REPUBLIC OF NAURU

CYBERCRIME ACT 2015

No. 14 of 2015

An Act to provide for the prevention of, investigation, suppression and imposition of penalties of computer related offences in Nauru and for other related purposes.

Certified: 12 May 2015

Contents

Enacted by the Parliament of Nauru as follows:

PART 1 - PRELIMINARY

1 Short title

This Act may be cited as the *Cybercrime Act 2015*.

2 Commencement

This Act commences on the date that it is certified by the Speaker.

3 Interpretation

In this Act, unless the context otherwise requires:

'access' in relation to an electronic system, means to instruct, communicate with, store data in, receive data from, or otherwise make use of any of the resources of the electronic system;

'access provider' means any natural or legal person providing an electronic data transmission service by transmitting information provided by or to a user of the service in a communication network or providing access to a communication network;

'caching provider' means any natural or legal 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;

'child' shall mean any person under the age of 18 years;

'child pornography material' means:

(a) material that depicts a person, or a representation of a person, who is, or appears to be, under 18 years of age and who:

(i) is engaged in, or appears to be engaged in, a sexual pose or sexual activity (whether or not in the presence of other persons); or

(ii) is in the presence of a person who is engaged in, or appears to be engaged in, a sexual pose or sexual activity;

and does this in a way that reasonable persons would regard as being, in all the circumstances, offensive; or

(b) material the dominant characteristic of which is the depiction, for a sexual purpose, of:

(i) a sexual organ or the anal region of a person who is, or appears to be, under 18 years of age; or

(ii) a representation of such a sexual organ or anal region; or

(iii) the breasts, or a representation of the breasts, of a female person who is, or appears to be, under 18 years of age;

in a way that reasonable persons would regard as being, in all circumstances, offensive;

(c) material that describes a person who is, or is implied to be, under 18 years of age and who:

(i) is engaged in, or is implied to be engaged in, a sexual pose or sexual activity (whether or not in the presence of other persons); or

(ii) is in the presence of a person who is engaged in, or is implied to be engaged in, a sexual pose or sexual activity;

and does this in a way that reasonable persons would regard as being, in all the circumstances, offensive; or

(d) material that describes:

(i) a sexual organ or the anal region of a person who is, or is implied to be, under 18 years of age; or

(ii) the breasts of a female person who is, or is implied to be, under 18 years of age;

and does this in a way that reasonable persons would regard as being, in all the circumstances, offensive.

'computer' means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

'critical infrastructure' means electronic systems, devices, networks, computer programs, electronic data, so vital to the country that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters;

'data' means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

'Department' means the Department responsible for the administration of this law;

'device' includes but is not limited to:

(a) components of electronic systems such as computer, mobile phones graphic cards, memory chips;

(b) storage components such as 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 data (or computer data)' means any representation of facts, concepts, information (being either texts, sounds or images) machine-readable code or instructions, in a form suitable for processing in an electronic system, including a program suitable to cause an electronic system to perform a function;

'electronic data storage medium (or computer data storage media)' 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 (or computer system)' means a device or a group of inter-connected or related devices, including the Internet, one or more which, pursuant to a program, performs automatic processing of data or any other function;

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

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

(b) causing electromagnetic interference to an electronic system;

(c) corrupting an electronic system by any means;

(d) inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing electronic data;

'hosting provider' means any natural or legal person providing an electronic data transmission service by storing of information provided by a user of the service;

'hyperlink' means a characteristic 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 natural or legal person providing one or more hyperlinks;

'interception' includes but is not limited to the acquiring, viewing and capturing of any electronic, optical, magnetic, oral or other means, during transmission through the use of any technical device;

'internet service provider' means a natural or legal person that provides to users, services mentioned in section 32 - 36 of this Act;

'material' includes, but is not limited to, any texts, images, audio, video and any other electronic record;

'multiple electronic messages' mean a mail message, including E-Mail and instant messaging sent to more than one thousand recipients;

'pornography' means material containing the explicit description or display of sexual organs or activity, whether printed or visual;

'Registrar' means the Registrar of the Supreme Court of Nauru;

'Republic' means the Republic of Nauru;

'remote forensic tool' means an investigative tool such as software 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;

'Secretary' means the head of the Department;

'seize' includes:

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

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

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

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

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

(f) seize or similarly secure an electronic system or part of it or an electronic data storage medium;

'service providers' include, but are not limited to internet service providers, access providers, hosting providers, caching providers, hyperlink providers and search engine providers;

'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;

'utilise' shall include:

(a) developing of a remote forensic tool;

(b) adopting of a remote forensic tool; and

(c) purchasing of a remote forensic tool.

4 Jurisdiction

(1) Where an offence under this Act is committed by any person outside the Republic, he shall be deemed to have committed the offence within the Republic.

(2) For the purposes of this section, this Act shall apply as if, for the offence in question;

(a) the accused; or

(b) the computer, program or data,

was in the Republic at the material time.

5 Admissibility of electronic evidence

In proceedings for an offence against a law of Nauru, the fact that evidence has been generated from an electronic system does not prevent that evidence from being admissible.

PART 2 – OFFENCES

6 Illegal access

(1) For the purposes of this section, a computer shall be treated as a "protected computer" if the person committing the offence knew, or ought reasonably to have known, that the computer or program data is used directly in connection with or necessary for:

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

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

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

(d) the protection of public safety including system related to essential emergency services.

(2) A person, who wilfully, without lawful excuse, accesses the whole or any part of a protected computer, commits an offence punishable on conviction, to imprisonment for a period not exceeding 7 years.

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

7 Illegal interception

A person who intentionally, without right and with dishonest or otherwise unlawful intent, intercepts or attempts to intercept by technical means:

(a) a transmission not intended for public reception of electronic data to, from or within an electronic system; or

(b) electromagnetic emissions from an electronic system,

commits an offence punishable on conviction, to imprisonment for a period not exceeding 7 years.

8 Illegal data interference

A person who, wilfully or recklessly, without lawful excuse:

(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 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 authorised to access it,

commits an offence punishable on conviction, to imprisonment for a period not exceeding 7 years.

9 Data espionage

A person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification, obtains for himself or for another, electronic data which are not meant for him, and which are specially protected against unauthorised access, commits an offence punishable on conviction, to imprisonment for a period not exceeding 7 years.

10 Illegal system interference

(1) A person who, wilfully or recklessly, without lawful excuse hinders or interferes:

(a) with the functioning of an electronic system if he or she knows or ought to know that danger to life is likely to result; or

(b) with a person who is lawfully using or operating an electronic system if he or she knows or out to know that danger to life is likely to result; or

(c) with an electronic system that is exclusively for the use of critical infrastructure operations, or in the case in which such is not exclusively for the use of critical infrastructure operations, but it is used in critical infrastructure operations and such conduct affects that use or impacts the operations of critical infrastructure.

commits an offence punishable on conviction, to imprisonment for a period not exceeding 7 years.

11 Making, selling, distributing or possessing software or device for committing a crime

(1) A person who does any of the following with the sole purpose or principal use of which the person knows to be the commission of a crime, knowing or being reckless as to whether it will be used for the commission of a crime:

(a) invites another person to acquire from the person any software, device or other electronic information that would enable the other person to access an electronic systems without authorisation;

(b) offers or exposes for sale or supply to another person any software, device or other electronic information that would enable the other person to access an electronic system without authorisation;

(c) agrees to sell or supply to another person any software, device or other electronic information that would enable the other person to access an electronic system without authorisation;

(d) has in his or her possession for the purpose of sale or supply to another person any software, device or other electronic information that would enable the other person to access an electronic system without authorisation,

commits an offence punishable on conviction to imprisonment for a term not exceeding 7 years.

(2) A person who:

(a) has in his or her possession any software, device or other electronic information that would enable him or her to access an electronic system without authorisation; and

(b) intends to use that software, device or other electronic information to commit a crime,

commits an offence punishable on conviction to imprisonment for a term not exceeding 7 years.

12 Computer-related forgery

A person who wilfully, without lawful excuse, inputs, alters, deletes, or suppresses electronic data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible commits an offence punishable on conviction, to imprisonment for a period not exceeding 10 years.

13 Computer-related fraud

A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, 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 or dishonest intent of procuring, without right, an economic benefit for oneself or for another person, the penalty shall be imprisonment for a period not exceeding 10 years.

14 Child pornography

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

(a) produces child pornography material for the purpose of its distribution through an electronic system;

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

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

(d) procures or obtains child pornography material through an electronic system for oneself or for another person;

(e) possesses child pornography material in an electronic system or on a data storage medium; and

(f) knowingly obtains access, through information and communication technologies, to child pornography material,

commits an offence punishable on conviction, to imprisonment for a period not exceeding 10 years.

(2) It is a defence to a charge of an offence under subsection (1) (b), (c), (d), (e) and (f) if the person establishes that the child pornography material was a bona fide law enforcement purpose. If child pornography material was stored for such a purpose, the authorised person needs to ensure that it is deleted as soon as it is not legally required anymore.

15 Solicitation of children

A person, who intentionally, through the use of information and communication technology, proposes to a child to meet him or her, with the intent of committing an offence and where such proposal has been followed by material acts leading to such meeting, commits an offence punishable upon conviction to imprisonment for a period not exceeding 10 years.

16 Publishing of indecent or obscene information or material in electronic form

(1) A person who publishes or transmits or causes to be published in electronic form:

(a) any material or information which is lascivious or appeals to the prurient interest; or

(b) if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the information or material contained or embodied in it,

commits an offence and is punishable on conviction to imprisonment for a period not exceeding 10 years or a fine not exceeding $30,000 or both.

(2) It is a defence to a charge of an offence under subsection (1) if the person establishes that the possession of such indecent or obscene information or material was for a bona fide law enforcement purpose. If child pornography was stored for such a purpose, the authorised person needs to ensure that it is deleted as soon as it is not legally required anymore.

17 Identity-related crimes

A person who wilfully, without lawful excuse, by using an electronic system in any stage of the offence, intentionally transfers, possesses, or uses a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a criminal offence as provided under any other law of Nauru, is punishable on conviction, to imprisonment for a period not exceeding 7 years.

18 SPAM

A person who, intentionally, without lawful excuse or justification:

(a) initiates the transmission of multiple electronic messages from or through such electronic system with the intent to deceive or mislead users; or

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

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

commits an offence punishable, on conviction, by imprisonment for a period not exceeding 5 years.

19 Disclosure of details of an investigation

An Internet service provider who receives a Court order related to a criminal investigation that explicitly stipulates that confidentiality is to be maintained or such obligations is stated by law and that Internet service provider, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, discloses:

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

(b) anything done under the order; or

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

commits an offence punishable, on conviction, by imprisonment for a period not exceeding 10 years or a fine of $100,000 or both.

20 Failure to permit assistance

A person other than the suspect of an offence who wilfully refuses to permit or assist a person based on an order as specified by Part 3 of this Act commits an offence punishable, on conviction, by imprisonment for a period not exceeding 5 years or a fine of $50,000 or both.

21 Sending or publishing information or material through electronic communication

A person who sends or publishes, by means of electronic communication:

(a) any information or material that may be classed as politically subversive, defamatory or seditious; and

(b) such information or material is likely to threaten national defence, public safety, public order, public morality or public health,

commits an offence punishable on conviction, to imprisonment for a period not exceeding 7 years.

22 Harassment utilising means of electronic communication

A person who initiates any electronic communication with the intent to coerce, intimidate, harass, or cause emotional distress to a person, using an electronic system to support severe, repeated, and hostile behaviour and such communication is likely to threaten national defence, public safety, public order, public morality or public health, commits an offence punishable on conviction, to imprisonment for a period not exceeding 7 years.

23 Racial and religious offences

A person who through electronic communication or who initiates any electronic communication, uses language that is threatening, abusive or insulting in nature and with the intent to stir up racial or religious hatred that is likely to threaten national defence, public safety, public order, public morality or public health, is guilty of an offence punishable on conviction, to imprisonment for a period not exceeding 7 years.

PART 3 – PROCEDURAL LAW

24 Search and seizure

(1) If a Court on application by a police officer, is satisfied on the basis of information that there are reasonable grounds to suspect that there may be in a place, an electronic system or electronic data:

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

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

a judge, magistrate or registrar may issue a warrant authorising a police officer**,** with such assistance as may be necessary to enter the place to search and seize the thing or electronic data including search or similarly access:

(i) an electronic system or part of it and electronic data stored within; and

(ii) an electronic-data storage medium in which electronic data may be stored in the territory of the country.

(2) Any person who exercises a search or seizure under this section, shall at the time or as soon as practicable:

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

(b) give a copy of that list to the Director of Public Prosecutions; and

(c) the occupier of the premises; or

(d) the person in control of such electronic devices.

(3) Subject to subsection (4), on request, any police officer or another authorised person shall:

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

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

(4) The police officer or another authorised person may refuse to give access or provide copies if he or she has reasonable grounds for believing that giving the access, or providing the copies may:

(a) constitute a criminal offence; or

(b) prejudice:

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

(ii) another ongoing investigation; or

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

(5) If a police officer who is undertaking a search based on subsection (1), has grounds to believe that the data sought is stored in another electronic device or part of it in its territory, and such data is lawfully accessible from or available to the initial system, he or she shall be able

to expeditiously extend the search or similar accessing to the other system.

(6) A police officer who is undertaking a search is empowered to seize or similarly secure electronic data accessed according to subsections (1) or (2).

(7) In order to properly execute a search and seizure order, a police officer may employ the assistance of a person considered an expert in the area of information technology, computing and computers and other similar experience.

25 Assistance

A person who is not a suspect of a crime but is in possession or control of an electronic device or electronic data that is the subject of a search under section 24 shall permit, and assist if required by the police officer making the search to:

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

(b) obtain and copy that electronic data;

(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.

26 Production order

If a Court on application by a police officer is satisfied on the basis of information that specified electronic data or a printout or other information is reasonably required for the purpose of a criminal investigation or criminal proceedings, may order:

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

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

27 Expedited preservation

(1) Where a police officer is satisfied that:

(a) electronic data is 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 police 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.

(2) A judge, magistrate or registrar may upon application authorise an extension not exceeding 14 days.

28 Partial disclosure of traffic data

If a judge, magistrate or registrar is satisfied on the basis of an application by a police officer that specified data stored in an electronic device or system of electronic devices is required for the purpose of a criminal investigation or criminal proceedings, the judge, magistrate or registrar may order such person to disclose sufficient traffic data about a specified communication to identify:

(a) the service providers; and

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

29 Collection of traffic data

(1) If a judge, magistrate or registrar on application by police officer is satisfied on the basis of information that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the judge, magistrate or registrar may, by written notice given to a person in control of such data, request that person to:

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

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

(2) If a judge, magistrate or registrar on application by a police officer, is satisfied on the basis of information that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the judge, magistrate or registrar may authorise the police officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means.

30 Interception of content data

If a judge, magistrate or registrar on application by a police officer is satisfied on the basis of information that content of electronic communication is reasonably required for the purposes of a criminal investigation, the judge, magistrate or registrar may:

(a) order an Internet service provider whose service is available in Nauru through 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) authorise a police officer to collect or record that data through application of technical means.

31 Forensic tool

(1) If a judge, magistrate or registrar on application by a police officer is satisfied on the basis of information, that in an investigation concerning an offence under this Act, there are reasonable grounds to believe that essential evidence can only be collected by applying a remote forensic tool, that is reasonably required for the purposes of a criminal investigation, the judge, magistrate or registrar may:

(a) authorise a police officer to utilise a remote forensic tool with the specific task required for the investigation;

(b) and install it on the suspect's electronic system in order to collect the relevant evidence.

(2) The application must contain the following information:

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

(b) description of the targeted electronic system; and

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

(d) reasons for the necessity of the utilisation.

(3) Within such investigation it is necessary to ensure that modifications to the electronic system of the suspect are limited to those essential for the investigation and that any changes if possible can be undone after the end of the investigation. During the investigation it is necessary to log:

(a) the technical means 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.

(4) Information obtained by the use of such software need to be protected against any modification, unauthorised deletion and unauthorised access.

(5) The duration of authorisation in section 31(1) is limited to 3 months and if the conditions of the authorisation are no longer met, the actions taken are to stop immediately.

(6) The authorisation to install the tool includes remotely accessing the suspect's computer system.

(7) If the installation process requires physical access to a place, the requirements of section 24 need to be fulfilled.

(8) If necessary a police officer may, pursuant to the order granted in (1) above, request that the Court order an Internet service provider to support the installation process.

PART 4 – LIABILITY

32 Access provider

(1) An Access provider is not criminally liable for providing access and transmitting information on conditions that the provider:

(a) does not initiate the transmission;

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

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

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

33 Hosting provider

(1) A Hosting provider is not criminally liable for the information stored at the request of a user of a service, on the condition that:

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

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

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

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

34 Caching provider

A Caching provider is not criminally liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other users of the service upon their request, on the conditions that:

(a) the Caching provider does not modify the information;

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

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

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

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

35 Hyperlinks provider

A Hyperlink provider who enables the access to information provided by third person by providing an electronic hyperlink is not liable for the information if:

(a) the Hyperlink provider expeditiously removes or disables access to the information after receiving an order from a court to remove the link; and

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

36 Search engine provider

A provider who makes or operates a search engine that either automatically or based on entries by others, creates an index of Internet-related content or makes available electronic tools to search for information provided by third parties, is not liable for search results on conditions that the provider:

(a) does not initiate the transmission; and

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

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

37 Monitoring obligation

(1) Service providers have a general obligation to monitor and store the information which they transmit or store on behalf of another, as well as a general obligation to actively seek facts or circumstances indicating illegal activity to avoid criminal liability.

(2) Any information stored under subsection (1) shall be kept for a period of up to 12 months before service providers can delete or destroy it.

(3) Information monitored or stored is to be treated as private and confidential and shall only be accessible through an order by a Court in connection with an offence that has been committed.

38 Act to have overriding effect

The provisions of this Act shall have effect even if there is anything inconsistent contained in any other law for the time being in force in Nauru.

39 Regulations

The Cabinet may make regulations, not inconsistent with this Act, prescribing all matters that are necessary or convenient to be prescribed for carrying out or giving effect to the provisions in this Act.