REPUBLIC OF VANUATU

BILL FOR THE CYBERCRIME ACT NO. OF 2015

Arrangement of Sections

REPUBLIC OF VANUATU

BILL FOR THE CYBERCRIME ACT NO. OF 2015

An Act to provide for computer offences and other 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:

child means a person under the age of 18 years;

electronic includes but not limited to electrical, digital, analogue, magnetic, optical, biochemical, electrochemical, electromechanical, electromagnetic, radio electric or wireless technology;

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

electronic data means any representation of facts, concepts, information (consisting of either texts, images, audio or video) machine- readable code or instructions, in a form suitable for processing in an electric system, including a program suitable to cause an electronic system to perform a function.

electronic 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 electronic systems such as computer, graphic cards, mobile phones, memory, chips;

(b) storage components such hard drives, memory cards, compact discs, tapes;

(c) input devices such as keyboards, mouse, track pad, scanner, digital cameras;

(d) output devices such as printer, screens;

electronic 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.

electronic system means any electronic device or a group of interconnected or related devices, one or more of which, pursuant to a program or manual or any external instruction, performs automatic processing of information or electronic data and may also include a permanent, removable or any other electronic storage medium;

information includes text, message, data, voice, sound, database, video, signals, software, computer programs, codes including object code and source code;

interception means tapping into an electronic communication not directed to the one who is tapping in including but is not limited to the acquiring, viewing and capturing of any electronic communication whether by wire, wireless, electronic, optical, magnetic, or other means, during transmission through the use of any technical device;

traffic data means electronic data that:

(a) relates to a communication by means of an electronic system; and

(b) is generated by an electronic 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.

PART 2 OFFENCES

2 Illegal access

(1) For the purposes of this section:

critical infrastructure means electronic systems, devices, networks, computer programs and electronic data vital for:

(a) the security, defence or international relations of the State; or

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

(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, courts, public transportation, public key infrastructure, payment systems infrastructure or e-commerce infrastructure; or

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

(e) the purpose declared as such by the government in accordance with the prescribed procedure; or

(f) containing the data or database protected as such, by any other law;

(2) A person who intentionally or without lawful excuse, accesses the whole or any part of an electronic system by infringing a security measure, 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.

(3) A person who intentionally or without lawful excuse, accesses the whole or any part of a critical infrastructure, person commits an offence and is liable on conviction to a fine not exceeding VT4,000, 000 or to a term of imprisonment not exceeding 5 years, or both.

(4) A body corporate who commits an offence under subsection (1) is liable on conviction to a fine not exceeding VT4, 000, 000.

(5) A body corporate who commits an offence under subsection (2) is liable on conviction to a fine not exceeding VT4, 000, 000.

3 Illegal remaining

(1) A person who intentionally or without lawful excuse, remains logged in an electronic system or part of an electronic system or continues to use an electronic system after the authorised time to use the electronic system has expired, commits an offence and is liable on conviction to a fine not exceedingVT1, 000, 000, or to a term of imprisonment not exceeding 3 years, or both.

(2) A body corporate who commits an offence under this section is liable on conviction to a fine not exceeding VT2, 000, 000.

4 Illegal interception

(1) A person who intentionally or without lawful excuse, intercepts by any technical means:

(a) any non-public transmission to, from or with an electronic system; or

(b) electromagnetic emission from an electronic system,

commits an offence and is liable on conviction to a fine not exceedingVT3, 000, 000, or to a term of imprisonment not exceeding 3 years, or both.

(2) A body corporate who commits an offence under this section is liable on conviction to a fine not exceeding VT3, 000, 000.

5 Data interference

(1) A person who intentionally or without lawful excuse, interferes with an electronic data owned or managed by someone else and does any of the following acts:

(a) damages or deteriorates electronic data; or

(b) deletes electronic data; or

(c) alters electronic data; or

(d) renders electronic data meaningless, useless or ineffective; or

(e) obstructs, interrupts or interferes with any person the lawful use of electronic data; or

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

(g) denies access to electronic data to any person authorized to access it,

commits an offence and is liable on conviction to a fine not exceeding VT500, 000, or to a term of imprisonment not exceeding 2 years, or both.

(2) A body corporate who commits an offence under this section is liable on conviction to a fine not exceeding VT1, 000, 000.

6 Data Espionage

(1) A person who intentionally or without lawful excuse, obtains for himself or herself or for another person, electronic data which are not meant for the public and is protected against unauthorized access, commits an offence and is liable on conviction to a fine not exceeding VT1, 000, 000, or to a term of imprisonment not exceeding 2 years., or both.

(2) A body corporate who commits an offence under this section is liable on conviction to a fine not exceeding VT2, 000, 000.

7 System interference

(1) For the purposes of this section:

critical infrastructure operations means operations carried out that are essential for the functioning of the society and the economy as a whole and whose disruption or suppression would have a debilitating impact on public health and safety, commerce, and national security, or any combination of this. This includes but not limited to transportation and communication, water and power lines, food supply, and public institutions including schools, post services and the police.

critical operations means an operation not covered under critical infrastructure

hinders in relation to an electronic system includes but is not limited to:

(a) cutting the electricity supply to an electronic system; or

(b) causing electromagnetic interference to an electronic system; or

(c) corrupting an electronic system by any means; or

(d) damaging, deleting, deteriorating, altering or suppressing electronic data.

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

(a) hinders, denies or interferes with the functioning of an electronic system; or

(b) hinders, denies or interferes with a person who is lawfully using or operating an electronic system,

commits an offence and is liable on conviction to a fine not exceedingVT1, 000, 000, or to a term of imprisonment not exceeding 2 years, or both.

(3) A body corporate who commits an offence under this section is liable on conviction to a fine not exceeding VT2,000,000 .

(4) A person who intentionally or without lawful excuse, hinders or interferes with an electronic system that is:

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

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

commits an offence and is liable on conviction to a fine not exceedingVT10, 000, 000, or to a term of imprisonment not exceeding15 years, or both.

(5) A body corporate who commits an offence under this section is liable on conviction to a fine not exceeding VT20, 000. 000.

8 Illegal devices

(1) A person who intentionally or without lawful excuse, produces, sells, procures for use, imports, exports, distributes or otherwise makes available:

(a) a software, electronic system or an electronic device; or

(b) a password, access code or similar data by which the whole or any part of an electronic system or electronic data that is capable of being accessed,

commits an offence and is liable on conviction to a fine not exceedingVT1,000,000, or to a term of imprisonment not exceeding3 years, or both.

(2) A body corporate who commits an offence under this section is liable on conviction to a fine not exceeding VT3, 000, 000.

9 Computer- related forgery

(1) A person who intentionally or 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, 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 to a fine not exceedingVT1, 000, 000, or to a term of imprisonment not exceeding3 years, or both. .

(2) A body corporate who commits an offence under this section is liable on conviction to a fine not exceedingVT5, 000, 000.

(3) In addition to subsection (1), if a person sends out multiple electronic messages from or through electronic systems, the person commits an offence and is liable on conviction to a fine not exceedingVT1,000,000, or to a term of imprisonment not exceeding 3 years, or both.

10 Computer related fraud

(1) A person who intentionally or without lawful excuse causes a loss of property to another person by:

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

(b) any interference with the functioning of an electronic system,

with fraudulent intent of procuring personal gain for another person, commits an offence and is liable on conviction to a fine not exceedingVT1, 000, 000, or to a term of imprisonment not exceeding 3 years, or both.

(2) A body corporate who commits an offence under this section is liable on conviction to a fine not exceeding VT5, 000. 000.

11 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 an electronic system; or

(b) offers or makes available child pornography through an electronic system; or

(c) distributes or transmits child pornography through an electronic system; or

(d) obtains child pornography through an electronic system for person use or for another person; or

(e) possesses child pornography in an electronic system or on an electronic storage medium,

commits an offence and is liable on conviction to a fine not exceedingVT2, 000, 000, or to a term of imprisonment not exceeding5 years, or both.

(3) A body corporate who commits an offence under this section is liable on conviction to a fine not exceedingVT10, 000, 000.

(4) A person does not commit an offence under subsection (2) if the person establishes that the child pornography was offered, distributed, procured or kept for religious, research, law enforcement or medical purposes.

(5) In addition to subsection (4), the person must ensure the child pornography is deleted as soon as it is no longer legally required.

12 Pornography

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

(a) produces pornography for the purposes of its distribution through an electronic system; or

(b) offers or makes available pornography through an electronic system; or

(c) distributes or transmits pornography through an electronic system;

(d) obtains pornography through an electronic system; or

(e) possesses pornography in an electronic system or on an electronic storage medium,

commits an offence and is liable on conviction to a fine not exceedingVT1, 000 000, or to a term of imprisonment not exceeding3 years, or both.

(2) A body corporate who commits an offence under this section is liable on conviction to a fine VT3, 000, 000.

(3) A person does not commit an offence under subsection (1) if the person establishes that the pornography was offered, distributed, procured or kept for bona fide religious, research, law enforcement or medical purposes.

(4) In addition to subsection (3), the person must ensure the pornography is deleted as soon as it is no longer legally required.

13 Identity- related crime

(1) A person who intentionally or without lawful excuse, at any time uses an electronic system:

(a) transfers,; or

(b) possesses; or

(c) uses,

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 to a fine not exceedingVT1, 000, 000, or to a term of imprisonment not exceeding3 years, or both.

(2) A body corporate who commits an offence under this section is liable on conviction to a fine VT3, 000, 000 .

14 Spam

(1) For the purposes of this section:

spam means the unsolicited transmission of a harmful, fraudulent, misleading or illegal electronic mail message to any person or causing an electronic system to show such message for commercial or illegal purpose.

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

(a) initiates the transmission of spam; or

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

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

commits an offence and is liable on conviction to a fine of VT1, 000, 000, or to a term of imprisonment of 3 years, or both.

(3) A body corporate who commits an offence under this section is liable on conviction to a fine VT2, 000, 000.

15 Disclosure of information of an investigation

A service provider including its employees, who receives an order from a Court, relating to a criminal investigation that provides that confidentiality is to be maintained or such obligation stated by law and the service provider continues or proceeds 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 to a fine not exceeding VT2, 000, 000, or to a term of imprisonment not exceeding 5 years, or both.

16 Cyber stalking

(1) For the purposes of this section:

cyber stalking means the continuous act to coerce, intimidate, harass, insult or annoy a person through electronic systems or electronic devices.

(2) A person who directly or indirectly uses any electronic communication to do cyber stalking, commits an offence and is liable on conviction to a fine not exceeding VT1, 000, 000, or to a term of imprisonment not exceeding 3 years, or both.

(3) A body corporate who commits an offence under this section is liable on conviction to a fine not exceeding VT1, 000, 000.

17 Solicitation of children

A person who uses an electronic system to propose to a child to meet him or her with the intention to sexually exploit the child, 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 of 5 years, or both.

18 Defamation

A person who uses any electronic device or electronic system to speak, write, make gestures or any other method, to maliciously expose any person alive or dead to public hatred, contempt or ridicule, or to harm the reputation of that other person, commits an offence and is liable on conviction to a fine not exceeding VT1, 000, 000, or to a term of imprisonment not exceeding 5 years, or both.

19 Religious offence

A person who uses any electronic device or electronic system to insult the religion of any class of persons commits an offence and is liable on conviction to a fine not exceeding VT1, 000, 000, or to a term of imprisonment not exceeding 2 years, or both.

20 Aiding and abetting

A person who aids or abets an person to commit an offence under this Act commits an offence and is liable on conviction to a fine not exceeding VT1, 000, 000 or to a term of imprisonment not exceeding 2 years, or both.

PART 3 INVESTIGATIONS

21 Appointment of authorised officers

The Minister may, on the recommendation of the Chief Information Officer, by notice published in the Gazette, appoint a person or category of persons as an authorised officer or authorised officers for the purposes of this Act.

22 Search and seizure

(1) For the purposes of this section:

seize includes:

(a) activating any onsite electronic system and electronic storage media; or

(b) making and retaining a copy of electronic data, including by using onsite equipment; or

(c) maintaining the integrity of the relevant stored electronic data; or

(d) rendering inaccessible, or removing, electronic data in the accessed electronic system; or

(e) taking a printout of output of electronic data; or

(f) secure an electronic system or part of it or an electronic storage medium.

(2) A Court may, if it is satisfied upon an application made to it by an authorised officer, that there are reasonable grounds to suspect that there may be in any place an electronic device or electronic data that:

(a) may be material evidence in proving an offence; or

(b) has been acquired by a person as a result of an offence,

issue a warrant authorising the authorised officer with such assistance as may be necessary to enter a place to search and seize electronic devices or electronic data or both electronic devices and electronic data.

(3) Search under subsection (2), includes having access to an:

(a) electronic system or part of it and electronic data stored therein; and

(b) electronic storage medium in which electronic data may be stored.

(4) A person who carries out a search or seizes electronic devices or electronic data must as soon as practicable:

(a) prepare a list of what was searched and seized; and

(b) specify in the list the time and date of what was searched and seized.

(5) The person must provide to the occupier of the premises or to the person who had custody of or control of the electronic devices.

(6) An authorised officer may, upon request, permit a person who had custody or control of the electronic devices or someone acting on their behalf to:

(a) access and copy electronic data on the system; or

(b) provide a copy of the electronic data.

(7) An authorised officer may refuse to provide access or provide copies if he or she has reasonable grounds to believe that in doing so it will:

(a) constitute a criminal offence; or

(b) prejudice:

(i) the investigation in relation to which the warrant was issued; or

(ii) another investigation; or

(iii) any civil proceedings and criminal proceedings that may be in relation to any of those investigations.

(8) If there are reasonable grounds to believe that data has originated from an electronic system outside of Vanuatu and such data can lawfully accessible from an another electronic system, the authorised officer is to make an application to extend the warrant to access the other system.

23 Assistance

A person who is not a suspect of a crime under this Act, but is in possession or control of an electronic device or electronic data that is subject to a search warrant under section 22, may at his or her own cost permit or assist an authorised officer when carrying out the search to:

(a) access and use the electronic device or electronic data; and

(b) obtain a copy of that electronic data; and

(c) use an electronic device to make copies; and

(d) obtain an intelligible output from an electronic device in a format that can be read.

24 Production order

If a Court, upon an application by an authorised officer is satisfied that a specified electronic data or a printout or other information is reasonably required for the purpose of a criminal investigation or civil proceedings and criminal proceedings, may issue all or any of the following order:

(a) a person in control of an electronic device or electronic system of electronic devices to produce specified electronic data or printout of such information;

(b) a service provider to produce information about persons who subscribe to or use their services.

25 Expedited preservation

(1) If a authorised officer is satisfied that:

(a) electronic data stored in an electronic device is reasonably required for the purpose of a criminal investigation; and

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

the authorised officer may, by written notice given to a person in control of the electronic device, require the person to ensure that the data specified in the notice be preserved for a period of up to 7 days as specified in the notice.

(2) A Court may, upon an application made to it by a police officer or a law authority, authorize an extension of not more than 14 days.

26 Partial disclosure of traffic data

If a Court is satisfied upon an application made to it by a authorised officer, that specified data stored in an electronic device or system of electronic devices is required for the purpose of a criminal investigation or civil proceedings and criminal proceedings, the Court may order such person to disclose sufficient traffic data about a specified communication to identify the:

(a) service providers; and

(b) path through which the communication was transmitted.

27 Collection of Traffic Data

(1) If a Court is satisfied upon an application made to it by a authorised officer, is satisfied that there are reasonable grounds to believe that traffic data is associated with a specified communication and is required for the purposes of a criminal investigation, the Court may order a person in control of such data to:

(a) collect or record traffic data associated with a specified communication during a specified period; and

(b) permit and assist the authorised officer to collect or record that data.

(2) If a Court, upon an application made to it by a authorised officer, is satisfied that there are reasonable grounds to believe that traffic data is reasonably required for the purposes of a criminal investigation, the Court may authorize for the collection or record of traffic data associated with specified communication during specified period through application of technical means.

28 Interception of Content Data

(1) If a Court, is satisfied upon an application made to it by a authorised officer, that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the Court may:

(a) order a service provider whose service is available through an application of technical means to collect or record, to permit or assist competent authorities with the collection or recording of

content data associated with specified communications transmitted by means of an electronic system; or

(b) authorize an authorised officer to collect or record that data through application of technical means.

(2) For the purposes of paragraph (1)(b), **technical means** means methods to be used by an authorized officer to collect or record data through the use of technology and does not include by any physical interception.

29 Remote Forensic Tools

(1) For the purposes of this section:

Remote Forensic Tool means an investigative tool such as software or hardware installed on or applied with regard to an electronic system and used to perform tasks that include but are not limited to keystroke logging or transmission of an IP-address.

(2) Upon an application of an authorized officer, if a Court is satisfied that there are reasonable grounds to believe that evidence cannot be collected by any means authorized under this Part, the Court may authorize an authorised officer to install a remote forensic tool on a service provider's electronic system in order to collect relevant data required in an investigation concerning an offence provided for under:

(a) Part 2 of this Act; or

(b) Part 3 of the Penal Code Act[CAP 135]; or

(c) Part 10 of the Telecommunications Act [CAP 206].

(3) An application to the Court under subsection (2), must contain the following information:

(a) the name and address of the person suspected of committing the offence and and his or her service provider, and

(b) a description of the targeted electronic system, and

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

(d) the reasons for the necessity of the utilization.

(4) During an investigation it is necessary to ensure that modifications to the electronic system of the suspect or his or her service provider are limited to such modifications relevant in the investigation and that any changes, if possible, can be undone after the end of the investigation.

(5) During an investigation it is necessary to log in:

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

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

(c) any information obtained.

(6) Any information obtained under paragraph (3)(c) by the use of a software must be protected from any modification, unauthorized deletion and unauthorized access.

(7) The duration of an authorization made under subsection (2), must not be more than 3 months, however, if the conditions of the authorization are no longer met, the authorisation is to cease immediately.

(8) If to install a remote forensic tool on the service provider's electronic system, as provided under subsection (2), requires physical access to its location, access must be permitted.

(9) If necessary the authorised officer may, pursuant to the order granted under subsection (2), request that the Court order a service provider to support the installation process for a remote forensic tool.

PART 4 LIABILITY

30 No monitoring obligation

(1) For the purposes of this section:

internet service provider means a person that provides to users internet services.

(2) Internet service providers do not have a general obligation to monitor the information which they transmit or store on behalf of another person, nor do they have a general obligation to actively seek facts or circumstances indicating illegal activity to avoid criminal liability.

31 Access provider

(1) For the purpose of this Act:

access provider means any person providing any electronic communication transmission service by transmitting information provided by or to a user of the service in communication network or providing access to a communication network.

(2) A civil proceedings and criminal proceedings must not be brought against a access provider over anything done or omitted to be done in good faith by him or her in the execution or purported executions of his or her services.

(3) Subsection (2) does not apply if the access provider acted in bad faith in executing his or her services.

32 Hosting Provider

(1) For the purposes of this section:

hosting provider means any person providing an electronic data transmission service by storing of information provided by a user of the service.

(2) A civil proceedings and criminal proceedings must not be brought against a host provider over anything done or omitted to be done in good faith by him or her in the execution or purported executions of his or her services.

(3) Subsection (2) does not apply if the host provider acted in bad faith in executing his or her services.

(4) In addition to subsection (2), subsection (3) does not apply when the user of the service is acting under the authority or the control of the hosting provider.

(5) The hosting provider is not subject to subsection (3) if he or she is to remove information by way of a Court order, and the hosting provider is exempted from any contractual obligation with customers to ensure the availability of the service.

33 Caching provider

(1) For the purpose of this section:

caching provider means any person providing an electronic data transmission service by automatic, intermediate and temporary storing information, performed for the sole purpose of making more efficient the information's onward transmission to other users of the service upon their request.

(2) A civil proceedings and criminal proceedings must not be brought against a caching provider over anything done or omitted to be done in good faith by him or her in the execution or purported executions of his or her services.

(3) Subsection (2) does not apply if the caching provider acted in bad faith in executing his or her services.

34 Hyperlink provider

(1) For the purposes of this section:

hyperlink means characteristics or property of an element such as symbol, word, phrase, sentence or image that contains information about another source and points to and causes to display another document when executed;

hyperlink provider means any person providing one or more hyperlink.

(2) A civil proceedings and criminal proceedings must not be brought against a caching provider over anything done or omitted to be done in good faith by him or her in the execution or purported executions of his or her services.

(3) Subsection (2) does not apply if the caching provider acted in bad faith in executing his or her services.

35 Search engine provider

(1) For the purpose of this section:

search engine provider means any person providing search services to identify documents of interest by specifying certain criteria.

(2) A civil proceedings and criminal proceedings must not be brought against a service engine provider over anything done or omitted to be done in good faith by him or her in the execution or purported executions of his or her services.

(3) Subsection (2) does not apply if the service engine provider acted in bad faith in executing his or her services.

PART 5 MISCELLANEOUS

36 Jurisdiction

This Act applies to an act done or an omission made:

(a) in the territory of the State; or

(b) on a ship or aircraft registered in the State; or

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

(d) by a national of the State outside the jurisdiction of any country.

37 Admissibility of electronic evidence

In any proceedings, evidence generated from an electronic system does not prevent that evidence from being admissible.

38 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.

39 Commencement

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