Child pornography.

[*]**12.** (1) A person who knowingly—

(a) publishes child pornography through a computer system;

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

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

commits an offence and is liable, on conviction on indictment—

(i) in the case of an individual, to a fine of fifty thousand dollars or to imprisonment for a term of five years or to both such fine and imprisonment;

(ii) in the case of a corporation, to a fine of two hundred and fifty thousand dollars.

(2) The provisions of subsection (1) paragraph (a) or (c) shall not be applicable to a person who establishes that the child pornography was for a *bona fide* scientific, research, medical or law enforcement purpose.

(3) In this section—

"child pornography" includes material that visually depicts—

(a) a minor engaged in sexually explicit conduct; or

(b) a person who appears to be a minor engaged in sexually explicit conduct; or

[*] Formerly section 13. Original section 12 was repealed by Act 26 of 2012 and sections 13 and 14 were renumbered.

(c) realistic images representing a minor engaged in sexually explicit conduct;

"publish" includes—

(a) 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; or

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

(c) 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 (a).

Unlawful communications.

13. (1) Where a person without lawful excuse or justification knowingly uses a computer system to send a message, letter, or electronic communication that—

(a) is obscene;

(b) constitutes a threat; or

(c) is menacing in character,

to a recipient and intends to cause the recipient or any other person who is the subject of that message or letter or electronic communication to feel intimidated, molested, harassed or threatened, he commits an offence and is liable on summary conviction to a fine of ten thousand dollars or to imprisonment for a term of twelve months or to both such fine and imprisonment.

(2) Where a person without lawful excuse or justification publishes the message, letter or electronic communication referred to in subsection (1), to any other person not being a person who is the subject of the message, letter or electronic communication, then that first person commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars or to imprisonment for a term of two years or to both such fine and imprisonment.

(3) For the purposes of subsection (1), communication that constitutes a threat or is menacing in character includes communication that causes substantial emotional distress.

(Inserted by Act 26 of 2012)

Computer-related forgery.

14. (1) A person who knowingly, without lawful excuse or justification or in excess of a lawful excuse or justification—

(a) makes an input;

(b) alters;

(c) deletes; or

(d) suppresses computer data,

resulting in inauthentic computer data with intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the computer data is directly readable and intelligible, commits an offence, and shall be liable on summary conviction, to imprisonment for a period not exceeding five years.

(2) If the offence created by subsection (1) is committed by sending out multiple electronic mail messages from or through computer systems, the person shall be liable, on conviction, to a fine not exceeding one hundred thousand dollars or imprisonment for a term not exceeding ten years, or both.

Data espionage.

15. A person who, knowingly, without lawful excuse or justification or in excess of a lawful excuse or justification, obtains for himself or herself from another computer data which are not meant for him or her and which are specially protected against unauthorised access, commits an offence, and shall be liable, on summary conviction, to a fine not exceeding fifty thousand dollars, or to imprisonment for a term not exceeding five years, or both.

Identity-related crimes.

16. A person who knowingly, without lawful excuse or justification or in excess of a lawful excuse or justification, uses a computer system at any stage of an offence to transfer, possess, or use a means of identification of another person with the intent to commit, aid or abet, or in connection with, any unlawful activity that constitutes a crime, commits an offence, and shall be liable, on summary conviction, to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding five years, or both.

Spam.

17. A person who knowingly, without lawful excuse or justification—

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

(b) uses a protected computer system to relay or retransmit multiple electronic mail messages, with intent to deceive or mislead users, or any electronic mail or internet service provider, as to the origin of such messages; or

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

commits an offence, and shall be liable, on summary conviction, to a fine not exceeding fifty thousand dollars, or to imprisonment for a term not exceeding five years, or both.

(Inserted by Act 26 of 2012)

PART III

PROCEDURAL POWERS

Warrant.

18. [*](1) Where a Magistrate is satisfied, on the basis of information given on oath by a police officer, that there are reasonable grounds to suspect that there may be in a place or premises a thing or computer data—

[*] Act 26 of 2012 renumbered original section 15 as section 18, renumbered original subsections (4) to (6) as subsections (6) to (8), and inserted new subsections (4) and (5).

(a) which may be material as evidence in proving an offence under this Act; or

(b) which has been acquired by a person as a result of an offence committed under this Act,

the Magistrate may issue a warrant authorising the police officer to enter the place or premises and search and seize the thing or computer using such assistance as may be necessary, and the search may include a search or access to a computer system or part of it and the computer data stored in that system as well as a computer data storage medium in which the computer data may be stored in Saint Christopher and Nevis.

(Substituted by Act 26 of 2012)

(2) A warrant issued under this section may authorise or require—

(a) a police officer to—

(i) seize any computer, data, program, information, document or thing if he reasonably believes that it is evidence that an offence under this Act has been or is about to be committed;

(ii) have access to and inspect and check the operation of any computer to which this section applies;

(iii) use or cause to be used any computer to search any data contained in or available to such computer;

(iv) have access to any information, code or technology which has the capability of converting encrypted data contained or available to such computer into readable and comprehensible format or text for the purpose of investigating any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section;

(b) an authorised person to render assistance to the police officer in the execution of the warrant;

(c) any person in possession of decryption information necessary to decrypt data required for the purpose of investigating any such offence.

(3) A police officer may, where it is reasonably required, request a person who is not a suspect of a crime but who has knowledge about the functioning of a computer system or measures applied to protect the computer data in the computer system which is the subject of a search under this section to assist the police officer, and the person so requested shall permit and assist the police officer to make the search by—

(a) providing information that enables the undertaking of measures referred to in this section;

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

(c) obtaining and copying such computer data;

(d) using equipment to make copies; and

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

(Substituted by Act 26 of 2012)

(4) Where a police officer who is undertaking a search pursuant to the provisions of subsection (1) has reasonable grounds to believe that the computer data which is being sought is stored in another computer system or part of it is stored in Saint Christopher and Nevis, and such data is lawfully accessible from or available to the initial system, the police officer shall apply to the Magistrate in Chambers to expeditiously extend the search for the other computer system or the accessing of such system.

(Inserted by Act 26 of 2012)

(5) A person referred to in subsection (4) who fails, without lawful excuse or justification or in excess of a lawful excuse or justification, to permit or assist a police officer as required by the provisions of subsection (4) commits an offence, and shall be liable, on summary conviction, to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding one year, or both.

(Inserted by Act 26 of 2012)

(6) Any person who obstructs the lawful exercise of the powers under subsection (2)(a) or who fails to comply with a request under subsection (2)(b) or (c) shall be guilty of an offence and shall be liable on conviction to a fine of ten thousand dollars or to imprisonment for a term of three years or to both such fine and imprisonment.

(7) For the purposes of this section—

"decryption information" means information or technology that enables a person to readily convert encrypted data from its unreadable and incomprehensible format to its plain text version;

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

"plain text version" means original data before it has been converted transformed or scrambled, to an unreadable or incomprehensible format.

(8) For the purposes of this Part, "authorised person" means a person who has the relevant training and skill in computer systems and who is authorised in writing by the Chief of Police.

Order for production of data.

[*]**19.** If a magistrate is satisfied on the basis of an *ex parte* application by a police officer that specified data stored in a computer system is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that—

(a) a person in St. Christopher and Nevis in control of a computer system, produce from the system specified computer data or a printout or other intelligible output of that data; and

(b) an internet service provider in St. Christopher and Nevis produce information about persons who subscribe to or otherwise use the service.

[*] Act 26 of 2012 renumbered original sections 16 to 19 as sections 19 to 22.

Record of and access to seized data.

20. (1) If a computer system or computer data has been removed or rendered inaccessible, following a search or a seizure under section 18, 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 seizure; and

(b) give a copy of that list to—

(i) the occupier of the premises; or

(ii) the person in control of the computer system.

(2) Subject to subsection (3), on request, a police officer or another authorised person shall—

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

(b) give the person a copy of the computer data.

(3) The police officer or another authorised person may refuse to give access or provide copies if he or she 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 was carried out; or

(ii) another ongoing investigation; or

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

Traffic data.

21. If a magistrate is satisfied on the basis of an *ex parte* application by a police officer that specified data stored in a computer system is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that a person in control of the computer system disclose sufficient traffic data about a specified communication to identify—

(a) the service providers; and

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

Interception of electronic communications.

22. (1) If a magistrate is satisfied on the basis of an information on oath that there are reasonable grounds to suspect that the content of electronic communications is reasonably required for the purposes of a criminal investigation or criminal proceedings, the magistrate may—

(a) order an internet service provider whose service is available in St. Christopher and Nevis, through application of technical means, to collect or record or to permit or assist competent authorities with the

collection or recording of content data associated with specified communications transmitted by means of a computer system; or

(b) authorise a police officer to collect or record that data through application of technical means.

(2) An internet service provider who without lawful authority discloses—

(a) the fact that an order under subsection (1), or sections 18 to 21 has been made; or

(b) anything done under the order; or

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

commits an offence and is liable on conviction to a fine of fifty thousand dollars.

(3) An internet service provider is not liable under a civil or criminal law of St. Christopher and Nevis for the disclosure of any data or other information that he discloses under this section or sections 18 to 21.

Expedited preservation of computer data.

23. (1) Where a police officer is satisfied that there are grounds to believe that computer data which is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the police officer may, by written notice given to a person in control of the computer data, require the person to ensure that the computer data specified in the notice is preserved for a period of up to seven days as specified in the notice.

(2) The period referred to in subsection (1) may be extended beyond the seven days if, on an *ex parte* application, a Magistrate authorises an extension for a further specified period of time.

Use of forensic software.

24. (1) If a judge is satisfied, upon application and on the basis of information given on oath, that in an investigation concerning an offence there are reasonable grounds to believe that essential evidence cannot be collected by applying other provisions of this Act but is reasonably required for the purposes of a criminal investigation, the judge may authorise a police officer to utilise a remote forensic software with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence.

(2) The application made pursuant to the provisions of subsection (1) shall contain the following information—

(a) suspect of the offence, if possible with name and address;

(b) description of the targeted computer system;

(c) description of the intended measure, extent and duration of the utilisation; and

(d) reasons for the necessity of the utilisation.

(3) In granting the authorisation, the judge may require that in such investigation the police officer should ensure that modifications to the computer system of the suspect are limited to those essential for the investigation and that any changes if possible can be undone after the end of the investigation.

(4) During the investigation it shall be necessary to log—

(a) the technical means used and time and date of the application;

(b) the identification of the computer system and details of the modifications undertaken within the investigation;

(c) any information obtained.

(5) Information obtained by the use of the software shall be protected against any modification, unauthorised deletion and unauthorised access.

(6) The duration of authorisation granted pursuant to the provisions of subsection (1) shall be for a period of three months, and if the conditions of the authorisation are no longer met, the action taken shall stop immediately.

(7) For the purposes of this section, the authorisation to install the software includes remotely accessing the suspect's computer system.

(8) If the installation process requires physical access to a place the requirements of section 18 shall be fulfilled.

(9) If necessary, a police officer may, pursuant to the authorisation under subsection (1), request that the court order an internet service provider to support the installation process.

Disclosure of details of an investigation.

25. An internet service provider who receives an order related to a criminal investigation that explicitly stipulates that confidentiality is to be maintained or such obligation is stated by law and such internet service provider intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, discloses—

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

(b) anything done under the order; or

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

the internet service provider commits an offence, and shall be liable, on summary conviction, to a fine not exceeding ten thousand dollars.

(Inserted by Act 26 of 2012)

Evidence.

[*]**26.** Notwithstanding the provisions of any Act to the contrary, any electronic evidence that is collected pursuant to this Act shall be treated in the same manner as evidence that is non-electronic.

Arrest without warrant.

27. A police officer may arrest without warrant any person reasonably suspected of committing an offence under this Act.

Regulations.

28. The Minister may generally make regulations to give effect to the provisions of this Act.

(Inserted by Act 26 of 2012)

———

[*] Act 26 of 2012 renumbered original sections 20 and 21 as sections 26 and 27.