M O N T S E R R A T

PENAL CODE (AMENDMENT) BILL 2020

No. of 2020

ARRANGEMENT OF SECTIONS

Montserrat

Penal Code (Amendment) Bill, 2020

No. of 2020

I ASSENT

Governor

DATE:

M O N T S E R R A T

No. of 2020

A BILL FOR

AN ACT TO AMEND THE PENAL CODE BY MAKING PROVISION FOR OFFENCES RELATED TO CYBERCRIME.

BE IT ENACTED by the Queen's Most Excellent Majesty, by and with the advice and consent of the Legislative Assembly of Montserrat, and by the Authority of the same as follows:—

1. Short title and commencement

This Act may be cited as the Penal Code (Amendment) Act, 2020.

2. Interpretation

In this Act, **"principal Code"** means the Penal Code (Cap. 4.02).

4. Part 20A inserted

The principal Code is amended by inserting after Part 20 the following as Part 20A:

"**PART 20A**

CYBERCRIME

289A Interpretation

In this Part—

"child" means a person under the age of eighteen years;

"child pornography" means material that—

(a) depicts or presents a child engaged in sexual activity or conduct;

(b) depicts or presents a child in a sexually explicit pose;

(c) depicts or presents, for sexual purposes, parts of a child's body pasted to visual representations of parts of an adult's body or vice versa;

(d) depicts or presents, for sexual purposes, parts of a child's body which have been rendered complete by computer generated images or by other methods of visual representation;

(e) depicts or presents a person appearing to be a child engaged in sexual conduct; or

(f) realistically represents a person appearing to be a child engaged in sexual conduct, and includes, but is not limited to, any visual material including images, animations or videos, or audio or text material, but does not include any visual representation produced or reproduced for the purpose of education, counselling, promotion of reproductive health or as part of a criminal investigation or prosecution or civil

proceedings or in the lawful performance of a person's profession, duties and functions;

"computer data" means any representation of—

(a) facts;

(b) concepts;

(c) information including text, sound, image or video; or

(d) machine-readable code or instructions, that is in a form suitable for processing in a computer system and is capable of being sent, received or stored, and includes a program that can cause a computer system to perform a function;

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

"computer program" or **"program"** means data which represents instructions or statements that, when executed in a computer system, can cause the computer system to perform a function;

"computer system" means a device or a group of inter-connected or related devices which follows a program or external instruction to perform automatic processing of information or electronic data;

"Data Controller" means any person who either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data, but does not include a data processor;

"device" includes—

(a) a component of a computer system such as a graphic card or memory chip;

(b) a storage component such as a hard drive, memory card, compact disc or tape;

(c) input equipment such as a keyboard, mouse, track pad, scanner or digital camera; or

(d) output equipment such as a printer or screen;

"electronic" means relating to technology, having electrical, digital, magnetic, optical, biometric, electrochemical, wireless, electromagnetic or similar capabilities;

"function" in relation to a computer system includes logic, control, arithmetic, deletion, storage or retrieval and communication or telecommunication to, from or within a computer;

"hinder" in relation to a computer system includes—

(a) disconnecting the electricity supply to a computer system;

(b) causing electromagnetic interference to a computer system;

(c) corrupting a computer system; and

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

"information society services" means any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service;

"intercept" in relation to computer data communication includes listening to, monitoring, viewing, reading or recording, by any means, such communication during transmission without the knowledge of the person making or receiving the communication;

"internet service provider" includes a person who provides the services mentioned in sections 38 to 43;

"multiple electronic mail messages" means any unsolicited electronic message, including electronic mail and instant message, that is sent to more than a thousand recipients at a time; and

"traffic data" means computer data that—

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

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

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

289B Illegal access to computer system

A person who, intentionally and without lawful excuse or justification, accesses a computer system or any part of a computer system commits an offence and is liable on—

(a) summary conviction, to a fine of [$150,000] or to [three] years' imprisonment or to both;

(b) conviction on indictment, to a fine of [$500,000] or to [seven] years' imprisonment or to both.

289C Illegal remaining in computer system

A person who, intentionally and without lawful excuse or justification, remains logged into a computer system or part of a computer system or continues to use a computer system, commits an offence and is liable on—

(a) summary conviction, to a fine of [$150,000] or to [three] years' imprisonment or to both;

(b) conviction on indictment, to a fine of [$500,000] or to [seven] years' imprisonment or to both.

289D Illegal interception

(1) A person who, intentionally and without lawful excuse or justification, intercepts—

(a) any subscriber information or traffic data or any communication to, from or within a computer system; or

(b) any electromagnetic emission from a computer system,

commits an offence.

(2) A person who commits an offence under subsection (1) is liable on—

(a) summary conviction, to a fine of [$150,000] or to [three] years' imprisonment or to both;

(b) conviction on indictment, to a fine of [$500,000] or to [seven] years' imprisonment or to both.

289E Illegal data interference

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

(a) damages computer data or causes computer data to deteriorate;

(b) deletes computer data;

(c) alters computer data;

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

(e) obstructs, interrupts or interferes with the lawful use of computer data;

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

(g) denies access to computer data to a person authorized to access it,

commits an offence.

(2) A person who commits an offence under subsection (1) is liable on—

(a) summary conviction, to a fine of [$150,000] or to [three] years' imprisonment or to both;

(b) conviction on indictment, to a fine of [$500,000] or to [seven] years' imprisonment or to both.

289F Illegal acquisition of data

A person who, intentionally and without lawful excuse or justification, obtains for himself or for another person, computer data which is not meant for him or the other person and which is protected against unauthorised access, commits an offence and is liable on—

(a) summary conviction, to a fine of [$150,000] or to [three] years' imprisonment or to both;

(b) conviction on indictment, to a fine of [$500,000] or to [seven] years' imprisonment or to both.

289G Illegal system interference

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

(a) hinders or interferes with the functioning of a computer system; or

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

commits an offence.

(2) A person who commits an offence under subsection (1) is liable on—

(a) summary conviction, to a fine of [$150,000] or to [three] years' imprisonment or to both;

(b) conviction on indictment, to a fine of [$500,000] or to [seven] years' imprisonment or to both.

289H Offences affecting critical infrastructure

(1) Despite the penalties set out in sections 3 to 8, where a person commits an offence under any of those sections and the offence results in hindering or interference with a computer system that—

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

(b) affects the use, or impacts the operation, of critical infrastructure,

the person is liable on conviction on indictment to a fine of [$1,000,000] or to [fifteen] years' imprisonment.

(2) For the purposes of this section, **"critical infrastructure"** means any computer system, device, network, computer program, computer data, so vital to Montserrat that the incapacity or destruction of, or interference with, such system, device, network, computer program or computer data would have a debilitating impact on—

(a) security, defence or international relations of Montserrat; or

(b) provision of services directly related to national or economic security, banking and financial services, public utilities, the energy sector, communications infrastructure, public transportation, public health and safety, or public key infrastructure.

289I Illegal devices

(1) A person who produces, sells, procures for use, imports, exports, distributes or otherwise makes available or has in his possession—

(a) a device, including a computer program, that is designed or adapted for the purpose of committing an offence under this Act; or

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

with the intent that it be used for the purpose of committing an offence under this Act commits an offence.

(2) A person who commits an offence under subsection (1) is liable on—

(a) summary conviction, to a fine of [$150,000] or to [three] years' imprisonment or to both;

(b) conviction on indictment, to a fine of [$500,000] or to [seven] years' imprisonment or to both.

289J Identity-related crimes

(1) A person who, intentionally and without lawful excuse or justification transfers, possesses or uses a means of identification, other than his own, with the intent of committing, or aiding or abetting, the commission of, an unlawful act through the use of a computer system commits an offence.

(2) A person who commits an offence under subsection (1) is liable on—

(a) summary conviction, to a fine of [$150,000] or to [three] years' imprisonment or to both;

(b) conviction on indictment, to a fine of [$500,000] or to [seven] years' imprisonment or to both.

289K Computer-related forgery

(1) A person who, intentionally and without lawful excuse or justification inputs, alters, deletes, or suppresses computer 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 computer data is directly readable and intelligible, commits an offence.

(2) A person who commits an offence under subsection (1) is liable on—

(a) summary conviction, to a fine of [$200,000] or to [three] years' imprisonment or to both;

(b) conviction on indictment, to a fine of [$500,000] or to [seven] years' imprisonment or to both.

(3) A person who commits an offence under subsection (1) by sending out multiple electronic mail messages from or through a computer system is liable on conviction to a fine of [$25,000] and [three] years' imprisonment in addition to the penalty set out in subsection (2).

289L Computer-related fraud

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

(a) inputs, alters, deletes or suppresses computer data; or

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

with the fraudulent or dishonest intent of procuring an economic benefit for himself or another person and thereby causes a loss of, or damage to, property commits an offence.

(2) A person who commits an offence under subsection (1) is liable on—

(a) summary conviction, to a fine of [$200,000] or to [three] years' imprisonment or to both;

(b) conviction on indictment, to a fine of [$500,000] or to [seven] years' imprisonment or to both.

289M Violation of privacy

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

(a) captures;

(b) stores in, publishes or transmits through a computer system, the image of a private area of another person without consent where the other person has a reasonable expectation that—

(i) the other person could disrobe in privacy; or

(ii) the private area of the other person would not be visible to the public, regardless of whether he is in a public or private place,

commits an offence.

(2) A person who commits an offence under subsection (1) is liable on—

(a) summary conviction, to a fine of [$100,000] or to [two] years' imprisonment or to both;

(b) conviction on indictment, to a fine of [$250,000] or to [five] years' imprisonment or to both.

(3) For the purposes of this section—

"capture" in relation to an image, means to videotape, photograph, film or record by any means; and

"private area" means the genitals, pubic area, buttocks or breast;

289N Child pornography

(1) A person who, intentionally—

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

(b) offers to make available child pornography through a computer system;

(c) distributes or transmits child pornography through a computer system;

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

(e) possesses child pornography in a computer system or on a computer data storage medium; or

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

commits an offence.

(2) A person who commits an offence under subsection (1) is liable on—

(a) summary conviction, to a fine of [$300,000] or to [five] years' imprisonment or to both;

(b) conviction on indictment, to a fine of [$750,000] or to [twenty] years' imprisonment or to both.

289O Conditions applicable to child's consent in relation to information society services

(1) If consent is provided, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful if the child is at least [sixteen] years of age.

(2) If the child is below the age of [sixteen] years, the processing of the personal data of the child shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

(3) The Data Controller shall make reasonable efforts to verify in respect of a child under subsection (2) that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

(4) Section 16 (1) shall not affect the general contract law of Montserrat in relation to minors and children.

289P Harassment utilising means of electronic communication

(1) A person who uses a computer system to intentionally or recklessly cyberbully another person commits an offence.

(2) A person who uses a computer system to disseminate any information, statement or image, knowing the same to be false, and who—

(a) damages the reputation of another person; or

(b) subjects another person to public ridicule, contempt, hatred or embarrassment,

commits an offence.

(3) A person who, intentionally or recklessly—

(a) uses a computer system to disseminate any information, statement or image; and

(b) exposes the private affairs of another person, thereby subjecting that other person to public ridicule, contempt, hatred or embarrassment,

commits an offence.

(4) A person who commits an offence under this section is liable on—

(a) summary conviction, to a fine of [$100,000] or to [two] years' imprisonment or to both;

(b) conviction on indictment, to a fine of [$200,000] or to [five] years' imprisonment or to both.

(5) For the purpose of this section, **"cyberbully"** means to use a computer system repeatedly or continuously to convey information which causes—

(a) fear, intimidation, humiliation, distress or other harm to another person; or

(b) detriment to another person's health, emotional well-being, self-esteem or reputation.

289Q Spam

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

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

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

and thereby causes harm to a person or damage to a computer system commits an offence.

(2) A person who intentionally falsifies the header information of an electronic mail message for the purpose of committing an offence under subsection (1) commits an offence.

(3) A person who commits an offence under this section is liable on—

(a) summary conviction, to a fine of [$100,000] or to [two] years' imprisonment or to both;

(b) conviction on indictment, to a fine of [$500,000] or to [five] years' imprisonment or to both.

289R Spoofing

(1) A person who establishes a website or sends an electronic mail message with a counterfeit source—

(a) with the intention that a visitor to a computer system or recipient of an electronic mail message will believe it to be an authentic source; or

(b) to attract or solicit a person or computer system,

for the purpose of gaining unauthorised access to commit a further offence or obtain information which can be used to commit an unlawful act, commits an offence.

(2) A person who commits an offence under subsection (1) is liable on—

(a) summary conviction, to a fine of [$100,000] or to [two] years' imprisonment or to both;

(b) conviction on indictment, to a fine of [$200,000] or to [five] years' imprisonment or to both.

289S Offence by body corporate under this Part

Where a body corporate commits an offence under this Act and a court is satisfied that a director, manager, secretary or other similar officer of the body corporate or, or any person who purports to act in such capacity—

(a) connived in or consented to the commission of the offence; or

(b) failed to exercise due diligence to prevent the commission of the offence, the director, manager, secretary or other similar officer or person

purporting to act in that capacity also commits the offence.

289T No monitoring obligation

(1) Subject to subsection (2), an internet service provider who provides a conduit for the transmission of information, is not responsible for—

(a) monitoring the information which it transmits or stores on behalf of another person in order to ascertain whether its processing would constitute or give rise to liability under this Part; or

(b) actively seeking facts or circumstances indicating illegal activity in order to avoid liability under this Part.

(2) Subsection (1) does not relieve an internet service provider from complying with any court order, injunction, writ or other legal requirement, which obliges an internet service provider to terminate or prevent an infringement based on any written law.

289U Access provider

(1) An access provider is not liable under this Part for providing access and transmitting information if the access provider does not—

(a) initiate the transmission;

(b) select the receiver of the transmission; or

(c) select or modify the information contained in the transmission.

(2) For the purpose of this section—

"access provider" means a person who provides a service to facilitate the transmission of computer data between two or more computer systems by transmitting

information provided by or to a user of the service in a communication network or provides access to a communication network;

"communication network" means a set of devices or nodes connected by communication links, which is used to provide for the transfer of computer data between users located at various points or other similar services; and

"transmit" or **"provide access"** includes the automatic, intermediate and transient storage of information transmitted in so far as it takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for a period longer than is reasonably necessary for the transmission.

289V Hosting provider

(1) A hosting provider is not liable under this Part for the storage of information in contravention of this Part if—

(a) the hosting provider expeditiously removes or disables access to the information after receiving an order from a court to remove specific illegal information stored; or

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

(2) This section 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 removes information after receiving an order under subsection (1), that hosting provider is exempted from contractual obligations with their customer to ensure the availability of the service.

(4) For the purpose of this section, **"hosting provider"** means a person who provides a service to facilitate the transmission of computer data between two or more computer systems by storing information provided by a user of their service.

289W Caching provider

(1) A caching provider is not liable for the storage of information in contravention of this Part if the caching provider—

(a) does not modify the stored information;

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

(c) updates stored information in accordance with any written law or in a manner widely recognized and used in the information communication technology industry;

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

(e) acts expeditiously to remove or to disable access to the information the caching provider has stored upon obtaining knowledge of the fact that—

(i) the stored information at the initial source of the transmission has been removed from the network;

(ii) access to the stored information has been disabled; or

(iii) a court has ordered the removal or disablement of the stored information.

(2) For the purposes of this section, **"caching provider"** means a person who provides a service to facilitate the transmission of computer data between two or more computer systems by the automatic, intermediate and temporary storage of information, where such storage is for the sole purpose of making the onward transmission of the information to other users of the service more efficient.

289X Hyperlinks provider

(1) A provider who enables the access to information provided by another person by providing an electronic hyperlink is not liable for the information that is in contravention of this Part if the provider—

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

(b) upon obtaining knowledge or awareness, by ways other than an order from a court, expeditiously informs the Attorney General to enable the Attorney General to evaluate the nature of the information and if necessary, apply to a court for an order to remove the content.

(2) For the purposes of this section, **"hyperlink"** means a characteristic or property of an element such as a symbol, word, phrase, sentence, or image that contains information about another source and points to and causes to display another document when executed.

289Y Search engine provider

A provider who 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 another person, is not liable under this Part for the search results on condition if 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.".

SPEAKER

Passed by the Legislative Assembly this day of , 2020.

CLERK OF THE LEGISLATIVE ASSEMBLY