



REPUBLIC OF VANUATU

CYBERCRIME ACT NO. 22 OF 2021

Arrangement of Sections

PART 1 PRELIMINARY

1	Interpretation	4
2	Purpose.....	8

PART 2 COMPUTER OFFENCES

3	Illegal access	9
4	Illegal interception.....	9
5	Unauthorised interference	10
6	Misuse of devices	11

PART 3 COMPUTER RELATED OFFENCES

7	Child pornography	13
8	Hosting child pornography.....	13
9	Identity- related crime.....	14
10	Cyber stalking	14
11	Solicitation of children.....	15
12	Computer related forgery	15
13	Computer related fraud	16
14	Illegal access with intent to commit or facilitate further offences	16

PART 4 PROCEDURES

Division 1 Disclosure of information, assistance and production of computer data

15	Disclosure of information of an investigation.....	17
16	Assistance.....	17
17	Production of computer data	18

Division 2 Preservation Order

18	Preservation order.....	19
19	Revocation of preservation order	20

20	Service provider or authorised representative to disclose traffic data	20
----	--	----

Division 3 Subscriber data, traffic data and content data

21	Request for disclosure of subscriber data	20
22	Request for disclosure of traffic data.....	20
23	Request for access to traffic data in real time	21
24	Disclosure of content data.....	22
25	Subscriber data, traffic data and content data to be used for lawful purposes only.....	23

Division 4 Disclosure to a foreign law enforcement agency

26	Disclosure to a foreign law enforcement agency	23
----	--	----

Division 5 Interception warrant

27	Commissioner to authorise applications.....	24
28	Application for interception warrant	24
29	Content and terms of an interception warrant	25
30	Granting of an interception warrant.....	27
31	Period and extension of interception warrant.....	28
32	Urgent interception warrant	28
33	Service provider to be served with interception warrant	29
34	Admissibility of evidence	30
35	Minor defect in connection with interception warrant or urgent interception warrant.....	30
36	Prohibition on disclosure of communications intercepted and recordings.....	31
37	Revocation of interception warrant or an urgent interception warrant	31

Division 6 Provisions relating to computer warrants

38	Commissioner to authorise applications.....	31
39	Application for a computer warrant.....	32
40	Granting of computer warrant.....	33
41	Contents of computer warrant.....	34
42	Extension of a computer warrant.....	34
43	Application for an urgent computer warrant.....	34
44	Granting of an urgent computer warrant.....	36
45	Effects of a computer warrant and an urgent computer warrant	36
46	Access to seized data	38
47	Securing or rendering inaccessible data under a computer warrant or an urgent computer warrant	39
48	Assisting police officer in executing computer warrant	40
49	Exercising reasonable care.....	40
50	Receipt for items seized under computer warrant	41
51	Measures to control retention of seized data storage medium, computer network or computer system.....	42

52	Destruction of certain data seized under a computer warrant or an urgent computer warrant.....	42
53	Prohibition on disclosure of information, records and data.....	42
54	Evidentiary certificates for service providers	43
55	Hindering or obstructing the lawful exercise of powers.....	43
56	Obligations of service providers.....	43

PART 5 INTERNATIONAL COOPERATION

57	General principles relating to mutual assistance	45
58	Public Prosecutor to make and act on mutual assistance requests	45
59	Additional information	46
60	Expedited preservation of stored computer data	47
61	Expedited disclosure of preserved traffic data	47
62	Mutual assistance regarding accessing of stored computer data.....	48
63	Trans-border access to stored computer data with consent or where publicly available.....	50
64	Mutual assistance in the real-time collection of traffic data	50
65	Mutual assistance regarding the interception of content data	51
66	24/7 Network.....	52
67	Report on special investigative powers	53
68	State not required to give undertaking for costs.....	54

PART 6 MISCELLANEOUS

69	Authorised officer.....	55
70	Protection from liability.....	55
71	Regulations.....	55
72	Commencement.....	55

REPUBLIC OF VANUATU

Assent: 20/07/2021
Commencement: 22/09/2021

CYBERCRIME ACT NO. 22 OF 2021

An Act to regulate the use of computer systems, programs and data and for related matters.

Be it enacted by the President and Parliament as follows-

PART 1 PRELIMINARY

1 Interpretation

In this Act, unless the contrary intention appears:

authorised officer means a police officer appointed as an authorised officer under section 69;

authorised representative means:

- (a) the Chief Executive Officer or Managing Director of a service provider or a body corporate of which the service provider is a subsidiary; or
- (b) the Secretary of a service provider or a body corporate of which the service provider is a subsidiary; or
- (c) an employee authorised, in writing, by the Managing Director or Secretary of a service provider or a body corporate of which the service provider is a subsidiary;

child means a person under the age of 18 years;

Commissioner means the Commissioner of Police appointed under the Police Act [CAP 105];

communication means transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by electronic means;

computer data includes:

- (a) data entered or copied into a computer system; and

- (b) data held in a removable storage medium in a computer system; and
- (c) data held in a computer storage medium on a computer network of which the computer system forms part; and
- (d) data held in other computer storage mediums including cloud; and
- (e) any representation of information, knowledge, facts, concepts or instruction, which is being prepared or has been prepared and is intended to be processed, is being processed, or has been processed in a computer or a computer network; and
- (f) any form, whether readable only by a computer or only by a human or by either, including, but not limited to computer printouts, magnetic storage media, punched cards or stored internally in the memory of the computer;

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 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 system means:

- (a) a computer; or
- (b) two or more interconnected computers; or
- (c) any communication links between computers or to remote terminals or another device; or
- (d) two or more interconnected computers combined with any communication links between computers or to remote terminals or another device,

which also includes any part of the items described in paragraphs (a) to (d), and all related inputs, outputs, processing, storage, software or communication facilities, the cloud, and stored data;

computer warrant means a warrant granted under section 40;

content data means the substance of a specified communication that is intercepted;

Court means the Supreme Court of Vanuatu;

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

data storage medium means anything that contains or designed to contain data for use by a computer system;

device means any hardware or equipment which performs one or more specific functions and operates on any form or combination of electrical energy and includes but is not limited to:

- (a) components of computer systems such as computers, graphic cards, mobile phones or memory chips; or
- (b) storage components such as hard drives, memory cards, compact discs or tapes; or
- (c) input devices such as keyboards, mice, track pads, scanners or digital cameras; or
- (d) output devices such as printers or screens;

foreign country has the same meaning as in the Mutual Assistance in Criminal Matters Act [CAP 285];

foreign serious offence has the same meaning as in the Proceeds of Crime Act [CAP 284];

information means information, whether in the form of data, text, sounds, images or in any other form;

intelligible output means information from a computer system in whatever form that is able to be read and understood;

interception means the monitoring or recording of non-public transmissions of data to, from or within a computer system;

interception device has the same meaning as in the Police Powers Act No. 37 of 2017;

interception warrant means a warrant granted under section 30;

makes available includes, but not limited to, describing how to obtain access, or describing methods that are likely to facilitate access;

Minister means the Minister responsible for Information Communication and Technology;

Mutual Assistance in Criminal Matters Act means the Mutual Assistance in Criminal Matters Act [CAP 285];

police officer means any member of the Vanuatu Police Force established by the Police Act [CAP 105];

program means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function and make references to a program including references to part of a program;

real time means when information is being generated or transmitted;

serious offence has the same meaning as in the Proceeds of Crime Act [CAP 284];

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 the users of that entity; and
- (c) a service provider under the Telecommunications, Radiocommunications and Broadcasting Regulation Act No. 30 of 2009;

specified offence means an offence against a law of Vanuatu for which the maximum penalty is imprisonment for a term not exceeding 4 years;

subscriber data:

- (a) means any data held by a service provider (whether in the form of computer data or any other form) in relation to a person using or renting its services (a “subscriber”) by which the following can be established:
 - (i) the type of service used, the technical provisions taken in relation to the service and the period of service; and

- (ii) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; and
 - (iii) any other data on the site of the installation of the equipment needed to use the service, available on the basis of the service agreement or arrangement; and
- (b) does not include traffic or content data;

traffic data means electronic data that:

- (a) relates to a communication by means of a computer system; and
- (b) is generated by a computer system that is part of the chain of communication; and
- (c) shows the communication's origin, destination, route, time, date, size, duration or the type of underlying services;

urgent computer warrant means a warrant granted under section 44;

urgent interception warrant means a warrant granted under section 32.

2 Purpose

The purpose of this Act is:

- (a) to protect the confidentiality, integrity and availability of computer systems, programs and data; and
- (b) to prevent the abusive use of computer systems, programs and data; and
- (c) to enable the gathering of forensic material for the investigation and prosecution of breaches of this Act; and
- (d) to facilitate international co-operation.

PART 2 COMPUTER OFFENCES

3 Illegal access

- (1) For the purposes of this section, **critical infrastructure** means vital computer systems, physical facilities, processes, supply chains, information technologies, communication networks, devices, public utilities and essential services.
- (2) A person who intentionally and without lawful excuse, accesses the whole or part of a computer system by infringing a security measure, commits an offence and is liable on conviction:
 - (a) in the case of an individual- to a fine not exceeding VT2,000,000 or to a term of imprisonment not exceeding 5 years, or both; or
 - (b) in the case of a body corporate- to a fine not exceeding VT4,000,000.
- (3) A person who intentionally and without lawful excuse, accesses the whole or part of a critical infrastructure, commits an offence and is liable on conviction:
 - (a) in the case of an individual- to a fine not exceeding VT2,000,000 or to a term of imprisonment not exceeding 5 years, or both; or
 - (b) in the case of a body corporate- to a fine not exceeding VT4,000,000.
- (4) A person does not commit an offence under this section if that person:
 - (a) is entitled to have access to the program or data; or
 - (b) has consent to have access to the program or data.

4 Illegal interception

- (1) A person must not intentionally and without lawful excuse, intercept by any technical means:
 - (a) any non-public transmission of computer data to, from or within a computer system; or
 - (b) electromagnetic emission from a computer system carrying such computer data.

- (2) Despite subsection (1), the Commissioner may, by Order, authorise for the interception of any non-public transmission or electromagnetic emission.
- (3) A person who intentionally and without lawful excuse, intercepts the whole or part of a critical infrastructure, commits an offence and is liable on conviction:
 - (a) in the case of an individual- to a fine not exceeding VT2,000,000 or to a term of imprisonment not exceeding 5 years, or both; or
 - (b) in the case of a body corporate- to a fine not exceeding VT4,000,000.

5 Unauthorised interference

- (1) For the purposes of this section, **unauthorised interference** means:
 - (a) a person whose act causes the interference and is not entitled to determine whether the interference should be made; and
 - (b) the person does not have consent to the interference from a person who is entitled.
- (2) A person who intentionally and without authorisation does any act which causes an unauthorised interference to a computer system, program or data, commits an offence and is liable on conviction
 - (a) in the case of an individual- to a fine not exceeding VT7,000,000 or to a term of imprisonment not exceeding 40 years, or both; or
 - (b) in the case of a body corporate- to a fine not exceeding VT100,000,000.
- (3) A person who causes an unauthorised interference resulting in serious harm in all or any of the following:
 - (a) a financial loss of more than VT1,000,000;
 - (b) threatens national security;
 - (c) causes physical injury or death to any person;
 - (d) threatens public health or public safety,commits an offence and is liable on conviction:

- (a) in the case of an individual- to a fine not exceeding VT50,000,000 or to a term of imprisonment not exceeding 50 years, or both; or
 - (b) in the case of a body corporate- to a fine not exceeding VT100,000,000.
 - (4) A person who recklessly causes an unauthorised interference commits an offence and is liable on conviction:
 - (a) in the case of an individual- to, a fine not exceeding VT10,000,000 or to a term of imprisonment not exceeding 40 years, or both;
 - (b) in the case of a body corporate- to a fine not exceeding VT100,000,000.
 - (5) For the purposes of this section, it is immaterial that the unauthorised interference is not directed at:
 - (a) any particular computer system, program or data; or
 - (b) a program or data of any kind; or
 - (c) a program or data held in any particular computer system.
 - (6) In addition to subsection (5), it is immaterial whether an unauthorised interference or any intended effect of it is permanent or temporary.
- 6 Misuse of devices**
- (1) A person who intentionally or without lawful excuse, produces, sells, procures for use, imports, exports, distributes or makes available:
 - (a) a software, computer system or an electronic device; or
 - (b) a password, access code or similar data by which the whole or any part of a computer system or electronic data that is capable of being accessed,
- for intercepting or unauthorised interference, commits an offence and is liable on conviction
- (i) in the case of an individual- to a fine not exceeding VT1,000,000, or to a term of imprisonment not exceeding 3 years, or both; or

- (ii) in the case of a body corporate- to a fine not exceeding VT3,000,000.

(2) Despite subsection (1), it is not an offence under this section if:

- (a) any act is for an authorised training, testing or protection of a computer system; or
- (b) any undertaking is to comply with a Court order issued or in exercise of any power under this Act or any other Act.

PART 3 COMPUTER RELATED OFFENCES

7 Child pornography

(1) For the purposes of this section, **child pornography** includes any material, but not limited to any audio, visual or text material that represents:

- (a) a child engaged in sexually explicit conduct; or
- (b) a person appearing to be a child engaged in sexually explicit conduct; or
- (c) images, animations or videos representing a child engaged in sexually explicit conduct.

(2) A person who intentionally or without lawful excuse:

- (a) produces child pornography for the purpose of its distribution through a computer system; or
- (b) offers or solicits, or makes available child pornography through a computer system; or
- (c) distributes or transmits child pornography through a computer system; or
- (d) obtains or solicits child pornography through a computer system for personal use or for another person; or
- (e) possesses child pornography in a computer system or on an electronic storage medium,

commits an offence and is liable on conviction

- (a) to a fine not exceeding VT5,000,000 or to a term of imprisonment not exceeding 10 years, or both; or
- (b) in the case of a body corporate- to a fine not exceeding VT15,000,000.

8 Hosting child pornography

(1) A person commits an offence if the person:

- (a) is a service provider; and

(b) is aware, or becomes aware, that the service provided by the person can be used to access particular material that the person has reasonable grounds to believe:

(i) is a child pornography material; and

(ii) does not refer details of the material to the Vanuatu Police Force within a reasonable time after becoming aware of the existence of the material.

(2) A person who commits an offence under subsection (1), is liable on conviction:

(a) in the case of an individual- to a fine not exceeding VT5,000,000 or to a term of imprisonment not exceeding 10 years, or both; or

(b) in the case of a body corporate- to a fine not exceeding VT10,000,000.

9 Identity- related crime

A person who intentionally or without lawful excuse uses a computer system:

(a) to transfer; or

(b) to possess; or

(c) to use,

the identification of another person with the intention to commit, aid or abet or connect with any unlawful activity, commits an offence and is liable on conviction:

(i) in the case of an individual- to a fine not exceeding VT3,000,000 or to a term of imprisonment not exceeding 3 years, or both; or

(ii) in the case of a body corporate- to a fine not exceeding VT5,000,000.

10 Cyber stalking

(1) For the purposes of this section, **cyber stalking** means an act to coerce, intimidate, harass, insult or annoy a person through computer systems or electronic devices.

(2) A person who, directly or indirectly, uses any electronic communication for cyber stalking, commits an offence and is liable on conviction:

- (a) in the case of an individual- to a fine not exceeding VT1,000,000 or to a term of imprisonment not exceeding 3 years, or both; or
- (b) in the case of a body corporate- to a fine not exceeding VT3,000,000.

11 Solicitation of children

An individual who uses a computer system:

- (a) to propose to a child or
- (b) to propose to someone that the person believes to be a child,

to meet him or her or another person with the intention that the child be sexually exploited by him or her or another person, whether or not such proposal has been followed by material acts, commits an offence and is liable on conviction to a fine not exceeding VT2,000,000 or to a term of imprisonment not exceeding 5 years, or both.

12 Computer related forgery

A person who intentionally and without lawful excuse, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable or intelligible and wrongfully:

- (a) gains; or
- (b) inputs; or
- (c) alters; or
- (d) deletes; or
- (e) suppresses,

electronic data, commits an offence and is liable on conviction:

- (i) in the case of an individual- to a fine not exceeding VT5,000,000, or to a term of imprisonment not exceeding 12 years, or both; or
- (ii) in the case of a body corporate- to a fine not exceeding VT10,000,000.

13 Computer related fraud

A person who intentionally and without lawful excuse causes a loss of property to another person by:

- (a) any input, alteration, deletion or suppression of data; or
- (b) any interference with the functioning of a computer system,

with fraudulent intent of procuring personal gain for another person, commits an offence and is liable on conviction:

- (i) in the case of an individual- to a fine not exceeding VT5,000,000, or to a term of imprisonment not exceeding 12 years, or both; or
- (ii) in the case of a body corporate- to a fine not exceeding VT10,000,000.

14 Illegal access with intent to commit or facilitate further offences

- (1) A person is guilty of an offence under this section if the person commits an offence, under section 3, with the intent:

- (a) to commit an offence to which this section applies; or
- (b) to facilitate the commission of such an offence (whether by the person committing the offence or by any other person),

and the offence the person intends to commit or facilitate is a further offence.

- (2) It is immaterial for the purposes of this section whether the further offence is committed on the same occasion as the unauthorised access offence or on any future occasion.
- (3) A person may be charged with an offence under this section even though the facts are such that the commission of the further offence is impossible.
- (4) A person who intentionally accesses, without lawful excuse, the whole or any part of a computer system and commits or facilitates a further offence, is liable on conviction:
 - (a) in the case of an individual- to a fine not exceeding VT7,000,000 or to a term of imprisonment not exceeding 7 years, or both; or
 - (b) in the case of a body corporate- to a fine not exceeding VT9,000,000.

PART 4 PROCEDURES

Division 1 Disclosure of information, assistance and production of computer data

15 Disclosure of information of an investigation

- (1) For the purposes of this section, a **service provider** includes all or any employee, agent and contractor of the service provider.
- (2) A service provider who receives an order from a Court, relating to a criminal investigation that provides that confidentiality is to be maintained or such obligation is stated by law and the service provider discloses or continues to disclose:
 - (a) the fact that an order 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:
 - (i) in the case of an individual- to a fine not exceeding VT2,000,000, or to a term of imprisonment not exceeding 5 years, or both; or
 - (ii) in the case of a body corporate- to a fine not exceeding VT5,000,000.

16 Assistance

A person who is not a suspect of a crime under this Act, but is in possession or control of a device or data that is subject to a computer warrant under Division 6, must, at his or her own cost, permit or assist an authorised officer when carrying out the search:

- (a) to access and use the device or data; and
- (b) to obtain a copy of that data; and
- (c) to use the device to make copies; and
- (d) to obtain an intelligible output from a device in a format that can be read.

17 Production of computer data

- (1) This section applies if a police officer makes an application to the Court that data held in a data storage medium, or a computer network or a computer system, or a printout or any other information, is reasonably necessary for a criminal investigation or a proceeding that involves a specified offence against the laws of Vanuatu or a serious offence against the laws of a foreign country.
- (2) The Court may order:
 - (a) a person in control of the data storage medium, the computer network or the computer system to produce in a manner specified in the order a specified data or a printout or other intelligible output of that data; and
 - (b) a person who has access to a specified computer system process to compile the data held in the system and give it to a specified person.
- (3) Prior to making an order under subsection (2), the Court must consider the following:
 - (a) the seriousness of the offence to which the criminal investigation or proceeding relates; and
 - (b) the reliability of the information on which the application is based, including the nature of the source of the information; and
 - (c) whether the public interest in the production of data from the computer system or data storage medium outweighs the right to privacy of a person whose privacy may be affected as a result of the production; and
 - (d) whether there is sufficient connection between the evidence sought and the offence to which the criminal investigation or proceeding relates; and
 - (e) whether any condition should be included in the order; and
 - (f) any other matter that the Court considers relevant.

Division 2 Preservation Order

18 Preservation order

- (1) The Commissioner may, for the purposes of retaining computer data, including traffic data or content data, in a person's possession or control, apply to Court for a preservation order.
- (2) The Court may grant a preservation order if it is satisfied on reasonable grounds that the preservation of the computer data is reasonably necessary for law enforcement purposes or for a criminal investigation or proceeding involving a serious offence against a law of a foreign country.
- (3) A preservation order:
 - (a) comes into force when the service provider receives it; and
 - (b) remains in force for the period stated in the preservation order or until revoked by the Court under section 19.
- (4) A preservation order must not remain in force for a period exceeding 90 days.
- (5) Despite subsection (4), if the Court is satisfied that more time is needed to obtain what is required under the preservation order, the Court may extend the period for which the preservation order is in force, for another 90 days.
- (6) A person issued with a preservation order must keep the order and all information in the order confidential.
- (7) A person who, without reasonable excuse fails:
 - (a) to comply with an order granted under subsection (2); or
 - (b) to keep all information about the order confidential as provided under subsection (6),commits an offence and is punishable on conviction:
 - (i) in the case of an individual-to a fine not exceeding VT1,000,000, or to a term of imprisonment not exceeding 3 years, or both; or
 - (ii) in the case of a body corporate-to a fine not exceeding VT2,000,000.

19 Revocation of preservation order

- (1) If the Court is satisfied on reasonable grounds that the preservation order is no longer required, it is to revoke the preservation order any time before it expires.
- (2) If a preservation order is revoked, a police officer must immediately notify the service provider or its authorised representative about the revocation, and provide the service provider or its authorised representative a copy of the revocation.

20 Service provider or authorised representative to disclose traffic data

A service provider or its authorised representative issued with a preservation order must disclose, as soon as practicable, sufficient amount of traffic data to enable a police officer to identify any other service providers involved in the transmission of the communication.

Division 3 Subscriber data, traffic data and content data

21 Request for disclosure of subscriber data

- (1) The Commissioner may, in writing, request a service provider to disclose subscriber data if he or she is satisfied that the disclosure is necessary:
 - (a) for law enforcement purposes; or
 - (b) for the enforcement of a foreign serious offence under the Mutual Assistance in Criminal Matters Act.
- (2) A service provider must comply with the request under subsection (1), as soon as practicable, after receiving the request.
- (3) A service provider who fails to comply with subsection (2), commits an offence and is liable on conviction to a fine not exceeding VT1,000,000.

22 Request for disclosure of traffic data

- (1) The Commissioner may, in writing, request a service provider to disclose records of traffic data that came into existence before the time the disclosure is sought, if the disclosure is reasonably necessary:
 - (a) for law enforcement purposes; or
 - (b) for the enforcement of a foreign serious offence made under the Mutual Assistance in Criminal Matters Act.

- (2) Prior to making a request under subsection (1), the Commissioner must:

- (a) be satisfied that the public interest in the disclosure of the data substantially outweighs the right to privacy of a person whose privacy may be affected as a result of the disclosure; and
- (b) consider any matters relevant to giving the approval, including the following:
 - (i) the volume and nature of the data to be disclosed; or
 - (ii) the gravity of the conduct being investigated; or
 - (iii) the likely usefulness of the data to the investigation; or
 - (iv) the purpose for which access to the data is requested.
- (3) A service provider must comply with a request under subsection (1), as soon as practicable, after receiving the request.
- (4) A service provider who fails to comply with subsection (3) commits an offence and is liable on conviction to a fine not exceeding VT2,000,000.

23 Request for access to traffic data in real time

- (1) The Commissioner may, in writing, request a service provider to provide access to records of traffic data in real time for up to 90 days, if the access is reasonably necessary for:
 - (a) the enforcement of an offence punishable, on conviction, by imprisonment for a term not exceeding 2 years under this Act or any other Act; or
 - (b) for the enforcement of a foreign serious offence made under the Mutual Assistance in Criminal Matters Act.
- (2) Prior to making a request under subsection (1), the Commissioner must:
 - (a) be satisfied that the public interest in accessing the records substantially outweighs the right to privacy of a person whose privacy may be affected as a result of the access; and
 - (b) consider any matters relevant to giving the approval, including the following:
 - (i) the volume and nature of the records to be disclosed; or
 - (ii) the gravity of the conduct being investigated; or

- (iii) the likely usefulness of the records to the investigation; or
 - (iv) the purpose for which access to the records is requested.
- (3) The Commissioner must, in writing, cancel a request under subsection (1) any time before it expires, if he or she is satisfied that the request is no longer required.
- (4) The Commissioner must, in writing, notify the service provider or an authorised representative about the cancellation under subsection (3), and provide a copy of the cancellation immediately after the request is cancelled.

24 Disclosure of content data

- (1) An authorised officer may apply to the Court for an order to allow access to and disclosure of content data as follow:
 - (a) a person engaged in, or suspected on reasonable grounds to be engaged in, the commission of:
 - (i) a specific offence; or
 - (ii) a foreign serious offence under the Mutual Assistance in Criminal Matters Act, and
 - (b) a service that has been used, is being used or is likely to be used by a person under paragraph (a).
- (2) The authorised officer in making an application under subsection (1), is to state in the application:
 - (a) the details of each service provider subject to the order; and
 - (b) the offence or offences to which the application relates; and
 - (c) the information and evidence relied upon; and
 - (d) if a preservation order has been issued.
- (3) The authorised officer is to provide to the Court any further information as the Court may require concerning the grounds on which the order is sought.

25 Subscriber data, traffic data and content data to be used for lawful purposes only

- (1) Subscriber data obtained under section 21 is to be used:
 - (a) for the purposes for which it was originally obtained; or
 - (b) to enforce any criminal law imposing a pecuniary penalty, or to protect the public revenue; or
 - (c) to enforce a foreign forfeiture order or a foreign pecuniary penalty order in connection with a foreign serious offence under the Mutual Assistance in Criminal Matters Act.
- (2) Traffic data obtained in real time is to be used:
 - (a) for the purpose for which it was originally obtained; or
 - (b) to enforce any criminal law imposing a pecuniary penalty, or to protect the public revenue; or
 - (c) to enforce a foreign serious offence according to an authorisation made under the Mutual Assistance in Criminal Matters Act.
- (3) Content data preserved under section 18 is to be used:
 - (a) for the purposes for which the content data was originally obtained; or
 - (b) to enforce a specified offence or an offence under this Part; or
 - (c) to enforce a foreign serious offence according to an authorisation made under the Mutual Assistance in Criminal Matters Act.
- (4) If the Commissioner is satisfied that the information obtained is no longer required, the Commissioner must arrange for the destruction of the data and any reproduction of the data to be under the control of the Vanuatu Police Force.

Division 4 Disclosure to a foreign law enforcement agency

26 Disclosure to a foreign law enforcement agency

- (1) Information obtained under this Part must not be disclosed to a foreign law enforcement agency unless the disclosure has been authorised by the Commissioner.

- (2) The Commissioner must not authorise a disclosure under this Part, unless he or she is satisfied that:
 - (a) the disclosure is reasonably necessary for the enforcement of a foreign serious offence; and
 - (b) is appropriate in all the circumstances.

Division 5 Interception warrant

27 Commissioner to authorise applications

- (1) The Commissioner may authorise an application for:
 - (a) an interception warrant; or
 - (b) the renewal of an interception warrant; or
 - (c) an urgent interception warrant.
- (2) The Commissioner must not authorise an application referred to in subsection (1), unless the Commissioner is satisfied that there are reasonable grounds to suspect that a person:
 - (a) is planning, participating in or committing a specified offence; or
 - (b) has planned, participated in or committed a specified offence.

28 Application for interception warrant

- (1) If the Commissioner has authorised an application for an interception warrant under section 27, a police officer is to apply to the Court to grant the interception warrant to:
 - (a) intercept a private communication by means of an interception device; or
 - (b) record visually or observe an activity of a person by means of an interception device; or
 - (c) use both an interception device and an optical surveillance device.
- (2) The application must be in writing and made on oath by a police officer, and must set out:
 - (a) the person or customer, if known, whose communication is required to be intercepted; and

- (b) the service provider to whom the direction to intercept the communication must be addressed, if applicable; and
 - (c) the facts relied upon to demonstrate that there are reasonable grounds for suspecting that a person is planning, participating in or committing, or has planned, participated in or committed, a specified offence; and
 - (d) a description of the manner in which it is proposed to intercept private communications or record or observe activities; and
 - (e) the extent to which other methods for the investigation of the offence, other than an interception warrant, have been used by or are available to the police officer; and
 - (f) either:
 - (i) the name and address, if known, of the person whose private communications or a record or observations of whose activities there are reasonable grounds for suspecting will assist the police investigation of the case; or
 - (ii) if the name and address of the suspect are not known, a general description of the premises, place, item or type of facility in respect of which it is proposed to intercept private communications or record or observe activities; and
 - (g) the period for which a warrant is requested.
- (3) For the purpose of this section, **optical surveillance device** has the same meaning as in the Police Powers Act No. 37 of 2017.

29 Content and terms of an interception warrant

- (1) An interception warrant must be in the prescribed form and state the following information:
- (a) the offence or offences in respect of which the warrant is granted; and
 - (b) if the warrant relates to the use of an interception device on premises:
 - (i) the name and address of the suspect whose private communications may be intercepted or whose activities may be recorded or observed; or

- (ii) if the suspect's name and address are not known, a general description of the premises, place, item or type of facility in respect of which the private communications will be intercepted or activities recorded or observed; and
 - (c) if the warrant authorises the use of an interception device in respect of the conversations, activities or location of a person, state the name of the person (if known) or the fact that the person's identity is unknown; and
 - (d) any other terms and conditions that the Court considers necessary for the purpose of public interest.
- (2) An interception warrant has the effect, according to its terms, of authorising:
 - (a) the interception of private communications by means of an interception device; or
 - (b) the recording visually or observing of an activity of a person by means of an interception device; or
 - (c) activities referred to in paragraphs (a) and (b).
- (3) In addition to subsection (2), an interception warrant authorises:
 - (a) the retrieval of an interception device; and
 - (b) the entry, with such reasonable force as necessary, to any premises for the purposes of placing, servicing or retrieving an interception device; and
 - (c) the connection of the interception device to any source of electricity and the use of electricity from that source to operate the device; and
 - (d) the provision of assistance or technical expertise to the police officer primarily responsible for the execution of the warrant in the installation, use, maintenance or retrieval of the interception device.
- (4) If the warrant authorises the placing of an interception device in a residential or business premises of:
 - (a) a lawyer, clergyman or a medical practitioner; or

- (b) a person specified by the Court,

the Court may attach conditions that it considers necessary to avoid, as far as practicable, the interception of information or recording or observing of activities of a professional character to which the lawyer, clergyman, medical practitioner or such other person specified by the Court is a party.

- (5) To avoid doubt, an interception warrant is not limited to a particular premise, and can apply in relation to an interception device designed to intercept communications, or observe or record activities involving a person wherever that person may be.

30 Granting of an interception warrant

- (1) The Court may grant an interception warrant if it is satisfied that there are reasonable grounds:
 - (a) to suspect that a person is planning, participating in or committing, or has planned, participated in or committed, a specified offence; and
 - (b) to believe that evidence relevant to the investigation of a case will be obtained through the use of an interception warrant to intercept private communications, records or observe activities; and
 - (c) the proposed interception is justified by the social harm of the suspected offence against which it is directed.
- (2) In addition to subsection (1), the Court, prior to granting an interception warrant, must consider the following:
 - (a) the seriousness of the offence to which the criminal investigation or proceeding relates; and
 - (b) the reliability of the information on which the application is based, including the nature of the source of the information; and
 - (c) if the public interest in the production of data from the computer system or data storage medium outweighs the right to privacy of a person, whose privacy may be affected as a result of the production; and
 - (d) if there is sufficient connection between the evidence sought and the offence to which the criminal investigation or proceeding relates; and

- (e) if any condition should be included in the warrant; and
- (f) if the foreign country has made a request for mutual assistance under this Act or the Mutual Assistance in Criminal Matters Act and the Public Prosecutor has authorised the use of a lawful investigative power; and
- (g) any other matters that the Court considers relevant.

31 Period and extension of interception warrant

- (1) An interception warrant is valid for the period specified in the warrant, being a period not exceeding 90 days.
- (2) Subject to subsection (1), the Court may grant an extension of an interception warrant upon an application made before the warrant expires.
- (3) An application for an extension of an interception warrant must:
 - (a) provide the reason and period for which the renewal is required; and
 - (b) be accompanied by full particulars, together with times and dates, of any interceptions made or attempted under the interception warrant and an indication of the nature of the information that has been obtained by such interception; and
 - (c) be supported by such other information as the Court may consider necessary.
- (4) The Court may extend an interception warrant if it is satisfied that the circumstances described in section 30 still apply.

32 Urgent interception warrant

- (1) The Court may grant an urgent interception warrant if it is satisfied that:
 - (a) the circumstances to which the application relates are urgent; or
 - (b) the delay that would be caused by the application being made in person would frustrate the effective execution of the warrant.
- (2) A police officer may make an application for an urgent interception warrant orally, by telephone, email, facsimile or other electronic means.
- (3) The Court may, orally or in writing, grant an urgent interception warrant:

- (a) for the interception of private communications; or
 - (b) for the recording of activities in respect of a particular premises; or
 - (c) for a particular person; or
 - (d) for a particular place; or
 - (e) for a particular item; or
 - (f) for a particular type of facility,
- and in a particular manner.
- (4) The contents and terms of an interception warrant under section 29 apply to the contents and terms of an urgent interception warrant.
 - (5) An urgent interception warrant is valid for 48 hours commencing from the time on which it is issued.
 - (6) Subject to subsection (1), the Court must, as soon as practicable, give a copy of the warrant to a police officer who applied for the urgent interception warrant under subsection (2).
 - (7) If it is not reasonably practicable for the Court to give a copy of the urgent interception warrant to the police officer:
 - (a) the Court must inform the police officer of the terms of the urgent interception warrant and the date and time the warrant was signed; and
 - (b) the police officer must make a record of the following details:
 - (i) the name of the Judge who issued the urgent interception warrant; and
 - (ii) the date and time the urgent interception warrant was signed.
- 33 Service provider to be served with interception warrant**
- (1) If an interception warrant is issued under this Division to intercept a private communication, the authorised officer must:
 - (a) inform the service provider about the warrant; and

(b) serve a copy of the warrant to the service provider.

(2) The service provider must comply with the warrant as soon as it is served.

34 Admissibility of evidence

(1) Any information or recording obtained pursuant to an interception warrant or an urgent interception warrant is admissible as evidence in any proceedings for the prosecution of a specified offence.

(2) Any information or recording obtained in breach of subsection 29(4) is not admissible evidence.

35 Minor defect in connection with interception warrant or urgent interception warrant

(1) This section applies if:

- (a) information or a recording is purportedly obtained through the use of an interception device authorised under an interception warrant or an urgent interception warrant; and
- (b) there is a minor defect or irregularity in relation to the interception warrant or urgent interception warrant and, but for that defect or irregularity, the interception warrant or urgent interception warrant would have been sufficient authority for the action taken.

(2) This section applies if:

- (a) the use of the interception device is to be taken as being valid; and
- (b) any information or recording obtained pursuant to the interception warrant or urgent interception warrant is admissible as evidence as if the interception warrant or urgent interception warrant did not have that defect or irregularity.

(3) A reference in subsection (1), to a defect or irregularity in relation to an interception warrant or urgent interception warrant is a reference to a defect or irregularity (other than a substantial defect or irregularity):

- (a) in, or in connection with, the issue of, a document purporting to be that interception warrant or urgent interception warrant; or
- (b) in connection with the execution of that interception warrant or urgent interception warrant or the execution of a document purporting to be that interception warrant or urgent interception warrant.

36 Prohibition on disclosure of communications intercepted and recordings

- (1) A person who:
- (a) intercepts or assists in the interception of a private communication in accordance with an interception warrant or urgent interception warrant; or
 - (b) acquires knowledge of a private communication as a direct or indirect result of that interception; or
 - (c) makes a record of the activities of a person,
- is prohibited to disclose in whole or in part the substance or meaning of that communication or recording.
- (2) A person who contravenes subsection (1) commits an offence punishable on conviction:
- (a) in the case of an individual- to a fine not exceeding VT2,000,000 or a term of imprisonment not exceeding 5 years, or both; or
 - (b) in the case of a body corporate- to a fine not exceeding VT4,000,000.

37 Revocation of interception warrant or an urgent interception warrant

- (1) A police officer may, at any time, apply to the Court to revoke an interception warrant or an urgent interception warrant.
- (2) The Court must revoke an interception warrant or an urgent interception warrant if it is satisfied that the warrant is no longer required.
- (3) If an interception warrant or urgent interception warrant to intercept a private communication is revoked, the police officer must notify the service provider's or its authorised representative about the revocation, and give the service provider or its authorised representative a copy of the revocation, immediately after the warrant is revoked.

Division 6 Provisions relating to computer warrants

38 Commissioner to authorise applications

- (1) The Commissioner may authorise an application for:
- (a) a computer warrant or renewal of a computer warrant; or

- (b) an urgent computer warrant.
- (2) The Commissioner must not authorise an application referred to in subsection (1), unless the Commissioner is satisfied that there are reasonable grounds to suspect that there may be on the person or at the place a data storage medium, or a computer network or a computer system that:
 - (a) may be material evidence of the commission of a specified offence; or
 - (b) may be material evidence of the commission of a foreign serious offence; or
 - (c) has been acquired by a person as a result of the commission of an offence.

39 Application for a computer warrant

- (1) If the Commissioner has authorised an application for a computer warrant under section 38, an authorised officer is to apply to the Court to grant a computer warrant to access:
 - (a) a place specified in the warrant; or
 - (b) a data storage medium at the location specified in the warrant; or
 - (c) a computer network at the location specified in the warrant; or
 - (d) a computer system at the location specified in the warrant.
- (2) An application must be in writing and made on oath by an authorised officer, and must set out:
 - (a) if a person is to be searched, the person's name, age and address; and
 - (b) if a place is to be searched:
 - (i) a description of the place to be searched; and
 - (ii) if the place is occupied, the name and age of any occupiers of the place, if known; and
 - (c) the offence to which the application relates; and

- (d) a description of the nature of the data storage medium, computer network, computer system or suspected to be evidential material; and
- (e) the information relied on to support the reasonable suspicion that evidence on the commission of an offence:
 - (i) is in or under the control of the person or at the place when the computer warrant is executed; or
 - (ii) is likely to be in or under the control of the person or at the place when the computer warrant is executed; and
- (f) if a computer warrant was issued previously in relation to the person or place; and
- (g) if authority to execute the computer warrant at night is being sought, why it is necessary to execute the computer warrant at night; and
- (h) the period the computer warrant is required.

40 Granting of computer warrant

- (1) The Court may grant a computer warrant if the Court is satisfied with the application of the authorised officer made under section 39.
- (2) Without limiting subsection (1), prior to granting a computer warrant, the Court must consider the following:
 - (a) the seriousness of the offence to which the criminal investigation or proceeding relates; and
 - (b) the reliability of the information on which the application is based, including the nature of the source of the information; and
 - (c) whether the public interest in the production of data from the computer system or data storage medium outweighs the right to privacy of a person whose privacy may be affected as a result of the production; and
 - (d) whether there is sufficient connection between the evidence sought and the offence to which the criminal investigation or proceeding relates; and

- (e) whether any condition should be included in the computer warrant; and
- (f) the proposed duration of the computer warrant; and
- (g) any other matters that the Court considers relevant.

41 Contents of computer warrant

A computer warrant must state the following information:

- (a) if a person is to be searched, the person's name, age and address; and
- (b) if a place is to be searched:
 - (i) a description of the place to be searched; and
 - (ii) if the place is occupied, the name and age of any occupiers of the place, if known; and
- (c) the offence to which the application relates; and
- (d) the types of evidential material that may be searched for; and
- (e) the power of the authorised officer to secure or render inaccessible a data storage medium, computer network or computer system; and
- (f) the date and time the computer warrant expires; and
- (g) any conditions imposed in relation to executing the computer warrant.

42 Extension of a computer warrant

- (1) The Court must specify in the computer warrant the date and time the computer warrant expires.
- (2) The Court may extend the date and time, when a computer warrant expires, if it is satisfied that the purpose for which the warrant was granted cannot be satisfied before the warrant is expired.

43 Application for an urgent computer warrant

- (1) If the Commissioner has authorised an application for an urgent computer warrant under section 38, an authorised officer may apply to the Court to grant an urgent computer warrant to access:
 - (a) a place specified in the warrant; or

- (b) a data storage medium at the location specified in the warrant; or
 - (c) a computer network at the location specified in the warrant; or
 - (d) a computer system at the location specified in the warrant.
- (2) An authorised officer may make an application for an urgent interception warrant orally, by telephone, email, facsimile or other electronic means.
- (3) The authorised officer in making an application under subsection (2) must set out:
 - (a) if a person is to be searched, the person's name, age and address; and
 - (b) if a place is to be searched:
 - (i) a description of the place to be searched; and
 - (ii) if the place is occupied, the name and age of any occupiers of the place, if known; and
 - (c) the offence to which the application relates; and
 - (d) a description of the nature of the data storage medium, computer network, computer system or suspected to be evidential material; and
 - (e) the information relied on to support the reasonable suspicion that evidence on the commission of an offence:
 - (i) is in or under the control of the person or at the place; or
 - (ii) is likely to be in or under the control of the person or at the place when an urgent computer warrant is executed; and
 - (f) if an urgent computer warrant was issued previously in relation to the person or place; and
 - (g) if authority to execute an urgent computer warrant at night is being sought, why it is necessary to execute the urgent computer warrant at night; and
 - (h) the period an urgent computer warrant is required.

- (4) The authorised officer must as soon as practicable, after the granting of the urgent computer warrant, send his or her application, in writing, to the Court.

44 Granting of an urgent computer warrant

- (1) The Court may grant an urgent computer warrant if the Court is satisfied with the application of the authorised officer made under section 43.
- (2) Without limiting subsection (1), prior to granting an urgent computer warrant, the Court must consider the following:
- (a) the urgency of the situation requiring an urgent computer warrant; and
 - (b) the seriousness of the offence to which the criminal investigation or proceeding relates; and
 - (c) the reliability of the information on which the application is based, including the nature of the source of the information; and
 - (d) whether the public interest in the production of data from the computer system or data storage medium outweighs the right to privacy of a person whose privacy may be affected as a result of the production; and
 - (e) whether there is sufficient connection between the evidence sought and the offence to which the criminal investigation or proceeding relates; and
 - (f) whether any condition should be included in the urgent computer warrant; and
 - (g) the proposed duration of the urgent computer warrant; and
 - (h) any other matters that the Court considers relevant.

45 Effects of a computer warrant and an urgent computer warrant

- (1) An authorised officer is authorised, under a computer warrant or an urgent computer warrant granted under sections 40 and 44, to:
- (a) seize an item that the authorised officer believes on reasonable grounds to be:
 - (i) evidential material in relation to an offence to which the warrant relates; or

- (ii) evidential material that is relevant to another offence under this Act or any other Act; and
- (b) access a data storage medium, or a computer network or a computer system for the purposes of obtaining information and records, and collate, copy or extract data; and
- (c) access, seize or secure any equipment, data storage medium, or other item by which information, records or data may be stored; and
- (d) require a person with a knowledge of a data storage medium, or a computer network or a computer system to assist the authorised officer in accessing the data storage medium, the computer network or the computer system; and
- (e) if an authorised officer suspects on reasonable grounds that the data that is accessible from the computer system might be the data that could be accessed, collated or seized under the warrant, or other item under paragraph(a), the authorised officer may:
 - (i) operate the computer system to access the data; or
 - (ii) operate another computer system accessible from the computer system operated under subparagraph (i) to access data; or
 - (iii) copy any or all of the data to another data storage medium or a computer network or a computer system; or
 - (iv) if, by using facilities at the place, the data can be put in a documentary form, operate the facilities to put that data in that form and seize the produced documents; and
- (f) move data storage medium or a computer network or a computer system at the place searched to another place for examination in order to determine whether it contains data that could be accessed, collated or seized under the warrant if:
 - (i) the occupier of the place consents; or
 - (ii) it is significantly more practicable to do so, having regard to the time it will take to copy the data, and there are reasonable grounds to suspect that the data that could be accessed, collated or seized under the warrant; and

- (g) do anything reasonably necessary to prevent loss, destruction or damage to anything connected with the offence or any other offence; and
 - (h) use other authorised officers or persons as reasonably necessary for the execution of the warrant; and
 - (i) search a person who is at the place when the warrant is executed if the authorised officer suspects, on reasonable grounds, that the person has any evidential material in the his or her possession.
- (2) If an authorised officer seizes a data storage medium, a computer network, a computer system, equipment, device or other items under subsection (1), the authorised officer:
 - (a) may take possession of it; and
 - (b) may retain it for such a time as he or she considers necessary for the purposes of this Act.
- (3) An authorised officer must return any item detained under subsection (2) to its owner if:
 - (a) it is no longer necessary to seize the item; or
 - (b) it is decided that the item is not to be used in evidence, except where the authorised officer believes, on reasonable grounds, that the possession of data may constitute an offence.

46 Access to seized data

- (1) Subject to subsection (2), on request, a police officer executing a computer warrant may:
 - (a) allow a person who had the custody or control of the data storage medium, computer network or computer system, or someone acting on the person's behalf, to access and copy of the data; or
 - (b) give that person a copy of that data held in the computer system.
- (2) The police officer may refuse to give access to, or provide copies of data held in a data storage medium, computer network or computer system, if the police officer believes on reasonable grounds that giving the access or providing the copies may:
 - (a) constitute an offence under this Act or any other Act; or

- (b) prejudice a criminal investigation or proceedings.

47 Securing or rendering inaccessible data under a computer warrant or an urgent computer warrant

- (1) For the purposes of this section, **expert** means a person qualified in digital forensics.
- (2) An authorised officer executing a computer warrant or an urgent computer warrant may do whatever is necessary to secure or render inaccessible a data storage medium, computer network or computer system if the police officer suspects, on reasonable grounds, that:
 - (a) evidence of the commission of an offence may be accessible by operating the data storage medium, computer network or computer system; and
 - (b) expert assistance is needed to operate the data storage medium, computer network or computer system; and
 - (c) if the police officer does not take action under this subsection, the evidence may be destroyed, altered or otherwise interfered with.
- (3) The police officer is to, by way of notice, notify the person who has custody or control of the data storage medium, computer network or computer system:
 - (a) the intention of the police officer to secure or render inaccessible the data storage medium, computer network and computer system; and
 - (b) that the data storage medium, computer network and computer system may be secured or inaccessible for up to 28 days.
- (4) The data storage medium, computer network or computer system may be secured or inaccessible until any of the following occurs:
 - (a) 28 days after the data storage medium, computer network or computer system is first secured or rendered inaccessible; or
 - (b) the data storage medium, computer network or computer system has been operated by an expert.
- (5) The police officer may apply to the Court for an extension of the time referred in paragraph (4)(a), if, the police officer believes, on reasonable grounds, that the expert assistance will not be available within that time.

- (6) The police officer may make more than 1 application under subsection (5) until the expert assistance is available.
- (7) The police officer must, by way of notice, notify the person who has custody or control of the data storage medium, computer network or computer system:
 - (a) the intention of the police officer to apply for an extension; and
 - (b) that the person is entitled to be heard in relation to the application.

48 Assisting police officer in executing computer warrant

- (1) A police officer may direct a person in possession or control of, or with knowledge of, the data storage medium, computer network or computer system to assist the police officer to:
 - (a) access and operate the data storage medium, computer network or computer system to access any computer data (including data stored at any place or on a separate data storage medium); and
 - (b) obtain and copy the data; and
 - (c) use equipment to make copies of the data; and
 - (d) obtain an intelligible output from the computer system in a format that can be read; and
 - (e) do anything that the police officer reasonably requires.
- (2) A person who fails without reasonable excuse to comply with a direction under subsection (1), commits an offence and is liable on conviction:
 - (a) in the case of an individual – to a fine not exceeding VT 1,000,000 or a term of imprisonment not exceeding 3 years or both; or
 - (b) in the case of a body corporate – to a fine not exceeding VT 2,000,000.

49 Exercising reasonable care

- (1) For the purposes of this section, **damage**, in relation to data, includes damage by erasing of the data or addition of other data but does not include the reasonable alteration of data by digital forensic processes.

- (2) A police officer, or a person assisting the police officer, when examining or retaining a data storage medium, computer network or computer system under a computer warrant or an urgent computer warrant must take reasonable care to prevent any damage to the following:
- (a) the data storage medium, computer network or computer system; and
 - (b) data stored on, or accessed by operating the data storage medium, computer network or computer system; and
 - (c) programs associated with the use of the data storage medium, computer network or computer system, or with the use of the data stored in the data storage medium, computer network or computer system.
- 50 Receipt for items seized under computer warrant**
- (1) For the purpose of this section, **receipt** means an inventory of all items collected during the execution of the computer warrant or urgent computer warrant.
- (2) If a computer warrant authorises a police officer to seize an item, the police officer must, after seizing the item, give the person searched or occupier of the place searched, a receipt for the item seized or leave a receipt for the item seized in a noticeable place at the place searched.
- (3) The receipt must include sufficient information to identify the following:
- (a) the item that was seized; and
 - (b) the time the item was seized; and
 - (c) the person who seized the item; and
 - (d) the place the item was taken; and
 - (e) the time the item is to be returned.
- (4) This section does not apply if a police officer believes, on reasonable grounds, that:
- (a) no person appears to be in possession of the item; or
 - (b) the item is abandoned.

51 Measures to control retention of seized data storage medium, computer network or computer system

- (1) A police officer who seizes a data storage medium, computer network or a computer system under a computer warrant or an urgent computer warrant, must, take reasonable steps to reduce the need for extended retention of data storage medium, computer network or computer system as evidence by doing any of the following as soon as practicable:
- (a) arranging for the data storage medium, computer network or computer system, or part thereof, to be copied; or
 - (b) arranging for any necessary test or examination of the data storage medium, computer network or computer system; or
 - (c) gathering any other available secondary evidence in relation to the data storage medium, computer network or computer system.
- (2) Despite subsection (1), a police officer may retain the data storage medium, computer network or computer system for a reasonable time if the police officer believes, on reasonable grounds, that it is necessary to do so to prevent the commission of an offence.

52 Destruction of certain data seized under a computer warrant or an urgent computer warrant

If the Commissioner is satisfied that data accessed or copied under a computer warrant or an urgent computer warrant is no longer useful for law enforcement purposes, the Commissioner must arrange for the destruction of the data, and any reproduction, under the control of the Vanuatu Police Force.

53 Prohibition on disclosure of information, records and data

- (1) A person who obtains information, extracts, records or data pursuant to a request, order or warrant under this Part must not knowingly disclose in whole or in part the information, extracts, records or data otherwise in the performance of his or her duties.
- (2) A person who contravenes subsection (1), commits an offence and is liable on conviction:
- (a) in the case of an individual- to a fine not exceeding VT1,000,000, or a term of imprisonment not exceeding 3 years, or both; or
 - (b) in the case of a body corporate- to a fine not exceeding VT2,000,000.

54 Evidentiary certificates for service providers

- (1) An authorised representative may issue an evidentiary certificate sworn by the authorised representative, setting out the facts, that the authorised representative considers relevant in relation to acts or things done by, or in relation to, the service provider in order:
- (a) to comply with a request for disclosure of subscriber data, traffic data or content data under sections 21, 22, and 24; or
 - (b) to comply with a request for access to traffic data in real time under section 23; or
 - (c) to comply with a preservation order under Division 2; or
 - (d) to enable an interception warrant to be executed.
- (2) An evidentiary certificate issued under subsection (1):
- (a) must be received as evidence in the proceeding without further proof; and
 - (b) is conclusive evidence of the matters stated in it.

55 Hindering or obstructing the lawful exercise of powers

- (1) A person commits an offence if without reasonable excuse that person:
- (a) hinders or obstructs a police officer, or a person assisting a police officer, in carrying out his or her duties under this Act; or
 - (b) intends to hinder or obstruct the police officer or a person assisting the police officer.
- (2) A person who commits an offence under subsection (1), is liable on conviction:
- (a) in the case of an individual- to a fine not exceeding VT1,000,000, or a term of imprisonment not exceeding 3 years, or both; or
 - (b) in the case of a body corporate- to a fine not exceeding VT2,000,000.

56 Obligations of service providers

- (1) A service provider must prevent communications networks and facilities from being used in, or in relation to, the commission of offences against this Act or any other Act.

- (2) A service provider or an authorised representative who receives a request for information under this Act must maintain the confidentiality of any procedures and information relating to the request.
- (3) A service provider or an authorised representative, who fails, without reasonable excuse, to comply with subsection (2) commits an offence and is liable on conviction, to a fine not exceeding VT2,000,000.
- (4) A service provider or an authorised representative, commits an offence if the service provider or the authorised representative fails to comply with a lawful request made by a police officer under this Act and is liable on conviction to a fine not exceeding VT2,000,000.
- (5) A reference in this section to giving assistance includes a reference to giving such assistance as is reasonably necessary for the following purposes:
 - (a) enforcing the criminal law and laws imposing pecuniary penalties; and
 - (b) assisting the enforcement of the criminal laws in force in a foreign country; and
 - (c) protecting the public revenue; and
 - (d) safe-guarding national security.

PART 5 INTERNATIONAL COOPERATION

57 General principles relating to mutual assistance

Vanuatu may cooperate with any foreign country, any foreign agency or any international agency for the purposes of investigations or proceedings concerning offences related to computer systems and data or for the collection of evidence in electronic form of a criminal offence pursuant to this Act and the Mutual Assistance in Criminal Matters Act.

58 Public Prosecutor to make and act on mutual assistance requests

- (1) The Public Prosecutor may make requests for mutual assistance in any investigation or proceeding commenced in Vanuatu, relating to any computer or computer related offence.
- (2) The Public Prosecutor may, in respect of any request from a foreign country for mutual assistance in any investigation or proceeding commenced in that foreign country:
 - (a) grant the request, in whole or in part, on such terms and conditions as he or she thinks fit; or
 - (b) refuse according to the terms set out under sections 8, 9 and 10 of the Mutual Assistance in Criminal Matters Act; or
 - (c) after consulting with the appropriate authority of the foreign country, postpone the request, in whole or in part on the ground that granting the request immediately would be likely to prejudice the conduct of an investigation or proceeding in Vanuatu.
- (3) A mutual assistance request under this section is to be executed according to the procedures specified by the foreign country, except where incompatible with the laws of Vanuatu.
- (4) Prior to refusing or postponing assistance, the Public Prosecutor is to, where appropriate after having consulted with the foreign country, consider whether the request may be granted partially or subject to conditions.
- (5) The Public Prosecutor is to immediately inform the foreign country of the outcome of the execution of a request for mutual assistance.
- (6) In addition to subsection (5), the Public Prosecutor is to inform the foreign country of any reasons:
 - (a) to render impossible the execution of the request; or

- (b) to delay the execution of the request significantly; or
 - (c) to postpone the request; or
 - (d) to refuse the request.
- (7) The foreign country may request the Public Prosecutor to keep confidential the fact of any request made under this Act or the Mutual Assistance in Criminal Matters Act, as well as its subject, except to the extent necessary for its execution.
- (8) If the Public Prosecutor cannot comply with the request for confidentiality under subsection (7), he or she must immediately inform the foreign country, whether the request should still be executed.
- (9) Subsections (8) applies *mutatis mutandis* when the Public Prosecutor is the requesting country.
- (10) If the foreign country cannot comply with such conditions under subsection (2), it must notify the Public Prosecutor, who will then determine whether the information should still be provided.
- (11) If the foreign country accepts the information subject to the conditions, it is to be bound by them.
- (12) Subsections (1), (2) and (3) apply *mutatis mutandis* when spontaneous information is provided to the Public Prosecutor by a foreign country.

59 Additional information

- (1) The Public Prosecutor may, subject to this Act and without prior request, forward to a foreign country information obtained within the framework of his or her own investigations when he or she considers that the disclosure of such information is necessary:
- (a) to assist the foreign country in initiating or carrying out investigations or proceedings; or
 - (b) and might lead to a request for co-operation by the foreign country under this Act.
- (2) Prior to providing such information, the Public Prosecutor may request that the information be kept confidential or only used subject to conditions.

60 Expedited preservation of stored computer data

- (1) A foreign country may request or otherwise obtain an expedited preservation of data stored by means of a computer system, located within the territory of Vanuatu and in respect of which the requesting foreign country, foreign agency or any international agency intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.
- (2) A request for expedited preservation made under subsection (1) must specify the following:
 - (a) the authority seeking the preservation; and
 - (b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; and
 - (c) the stored computer data to be preserved and its relationship to the offence; and
 - (d) any available information identifying the custodian of the stored computer data or the location of the computer system; and
 - (e) the necessity of the expedited preservation; and
 - (f) that the foreign country 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 a request under subsection (1), the Public Prosecutor must take all appropriate measures to preserve expeditiously the specified data in accordance with the procedures and powers provided under this Act.
- (4) Any expedited preservation effected in response to the request is to be for a period not less than 60 days, in order to enable the foreign country to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data and following the receipt of such a request, the data is to continue to be expedited preserved until a final decision is taken on that pending request.
- (5) Subsections (1) and (2) must apply *mutatis mutandis* when a request for expedited preservation of stored computer data is done by Vanuatu.

61 Expedited disclosure of preserved traffic data

- (1) In the course of executing a request under section 22 or otherwise in relation to a serious offence in a foreign country, the law enforcement

agency, with respect to a specified communication, discovers that a service provider in another country is involved in the transmission of the communication, the Public Prosecutor is:

- (a) to expeditiously disclose to the requesting foreign country a sufficient amount of traffic data to identify that service provider; and
 - (b) to disclose the path through which the communication was transmitted.
- (2) Expedited disclosure of preserved traffic data under subsection (1) may only be withdrawn if:
- (a) the request concerns a political offence or an offence related to a political offence; or
 - (b) the Public Prosecutor considers that the execution of the request is likely to prejudice Vanuatu's sovereignty, security or public interest.

62 Mutual assistance regarding accessing of stored computer data

- (1) A foreign country may request to order or to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of Vanuatu, in relation to a foreign serious offence, including data that has been preserved pursuant to section 18.
- (2) A request for mutual assistance regarding accessing of stored computer data is to, as far as practicable:
- (a) give the name of the authority conducting the investigation or proceeding to which the request relates; and
 - (b) give a description of the nature of the criminal matter and a statement setting out a summary of the relevant facts and laws; and
 - (c) give a description of the purpose of the request and of the nature of the assistance being sought; and
 - (d) in the case of a request to restrain or confiscate assets believed on reasonable grounds to be located in the requested country:
 - (i) give details of the offence in question; or

- (ii) particulars of any investigation or proceeding commenced in respect of the offence,

and be accompanied by a copy of any relevant restraining or confiscation order; and
 - (e) give details of any procedure that the requesting country wishes to be followed by the requested country in giving effect to the request, particularly in the case of a request to take evidence; and
 - (f) include a statement setting-out any wishes of the requesting country concerning any confidentiality relating to the request and the reasons for those wishes; and
 - (g) give details of the period within which the requesting country wishes the request to be complied with; and
 - (h) where applicable, give details of the property, computer, computer system or device to be traced, restrained, seized or confiscated, and the grounds for believing that the property is believed to be in the requested country; and
 - (i) give details of the stored computer data, data or program to be seized and its relationship to the offence; and
 - (j) give any available information identifying the custodian of the stored computer data or the location of the computer, computer system or device; and
 - (k) include an agreement on the question of the payment of the damages or costs of fulfilling the request; and
 - (l) give any other information that may assist in giving effect to the request.
- (3) Upon receiving the request under this section, the investigating agency must take all appropriate measures to obtain necessary authorisation including any warrants to execute upon the request in accordance with the procedures and powers provided under this Act.
- (4) Upon obtaining necessary authorisation including any warrants to execute upon the request, the investigating agency may seek the support and cooperation of the foreign country during the search and seizure.

- (5) Upon conducting the search and seizure request, the investigating agency must provide the results of such search and seizure to the foreign country.
- (6) Subsections (1) and (2) must apply *mutatis mutandis* to requests for expedited preservation of stored computer data in the territory of a foreign country.

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

A police officer may, without the authorisation but subject to any applicable provisions of this Act:

- (a) access publicly available stored computer data, regardless of where the data is located geographically; and
- (b) access or receive, through a computer system in its territory, stored computer data located in another territory, if such police officer or another authorised person obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data through that computer system.

64 Mutual assistance in the real-time collection of traffic data

- (1) A foreign country may request, in relation to a foreign serious offence, to order or provide assistance in real-time collection of traffic data associated with specified communications in Vanuatu transmitted by means of a computer system.
- (2) A request for assistance under this section is to specify:
 - (a) the authority seeking the use of powers under this section; and
 - (b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; and
 - (c) the name of the authority with access to the relevant traffic data; and
 - (d) the location at which the traffic data may be held; and
 - (e) the intended purpose for the required traffic data; and
 - (f) sufficient information to identify the traffic data; and
 - (g) any further details relevant traffic data; and

- (h) the necessity for use of powers under this section; and
 - (i) the terms for the use and disclosure of the traffic data to third parties.
- (3) Upon receiving a request under subsection (1), the investigating agency must take all appropriate measures to obtain the necessary authorisation, including any warrants to execute upon the request, in accordance with the procedures and powers provided under this Act.
- (4) Upon obtaining the necessary authorisation, including any warrants to execute upon the request, the investigating agency may seek the support and cooperation of the foreign country, during the search and seizure.
- (5) Upon conducting the measures under this section, the investigating agency must provide the results of such measures as well as real-time collection of traffic data associated with specified communications to the foreign country.
- (6) Subsections (1) and (2) must apply *mutatis mutandis* to requests for real-time collection of traffic data in a foreign country.

65 Mutual assistance regarding the interception of content data

- (1) A foreign country may request to order or otherwise provide assistance in the real-time collection, or recording of content data of specified communications transmitted by means of a computer system in Vanuatu.
- (2) A request for assistance under subsection (1), so far as practicable, must specify:
 - (a) the authority seeking the use of powers under this section; and
 - (b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; and
 - (c) the name of the authority with access to the relevant communication; and
 - (d) the location or the nature of the communication; and
 - (e) the intended purpose for the required communication; and
 - (f) sufficient information to identify the communications; and
 - (g) details of the data of the relevant interception; and

- (h) the recipient of the communication; and
 - (i) the intended duration for the use of the communication; and
 - (j) the necessity for use of powers under this section; and
 - (k) the terms for the use and disclosure of the communication to third parties.
- (3) Upon receiving a request under this section, the Public Prosecutor must take all appropriate measures to execute upon the request in accordance with the procedures and powers provided under this Act.
- (4) Upon conducting the measures under subsection (3), the Public Prosecutor must provide the results of such measures as well as real-time collection or recording of content data of specified communications to the foreign country.
- (5) Subsections (1) and (2) must apply *mutatis mutandis* to requests for real-time collection of traffic data in a foreign country.

66 24/7 Network

- (1) The Public Prosecutor must ensure that the investigating agency responsible for investigating and prosecuting cybercrime must designate a point of contact available on a twenty-four hour, seven-days-a-week basis.
- (2) A designated point of contact under subsection (1), is to ensure assistance is immediately provided for the purpose of:
- (a) investigations or proceedings concerning criminal offences related to computer systems and data; or
 - (b) for the collection of evidence in electronic form of a criminal offence,

which assistance is to include facilitating, or directly carrying out the following measures:

- (i) the provision of technical advice; and
- (ii) computer data and expedited disclosure of preserved traffic data; and
- (iii) the collection of evidence, the provision of legal information, and locating of suspects,

within expeditious timelines, as may be, prescribed by the Regulations.

- (3) The point of contact is to be resourced with and possess the necessary capacity to securely and efficiently carry out communications with other points of contact in other territories, on an expedited basis.
- (4) The point of contact is to have the authority and be empowered to coordinate and enable access to international mutual assistance under this Act or if applicable extradition procedures, upon an expedited basis.

67 Report on special investigative powers

- (1) The Commissioner must, on or before the end of March of each year, submit an annual report to the Council of Ministers setting out general information and statistics relating to the use of special investigative powers for the previous year.
- (2) The report must include to a minimum:
 - (a) the number of undercover operations authorised; and
 - (i) the number of orders issued to preserve computer data; and
 - (ii) the number of requests for traffic data in real time; and
 - (iii) the number of applications to produce computer data; and
 - (b) the number of applications for interception warrants and computer warrants; and
 - (c) the number of applications for renewals of interception warrants and computer warrants; and
 - (d) the number of applications for urgent interception warrants and urgent computer warrants; and
 - (e) the number of controlled deliveries of property authorised; and
 - (f) the number of applications referred to under paragraphs (b), (c) and (d) that were granted, and the number that were refused; and
 - (g) the number of prosecutions that have been instituted in which evidence obtained directly or indirectly from:
 - (i) an interception carried out pursuant to an interception warrant or urgent interception warrant; or

- (ii) a data storage medium, computer network or computer system pursuant to a computer warrant or urgent computer warrant; or
 - (iii) an undercover operation; or
 - (iv) an order to preserve computer data; or
 - (v) a request to access to traffic data and traffic data in real time; or
 - (vi) an order to produce computer data; or
 - (vii) a controlled delivery of property has been adduced, and the result of those prosecutions; and
 - (viii) the number of interception warrants and computer warrants that did not result in any charges being laid within 90 days after the date on which the warrant expired; and
 - (ix) the number of undercover operations and controlled deliveries of property that did not result in any charges being laid within 90 days after the date on which the undercover operation or controlled delivery ended.
- (3) Nothing in this section requires the Commissioner to publicly disclose the operational details of a particular case.

68 State not required to give undertaking for costs

Despite any other Act or law, Vanuatu is not required to give an undertaking for costs for applying for a warrant.

PART 6 MISCELLANEOUS

69 Authorised officer

- (1) The Commissioner may appoint a police officer as an authorised officer to perform any functions or exercise any powers that may be performed or exercised for the purposes of this Act, for a period as may be determined by the Commissioner.
- (2) The Commissioner is to provide to each authorised officer, an identity card that will provide evidence of the identity of that police officer and of the appointment of that police officer as an authorised officer.
- (3) An authorised officer who holds an identity card issued under this section must, on the termination of his or her appointment, surrender the identity card to the Commissioner.

70 Protection from liability

- (1) A police officer or authorised officer is not subject to any civil or criminal liability, action, claim or demand for anything done or omitted to be done by the police officer or authorised officer in good faith in the execution or purported execution of his or her powers and functions under this Act.
- (2) A service provider or an authorised representative is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in performance of a duty imposed under this Act.

71 Regulations

The Minister may, make Regulations prescribing matters:

- (a) required or permitted by this Act to be prescribed; or
- (b) that are necessary or convenient to be prescribed for the better carrying out or giving effect to the provisions of this Act.

72 Commencement

This Act comes into force on the day on which it is published in the Gazette.



RÉPUBLIQUE DE VANUATU

LOI N°22 DE 2021 SUR LA CYBERCRIMINALITE

Sommaire

TITRE 1 DISPOSITIONS PRÉLIMINAIRES

1	Définitions	4
2	Objet	9

TITRE 2 INFRACTIONS INFORMATIQUES

3	Accès illégal	10
4	Interception illégale	10
5	Interférences non autorisées	11
6	Utilisation abusive de dispositifs	13

TITRE 3 DÉLITS INFORMATIQUES

7	Pornographie infantile	14
8	Hébergement de pédopornographie	15
9	Délit lié à l'identité	15
10	Cyberharcèlement	16
11	Sollicitation d'enfants	16
12	Falsification informatique	16
13	Fraude informatique	17
14	Accès illégal avec intention de commettre ou de faciliter d'autres infractions	18

TITRE 4 PROCÉDURES

Sous-titre 1 Divulcation d'informations, assistance et la production de données informatiques

15	Divulcation d'informations relatives à une enquête	19
16	Assistance	19
17	Production de données informatiques	20

Sous-titre 2 Ordonnance de conservation

18	Ordonnance de conservation	21
19	Révocation de l'ordonnance de conservation	22
20	Prestataire de service ou agent autorisé à divulguer des données relatives au trafic	22

Sous-titre 3 Données relatives aux abonnés, données relatives au trafic et données relatives au contenu

21	Demande de divulgation des données relatives aux abonnés	22
22	Demande de divulgation de données relatives au trafic	23
23	Demande d'accès aux données relatives au trafic en temps réel ..	24
24	Divulgation des données relatives au contenu	25
25	Les données relatives aux abonnés, au trafic et au contenu ne doivent être utilisées qu'à des fins licites	25

Sous-titre 4 Divulgation à un organisme étranger chargé de l'application de la loi

26	Divulgation à un service répressif étranger	27
----	---	----

Sous-titre 5 Mandat d'interception

27	Le Commissaire autorise les demandes	27
28	Demande de mandat d'interception	27
29	Contenu et conditions d'un mandat d'interception	29
30	Octroi d'un mandat d'interception	31
31	Durée et prolongation du mandat d'interception	32
32	Mandat d'interception urgente	32
33	Prestataire de services à qui doit être signifié un mandat d'interception 34	
34	Admissibilité des preuves	34
35	Défaut mineur en rapport avec le mandat d'interception ou le mandat d'interception urgente	34
36	Interdiction de divulguer les communications interceptées et les enregistrements 35	
37	Révocation du mandat d'interception ou du mandat d'interception urgent	36

Sous-titre 6 Dispositions relatives aux mandats informatiques

38	Le commissaire autorisera les demandes	36
39	Demande de mandat informatique	37
40	Octroi d'un mandat informatique	38
41	Contenu du mandat informatique	38
42	Prolongation d'un mandat informatique	39
43	Demande d'un mandat informatique urgent	39
44	Octroi d'un mandat informatique urgent	41
45	Effets du mandat informatique et du mandat informatique urgent ..	42
46	Accès aux données saisies	44
47	Sécuriser ou rendre inaccessibles des données en vertu d'un mandat	

	informatique ou d'un mandat informatique urgent	44
48	Aide à un fonctionnaire de police dans l'exécution d'un mandat informatique	
	46	
49	Faire preuve d'une diligence raisonnable	47
50	Réception de biens saisis en vertu d'un mandat informatique	47
51	Mesures visant à contrôler la conservation du support de stockagedes données, du réseau informatique ou du système informatique saisi.....	48
52	Destruction de certaines données saisies en vertu d'un mandat informatique ou mandat informatique urgent	
	49	
53	Interdiction de divulgation d'informations, de dossiers et de données	49
54	Certificats de preuve pour les prestataires de services.....	49
55	Entrave ou obstruction à l'exercice légal des pouvoirs.....	50
56	Obligations des prestataires de services.....	50

TITRE 5 COOPÉRATION INTERNATIONALE

57	Principes généraux relatifs à l'assistance réciproque.....	52
58	Le Procureur général doit présenter des demandes d'assistance réciproque et y donner suite.....	52
59	Informations complémentaires	53
60	Conservation accélérée des données informatiques stockées	54
61	Divulgence accélérée des données relatives au trafic conservées	55
62	Assistance mutuelle en matière d'accès aux données informatiques stockée	55
63	Accès transfrontalier à des données informatiques stockées avec le consentement de l'intéressé ou lorsqu'elles sont accessibles au public	57
64	Assistance mutuelle dans la collecte en temps réel de données relatives au trafic.....	58
65	Assistance mutuelle en matière d'interception des données relatives au contenu	59
66	Réseau 24/7	60
67	Rapport sur les pouvoirs d'enquête spéciaux.....	61
68	L'État n'est pas tenu de s'engager sur les coûts	63

TITRE 6 DISPOSITIONS DIVERSES

69	Agent autorisé.....	64
70	Protection contre la responsabilité	64
71	Règlements.....	64
72	Entrée en vigueur.....	64

RÉPUBLIQUE DE VANUATU

Promulguée : 20/07/2021

Entrée en vigueur : 22/09/2021

LOI N° DE 2021 SUR LA CYBERCRIMINALITÉ

Loi prévoyant la réglementation de l'utilisation des systèmes, programmes et données informatiques et les questions connexes.

Le Président de la République et le Parlement promulguent le texte suivant :

TITRE 1 DISPOSITIONS PRÉLIMINAIRES

1 Définitions

Dans la présente Loi, sous réserve du contexte :

agent autorisé désigne un agent de police nommé en tant que tel en vertu de l'article 69 ;

agent de police désigne tout membre du Corps de Police de Vanuatu établi par la Loi sur la Police [CAP 105] ;

Commissaire désigne le Commissaire de police nommé en vertu de la Loi sur la Police [CAP 105] ;

communication désigne le transfert de signes, de signaux, d'écrits, d'images, de sons, de données ou de renseignements de toute nature transmis en tout ou en partie par des moyens électroniques ;

Cour signifie la Cour Suprême de Vanuatu ;

délit grave a la même signification que dans la Loi sur les Produits d'activité criminelle [CAP 284] ;

délit grave étranger a la même signification que dans la Loi sur les Produits d'activité criminelle [CAP 284] ;

dispositif désigne tout matériel ou équipement qui remplit une ou plusieurs fonctions spécifiques et fonctionne avec toute forme ou combinaison d'énergie électrique et comprend, sans s'y limiter, les éléments suivants :

- a) les composants de systèmes informatiques tels que les ordinateurs, les cartes graphiques, les téléphones mobiles ou les puces à mémoire ; ou
- b) des éléments de stockage tels que les disques durs, les cartes mémoire, les disques

TITRE 6 DISPOSITIONS DIVERSES

compacts ou les bandes ; ou

- c) des dispositifs de saisie tels que des claviers, des souris, des pavéstactiles, des scanners ou des appareils photo numériques ; ou
- d) les appareils de sortie tels que les imprimantes ou les écrans ;

dispositif d'interception a la même signification que dans la Loi N°37 de 2017 sur les Pouvoirs de la Police ;

données désigne toute représentation de faits, de concepts ou d'informations sous une forme qui se prête au traitement dans un système informatique, y compris un programme permettant à un système informatique d'exécuter une fonction ;

données d'abonné :

- a) désigne toute donnée détenue par un prestataire de services (sousforme de données informatiques ou sous toute autre forme) concernant une personne utilisant ou louant ses services (un « abonné ») et permettant d'établir ce qui suit :
 - i) le type de service utilisé, les dispositions techniques prises en relation avec le service et la période de service ;
 - ii) l'identité de l'abonné, son adresse postale ou géographique, son numéro de téléphone et autre numéro d'accès, ainsi que les informations relatives à la facturation et au paiement, disponibles sur la base du contrat ou de l'accord de service ; et
 - iii) tout autre donnée sur le site d'installation de l'équipement nécessaire à l'utilisation du service, disponible sur la base du contrat ou de l'accord de service ; et
- b) ne comprend pas les données relatives au trafic ou au contenu ;

données du contenu désigne la substance d'une communication spécifique qui est interceptée ;

données informatiques comprennent :

- a) les données introduites ou copiées dans un système informatique ;
- b) les données conservées sur un support de stockage amovible dans un système informatique ;
- c) les données conservées sur un support informatique sur un réseau informatique dont le système informatique fait partie ; et
- d) les données conservées sur d'autres supports de stockage informatique, y compris « cloud » ;
- e) toute représentation d'informations, de connaissances, de faits, de concepts ou

TITRE 6 DISPOSITIONS DIVERSES

d'instructions, qui est en cours d'élaboration ou a été élaborée et qui est destinée à être traitée, est en cours d'élaboration ou a été traitée dans un ordinateur ou un réseau informatique

- f) toute forme, qu'elle soit lisible uniquement par un ordinateur ou uniquement par un être humain ou par l'un ou l'autre, y compris, mais sans s'y limiter, les imprimés d'ordinateur, les supports de stockage magnétiques, les cartes perforées ou stockées à l'intérieur de la mémoire de l'ordinateur ;

données relatives au trafic signifient les données électroniques qui :

- a) se rapportent à une communication au moyen d'un système informatique ;
- b) est généré par un système informatique qui fait partie de la chaîne de communication ; et
- c) indique l'origine, la destination, l'itinéraire, l'heure, la date, la taille, la durée ou le type de services sous-jacents de la communication ;

enfant désigne une personne âgée de moins de 18 ans ;

en temps réel signifie lorsque des informations sont générées ou transmises ;

information signifie l'information, qu'elle se présente sous forme de données, de texte, de sons, d'images ou sous toute autre forme ;

infraction spécifiée signifie une infraction à une loi de Vanuatu pour laquelle la peine maximale est un emprisonnement d'au moins 4 ans ;

interception signifie la surveillance ou l'enregistrement de transmissions non publiques de données à destination, en provenance ou à l'intérieur d'un système informatique ;

Loi sur l'Assistance réciproque en matière d'affaires criminelles désigne la Loi sur l'Assistance réciproque en matière d'affaires criminelles [CAP 285] ;

mandat informatique désigne un mandat accordé en vertu de l'article 40 ;

mandat d'interception désigne un mandat autorisé en vertu de l'article 30 ;

mettre à disposition signifie, sans s'y limiter, la description de la manière d'obtenir l'accès, ou la description des méthodes susceptibles de faciliter l'accès ;

Ministre désigne le ministre responsable des technologies de l'information et de la communication ;

mandat informatique urgent désigne un mandat délivré en vertu de l'article 43 ;

mandat d'interception urgent désigne un mandat délivré en vertu de l'article 30.

pays étranger a la même signification que dans la Loi sur l'Assistance réciproque en matière

TITRE 6 DISPOSITIONS DIVERSES
d'affaires criminelles [CAP 285] ;

prestataire de services désigne :

- a) une entité publique ou privée qui fournit aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ;
- b) toute autre entité qui traite ou stocke des données informatiques pour le compte de cette entité ou de ces utilisateurs ;
- c) un prestataire de services au sens de la Loi N°30 de 2009 relative à la Réglementation des télécommunications et des radiocommunications ;

programme désigne les données représentant des instructions ou des déclarations qui, lorsqu'elles sont exécutées dans un système informatique, font en sorte que le système informatique exécute une fonction et les références à un programme comprennent les références à une partie d'un programme ;

représentant autorisé signifie :

- a) le directeur général ou le directeur exécutif d'un prestataire de services ou d'une personne morale dont le prestataire de services est une filiale ; ou
- b) le secrétaire d'un prestataire de services ou d'une personne morale dont le prestataire de services est une filiale ; ou
- c) un employé autorisé, par écrit, par le directeur général ou le secrétaire d'un prestataire de services ou d'une personne morale dont le prestataire de services est une filiale ;

réseau informatique désigne tout système qui assure la communication entre un ou plusieurs systèmes informatiques et ses périphériques d'entrée ou de sortie, y compris, mais sans s'y limiter, les terminaux d'affichage et les imprimantes qui sont reliés par des installations de télécommunication ;

sortie intelligible est une information provenant d'un système informatique, sous quelque forme que ce soit, qui peut être lue et comprise.

support de stockage informatique signifie tout article ou matériel à partir duquel l'information peut être reproduite, avec ou sans l'aide d'un autre article ou dispositif.

système informatique désigne :

- a) un ordinateur ; ou
- b) deux ou plusieurs ordinateurs interconnectés ; ou
- c) toute liaison de communication entre ordinateurs ou avec des terminaux distants ou un autre dispositif,

qui comprend également toute partie des éléments décrits aux points a) à d) et tous les intrants, extrants, traitements, stockage, logiciels ou installations de communication, « cloud » et les

2 Objet

La présente Loi a pour objet :

- a) de protéger la confidentialité, l'intégrité et la disponibilité des systèmes, programmes et données informatiques ;
- b) d'empêcher l'utilisation abusive des systèmes, programmes et données informatiques ; et
- c) de permettre la collecte de matériel médico-légal pour l'enquête et la poursuite des infractions à la présente Loi ; et
- d) de faciliter la coopération internationale.

TITRE 2 INFRACTIONS INFORMATIQUES

3 Accès illégal

- 1) Aux fins de l'application du présent article, on entend par **infrastructures critiques** les systèmes informatiques, les installations physiques, les processus, les chaînes d'approvisionnement, les technologies de l'information, les réseaux de communication, les dispositifs, les services publics et les services essentiels.
- 2) Toute personne qui, intentionnellement et sans excuse légitime, accède à tout ou partie d'un système informatique en enfreignant une mesure de sécurité, commet une infraction qui l'expose sur condamnation :
 - a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 2 000 000 VT ou d'emprisonnement n'excédant pas 5 ans, ou les deux à la fois ;
 - b) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 4 000 000 VT.
- 3) Toute personne qui, intentionnellement ou sans excuse légitime, accède à tout ou partie d'une infrastructure critique, commet une infraction qui l'expose sur condamnation :
 - a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 2 000 000 VT ou d'emprisonnement n'excédant pas 5 ans, ou les deux à la fois ;
 - b) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 4 000 000 VT.
- 4) Une personne ne commet pas d'infraction au titre du présent article si :
 - a) elle est autorisée à avoir accès au programme ou aux données ; ou
 - b) elle a consenti à avoir accès au programme ou aux données.

4 Interception illégale

- 1) Une personne ne doit pas, intentionnellement et sans excuse légitime, intercepter par un moyen technique quelconque :
 - a) toute transmission non publique de données informatiques à destination, en provenance ou à l'intérieur d'un système informatique ; ou
 - b) l'émission électromagnétique d'un système informatique transportant de telles données informatiques.

TITRE 6 DISPOSITIONS DIVERSES

- 2) Nonobstant le paragraphe 1), le Commissaire de Police peut, par ordonnance, autoriser l'interception de toute transmission non publique ou de toute émission électromagnétique.
- 3) Toute personne qui, intentionnellement et sans excuse légitime, intercepte à tout ou partie d'une infrastructure critique, commet une infraction qui l'expose sur condamnation :
 - a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 2 000 000 VT ou d'emprisonnement n'excédant pas 5 ans, ou les deux à la fois ;
 - b) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 4 000 000 VT.

5 Interférences non autorisées

- 1) Aux fins du présent article, on entend par intervention non autorisée :
 - a) une personne dont l'acte cause l'interférence et qui n'est pas habilitée à déterminer si l'interférence doit être faite ;
 - b) une personne qui n'a pas le consentement d'une personne ayant droit à l'intervention.
- 2) Toute personne qui, intentionnellement et sans autorisation, accomplit un acte qui provoque une interférence non autorisée avec un système, un programme ou des données informatiques commet une infraction qui l'expose sur condamnation :
 - a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 7 000 000 VT ou d'emprisonnement n'excédant pas 40 ans, ou les deux à la fois ; ou
 - b) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 100 000 000 VT.
- 3) Toute personne qui provoque une interférence non autorisée entraînant un préjudice grave dans l'un ou plusieurs domaines suivants :
 - a) perte financière de plus de 1 000 000 VT;
 - b) menace la sécurité nationale ;
 - c) cause un préjudice physique ou la mort d'une personne ;
 - d) menace la santé ou la sécurité publique ; commet une infraction qui l'expose sur condamnation :
 - a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas

TITRE 6 DISPOSITIONS DIVERSES

50 000 000 VT ou d'emprisonnement n'excédant pas 50 ans, ou les deux à la fois ; ou

- b) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 100 000 000 VT.

- 4) Toute personne qui provoque de manière imprudente une interférence non autorisée commet une infraction qui l'expose sur condamnation :

- a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 10 000 000 VT ou d'emprisonnement n'excédant pas 40 ans, ou les deux à la fois ; ou
- b) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 100 000 000 VT.

- 5) Aux fins du présent article, il est indifférent que l'intervention non autorisée ne soit pas dirigée contre :

- a) un système informatique, un programme ou des données en particulier ;
- b) un programme ou des données de quelque nature que ce soit ; ou
- c) un programme ou des données détenus dans un système informatique particulier.

- 6) Outre le paragraphe 5), il est indifférent qu'une intervention non autorisée ou tout effet prévu de celle-ci soit permanent ou temporaire.

6 Utilisation abusive de dispositifs

- 1) Toute personne qui, intentionnellement ou sans excuse légitime, produit, vend, se procure pour utilisation, importe, exporte, distribue ou met à disposition de toute autre manière :

- a) un logiciel, un système informatique ou un dispositif électronique ; ou
- b) un mot de passe, un code d'accès ou des données similaires permettant d'accéder à tout ou partie d'un système informatique ou de données électroniques ;

pour intercepter ou provoquer une interférence non autorisée, comme une infraction qui l'expose sur condamnation :

- a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 1 000 000 VT ou d'emprisonnement n'excédant pas 3 ans, ou les deux à la fois ; ou
- b) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 3 000 000 VT.

- 2) Nonobstant le paragraphe 1), ne constitue pas une infraction au titre du présent article :

TITRE 6 DISPOSITIONS DIVERSES

- a) tout acte visant à former, tester ou protéger un système informatique de manière autorisée; ou
- b) tout acte entrepris, conforme à une ordonnance de la Cour émise dans l'exercice de tout pouvoir en vertu de la présente Loi ou de toute autre loi.

TITRE 3 DÉLITS INFORMATIQUES

7 Pornographie infantile

1) Aux fins du présent article, la **pornographie infantile (ou pédopornographie)** comprend tout matériel, sans s'y limiter, audio, visuel ou textuel qui représente :

- a) un enfant se livrant à un comportement sexuellement explicite ;
- b) une personne apparaissant comme un enfant se livrant à un comportement sexuellement explicite ; ou
- c) des images, des animations ou des vidéos représentant un enfant se livrant à un comportement sexuellement explicite.

2) Toute personne qui, intentionnellement ou sans excuse légitime :

- a) produit de la pornographie infantile en vue de sa diffusion par le biais d'un système informatique ;
- b) offre ou sollicite ou rend disponible de la pornographie infantile par le biais d'un système informatique ;
- c) distribue ou transmet de la pornographie infantile par le biais d'un système informatique ;
- d) obtient ou sollicite de la pédopornographie par le biais d'un système informatique pour son usage personnel ou pour celui d'une autre personne ; ou
- e) possède de la pornographie infantile dans un système informatique ou sur un support de stockage électronique ;

commet une infraction qui l'expose sur condamnation :

- a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 5 000 000 VT ou d'emprisonnement n'excédant pas 10 ans, ou les deux à la fois ; ou
- b) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 15 000 000 VT.

8 Hébergement de pédopornographie

1) Une personne commet une infraction si :

- a) elle est un prestataire de service ; e
- b) elle sait ou prend conscience que le service fourni par une personne peut être utilisé pour accéder à un matériel particulier par rapport auquel elle a des motifs raisonnables de croire :

- i) qu'il s'agit d'un matériel pédopornographique; et
 - ii) qu'il ne communique pas les détails du matériel aux forces de Police de Vanuatu dans un délai raisonnable après avoir pris connaissance de l'existence du matériel,
- 2) Une personne qui commet une infraction en vertu du paragraphe 1) s'expose sur condamnation :
 - a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 5 000 000 VT ou d'emprisonnement n'excédant pas 10 ans, ou les deux à la fois ; ou
 - b) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 10 000 000 VT.

9 Délit lié à l'identité

Toute personne qui, intentionnellement ou sans excuse légitime, utilise un système informatique pour :

- a) transférer ;
- b) posséder ; ou
- c) utiliser,

l'identification d'une autre personne dans l'intention de commettre une activité illégale, de l'aider, de l'encourager ou de la relier à une activité illégale, commet une infraction qui l'expose sur condamnation :

- i) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 3 000 000 VT ou d'emprisonnement n'excédant pas 3 ans, ou les deux à la fois ;
- ii) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 5 000 000 VT.

10 Cyberharcèlement

- 1) Aux fins du présent article, cyberharcèlement signifie un acte visant à contraindre, intimider, harceler, insulter ou ennuyer une personne au moyen de systèmes informatiques ou de dispositifs électroniques.
- 2) Toute personne qui, directement ou indirectement, utilise une communication électronique à des fins de cyberharcèlement commet une infraction qui l'expose sur condamnation :
 - a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas

TITRE 6 DISPOSITIONS DIVERSES

1 000 000 VT ou d'emprisonnement n'excédant pas 3 ans, ou les deux à la fois ;

- b) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 3 000 000 VT.

11 Sollicitation d'enfants

Toute personne qui utilise un système informatique :

- a) pour proposer à un enfant ; ou
- b) proposer à une personne qu'elle croit être un enfant,

de la rencontrer ou de rencontrer une autre personne dans l'intention de l'exploiter sexuellement, que cette proposition ait été suivie ou non d'actes matériels, commet une infraction qui l'expose sur condamnation à une peine d'amende n'excédant pas 2 000 000 VT ou d'emprisonnement n'excédant pas 5 ans, ou les deux à la fois.

12 Falsification informatique

Toute personne qui, intentionnellement ou sans excuse légitime, produit des données non authentiques dans l'intention de les considérer ou d'y donner suite à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles ou intelligibles, et qui, à tort :

- a) obtient ;
- b) introduit ;
- c) modifie ;
- d) supprime ; ou
- e) dissimule,

des données électroniques, commet une infraction qui l'expose sur condamnation :

- i) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 5 000 000 VT ou d'emprisonnement n'excédant pas 12 ans ou les deux à la fois ;
- ii) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 10 000 000 VT.

13 Fraude informatique

Toute personne qui, intentionnellement ou sans excuse légitime, cause une perte de biens à une autre personne par :

- a) l'introduction, l'altération, la suppression ou la dissimulation de données ; ou

- b) toute interférence avec le fonctionnement d'un système informatique,

dans l'intention frauduleuse de procurer un gain personnel à une autre personne, commet une infraction qui l'expose sur condamnation :

- i) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 5 000 000 VT ou d'emprisonnement n'excédant pas 12 ans, ou les deux à la fois ;
- ii) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 10 000 000 VT.

14 Accès illégal avec intention de commettre ou de faciliter d'autres infractions

- 1) Une personne est coupable d'une infraction au titre du présent article si elle commet une infraction en vertu de l'article 3 avec l'intention de :

- a) commettre une infraction à laquelle le présent article s'applique ; ou
- b) faciliter la perpétration d'une telle infraction (que ce soit par l'auteur de l'infraction ou par toute autre personne),

et l'infraction que la personne a l'intention de commettre ou d'en faciliter la perpétration est une nouvelle infraction.

- 2) Il est indifférent, aux fins du présent article, que la nouvelle infraction soit commise en même temps que l'infraction d'accès non autorisé ou à une date ultérieure.
- 3) Une personne peut être accusée d'une infraction au titre du présent article même si les faits sont tels que la perpétration de la nouvelle infraction est impossible.
- 4) Toute personne qui accède intentionnellement, sans excuse légitime, à tout ou partie d'un système informatique et commet ou facilite la perpétration d'une nouvelle infraction, s'expose sur condamnation :
 - a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 7 000 000 VT ou d'emprisonnement n'excédant pas 7 ans, ou les deux à la fois ; ou
 - b) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 9 000 000 VT.

TITRE 4 PROCÉDURES

Sous-titre 1 Divulgence d'informations, assistance et la production de données informatiques

15 Divulgence d'informations relatives à une enquête

- 1) Aux fins du présent article, un prestataire de services comprend tout ou partie des employés, agents et sous-traitants du prestataire de services.
- 2) Un prestataire de services qui reçoit une ordonnance d'un tribunal, relative à une enquête pénale, qui prévoit que la confidentialité doit être maintenue ou que cette obligation est prévue par la loi et que le prestataire de services divulgue ou continue de divulguer :
 - a) le fait qu'une ordonnance a été rendue ; ou
 - b) tout ce qui est fait en vertu de l'ordonnance ; ou
 - c) toute donnée recueillie ou enregistrée en vertu de l'ordonnance, commet une infraction qui l'expose sur condamnation :
 - i. dans le cas d'un particulier – à une peine d'amende n'excédant pas 2 000 000 VT ou d'emprisonnement n'excédant pas 5 ans, ou les deux à la fois ; ou
 - ii. dans le cas d'une personne morale – à une peine d'amende n'excédant pas 5 000 000 VT.

16 Assistance

Une personne qui n'est pas suspectée d'un crime en vertu de la présente Loi, mais qui possède ou contrôle un dispositif ou des données faisant l'objet d'un mandat informatique en vertu du Sous-titre 6, doit, à ses propres frais, autoriser ou aider un agent autorisé à effectuer la perquisition et :

- a) accéder et utiliser l'appareil ou les données ;
- b) obtenir une copie de ces données ;
- c) utiliser l'appareil pour faire des copies ; et
- d) obtenir une sortie intelligible d'un appareil dans un format lisible.

17 Production de données informatiques

- 1) Le présent article s'applique si un agent de police demande à un tribunal que des données contenues dans un support de stockage de données, un réseau d'ordinateurs ou un système informatique, ou un imprimé ou toute autre information, soit raisonnablement nécessaire pour une enquête ou une procédure pénale impliquant une infraction spécifiée aux lois de Vanuatu ou une infraction grave aux lois d'un pays étranger.
- 2) Le tribunal peut ordonner :
 - a) qu'une personne ayant le contrôle du support de stockage des données, du réseau d'ordinateurs ou du système informatique produise d'une manière précisée dans l'ordonnance des données spécifiques ou une impression ou toute sortie intelligible de ces données ; et
 - b) une personne qui a accès à un processus informatique spécifié pour compiler les données détenues dans le système et les donner à une personne spécifiée.
- 3) Avant de rendre une ordonnance en vertu du paragraphe 2), la Cour doit prendre en considération les éléments suivants :
 - a) la gravité de l'infraction sur laquelle porte l'enquête ou la procédure pénale ;
 - b) la fiabilité des informations sur lesquelles la demande est fondée, y compris la nature de la source des informations ;
 - c) si l'intérêt public dans la production de données à partir du système informatique ou du support de stockage de données l'emporte sur le droit à la vie privée d'une personne dont la vie peut être affectée du fait de la production ;
 - d) s'il existe un lien suffisant entre les preuves recherchées et l'infraction à laquelle se rapporte l'enquête ou la procédure pénale ;
 - e) si une condition doit être incluse dans l'ordonnance ; et
 - f) toute autre question que la Cour juge pertinente.

Sous-titre 2 Ordonnance de conservation

18 Ordonnance de conservation

- 1) Le Commissaire peut, aux fins de conserver des données informatiques, y compris les données relatives au trafic ou au contenu, en possession ou sous le contrôle d'une personne, demander au tribunal une ordonnance de conservation.
- 2) La Cour peut accorder une ordonnance de conservation si elle est convaincue, pour des motifs raisonnables, que la conservation des données informatiques est raisonnablement nécessaire à des fins répressives ou pour une enquête ou une procédure pénale portant sur une infraction grave à la législation d'un pays étranger.

- 3) Une ordonnance de conservation :
 - a) entre en vigueur lorsque le prestataire de services la reçoit ; et
 - b) reste en vigueur pendant la période indiquée dans l'ordonnance de conservation ou jusqu'à sa révocation par la Cour en vertu de l'article 19.
- 4) Une ordonnance de conservation ne doit pas rester en vigueur pendant une période de plus de 90 jours.
- 5) Nonobstant le paragraphe 4), si la Cour est convaincue qu'il faut plus de temps pour obtenir ce qui est requis par l'ordonnance de conservation, il peut prolonger la période pendant laquelle l'ordonnance de conservation est en vigueur, pour 90 jours supplémentaires.
- 6) La personne à qui une ordonnance de conservation a été délivrée doit garder l'ordonnance et toutes les informations la concernant confidentielles.
- 7) Une personne qui, sans excuse raisonnable, :
 - a) ne respecte pas une ordonnance émise en vertu du paragraphe 2) ;
 - b) ne garde pas confidentielles toutes les informations relatives à l'ordonnance conformément au paragraphe 6)commet une infraction qui l'expose sur condamnation :
 - i) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 1 000 000 VT ou d'emprisonnement n'excédant pas 3 ans ou les deux à la fois ; ou
 - ii) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 2 000 000 VT.

19 Révocation de l'ordonnance de conservation

- 1) Si la Cour estime pour des motifs raisonnables que l'ordonnance de conservation n'est plus nécessaire, elle doit révoquer l'ordonnance de conservation à tout moment avant expiration.
- 2) Si une ordonnance de conservation est révoquée, un agent de police doit en informer immédiatement le représentant autorisé du prestataire de services et lui remettre une copie de la révocation.

20 Prestataire de service ou agent autorisé à divulguer des données relatives au trafic

Un prestataire de service ou son agent autorisé faisant l'objet d'une ordonnance de conservation doit divulguer, dès que possible, une quantité suffisante de données relatives au trafic pour permettre à un agent de police d'identifier tout autre prestataire de service impliqué dans la

Sous-titre 3 Données relatives aux abonnés, données relatives au trafic et données relatives au contenu

21 Demande de divulgation des données relatives aux abonnés

- 1) Le Commissaire peut, par écrit, demander à un prestataire de services de divulguer les données relatives aux abonnés s'il est convaincu que cette divulgation est nécessaire :
 - a) à des fins répressives; ou
 - b) pour l'exécution d'une infraction étrangère grave en vertu de la Loi sur l'Assistance réciproque en matière d'affaires criminelles.
- 2) Le prestataire de services doit se conformer à la demande visée au paragraphe 1) dès que possible après l'avoir reçue.
- 3) Le prestataire de services qui ne se conforme pas au paragraphe 2) commet une infraction qui l'expose à une condamnation à une peine d'amende n'excédant pas 1 000 000 VT.

22 Demande de divulgation de données relatives au trafic

- 1) Le Commissaire peut, par écrit, demander à un prestataire de services de divulguer des enregistrements de données relatives au trafic qui ont été créés avant le moment où la divulgation est demandée, si cette divulgation est raisonnablement nécessaire :
 - a) à des fins d'application de la Loi ; ou
 - b) pour l'exécution d'une infraction grave commise à l'étranger en vertu de la Loi sur l'Assistance réciproque en matière d'affaires criminelles.
- 2) Avant de présenter une demande au titre du paragraphe 1), le Commissaire doit :
 - a) être convaincu que l'intérêt public, lors de la divulgation des données, l'emporte largement sur le droit à la vie privée d'une personne dont la vie privée peut être affectée par la divulgation ; et
 - b) examiner toute question pertinente pour donner l'approbation, notamment les suivantes :
 - i) le volume et la nature des données à divulguer ;
 - ii) la gravité de la conduite faisant l'objet de l'enquête ;
 - iii) l'utilité probable des données pour l'enquête ; et

TITRE 6 DISPOSITIONS DIVERSES

- iv) la finalité pour laquelle l'accès aux données est demandé.
- 3) Le prestataire de services doit répondre à la demande visée au paragraphe 1) dès que possible après l'avoir reçue.
- 4) Le prestataire de services qui ne se conforme pas au paragraphe 3) commet une infraction qui l'expose sur condamnation à une peine d'amende n'excédant pas 2 000 000 VT.

23 Demande d'accès aux données relatives au trafic en temps réel

- 1) Le Commissaire peut, par écrit, demander à un fournisseur de services de donner accès aux enregistrements de données relatives au trafic en temps réel pendant une période maximale de 90 jours si cet accès est raisonnablement nécessaire pour :
 - a) l'exécution d'une infraction punie, sur condamnation, d'une peine d'emprisonnement d'au moins 2 ans en vertu de la présente Loi ou de toute autre loi ; ou
 - b) pour l'exécution d'une infraction grave commise à l'étranger en vertu de la Loi sur l'Assistance réciproque en matière d'affaires criminelles.
- 2) Avant de présenter une demande au titre du paragraphe 1), le Commissaire doit :
 - a) être convaincu que l'intérêt public à accéder aux documents l'emporte largement sur le droit à la vie privée d'une personne dont la vie privée peut être affectée par l'accès ; et
 - b) examiner toute question pertinente pour donner l'approbation, notamment les suivantes :
 - i) le volume et la nature des documents à divulguer ;
 - ii) la gravité du comportement faisant l'objet de l'enquête ;
 - iii) l'utilité probable des documents pour l'enquête ; ou
 - iv) la raison pour laquelle l'accès aux documents est demandé.
- 3) Le Commissaire doit, par écrit, annuler une demande au titre du paragraphe 1) à tout moment avant qu'elle ne prenne fin, s'il est convaincu que la demande n'est plus nécessaire.
- 4) Le Commissaire doit, par écrit, informer le prestataire de services ou son représentant autorisé de l'annulation en vertu du paragraphe 3) et lui fournir une copie de l'annulation, immédiatement après l'annulation de la demande.

24 Divulgarion des données relatives au contenu

- 1) Un agent autorisé peut demander à la Cour d'ordonner l'accès aux données relatives au contenu et leur divulgation comme suit :
 - a) une personne ayant participé ou soupçonnée pour des motifs raisonnables d'avoir participé à la perpétration de :
 - i) une infraction spécifique ; ou
 - ii) une infraction étrangère grave en vertu de la Loi sur l'Assistance réciproque en matière d'affaires criminelles, et
 - b) un service qui a été utilisé, est utilisé ou est susceptible d'être utilisé par une personne en vertu du paragraphe a).
- 2) L'agent habilité à présenter une demande au titre du paragraphe 1) doit indiquer dans sa demande :
 - a) les détails de chaque service fourni sous réserve de l'ordonnance ; et
 - b) l'infraction ou les infractions auxquelles la demande se rapporte ; et
 - c) les informations et les preuves invoquées ; et
 - d) si une ordonnance de conservation a été délivrée.
- 3) L'agent habilité doit fournir toute information supplémentaire que la Cour requiert concernant les motifs pour lesquels l'ordonnance est demandée.

25 Les données relatives aux abonnés, au trafic et au contenu ne doivent être utilisées qu'à des fins licites

- 1) Les données relatives aux abonnés obtenues en vertu de l'article 21 doivent être utilisées :
 - a) aux fins pour lesquelles elles ont été obtenues à l'origine ;
 - b) pour faire respecter la loi pénale, une loi imposant une sanction pécuniaire ou pour protéger les recettes publiques ; ou
 - c) pour exécuter une ordonnance étrangère de confiscation ou une ordonnance étrangère de sanction pécuniaire en rapport avec une infraction grave commise à l'étranger en vertu de la Loi sur l'Assistance réciproque en matière d'affaires criminelles.
- 2) Les données relatives au trafic obtenues en temps réel doivent être utilisées :

TITRE 6 DISPOSITIONS DIVERSES

- a) aux fins pour lesquelles elles ont été obtenues à l'origine ;
 - b) pour faire respecter la loi pénale, une loi imposant une sanction pécuniaire ou pour protéger les recettes publiques ; ou
 - c) pour exécuter une infraction grave commise à l'étranger conformément à une autorisation délivrée en vertu de la Loi sur l'Assistance réciproque en matière d'affaires criminelles.
- 3) Les données relatives au contenu conservées conformément à l'article 18 sont utilisées :
- a) aux fins pour lesquelles les données relatives au contenu ont été obtenues à l'origine ; ou
 - b) pour faire respecter une infraction spécifiée ou une infraction prévue par la présente partie ; ou
 - c) pour exécuter une infraction grave commise à l'étranger conformément à une autorisation délivrée en vertu de la Loi sur l'Assistance réciproque en matière d'affaires criminelles.
- 4) Si le Commissaire est convaincu que les informations obtenues ne sont plus nécessaires, il doit faire en sorte que la destruction des données et toute reproduction des données soient placées sous le contrôle des Forces de Police de Vanuatu.

Sous-titre 4 Divulgarion à un organisme étranger chargé de l'application de la loi

26 Divulgarion à un service répressif étranger

- 1) Les renseignements obtenus en vertu de la présente partie ne doivent pas être communiqués à un organisme étranger chargé de l'application de la loi, sauf si la communication a été autorisée par le Commissaire.
- 2) Le Commissaire ne doit pas autoriser une divulgation en vertu de la présente partie à moins qu'il ne soit convaincu que :
 - a) que la communication est raisonnablement nécessaire pour l'exécution d'un délit grave à l'étranger ; et
 - b) est appropriée en toutes circonstances.

Sous-titre 5 Mandat d'interception

27 Le Commissaire autorise les demandes

- 1) Le Commissaire peut autoriser une demande de :

- a) un mandat d'interception ;
 - b) le renouvellement d'un mandat d'interception ; ou
 - c) un mandat d'interception urgent.
- 2) Le Commissaire ne peut autoriser la demande visée au paragraphe 1) que s'il est convaincu qu'il existe des motifs raisonnables de soupçonner qu'une personne :
- a) planifie une infraction spécifiée, y participe ou la commet ; ou
 - b) a planifié, participé ou commis une infraction spécifiée.

28 Demande de mandat d'interception

- 1) Si le Commissaire a autorisé une demande de mandat d'interception en vertu de l'article 27, un agent de police doit demander au tribunal de délivrer le mandat d'interception pour :
- a) intercepter une communication privée au moyen d'un dispositif d'interception ; ou
 - b) enregistrer visuellement ou observer une activité d'une personne au moyen d'un dispositif d'interception ; ou
 - c) utiliser à la fois un dispositif d'interception et un dispositif de surveillance optique.
- 2) La demande doit être faite par écrit et sous serment par un officier de police, et doit indiquer :
- a) la personne ou le client, s'il est connu, dont la communication doit être interceptée ; et
 - b) le prestataire de services auquel doit être adressée la directive d'intercepter la communication, le cas échéant ; et
 - c) les faits invoqués pour démontrer qu'il existe des motifs raisonnables de soupçonner qu'une personne prépare ou commet une infraction spécifiée, ou a préparé ou commis une telle infraction, ou y a participé ; et
 - d) une description de la manière dont il est proposé d'intercepter des communications privées ou d'enregistrer ou d'observer des activités ; et
 - e) la mesure dans laquelle d'autres méthodes d'enquête sur l'infraction, autres qu'un mandat d'interception, ont été utilisées par l'agent de police ou sont à sa disposition ; et
 - f) soit :

- i) le nom et l'adresse, s'ils sont connus, de la personne dont les communications privées ou un enregistrement ou des observations sur les activités qu'il y a des motifs raisonnables de soupçonner aideront l'enquête de police sur l'affaire ; ou
 - ii) si le nom et l'adresse du suspect ne sont pas connus, une description générale des locaux, du lieu, de la chose ou du type d'installation pour lesquels il est proposé d'intercepter des communications privées ou d'enregistrer ou d'observer des activités ; et
 - g) la période pour laquelle un mandat est demandé.
- 3) Aux fins du présent article, dispositif de surveillance optique a la même signification que dans la Loi N°37 de 2017 sur les Pouvoirs de la police.

29 Contenu et conditions d'un mandat d'interception

- 1) Le mandat d'interception doit être établi selon la forme prescrite et contenir les informations suivantes :
 - a) l'infraction ou les infractions pour lesquelles le mandat est accordé ; et
 - b) si le mandat porte sur l'utilisation d'un dispositif d'interception dans les locaux :
 - i) le nom et l'adresse du suspect dont les communications privées peuvent être interceptées ou dont les activités peuvent être enregistrées ou observées ; ou
 - ii) si le nom et l'adresse du suspect ne sont pas connus, une description générale des locaux, du lieu, de la chose ou du type d'installation pour lesquels les communications privées seront interceptées ou les activités enregistrées ou observées ; et
 - c) si le mandat autorise l'utilisation d'un dispositif d'interception en ce qui concerne les conversations, les activités ou le lieu où se trouve une personne, indiquer le nom de la personne (s'il est connu) ou le fait que son identité est inconnue ; et
 - d) toute autre condition que la Cour estime nécessaire pour des raisons d'intérêt public.
- 2) Un mandat d'interception a pour effet, selon ses termes, d'autoriser
 - a) l'interception de communications privées au moyen d'un dispositif d'interception ; ou
 - b) l'enregistrement visuel ou l'observation d'une activité d'une personne au moyen d'un dispositif d'interception ; ou
 - c) les activités visées aux points a) et b).

TITRE 6 DISPOSITIONS DIVERSES

- 3) Outre le paragraphe 2), un mandat d'interception autorise :
- a) la récupération d'un dispositif d'interception ; et
 - b) l'entrée, avec la force raisonnable nécessaire, dans tout local en vue de placer, d'entretenir ou de récupérer un dispositif d'interception ; et
 - c) la connexion du dispositif d'interception à toute source d'électricité et l'utilisation de l'électricité de cette source pour faire fonctionner le dispositif ; et
 - d) la fourniture d'une assistance ou d'une expertise technique à l'agent de police principalement responsable de l'exécution du mandat pour l'installation, l'utilisation, l'entretien ou la récupération du dispositif d'interception.
- 4) Si le mandat autorise le placement d'un dispositif d'interception dans un lieu d'habitation ou d'affaires de :
- a) un avocat, d'un membre du clergé ou d'un médecin ; ou
 - b) une personne désignée par la Cour,

la Cour peut fixer les conditions qu'elle estime nécessaires pour éviter dans la mesure du possible l'interception d'information ou d'enregistrement ou l'observation d'activités de caractère professionnel auxquelles l'avocat, l'ecclésiastique, le médecin ou toute autre personne désignée par la Cour est partie.

- 5) Pour éviter tout doute, un mandat d'interception ne doit pas nécessairement être limité à des locaux particuliers et peut s'appliquer à un dispositif d'interception conçu pour intercepter des communications ou observer ou enregistrer des activités impliquant une personne, où que cette personne se trouve.

30 Octroi d'un mandat d'interception

- 1) La Cour peut accorder un mandat d'interception si elle est convaincue qu'il existe des motifs raisonnables :
- a) de soupçonner qu'une personne planifie ou commet une infraction spécifiée, ou y participe ou l'a planifiée ou commise, ou y a participé ; et
 - b) de croire que des preuves pertinentes pour l'enquête sur l'affaire seront obtenues par l'utilisation d'un mandat d'interception pour intercepter des communications privées ou enregistrer ou observer des activités ; et
 - c) que l'interception proposée est justifiée par le préjudice social de l'infraction présumée contre laquelle elle est dirigée.
- 2) Outre le paragraphe 1), la Cour doit, avant d'accorder un mandat d'interception, prendre

TITRE 6 DISPOSITIONS DIVERSES

en considération les éléments suivants :

- a) la gravité de l'infraction sur laquelle porte l'enquête ou la procédure pénale ;
- b) la fiabilité des informations sur lesquelles la demande est fondée, y compris la nature de la source des informations ;
- c) si l'intérêt public dans la production de données à partir du système informatique ou du support de stockage des données l'emporte sur le droit à la vie privée d'une personne dont la vie privée peut être affectée par la production ;
- d) s'il existe un lien suffisant entre les preuves recherchées et l'infraction à laquelle se rapporte l'enquête ou la procédure pénale ;
- e) si une condition doit être incluse dans le mandat ;
- f) si le pays étranger a présenté une demande d'entraide en vertu de la présente Loi ou de la Loi sur l'Assistance réciproque en matière d'affaires criminelles et si le Procureur général a autorisé l'utilisation d'un pouvoir d'investigation légal ; et
- g) toute autre question que la Cour juge pertinente.

31 Durée et prolongation du mandat d'interception

- 1) Un mandat d'interception est valable pour la période spécifiée dans le mandat, soit une période n'excédant pas 90 jours.
- 2) Sous réserve du paragraphe 1), la Cour peut accorder une prolongation d'un mandat d'interception sur demande faite avant l'expiration du mandat (ou de tout renouvellement en cours du mandat).
- 3) Une demande de prolongation d'un mandat d'interception doit :
 - a) fournir la raison et la période pour lesquelles le renouvellement est requis ; et
 - b) être accompagnée de renseignements complets, ainsi que des dates et heures, sur toute interception effectuée ou tentée en vertu du mandat et d'une indication de la nature des informations qui ont été obtenues par cette interception ; et
 - c) être étayées par toute autre information que la Cour estime nécessaire.
- 4) La Cour peut prolonger un mandat d'interception si elle est convaincue que les circonstances décrites à l'article 28 sont toujours applicables.

32 Mandat d'interception urgente

- 1) La Cour peut accorder un mandat d'interception urgente si elle est convaincue que :

TITRE 6 DISPOSITIONS DIVERSES

- a) les circonstances auxquelles la demande se rapporte sont urgentes ; ou
- b) le retard qui serait causé par le fait que la demande soit faite en personne ferait obstacle à l'exécution effective du mandat.
- 2) Un agent de police peut faire une demande de mandat d'interception urgente oralement, par téléphone, par courrier électronique, par télécopie ou par tout autre moyen électronique.
- 3) La Cour peut, oralement ou par écrit, décerner un mandat d'interception urgente pour :
 - a) l'interception de communications privées ; ou
 - b) l'enregistrement d'activités concernant un local particulier ; ou
 - c) une personne particulière ; ou
 - d) un lieu particulier ; ou
 - e) une chose particulière ; ou
 - f) un type d'installation particulier, et d'une manière particulière.
- 4) Le contenu et les termes d'un mandat d'interception en vertu de l'article 29 s'appliquent au contenu et aux termes d'un mandat d'interception urgent.
- 5) Un mandat d'interception urgente est valable pendant 48 heures à compter de son émission.
- 6) Sous réserve du paragraphe 1), la Cour doit, dès que possible, remettre une copie du mandat à l'agent de police qui a demandé le mandat d'interception urgent conformément au paragraphe 2).
- 7) S'il n'est pas raisonnablement possible pour la Cour de donner une copie du mandat d'interception urgent à l'agent de police :
 - a) elle doit informer l'agent de police des conditions du mandat ainsi que de la date et de l'heure de sa signature ; et
 - b) l'agent de police doit consigner les informations suivantes :
 - i) le nom du juge qui a émis le mandat d'interception urgent ; et
 - ii) la date et l'heure de la signature du mandat d'interception urgent ; et

33 Prestataire de services à qui doit être signifié un mandat d'interception

- 1) Si un mandat d'interception est délivré sous cette division pour intercepter une communication privée, l'agent autorisé doit :
 - a) informer le prestataire de services de l'existence du mandat ; et
 - b) de signifier une copie du mandat au prestataire de services.
- 2) Le prestataire de services doit se conformer au mandat dès qu'il est signifié.

34 Admissibilité des preuves

- 1) Toute information ou tout enregistrement obtenu en vertu d'un mandat d'interception ou d'un mandat d'interception urgente est admissible comme preuve dans toute procédure de poursuite d'une infraction spécifiée.
- 2) Toute information ou tout enregistrement obtenu en violation du paragraphe 29. 4) ne constitue pas une preuve recevable.

35 Défaut mineur en rapport avec le mandat d'interception ou le mandat d'interception urgente

- 1) Le présent article s'applique si :
 - a) une information ou un enregistrement est censé être obtenu par l'utilisation d'un dispositif d'interception autorisé en vertu d'un mandat d'interception ou d'un mandat d'interception urgente ; et
 - b) il y a un défaut ou une irrégularité mineur(e) en relation avec le mandat d'interception ou le mandat d'interception urgente et, sans ce défaut ou cette irrégularité, le mandat d'interception ou le mandat d'interception urgente aurait été une autorité suffisante pour la mesure prise.
- 2) Le présent article s'applique si :
 - a) l'utilisation du dispositif d'interception doit être considéré comme valide ; et
 - b) toute information ou enregistrement obtenu en vertu du mandat d'interception ou du mandat d'interception urgente est admissible comme preuve comme si le mandat d'interception ou le mandat d'interception urgente ne comportait pas cette déformation ou irrégularité.
- 3) La référence au paragraphe 1) à un défaut ou à une irrégularité en rapport avec un mandat d'interception ou un mandat d'interception urgente est une référence à un défaut ou à une irrégularité (autre qu'un défaut ou une irrégularité substantielle) :
 - a) dans le cadre ou en relation avec la délivrance d'un document censé être ce mandat

d'interception ou ce mandat d'interception urgente ; ou

- b) en rapport avec l'exécution de ce mandat d'interception ou de ce mandat d'interception urgente ou avec l'exécution d'un document censé être ce mandat d'interception ou ce mandat d'interception urgente.

36 Interdiction de divulguer les communications interceptées et les enregistrements

- 1) Une personne qui :

- a) intercepte ou aide à intercepter une communication privée conformément à un mandat d'interception ou à un mandat d'interception urgente ; ou
- b) acquiert la connaissance d'une communication privée comme résultat direct ou indirect de cette interception ; ou
- c) consigne les activités d'une personne,

cette communication ne doit pas divulguer en tout ou partie la substance ou la signification de ou de cet enregistrement .

- 2) Toute personne qui enfreint le paragraphe 1) commet une infraction qui l'expose sur condamnation :
 - a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 2 000 000 VT ou d'emprisonnement n'excédant pas 5 ans, ou des deux à la fois ; ou
 - b) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 4 000 000 VT.

37 Révocation du mandat d'interception ou du mandat d'interception urgent

- 1) Un agent de police peut, à tout moment, demander à la Cour de révoquer un mandat d'interception ou un mandat d'interception urgent.
- 2) La Cour doit révoquer un mandat d'interception ou mandat d'interception urgent si elle est convaincue que le mandat n'est plus nécessaire.
- 3) Si un mandat d'interception ou mandat d'interception urgent visant à intercepter une communication privée est révoqué, l'agent de police doit informer le prestataire de services ou son représentant autorisé de la révocation, et donner au prestataire de services ou à son représentant autorisé une copie de la révocation, immédiatement après que le mandat a été révoqué.

Sous-titre 6 Dispositions relatives aux mandats informatiques

38 Le commissaire autorisera les demandes

TITRE 6 DISPOSITIONS DIVERSES

- 1) Le commissaire peut autoriser une demande de :
 - a) un mandat informatique ou le renouvellement d'un mandat informatique ; ou
 - b) un mandat informatique urgent.
- 2) Le Commissaire ne doit pas autoriser la demande visée au paragraphe 1), sauf s'il est convaincu qu'il existe des motifs raisonnables de soupçonner qu'il peut y avoir sur la personne ou sur le lieu un support de stockage de données, ou un réseau ou un système informatique qui :
 - a) peut constituer une preuve matérielle de la commission d'une infraction déterminée ;
 - b) peut constituer une preuve matérielle de la commission d'une infraction grave étrangère ;
 - c) a été acquise par une personne à la suite de la commission d'une infraction.

39 Demande de mandat informatique

- 1) Si le commissaire a autorisé une demande de mandat informatique en vertu de l'article 38, un agent autorisé doit demander à la Cour d'accorder un mandat informatique pour l'accès à :
 - a) un lieu spécifié dans le mandat ; ou
 - b) un support de stockage des données à l'endroit indiqué dans le mandat ; ou
 - c) un réseau informatique à l'endroit indiqué dans le mandat ;
 - d) un système informatique à l'endroit indiqué dans le mandat.
- 2) La demande doit être faite par écrit et sous serment par un agent habilité, et doit contenir :
 - a) si une personne doit être fouillée, ses nom, âge et adresse ; et
 - b) si un lieu doit être fouillé :
 - i) une description du lieu à fouiller ; et
 - ii) si le lieu est occupé, le nom et l'âge des occupants du lieu, s'ils sont connus ; et
 - c) l'infraction à laquelle la demande se rapporte ; et
 - d) une description de la nature du support de stockage des données, du réseau informatique, du système informatique ou de tout élément de preuve présumé ; et

- e) les informations sur lesquelles se fonde le soupçon raisonnable de preuve de la perpétration d'une infraction ;
- i) se trouve sur ou sous le contrôle de la personne ou dans le lieu où est exécuté le mandat informatique ;
- ii) est susceptible d'être sur ou sous le contrôle de la personne ou à l'endroit où le mandat informatique est exécuté ; et
- f) si un mandat informatique a déjà été délivré en rapport avec la personne ou le lieu ; et
- g) si l'autorisation d'exécuter le mandat relatif aux ordinateurs la nuit est demandée, pourquoi il est nécessaire d'exécuter le mandat relatif aux ordinateurs la nuit ; et
- h) la période pendant laquelle le mandat informatique est requis.

40 Octroi d'un mandat informatique

- 1) La Cour peut accorder un mandat informatique si elle est convaincue que la demande de l'agent autorisé est faite conformément aux paragraphes 391) et 2).
- 2) Sans limiter le paragraphe 1), avant d'accorder un mandat informatique, la Cour doit prendre en considération les éléments suivants :
 - a) la gravité de l'infraction sur laquelle porte l'enquête ou la procédure pénale ;
 - b) la fiabilité des informations sur lesquelles la demande est fondée, y compris la nature de la source des informations ;
 - c) si l'intérêt public dans la production de données à partir du système informatique ou du support de stockage des données l'emporte sur le droit à la vie privée d'une personne dont la vie privée peut être affectée par la production ;
 - d) s'il existe un lien suffisant entre les preuves recherchées et l'infraction à laquelle se rapporte l'enquête ou la procédure pénale ;
 - e) si une condition doit être incluse dans le mandat informatique ; et
 - f) la durée proposée du mandat informatique ; et
 - g) toute autre question que la Cour juge pertinente.

41 Contenu du mandat informatique

Un mandat informatique doit mentionner les informations suivantes :

- a) si une personne doit être fouillée, son nom, son âge et son adresse ; et

- b) si un lieu doit être fouillé :
- i) une description du lieu à fouiller ; et
- ii) si le lieu est occupé, le nom et l'âge des occupants du lieu, s'ils sont connus ; et
- c) l'infraction à laquelle la demande se rapporte ; et
- d) les types de pièces justificatives qui peuvent être recherchées ; et
- e) le pouvoir d'un agent autorisé de sécuriser ou de rendre inaccessible un support de stockage de données, un réseau ou un système informatique ; et
- f) la date et l'heure d'expiration du mandat informatique ; et
- g) toute condition imposée en relation avec l'exécution du mandat informatique.

42 Prolongation d'un mandat informatique

- 1) La Cour doit préciser dans le mandat informatique la date et l'heure de la fin du mandat de perquisition.
- 2) La Cour peut prolonger la date et l'heure de fin d'un mandat informatique si elle est convaincue que l'objectif pour lequel le mandat a été octroyé ne peut être atteint avant l'expiration du mandat.

43 Demande d'un mandat informatique urgent

- 1) Si le commissaire a autorisé une demande de mandat urgent d'accès à un ordinateur en vertu de l'article 38, un agent autorisé peut demander à la Cour d'accorder un mandat urgent d'accès à un ordinateur :
 - a) à un lieu spécifié dans le mandat ; ou
 - b) un support de stockage des données à l'endroit indiqué dans le mandat ; ou
 - c) un réseau informatique à l'endroit indiqué dans le mandat ;
 - d) un système informatique à l'endroit indiqué dans le mandat.
- 2) Un agent habilité peut faire une demande pour un mandat d'interception urgent oralement, par téléphone, courriel, télécopie ou par tout autre moyen électronique.
- 3) L'agent habilité présentant une demande conformément au paragraphe 2) doit spécifier :
 - a) si une personne doit être fouillée, ses nom, âge et adresse ; et
 - b) si un lieu doit être fouillé :

- i) une description du lieu à fouiller ; et
 - ii) si le lieu est occupé, le nom et l'âge des occupants du lieu, s'ils sont connus ; et
 - c) l'infraction à laquelle la demande se rapporte ; et
 - d) une description de la nature du support de stockage des données, du réseau informatique, du système informatique ou de tout élément de preuve présumé ; et
 - e) les informations sur lesquelles se fonde le soupçon raisonnable de preuve de la commission d'une infraction :
 - i) se trouve sur ou sous le contrôle de la personne ou dans le lieu
 - ii) est susceptible d'être sur ou sous le contrôle de la personne ou à l'endroit où un mandat informatique urgent est exécuté ; et
 - f) si un mandat informatique urgent a déjà été délivré en rapport avec la personne ou le lieu ; et
 - g) si l'autorisation d'exécuter un mandat urgent pour ordinateur la nuit est demandée, pourquoi il est nécessaire d'exécuter le mandat urgent pour ordinateur la nuit ; et
 - h) la période pendant laquelle un mandat informatique urgent est nécessaire.
- 4) L'agent habilité doit, dès que possible, après l'octroi du mandat informatique urgent, adresser sa demande, par écrit, à la Cour.

44 Octroi d'un mandat informatique urgent

- 1) La Cour peut accorder un mandat informatique urgent si elle est satisfaite de la demande présentée par l'agent habilité en vertu de l'article 43.
- 2) Sans limiter la portée du paragraphe 1), avant d'accorder un mandat urgent pour ordinateur, la Cour doit prendre en considération les éléments suivants :
 - a) l'urgence de la situation nécessitant un mandat urgent relatif aux ordinateurs ; et
 - b) la gravité de l'infraction sur laquelle porte l'enquête ou la procédure pénale ; et
 - c) la fiabilité des informations sur lesquelles la demande est fondée, y compris la nature de la source des informations ; et
 - d) si l'intérêt public dans la production de données à partir du système informatique ou du support de stockage des données l'emporte sur le droit à la vie privée d'une personne dont la vie privée peut être affectée par la production ; et
 - e) s'il existe un lien suffisant entre les preuves recherchées et l'infraction à laquelle se rapporte l'enquête ou la procédure pénale ; et

- f) si une condition doit être incluse dans le mandat informatique ; et
- g) la durée proposée du mandat informatique ; et
- h) toute autre question que la Cour juge pertinente.

45 Effets du mandat informatique et du mandat informatique urgent

1) L'agent habilité est autorisé, en vertu d'un mandat informatique ou d'un mandat informatique urgent accordé en vertu des articles 40 et 44, à :

- a) saisir un objet dont l'agent autorisé a des motifs raisonnables de croire qu'il est :
 - i) un élément de preuve en rapport avec une infraction visée par le mandat ; ou
 - ii) un élément de preuve pertinent pour une autre infraction à la présente Loi ou à toute autre loi ; et
- b) accéder à un support de stockage de données, à un réseau informatique ou à un système informatique afin d'obtenir des informations et des enregistrements, et rassembler, copier ou extraire des données ; et
- c) accéder, saisir ou sécuriser tout équipement, support de stockage de données ou autre élément permettant de stocker des informations, des enregistrements ou des données ; et
- d) demander à une personne ayant connaissance d'un support de données, d'un réseau informatique ou d'un système informatique d'aider l'agent habilité à accéder au support de données, au réseau informatique ou au système informatique ; et
- e) si un agent habilité a des motifs raisonnables de soupçonner que les données accessibles à partir du système informatique pourraient être les données auxquelles on pourrait avoir accès, qu'il pourrait rassembler ou saisir en vertu du mandat ou d'un autre élément visé au point a), l'agent habilité peut :
 - i) faire fonctionner le système informatique pour accéder aux données ; ou
 - ii) utiliser un autre système informatique accessible à partir du système informatique exploité en vertu du point i) pour accéder aux données ; ou
 - iii) copier tout ou partie des données sur un autre support de stockage des données ou sur un réseau ou un système informatique ; ou
 - iv) si, en utilisant les installations du lieu, les données peuvent être mises sous forme documentaire, exploiter les installations pour mettre ces données sous cette forme et saisir les documents produits ; et
- f) déplacer le support de stockage des données ou un réseau informatique ou un système informatique du lieu perquisitionné vers un autre lieu pour examen afin de déterminer s'il contient des données auxquelles on pourrait accéder, qu'on pourrait

TITRE 6 DISPOSITIONS DIVERSES

collationner ou qu'on pourrait saisir en vertu du mandat, le cas échéant ;

- i) l'occupant du lieu y consent ; ou
 - ii) il est nettement plus facile de le faire compte tenu du temps nécessaire pour copier les données et il existe des motifs raisonnables de soupçonner que les données auxquelles on pourrait accéder, qu'on pourrait rassembler ou qu'on pourrait saisir en vertu du mandat ; et
 - g) faire tout ce qui est raisonnablement nécessaire pour prévenir la perte, la destruction ou l'endommagement de tout ce qui est lié à l'infraction ou à toute autre infraction ; et
 - h) faire appel à d'autres agents ou personnes autorisés dans la mesure raisonnablement nécessaire à l'exécution du mandat ; et
 - i) de fouiller une personne qui se trouve sur les lieux au moment de l'exécution du mandat si l'ordonnateur soupçonne, pour des motifs raisonnables, que cette personne a des éléments de preuve en sa possession.
- 2) Si un agent habilité saisit un support de stockage de données, un réseau informatique, un système informatique, un équipement, un dispositif ou un autre article en vertu du paragraphe 1), l'agent autorisé :
- a) peut en prendre possession ; et
 - b) peut le conserver pendant la durée qu'il estime nécessaire aux fins de la présente Loi.
- 4) Un agent habilité doit restituer tout objet détenu en vertu du paragraphe 2) à son propriétaire si :
- a) il n'est plus nécessaire de saisir l'objet ; ou
 - b) il est décidé que l'objet ne doit pas être utilisé à des fins de preuve, sauf si l'agent habilité a des motifs raisonnables de croire que la possession de données peut constituer une infraction.

46 Accès aux données saisies

- 1) Sous réserve du paragraphe 2), sur demande, l'agent de Police qui exécute un mandat informatique doit :
- a) permettre à une personne qui avait la garde ou le contrôle du support de stockage des données, du réseau d'ordinateurs ou du système informatique, ou à une personne agissant en son nom, d'accéder aux données et de les copier ; ou
 - b) donner à cette personne une copie de ces données détenues dans le système informatique.

TITRE 6 DISPOSITIONS DIVERSES

- 2) L'agent de Police peut refuser de donner accès à des données détenues dans un support de stockage de données, un réseau d'ordinateurs ou un système informatique ou de fournir des copies de ces données s'il a des motifs raisonnables de croire que le fait de donner l'accès ou de fournir des copies peut :
 - a) constituer une infraction à la présente loi ou à toute autre loi ; ou
 - b) porter atteinte à une enquête ou à une procédure pénale.
- 47 **Sécuriser ou rendre inaccessibles des données en vertu d'un mandat informatique ou d'un mandat informatique urgent**
 - 1) Aux fins du présent article, expert s'entend d'un expert en criminalistique numérique
 - 2) Un agent habilité exécutant un mandat informatique ou un mandat informatique urgent peut faire tout ce qui est nécessaire pour sécuriser ou rendre accessible un support de stockage de données, un réseau d'ordinateur ou un système informatique s'il a des motifs raisonnables de soupçonner que :
 - a) les preuves de la commission d'une infraction peuvent être accessibles en utilisant le support de stockage de données, le réseau d'ordinateur ou le système informatique ;
 - b) une assistance d'expert est nécessaire pour faire fonctionner le support de stockage des données, le réseau d'ordinateurs ou le système informatique ; et
 - c) si il ne prend pas des mesures en vertu du présent paragraphe, les éléments de preuve peuvent être détruits, modifiés ou altérés de toute autre manière.
 - 3) L'agent de Police doit, par voie de notification, informer la personne qui a la garde ou le contrôle du support de stockage des données, du réseau d'ordinateur ou du système informatique :
 - a) de son intention de sécuriser ou de rendre inaccessible le support de stockage des données, le réseau d'ordinateur et le système informatique ; et
 - b) que le support de stockage des données, le réseau d'ordinateurs et le système informatique peuvent être sécurisés ou inaccessibles pendant 28 jours au maximum.
 - 4) Le support de stockage des données, l'ordinateur ou le système informatique peuvent être sécurisés ou inaccessibles jusqu'à ce que l'une des situations suivantes se produise :
 - a) 28 jours après que le support de stockage des données, le réseau d'ordinateurs ou le système informatique ait été sécurisé ou rendu inaccessible pour la première fois ; ou
 - b) le support de stockage des données, le réseau d'ordinateur ou le système informatique a été exploité par un expert.

- 5) L'agent de Police peut demander au tribunal une prolongation du délai visé à l'alinéa 3) a), s'il a des motifs raisonnables de croire que l'assistance d'un expert ne sera pas disponible dans ce délai.
- 6) L'agent de Police peut présenter plus d'une demande en vertu du paragraphe 4) jusqu'à ce que l'expertise soit disponible.
- 7) L'agent de Police, par voie de notification, informe la personne qui a la garde ou le contrôle du support de stockage des données, du réseau d'ordinateurs ou du système informatique :
 - a) son intention de demander une prolongation ; et
 - b) que la personne a le droit d'être entendue en ce qui concerne la demande.

48 Aide à un fonctionnaire de police dans l'exécution d'un mandat informatique

- 1) Un agent de Police peut ordonner à une personne en possession ou en contrôle du support de stockage des données, du réseau d'ordinateur ou du système informatique, ou ayant connaissance de ceux-ci, de l'aider à :
 - a) accéder au support de stockage des données, au réseau d'ordinateur ou au système informatique et de l'utiliser pour accéder à toute donnée informatique (y compris les données stockées en tout lieu ou sur un support de stockage des données distinct) ;
 - b) obtenir et copier les données ;
 - c) utiliser des équipements pour faire des copies des données ;
 - d) obtenir une sortie intelligible du système informatique dans un format lisible ; et
 - e) faire tout ce que l'agent de Police peut raisonnablement exiger.
- 2) Toute personne qui, sans excuse raisonnable, ne se conforme pas à une instruction donnée en vertu du paragraphe 1) commet une infraction qui l'expose sur condamnation :
 - a) dans le cas d'un particulier – à une peine d'amende n'excédant pas 1 000 000 VT ou d'emprisonnement n'excédant pas 3 ans, ou des deux à la fois ; ou
 - b) dans le cas d'une personne morale – à une peine d'amende n'excédant pas 2 000 000 VT.

49 Faire preuve d'une diligence raisonnable

- 1) Aux fins de la présente section, les dommages, liés aux données, comprennent les dommages causés par l'effacement des données ou l'ajout d'autres données, mais

TITRE 6 DISPOSITIONS DIVERSES

n'incluent pas l'altération raisonnable des données par des procédés de médecine légale numérique.

- 2) Un agent de Police, ou une personne qui l'assiste lors de l'examen ou de la conservation d'un support de stockage de données, d'un réseau informatique ou d'un système informatique en vertu d'un mandat informatique ou d'un mandat informatique urgent, doit prendre des mesures raisonnables pour éviter tout dommage aux éléments suivants :
 - a) au support de stockage des données, au réseau d'ordinateur ou au système informatique ; et
 - b) les données stockées sur le support de stockage des données, le réseau d'ordinateur ou le système informatique, ou auxquelles on accède en utilisant ce dernier ; et
 - c) les programmes associés à l'utilisation du support de stockage des données, du réseau d'ordinateur ou du système informatique, ou à l'utilisation des données stockées dans le support de stockage des données, le réseau d'ordinateur ou le système informatique.

50 Réception de biens saisis en vertu d'un mandat informatique

- 1) Aux fins du présent article, on entend par reçu un inventaire de tous les objets recueillis pendant l'exécution du mandat informatique ou mandat informatique urgent.
- 2) Si un mandat informatique autorise un agent de police à saisir une chose, l'agent de police doit, après avoir saisi la chose, remettre à la personne fouillée ou à l'occupant du lieu fouillé un reçu pour la chose saisie ; ou laisser un reçu pour la chose saisie dans un endroit bien visible du lieu.
- 3) Le reçu doit comporter des informations suffisantes pour identifier les éléments suivants :
 - a) la chose qui a été saisie ;
 - b) l'heure à laquelle la chose a été saisie ;
 - c) la personne qui a saisi la chose ;
 - d) le lieu où la chose a été prise ; et
 - e) l'heure à laquelle la chose doit être rendue.
- 4) Le présent article ne s'applique pas si un agent de police a des motifs raisonnables de croire que :
 - a) aucune personne ne semble être en possession de la chose ; ou
 - b) la chose est abandonnée.

51 Mesures visant à contrôler la conservation du support de stockage des données, du réseau informatique ou du système informatique saisi

- 1) Un agent de Police qui saisit un support de stockage de données, un réseau informatique ou un système informatique en vertu d'un mandat informatique ou mandat informatique urgent, doit prendre des mesures raisonnables pour réduire la nécessité d'une conservation prolongée du support de stockage de données, du réseau informatique ou du système informatique à titre de preuve en prenant l'une des mesures suivantes dès que possible :
 - a) en faisant en sorte que le support de stockage des données, le réseau informatique ou le système informatique, ou une partie de celui-ci, soit copié ; ou
 - b) en faisant procéder à tout test ou examen nécessaire du support de stockage des données, du réseau informatique ou du système informatique ; ou
 - c) en recueillant toute autre preuve secondaire disponible en rapport avec le support de stockage des données, l'ordinateur ou le système informatique.
- 2) Malgré le paragraphe 1), un officier de police peut conserver le support de stockage des données, le réseau informatique ou le système informatique pendant une durée raisonnable s'il a des motifs raisonnables de croire que cela est nécessaire pour empêcher la commission d'une infraction.

52 Destruction de certaines données saisies en vertu d'un mandat informatique ou mandat informatique urgent

Si le commissaire est convaincu que les données consultées ou copiées en vertu d'un mandat informatique ou mandat informatique ne sont plus utiles aux fins de l'application de la loi, il doit prendre les dispositions nécessaires pour la destruction des données, et toute reproduction, sous le contrôle des forces de police de Vanuatu.

53 Interdiction de divulgation d'informations, de dossiers et de données

- 1) La personne qui obtient des informations, des extraits, des dossiers ou des données à la suite d'une demande, d'une ordonnance ou d'un mandat en vertu de la présente partie ne doit pas, dans l'exercice de ses fonctions, divulguer sciemment, en tout ou en partie, les informations, extraits, dossiers ou données.
- 2) Toute personne qui enfreint le paragraphe 1) commet une infraction et qui s'expose à une condamnation :
 - a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 1 000 000 VT ou d'emprisonnement n'excédant pas 3 ans, ou les deux à la fois ; ou
 - b) dans le cas d'une personne morale – à une peine d'amende n'excédant pas 2 000 000 VT.

54 Certificats de preuve pour les prestataires de services

- 1) Un représentant autorisé peut délivrer une attestation sous serment du représentant, exposant les faits qu'il juge pertinents par rapport aux actes ou choses faits par le prestataire de services ou en relation avec lui afin de :
 - a) donner suite à une demande de divulgation de données relatives aux abonnés ou de données relatives au trafic en vertu des articles 21, 22 et 24 ; ou
 - b) répondre à une demande d'accès aux données relatives au trafic en temps réel en vertu de l'article 23 ; ou
 - c) se conformer à une ordonnance de conservation rendue en vertu de l'article 2 ; ou
 - d) permettre l'exécution d'un mandat d'interception.
- 2) Un certificat de preuve délivré en vertu du paragraphe 1) :
 - a) doit être reçu comme preuve dans la procédure sans autre preuve ; et
 - b) constitue une preuve concluante des éléments qui y sont énoncés.

55 Entrave ou obstruction à l'exercice légal des pouvoirs

- 1) Une personne commet une infraction si sans excuse raisonnable :
 - a) elle entrave ou empêche un agent de Police, ou une personne qui l'assiste, dans l'exercice de ses fonctions en vertu de la présente Loi ; ou
 - b) a l'intention d'entraver ou de gêner l'agent de Police ou une personne qui l'assiste.
- 2) Toute personne qui commet l'infraction visée au paragraphe 1) s'expose sur condamnation :
 - a) dans le cas d'une personne physique - à une peine d'amende n'excédant pas 1 000 000 VT ou d'emprisonnement n'excédant pas 3 ans, ou les deux à la fois ; ou
 - b) dans le cas d'une personne morale - à une peine d'amende n'excédant pas 2 000 000 VT.

56 Obligations des prestataires de services

- 1) Un prestataire de services doit empêcher que les réseaux et les installations de communication soient utilisés dans le cadre ou en relation avec la commission d'infractions à la présente loi ou à toute autre loi.
- 2) Un prestataire de services ou un représentant autorisé qui reçoit une demande d'information en vertu de la présente Loi doit préserver la confidentialité de toute procédure et de toute information relative à la demande.

TITRE 6 DISPOSITIONS DIVERSES

- 3) Un prestataire de services ou un représentant autorisé qui ne se conforme pas, sans excuse raisonnable, au paragraphe 2) commet une infraction qui l'expose sur condamnation, à une peine d'amende n'excédant pas 2 000 000 VT.
- 4) Un prestataire de services ou un représentant autorisé commet une infraction s'il ne se conforme pas à une demande légale faite par un agent de police en vertu de la présente Loi et s'expose sur condamnation, à une peine d'amende n'excédant pas 2 000 000 VT.
- 5) Dans le présent article, la référence à l'assistance comprend une référence à l'assistance raisonnablement nécessaire aux fins suivantes :
 - a) l'application du droit pénal et des lois imposant des sanctions pécuniaires ; et
 - b) aider à l'application des lois pénales en vigueur dans un État étranger ; et
 - c) la protection des recettes publiques ; et
 - d) la protection de la sécurité nationale.

TITRE 5 COOPÉRATION INTERNATIONALE

57 Principes généraux relatifs à l'assistance réciproque

Vanuatu peut coopérer avec tout pays étranger, tout organisme étranger ou tout organisme international aux fins d'enquêtes ou de procédures concernant des infractions liées aux systèmes et données informatiques ou pour la collecte de preuves sous forme électronique d'une infraction pénale en vertu de la présente Loi et de la Loi sur l'Assistance réciproque en matière d'affaires criminelles.

58 Le Procureur général doit présenter des demandes d'assistance réciproque et y donner suite

- 1) Le Procureur général peut présenter des demandes d'assistance réciproque dans le cadre de toute enquête ou procédure engagée à Vanuatu, concernant toute infraction informatique ou liée à l'informatique.
- 2) Le Procureur général peut, en ce qui concerne toute demande d'un pays étranger d'assistance réciproque dans le cadre d'une enquête ou d'une procédure engagée dans ce pays étranger :
 - a) faire droit à la demande, en tout ou en partie, selon les modalités et conditions qu'il juge appropriées ; ou
 - b) refuser conformément aux dispositions prévues aux articles 8, 9 et 10 de la Loi sur l'Assistance réciproque en matière d'affaires criminelles ; ou
 - c) après avoir consulté l'autorité compétente du pays étranger, reporter la demande, en tout ou en partie, au motif que le fait d'accéder immédiatement à la demande risquerait de nuire à la conduite d'une enquête ou d'une procédure à Vanuatu.

- 3) Une demande d'assistance réciproque en vertu du présent article doit être exécutée conformément aux procédures spécifiées par le pays étranger, sauf en cas d'incompatibilité avec les lois de Vanuatu.
- 4) Avant de refuser ou de reporter l'assistance, le Procureur général doit, le cas échéant après avoir consulté le pays étranger, examiner si la demande peut être acceptée en partie ou sous certaines conditions.
- 5) Le Procureur général doit immédiatement informer le pays étranger du résultat de l'exécution d'une demande d'entraide.
- 6) Outre le paragraphe 5), le Procureur général doit informer l'État étranger des motifs de la demande :
 - a) rendre impossible l'exécution de la demande ; ou
 - b) pour retarder sensiblement l'exécution de la demande ; ou
 - c) de reporter la demande ; ou
 - d) de refuser la demande.
- 7) L'État étranger peut demander au Procureur général de garder confidentiels le fait de toute demande faite en vertu de la présente Loi ou de la Loi sur l'Assistance réciproque en matière d'affaires criminelles ainsi que son objet, sauf dans la mesure nécessaire à son exécution.
- 8) Si le Procureur général ne peut pas se conformer à la demande de confidentialité en vertu du paragraphe 7), il doit immédiatement en informer le pays étranger si la demande doit encore être exécutée.
- 9) Le paragraphe 8) applique mutatis mutandis lorsque le Procureur général est le pays demandeur.
- 10) Si le pays étranger ne peut pas remplir les conditions visées au paragraphe 2), il doit en informer le Procureur général, qui déterminera alors si l'information doit encore être fournie.
- 11) Si le pays étranger accepte les informations sous réserve de ces conditions, il est lié par celles-ci.
- 12) Les paragraphes 1), 2) et 3) s'appliquent mutatis mutandis lorsque des informations spontanées sont fournies au procureur par un pays étranger.

59 Informations complémentaires

- 1) Le Procureur général peut, sous réserve de la présente Loi et sans demande préalable, transmettre à un pays étranger des informations obtenues dans le cadre de ses propres enquêtes lorsqu'il estime que la divulgation de ces informations est nécessaire :
 - a) pour aider le pays étranger à engager ou à mener à bien des enquêtes ou des procédures ; ou
 - b) et pourrait conduire à une demande de coopération de la part du pays étranger en vertu de la présente Loi.
- 2) Avant de fournir ces informations, le Procureur général peut demander que celles-ci soient tenues confidentielles ou qu'elles ne soient utilisées que sous certaines conditions.

60 Conservation accélérée des données informatiques stockées

- 1) Un pays étranger peut demander ou obtenir de toute autre manière une conservation accélérée des données stockées au moyen d'un système informatique, situé sur le territoire de Vanuatu et pour lequel le pays étranger requérant, l'agence étrangère ou toute agence internationale a l'intention de soumettre une demande d'assistance mutuelle pour la recherche ou l'accès similaire, la saisie ou la sécurisation similaire, ou la divulgation des données.
- 2) Une demande de conservation accélérée faite en vertu du paragraphe 1) doit préciser :
 - a) l'autorité qui demande la conservation ; et
 - b) l'infraction qui fait l'objet d'une enquête ou d'une procédure pénale et un bref résumé des faits qui s'y rapportent ; et
 - c) les données informatiques stockées à conserver et leur relation avec l'infraction ; et
 - d) toute information disponible permettant d'identifier le dépositaire des données informatiques stockées ou l'emplacement du système informatique ; et
 - e) la nécessité d'une conservation accélérée ; et
 - f) que le pays étranger a l'intention de présenter une demande d'assistance mutuelle pour la perquisition ou l'accès similaire, la saisie ou la sécurisation similaire, ou la divulgation des données informatiques stockées.
- 3) Dès réception d'une demande en vertu du paragraphe 1), le procureur doit prendre toutes les mesures appropriées pour conserver rapidement les données spécifiées conformément aux procédures et aux pouvoirs prévus par la présente loi.
- 4) Toute conservation accélérée effectuée en réponse à la demande doit être d'une durée d'au moins 60 jours, afin de permettre à l'État étranger de soumettre une demande de perquisition ou d'accès similaire, de saisie ou de sécurisation similaire, ou de divulgation des données et, suite à la réception d'une telle demande, les données doivent continuer

TITRE 6 DISPOSITIONS DIVERSES

à être conservées de manière accélérée jusqu'à ce qu'une décision finale soit prise sur cette demande en attente.

- 5) Les paragraphes 1) et 2) doivent s'appliquer mutatis mutandis lorsqu'une demande de conservation accélérée de données informatiques stockées est faite par Vanuatu.

61 Divulgence accélérée des données relatives au trafic conservées

- 1) Au cours de l'exécution d'une demande en vertu de l'article 22 ou autrement en relation avec une infraction grave dans un État étranger, le service répressif, en ce qui concerne une communication spécifiée, découvre qu'un prestataire de services dans un autre pays est impliqué dans la transmission de la communication, le Procureur général se doit :
- a) de divulguer rapidement au pays étranger requérant une quantité suffisante de données relatives au trafic pour identifier ce prestataire de services ; et
 - b) de révéler le chemin par lequel la communication a été transmise.
- 2) La divulgation accélérée de données relatives au trafic conservées en vertu du paragraphe 1) ne peut être retirée que si :
- a) la demande concerne une infraction politique ou une infraction liée à une infraction politique ; ou
 - b) le Procureur général estime que l'exécution de la demande est susceptible de porter atteinte à la souveraineté de Vanuatu, à sa sécurité ou à l'intérêt public.

62 Assistance mutuelle en matière d'accès aux données informatiques stockées

- 1) Un pays étranger peut demander d'ordonner ou de perquisitionner ou d'accéder de manière similaire, de saisir ou de sécuriser de manière similaire, et de divulguer des données stockées au moyen d'un système informatique situé sur le territoire de Vanuatu, en relation avec une infraction étrangère grave, y compris les données qui ont été conservées conformément à l'article 18.
- 2) Une demande d'entraide concernant l'accès à des données informatiques stockées doit, dans la mesure du possible :
- a) indiquer le nom de l'autorité qui mène l'enquête ou la procédure à laquelle la demande se rapporte ;
 - b) donner une description de la nature de l'affaire pénale et une déclaration présentant un résumé des faits et des lois pertinentes ;
 - c) décrire l'objet de la demande et la nature de l'assistance recherchée ;
 - d) dans le cas d'une demande de saisie ou de confiscation d'avoirs dont on a des motifs raisonnables de penser qu'ils se trouvent dans le pays requis :

TITRE 6 DISPOSITIONS DIVERSES

- i) donner des précisions sur l'infraction en question ; ou
 - ii) les détails de toute enquête ou procédure engagée en rapport avec l'infraction, et être accompagnée d'une copie de toute décision de restriction ou de confiscation pertinente ;
 - e) donner des précisions sur toute procédure que le pays requérant souhaite voir suivre par le pays requis pour donner suite à la demande, en particulier dans le cas d'une demande d'obtention de preuves ;
 - f) comprend une déclaration exposant les souhaits éventuels du pays demandeur concernant la confidentialité relative à la demande et les raisons de ces souhaits ;
 - g) indiquer le délai dans lequel le pays demandeur souhaite que la demande soit satisfaite ;
 - h) le cas échéant, donner des précisions sur les biens, l'ordinateur, le système informatique ou le dispositif à localiser, à retenir, à saisir ou à confisquer, ainsi que sur les motifs permettant de penser que ces biens se trouvent dans le pays requis ;
 - i) donner des détails sur les données informatiques stockées, les données ou le programme à saisir et leur relation avec l'infraction ;
 - j) donner toute information disponible permettant d'identifier le dépositaire des données informatiques stockées ou l'emplacement de l'ordinateur, du système ou du dispositif informatique ;
 - k) comporter un accord sur la question du paiement des dommages et intérêts ou des frais d'exécution de la demande ; et
 - l) donner toute autre information susceptible de contribuer à donner suite à la demande.
- 3) Dès réception de la demande en vertu du présent article, l'organisme d'enquête doit prendre toutes les mesures appropriées pour obtenir l'autorisation nécessaire, y compris tout mandat d'exécution de la demande conformément aux procédures et pouvoirs prévus par la présente loi.
- 4) Après avoir obtenu l'autorisation nécessaire, y compris tout mandat d'exécution, l'organisme d'enquête peut solliciter l'appui et la coopération du pays étranger pendant la perquisition et la saisie.
- 5) Lors de l'exécution de la demande de perquisition et de saisie, l'organisme d'enquête doit fournir les résultats de cette perquisition et de cette saisie au pays étranger.
- 6) Les paragraphes 1) et 2) doivent s'appliquer mutatis mutandis aux demandes de conservation accélérée de données informatiques stockées sur le territoire d'un pays étranger.

63 Accès transfrontalier à des données informatiques stockées avec le consentement de l'intéressé ou lorsqu'elles sont accessibles au public

Un agent de police peut, sans autorisation mais sous réserve des dispositions applicables de la présente Loi :

- a) accéder à des données informatiques stockées accessibles au public, quel que soit l'endroit où elles se trouvent géographiquement ; ou
- b) accéder ou recevoir, par l'intermédiaire d'un système informatique situé sur son territoire, des données informatiques stockées situées sur un autre territoire, si ce fonctionnaire de police ou une autre personne autorisée obtient le consentement légal et volontaire de la personne qui a l'autorité légale de divulguer les données par l'intermédiaire de ce système informatique.

64 Assistance mutuelle dans la collecte en temps réel de données relatives au trafic

- 1) Un pays étranger peut demander, en relation avec une infraction étrangère grave, d'ordonner ou de fournir une assistance pour la collecte en temps réel de données relatives au trafic associées à des communications spécifiées à Vanuatu, transmises au moyen d'un système informatique.
- 2) Une demande d'assistance au titre du présent article doit préciser :
 - a) l'autorité sollicitant l'utilisation des pouvoirs prévus par le présent article ;
 - b) l'infraction qui fait l'objet d'une enquête ou d'une procédure pénale et un bref résumé des faits qui s'y rapportent ;
 - c) le nom de l'autorité ayant accès aux données relatives au trafic pertinentes ;
 - d) le lieu où les données relatives au trafic peuvent être conservées ;
 - e) la finalité prévue pour les données relatives au trafic requises ;
 - f) des informations suffisantes pour identifier les données relatives au trafic ;
 - g) tout autre détail concernant les données relatives au trafic ;
 - h) la nécessité de recourir aux pouvoirs prévus au présent article ; et
 - i) les conditions d'utilisation et de divulgation des données relatives au trafic à des tiers.
- 3) Sur réception d'une demande en vertu du paragraphe 1), l'organisme d'enquête doit prendre toutes les mesures appropriées pour obtenir l'autorisation nécessaire, y compris tout mandat d'exécution de la demande conformément aux procédures et aux pouvoirs prévus par la présente Loi.

- 4) Après avoir obtenu l'autorisation nécessaire, y compris tout mandat d'exécution, l'organisme d'enquête peut solliciter l'appui et la coopération du pays étranger pendant la perquisition et la saisie.
- 5) Lors de l'exécution des mesures prévues par le présent article, l'organisme d'enquête doit fournir les résultats de ces mesures ainsi que la collecte en temps réel des données relatives au trafic associées aux communications spécifiées vers le pays étranger.
- 6) Les paragraphes 1) et 2) doivent s'appliquer mutatis mutandis aux demandes de collecte en temps réel de données relatives au trafic dans un pays étranger.

65 Assistance mutuelle en matière d'interception des données relatives au contenu

- 1) Un pays étranger peut demander d'ordonner ou de fournir une assistance pour la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique à Vanuatu.
- 2) Une demande d'assistance au titre du paragraphe 1) doit, dans la mesure du possible, préciser :
 - a) l'autorité qui sollicite l'utilisation des pouvoirs prévus par le présent article ;
 - b) l'infraction qui fait l'objet d'une enquête ou d'une procédure pénale et un bref résumé des faits qui s'y rapportent ;
 - c) le nom de l'autorité ayant accès à la communication concernée ;
 - d) le lieu ou la nature de la communication ;
 - e) l'objectif visé par la communication requise ;
 - f) des informations suffisantes pour identifier les communications ;
 - g) les détails des données de l'interception concernée ;
 - h) le destinataire de la communication ;
 - i) la durée prévue pour l'utilisation de la communication ;
 - j) la nécessité de recourir aux pouvoirs prévus au présent article ; et
 - k) les conditions d'utilisation et de divulgation de la communication à des tiers.
- 3) Dès réception d'une demande au titre du présent article, le procureur doit prendre toutes les mesures appropriées pour exécuter la demande conformément aux procédures et

TITRE 6 DISPOSITIONS DIVERSES
aux pouvoirs prévus par la présente Loi.

- 4) Lors de l'exécution des mesures prévues au paragraphe 3), le procureur doit fournir les résultats de ces mesures ainsi que la collecte ou l'enregistrement en temps réel des données relatives au contenu des communications spécifiées à l'étranger.
- 5) Les paragraphes 1) et 2) s'appliquent par analogie aux demandes de collecte en temps réel de données relatives au trafic dans un pays étranger.

66 Réseau 24/7

- 1) Le Procureur général doit veiller à ce que l'organisme d'enquête chargé de la recherche et de la poursuite de la cybercriminalité désigne un point de contact disponible vingt-quatre heures sur vingt-quatre, sept jours sur sept.
- 2) Un point de contact désigné en vertu du paragraphe 1) doit veiller à ce qu'une assistance soit immédiatement fournie aux fins de :
 - a) d'enquêtes ou de procédures concernant les infractions pénales liées à des systèmes et données informatiques ; ou
 - b) pour la collecte de preuves sous forme électronique d'une infraction pénale, cette assistance devant consister à faciliter ou, si la législation et la pratique de Vanuatu le permettent, à l'exécution directe des mesures suivantes :
 - i) la fourniture de conseils techniques ; et
 - ii) les données informatiques et la divulgation accélérée des données relatives au trafic conservées ; et
 - iii) la collecte de preuves, la fourniture d'informations juridiques et la localisation de suspects,

dans les délais rapides prescrits par le règlement.
- 2) Le point de contact doit être doté des ressources et des capacités nécessaires pour assurer de manière sûre et efficace les communications avec d'autres points de contact dans d'autres territoires, sur une base accélérée.
- 3) Le point de contact doit avoir le pouvoir et l'autorité de coordonner et de permettre l'accès à l'entraide internationale en vertu de la présente Loi ou, le cas échéant, aux procédures d'extradition, sur une base accélérée.

67 Rapport sur les pouvoirs d'enquête spéciaux

- 1) Le commissaire doit, au plus tard à la fin du mois de mars de chaque année, soumettre au Conseil des ministres un rapport annuel présentant des informations générales et des statistiques relatives à l'utilisation des pouvoirs d'enquête spéciaux pour l'année précédente.

- 2) Le rapport doit comprendre au minimum :
- a) le nombre d'opérations d'infiltration autorisées
 - i) le nombre d'ordonnances rendues pour la conservation de données informatiques ;
 - ii) le nombre de demandes de données relatives au trafic entemps réel ;
 - iii) le nombre de demandes de production de donnéesinformatiques ; et
 - b) le nombre de demandes de mandats d'interception et de mandatsinformatiques ;
 - c) le nombre de demandes de renouvellement de mandats d'interception et de mandats informatiques ;
 - d) le nombre de demandes de mandats d'interception urgents et de mandats informatiques urgents ;
 - e) le nombre de livraisons contrôlées de biens autorisées ;
 - f) le nombre de demandes visées aux points b), c) et d) qui ont étéacceptées et le nombre de celles qui ont été refusées ; et
 - g) le nombre de poursuites qui ont été engagées dans lesquelles despreuves ont été obtenues directement ou indirectement :
 - i) d'une interception effectuée en vertu d'un mandat d'interception ou d'un mandat d'interception urgente ;
 - ii) un support de stockage de données, un ordinateur ou un système informatique en vertu d'un mandat informatique oud'un mandat informatique urgent ;
 - iii) une opération d'infiltration ;
 - iv) une ordonnance de conservation de données informatiques ;
 - v) une demande d'accès aux données relatives au trafic et aux données relatives au trafic en temps réel ;
 - vi) un ordre de production de données informatiques ;
 - vii) une livraison contrôlée de biens a été présentée, et le résultat de ces poursuites ;
 - viii) le nombre de mandats d'interception et de mandats informatiques qui n'ont donné lieu à aucune inculpation dans les 90 jours suivant la date d'expiration du mandat ; et

TITRE 6 DISPOSITIONS DIVERSES

- ix) le nombre d'opérations d'infiltration et de livraisons contrôlées de biens qui n'ont donné lieu à aucune inculpation dans les 90 jours suivant la date à laquelle l'opération d'infiltration ou la livraison contrôlée a pris fin.
 - 3) Aucune disposition du présent article n'oblige le commissaire à divulguer publiquement les détails opérationnels d'un cas particulier.
- 68 L'État n'est pas tenu de s'engager sur les coûts**
Malgré toute autre loi, l'État n'est pas tenu de s'engager sur les frais de demande d'un mandat.

TITRE 6 DISPOSITIONS DIVERSES

69 Agent autorisé

- 1) Le Commissaire peut nommer un agent de Police, agent autorisé à exercer toute fonction ou tout pouvoir pouvant être exercé ou exécuté aux fins de la présente Loi, pour une période déterminée par le Commissaire.
- 2) Le Commissaire doit fournir à chaque agent autorisé une carte d'identité qui permettra de prouver l'identité de cet agent de police et sa nomination en tant qu'agent autorisé.
- 3) L'agent autorisé qui est titulaire d'une carte d'identité délivrée en vertu du présent article doit, à la fin de son mandat, remettre sa carte d'identité au Commissaire.

70 Protection contre la responsabilité

- 1) Un agent de police ou agent autorisé ne peut faire l'objet d'aucune responsabilité civile ou pénale, action, réclamation ou demande pour tout ce qu'il a fait ou omis de faire de bonne foi dans l'exécution ou la prétendue exécution de ses pouvoirs et fonctions en vertu de la présente Loi.
- 2) Un prestataire de services ou un représentant autorisé n'est pas responsable d'une action ou d'une autre procédure pour des dommages pour ou en relation avec un acte fait ou omis de bonne foi dans l'exécution d'un devoir imposé par la présente Loi.

71 Règlements

Le ministre peut prendre des règlements prescrivant des questions :

- a) qui doivent ou peuvent être prescrites en vertu de la présente Loi ; ou
- b) qui sont nécessaires ou utiles pour mieux appliquer ou donner effet aux dispositions de la présente Loi.

72 Entrée en vigueur

La présente Loi entre en vigueur à la date de sa publication au Journal officiel.