

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

[reference to the provisions of the Budapest Convention]

*Version 23 Feb 2022***Chapter I – Use of terms**

Article 1 – “Computer system”, “computer data”, “service provider”, “traffic data”

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Article 2 – Illegal access

Article 3 – Illegal interception

Article 4 – Data interference

Article 5 – System interference

Article 6 – Misuse of devices

Article 7 – Computer-related forgery

Article 8 – Computer-related fraud

Article 9 – Offences related to child pornography

Article 10 – Offences related to infringements of copyright and related rights

Article 11 – Attempt and aiding or abetting

Article 12 – Corporate liability

Article 13 – Sanctions and measures

Section 2 – Procedural law

Article 14 – Scope of procedural provisions

Article 15 – Conditions and safeguards

Article 16 – Expedited preservation of stored computer data

Article 17 – Expedited preservation and partial disclosure of traffic data

Article 18 – Production order

Article 19 – Search and seizure of stored computer data

Article 20 – Real-time collection of traffic data

Article 21 – Interception of content data

Section 3 – Jurisdiction

Article 22 – Jurisdiction

Chapter III – International co-operation

Article 24 – Extradition

Article 25 – General principles relating to mutual assistance

Article 26 – Spontaneous information

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 28 – Confidentiality and limitation on use

Article 29 – Expedited preservation of stored computer data

Article 30 – Expedited disclosure of preserved traffic data

Article 31 – Mutual assistance regarding accessing of stored computer data

Article 32 – Trans-border access to stored computer data with consent or where publicly available

Article 33 – Mutual assistance in the real-time collection of traffic data

Article 34 – Mutual assistance regarding the interception of content data

Article 35 – 24/7 Network

This profile has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Budapest Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.

State:	
Signature of the Budapest Convention:	N/A
Ratification/accession:	N/A

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
<p>Article 1 – “Computer system”, “computer data”, “service provider”, “traffic data”:</p> <p>For the purposes of this Convention:</p> <p>a “computer system” means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;</p> <p>b “computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;</p> <p>c “service provider” means:</p> <p>i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and</p> <p>ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;</p> <p>d “traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service</p>	<p>Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto (Cybercrime Act, 2020)</p> <p>Section 2. - Interpretation</p> <p>(1) In this Act–</p> <p>“Central Authority” means the Central Authority designated under the Mutual Legal Assistance Act;</p> <p>“child” means a person under the age of eighteen years;</p> <p>“child pornography” has the meaning assigned to it under the Commercial Sexual Exploitation of Children Act 2013;</p> <p>“Court” means the Supreme Court acting in its criminal jurisdiction;</p> <p>“communication” means–</p> <p>a) anything encrypted or unencrypted comprising of speech, music, sounds, visual images or data of any description; and</p> <p>b) encrypted or unencrypted signals serving for the impartation of anything–</p> <p>(i) between persons, a person and a thing or between things; or</p> <p>(ii) for the actuation or control of any apparatus;</p> <p>“communication data” means any–</p> <p>a) encrypted or unencrypted data comprised in or attached to a communication whether by the sender or otherwise, for the purpose of a communication network by means of which the communication is transmitted;</p> <p>b) encrypted or unencrypted information, that does not include the contents of a Interpretation. Act No. 8 of 2014. Act No. 3 of 2013.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>communication, other than data that falls within paragraph (a), that is made by a person–</p> <ul style="list-style-type: none"> (i) of any communication network; or (ii) any part of a communication network in connection with the provision to or use by any person of any communication service; <p>c) encrypted or unencrypted information that does not fall within paragraph (a) or (b) that is held or obtained by a person providing a communication service in relation to a person to whom the service is provided;</p> <p>“communication network” means any wire, radio, optical or other electromagnetic system used to route switch or transmit communication;</p> <p>“communication service” means a service that consists in the provision of access to and of facilities for making use of, any communication network, whether or not it is one provided by the person providing the service;</p> <p>“computer data” means any representation of–</p> <ul style="list-style-type: none"> a) facts; b) concepts; c) machine-readable code or instructions; or d) information, including text, audio, image or video, that is in a form suitable for processing in a computer system and is capable of being sent, received or stored; <p>“computer programme” means computer data which represents instructions or statements that, when executed in a computer system, can cause the computer system to perform a function;</p> <p>“computer system” means a device or group of interconnected or related devices, which follows a computer programme or external instruction to perform automatic processing of computer data, including a desktop computer, a laptop computer, a netbook computer, a tablet computer, a video game console, a smart phone, a personal digital assistant, or a smart television;</p> <p>“damage” means any impairment to the integrity or availability of data, a program, a computer system, communication network or information;</p> <p>“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 system;</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>"Minister" means the Minister with responsibility for national security;</p> <p>"person" includes a natural or legal person, an educational or financial institution or any legal or other entity;</p> <p>"security measure" means password, access code, encryption code or biometric information in the form of computer data and includes any means of limiting access to authorised persons or to secure recognition prior to granting access to communication data, a communication network, a computer system or computer data;</p> <p>"service provider" means–</p> <ul style="list-style-type: none"> a) any public or private entity that provides to users of its service the ability to communicate by means of a computer system; or b) any public or private entity that processes or stores computer data on behalf of a communication service or users of the service; <p>"subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services and by which can be established–</p> <ul style="list-style-type: none"> a) the type of communication service used, the technical provisions taken and the period of service; b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information available on the basis of the service agreement or arrangement; or c) any other information on the site of the installation of communication equipment available on the basis of the service agreement or arrangement; <p>"Storage Direction" means any Order of a court compelling a service provider to store and make available to a stipulated party a person's stored traffic data and subscriber information; and</p> <p>"traffic data" means any communication data–</p> <ul style="list-style-type: none"> (a) identifying, or purporting to identify, any person, apparatus or location to or from which the communication that is, may be or may have been transmitted, and "data" in relation to a postal article, means anything written on the outside of the postal article;

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>(b) identifying or selecting, or purporting to identify or select, apparatus through or by means of which the communication is or may be transmitted;</p> <p>(c) comprising signals for the actuation of–</p> <ul style="list-style-type: none"> (i) apparatus used for the purpose of a communication network for effecting, in whole or in part, the transmission of any communication; or (ii) any communication network in which that apparatus is comprised; <p>(d) identifying the data or other data as data comprised in or attached to a particular communication; or</p> <p>(e) identifying a computer file or a computer programme, access to which is obtained or which is run by means of the communication, to the extent only that the file or the programme is identified by reference to the apparatus in which it is stored, and a reference to traffic data being attached to a communication includes a reference to the data and the communication being logically associated with each other. (c) shows the communication's origin, destination, route, time, date, size, duration or the type of underlying services.</p>
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
<p>Article 2 – Illegal access</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.</p>	<p>Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto (Cybercrime Act, 2020)</p> <p>Section 3 – Illegal Access to a Computer System</p> <p>(1) A person commits an offence who, intentionally accesses a computer system or any part of a computer system of another person –</p> <ul style="list-style-type: none"> (a) without authorisation or in excess of authorisation; or (b) by infringing any security measure of the computer system. <p>(2) A person commits an offence who intentionally and without lawful excuse or justification continues to exceed the authorised access to the computer system of another person.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>(3) A person who commits an offence under this section is liable on–</p> <ul style="list-style-type: none"> (a) summary conviction to a fine of three thousand dollars and to a term of imprisonment for three years; (b) conviction on indictment to a fine of five thousand dollars and to a term of imprisonment for five years <p>Section 4. - Illegal access to computer data</p> <p>(1) A person commits an offence who, without authorisation accesses the computer system of another person with the intention to duplicate or modify the data–</p> <ul style="list-style-type: none"> (a) without authorisation or in excess of authorisation; or (b) by infringing a security measure. <p>(2) A person who commits an offence under subsection (1), is liable on–</p> <ul style="list-style-type: none"> (a) conviction to a fine of five thousand dollars and to a term of imprisonment for three years; or (b) conviction on indictment to a fine of ten thousand dollars and to a term of imprisonment for five years.
<p>Article 3 – Illegal interception</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.</p>	<p><u>Interception of Communications Act</u> Chapter 229:01 (revised edition 2011)</p> <p>Section 3. – Prohibition of interception</p> <p>(1) Except as provided in this section, any person who with intent intercepts communication in the course of its transmission by means of a public postal service or a communication network without authorisation, commits an offence and, on conviction on indictment, is liable to,</p> <ul style="list-style-type: none"> (a) a fine of not less than twenty five thousand dollars and not exceeding fifty thousand dollars or to a term of imprisonment not exceeding three years in the first instance; (b) a fine of not less than fifty thousand dollars and not exceeding one hundred thousand dollars or to a term of imprisonment not exceeding five years in the second instance; and (c) a fine of one hundred thousand dollars and a term of imprisonment not exceeding five years in the subsequent instances. <p>(2) A person who with intent intercepts a communication in the course of its transmission by means of a public postal service or a communication network for the purpose of commercial benefit, political advantage, or criminal activity commits an offence and, on conviction on indictment, is liable to,</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<ul style="list-style-type: none"> (a) a fine of not less than fifty thousand dollars and not exceeding one hundred thousand dollars or to a term of imprisonment not exceeding five years in the first instance; (b) a fine of not less than one hundred thousand dollars and not exceeding two hundred thousand dollars or to a term of imprisonment not exceeding ten years in the second instance; and (c) a fine of two hundred thousand dollars and a term of imprisonment not exceeding ten years in the subsequent instances. <p>(3) A person does not commit an offence under subsection (1) if,</p> <ul style="list-style-type: none"> (a) the communication is intercepted in accordance with an interception direction issued pursuant to section 6 of this Act or an entry warrant issued pursuant to section 9 of this Act; (b) that person has written or otherwise documented authorisation consenting to the interception from the person to whom or from whom the communication is transmitted; (c) the communication is acquired in accordance with the provisions of the Belize Telecommunications Limited Act, the Financial Intelligence Unit Act or any other law; or (d) the interception is of a communication made through a communication network that is so configured as to render the communication readily accessible to the general public. <p>(4) A court convicting a person of an offence under this Act may, in addition to any penalty which it imposes in respect of the offence, order the forfeiture or disposal of any device used in the of this Act, commission of the offence as provided by section 26 (3) to (9) of this Act.</p> <p>(5) For the purposes of this section, communication,</p> <ul style="list-style-type: none"> (a) communication in the course of transmission by means of a communication network in real time; or, (b) communication stored in a manner that enables the recipient to receive that communication or otherwise have access to it.

<p>Article 4 – Data interference</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.</p> <p>2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.</p>	<p>Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto (Cybercrime Act, 2020)</p> <p>Section 5 – Illegal Data interference</p> <p>(1) A person commits an offence if the person intentionally and without lawful excuse or justification–</p> <ul style="list-style-type: none"> (a) damages the computer data of another person; (b) obstructs, interrupts or interferes with another person’s lawful use of computer data; or (c) denies access to computer data to another person who is authorised to access the computer data. <p>(2) A person who commits an offence under subsection (1), is liable on–</p> <ul style="list-style-type: none"> (a) summary conviction to a fine of eight thousand dollars and to a term of imprisonment for three years; or (b) conviction on indictment to a fine of twelve thousand dollars and to a term of imprisonment for five years.
<p>Article 5 – System interference</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data</p>	<p>Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto (Cybercrime Act, 2020)</p> <p>Section 6 – Illegal System interference</p> <p>(1) A person commits an offence who, intentionally and without lawful excuse or justification, seriously hinders or interferes with the functioning of the computer system of another person by inputting, transmitting, damaging, modifying or suppressing computer data.</p> <p>(2) A person who commits an offence under sub-section (1), is liable- on–</p> <ul style="list-style-type: none"> (a) summary conviction to a fine of ten thousand dollars and to a term of imprisonment for three years; or (b) conviction on indictment to a fine of fifteen thousand dollars and to a term of imprisonment for five years. <p>(3) For the purposes of this section “seriously hinders” includes–</p> <ul style="list-style-type: none"> (a) disconnecting the electricity supply to the computer system; (b) causing electromagnetic interference to the computer system; or (c) corrupting the computer system.
<p>Article 6 – Misuse of devices</p>	<p>Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of</p>

<p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:</p> <p>a the production, sale, procurement for use, import, distribution or otherwise making available of:</p> <p>i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;</p> <p>ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and</p> <p>b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.</p> <p>2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.</p> <p>3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.</p>	<p>the offences of cybercrime; and to provide for matters connected therewith or incidental thereto (Cybercrime Act, 2020)</p> <p>Section 7 – Illegal devices and codes</p> <p>(1) A person commits an offence if the person intentionally and without lawful excuse or justification, possesses, procures for use, produces, sells, imports, exports, distributes, discloses or otherwise makes available</p> <p>(a) a device or a computer programme, that is designed or adapted; or</p> <p>(b) a computer password, access code, encryption 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, for the purpose of committing an offence under this Act or any other law.</p> <p>(2) A person who commits an offence under subsection (1) is liable</p> <p>(a) on summary conviction to a fine of three thousand dollars and to imprisonment for three years; or</p> <p>(b) on conviction on indictment to a fine of eight thousand dollars and to imprisonment for five years.</p>
<p align="center">Title 2 – Computer-related offences</p>	
<p>Article 7 – Computer-related forgery</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of 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 whether or not the data is directly readable and intelligible. A Party</p>	<p>Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto (Cybercrime Act, 2020)</p> <p>Section 8 – Computer-related forgery</p> <p>A person who inputs, alters, deletes or suppresses computer data, resulting in inauthentic data, with the intent that it be considered or acted upon by another</p>

<p>may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.</p>	<p>person as if it were authentic, regardless of whether or not the data is directly readable and intelligible, commits an offence and is liable</p> <ul style="list-style-type: none"> (a) on summary conviction to a fine of three thousand dollars and to imprisonment for three years; or (b) on conviction on indictment to a fine of five thousand dollars and to imprisonment for five years.
<p>Article 8 – Computer-related fraud</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:</p> <ul style="list-style-type: none"> a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, <p>with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.</p>	<p>Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto (Cybercrime Act, 2020)</p> <p>Section 9 – Identity related offences</p> <p>(1) A person commits an offence who, with the intent to defraud or deceive another person for the purpose of procuring an economic benefit for the person or another–</p> <ul style="list-style-type: none"> (a) inputs, alters, deletes or suppresses computer data; or (b) interferes with the functioning of a computer system. <p>(2) A person who commits an offence under sub-section (1), is liable on–</p> <ul style="list-style-type: none"> (a) summary conviction to a fine of five thousand dollars and to a term of imprisonment for five years; or (b) conviction on indictment to a fine of ten thousand dollars and to a term of imprisonment for ten years. <p>Section 10. - Identity related theft</p> <p>(1) A person commits an offence who, with the intent to assume the identity of another person, uses a computer system or computer data to–</p> <ul style="list-style-type: none"> (a) obtain, transfer, possess or use a means of identification of another person; or (b) make use of the security measures of another person. <p>(2) A person who commits an offence under subsection (1), is liable on–</p> <ul style="list-style-type: none"> (a) summary conviction to a fine of five thousand dollars and to a term of imprisonment for five years; or (b) conviction on indictment to a fine of ten thousand dollars and to a term of imprisonment for ten years.
<p>Title 3 – Content-related offences</p>	
<p>Article 9 – Offences related to child pornography</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:</p>	<p>Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto (Cybercrime Act, 2020)</p>

<p>a producing child pornography for the purpose of its distribution through a computer system;</p> <p>b offering or making available child pornography through a computer system;</p> <p>c distributing or transmitting child pornography through a computer system;</p> <p>d procuring child pornography through a computer system for oneself or for another person;</p> <p>e possessing child pornography in a computer system or on a computer-data storage medium.</p> <p>2 For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:</p> <p>a a minor engaged in sexually explicit conduct;</p> <p>b a person appearing to be a minor engaged in sexually explicit conduct;</p> <p>c realistic images representing a minor engaged in sexually explicit conduct</p> <p>3 For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.</p> <p>4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.</p>	<p>Section 11 – Child luring</p> <p>(1) A person commits an offence who, uses a computer system to communicate with a child with the intent to –</p> <p>(a) induce the child to engage in a sexual conversation or sexual activity with the child; or</p> <p>(b) encourage the child to produce child pornography; or</p> <p>(c) arrange a meeting with a child for the purpose of abusing or engaging in sexual activity with the child, or producing child pornography, whether or not the person takes any steps to effect the meeting.)</p> <p>(2) A person who commits an offence under subsection (1), is liable on–</p> <p>(a) summary conviction to a fine of ten thousand dollars and to a term of imprisonment for five years; or</p> <p>(b) conviction on indictment to a fine of fifteen thousand dollars and to a term of imprisonment for ten years.</p> <p><u>The Commercial Sexual Exploitation of Children (Prohibition) Act</u></p> <p>Section 7 – Offence of producing child pornography</p> <p>(1) A person who finances, produces, reproduces, publishes or makes any written material, photographic material, video, film, electronic publication, virtual or other media of any form of child pornography commits an offence and is liable on conviction on indictment to imprisonment for a term of ten years.</p> <p>(2) A person who coerces, induces, encourages, pays for, or exchanges any material benefit for, or otherwise causes any child to pose for any photographic material or to participate in any pornography video or film or audio, visual or other electronic representation of any child involved in any form of child pornography commits an offence and is liable on conviction on indictment to imprisonment for a term of ten years.</p> <p>(3) A person who imports, exports, distributes, finances, offers, trades, sells or possesses whether for personal use or for distribution or sale via printed media or electronic media including video, compact disks, digital video disks, phone messaging, computer image, internet, virtual media or by any other means any form of child pornography commits an offence and is liable on conviction on indictment to imprisonment for a term of twelve years.</p> <p>(4) It is not a defence to a charge under this section that the accused believed that a person shown in the representation that is alleged to constitute child pornography was or was depicted as being eighteen years of age or more, nor shall it be a defence that the person depicted in the visual representation is eighteen years or older if the person was shown to represent a child at the time of making the said pornographic representation.</p>
<p align="center">Title 4 – Offences related to infringements of copyright and related rights</p>	

<p>Article 10 – Offences related to infringements of copyright and related rights</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.</p> <p>3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.</p>	<p>Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto (Cybercrime Act, 2020)</p> <p>Section 16. - Infringement of Copyright, patents and designs and trademarks</p> <p>(1) A person commits an offence who, uses a computer system to infringe on the rights of–</p> <ul style="list-style-type: none"> (a) a copyright owner; (b) a proprietor of a patent; (c) a proprietor of a registered design; or (d) a proprietor of a registered trademark. <p>(2) A person who commits an offence under sub-section (1), is liable on summary conviction to a fine of three thousand dollars and to a term of imprisonment for three years.</p> <p>See also the Copyright Act Chapter 252 (2000)</p>
Title 5 – Ancillary liability and sanctions	

<p>Article 11 – Attempt and aiding or abetting</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.</p> <p>3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.</p>	<p>Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto (Cybercrime Act, 2020)</p> <p>Section 17. - Attempt, aiding or abetting</p> <p>A person who intentionally–</p> <ul style="list-style-type: none"> (a) advises, incites, attempts, aids, abets, counsels, procures or facilitates the commission of any offence under this Act; or (b) conspires with another person to commit an offence under this Act, commits an offence and shall be punished for the offence as if he had committed the offence as a principal offender.
<p>Article 12 – Corporate liability</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:</p> <ul style="list-style-type: none"> a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. <p>2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.</p> <p>3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.</p> <p>4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.</p>	<p>Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto (Cybercrime Act, 2020)</p> <p>Section 42. - Corporate liability</p> <p>(1) Where a body corporate commits an offence under this Act, the body corporate is liable to the fine applicable in respect of the offence.</p> <p>(2) Where a body corporate commits an offence under this Act and the Court is satisfied that a director, manager, secretary, or other similar officer, of that body corporate–</p> <ul style="list-style-type: none"> (a) consented or connived in the commission of the offence; or (b) failed to exercise due diligence to prevent the commission of the offence, that director, manager, secretary, or other similar officer commits an offence. <p>(3) A person who commits an offence under sub-section (2) is liable on–</p> <ul style="list-style-type: none"> (a) summary conviction to a fine of ten thousand dollars and to imprisonment for three years; and (b) on conviction on indictment to a fine of twenty thousand dollars and to imprisonment for five years.
<p>Article 13 – Sanctions and measures</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.</p>	<p>The Cybercrime Act establishes sanctions under each substantive offence.</p> <p>Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto (Cybercrime Act, 2020)</p>

<p>2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.</p>	<p>Section 41. – Use of computer system to commit offence under other law Where an offence, under any other law, is committed through the use of a computer system, the offender is liable on conviction to a fine of four times the penalty stated in the other law.</p>
<p>Section 2 – Procedural law</p>	
<p>Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:</p> <ul style="list-style-type: none"> a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. <p>3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.</p> <p>b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:</p> <ul style="list-style-type: none"> i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, <p>that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21</p>	<p>Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto (Cybercrime Act, 2020)</p> <p>Section 35. - Evidence In any criminal proceedings under this Act or any other law–</p> <ul style="list-style-type: none"> (a) any computer data or traffic data, generated, retrieved or reproduced from a computer system, and whether in electronic or printed form; or (b) any computer acquired in respect of any offence, shall be admissible as evidence.

Article 15 – Conditions and safeguards

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

The protection of human rights and safeguards are contained in the Constitution of Belize. These are the following:

Section 3 Fundamental rights and freedoms

Whereas every person in Belize is entitled to the fundamental rights and freedoms of the individual, that is to say, the right, whatever his race, place of origin, political opinions, colour, creed or sex, but subject to respect for the rights and freedoms of others and for the public interest, to each and all of the following, namely-

(a) life, liberty, security of the person, and the protection of the law;

Protection of family life, privacy, privacy of the home and other property:

Section 3

(c) protection for his family life, his personal privacy, the privacy of his home and other property and recognition of his human dignity;

Section 5 Protection of right to personal liberty

(1) A person shall not be deprived of his personal liberty save as may be authorised by law in any of the following cases, that is to say:

(a) in consequence of his unfitness to plead to a criminal charge or in execution of the sentence or order of a court, whether established for Belize or some other country, in respect of a criminal offence of which he has been convicted;

(b) in execution of the order of the Supreme Court or the Court of Appeal punishing him for contempt of the Supreme Court or the Court of Appeal or of another court or tribunal;

(c) in execution of the order of a court made to secure the fulfilment of any obligation imposed on him by law;

(d) for the purpose of bringing him before a court in execution of the order of a court;

(e) upon a reasonable suspicion of his having committed, or being about to commit, a criminal offence under any law;

(f) under the order of a court or with the consent of his parent or guardian, for his education or welfare during any period ending not later than the date when he attains the age of eighteen years;

(g) for the purpose of preventing the spread of an infectious or contagious disease;

	<p>(h) in the case of a person who is, or is reasonably suspected to be, of unsound mind, addicted to drugs or alcohol, or a vagrant, for the purpose of his care or treatment or the protection of the community;</p> <p>(i) for the purpose of preventing his unlawful entry into Belize, or for the purpose of effecting his expulsion, extradition or other lawful removal from Belize or for the purpose of restraining him while he is being conveyed through Belize in the course of his extradition or removal as a convicted prisoner from one country to another; or</p> <p>(j) to such extent as may be necessary in the execution of a lawful order requiring him to remain within a specified area within Belize, or prohibiting him from being within such an area, or to such extent as may be reasonably justifiable for the taking of proceedings against him with a view to the making of any such order or relating to such an order after it has been made, or to such extent as may be reasonably justifiable for restraining him during any visit that he is permitted to make to any part of Belize in which, in consequence of any such order, his presence would otherwise be unlawful.</p> <p>(2) Any person who is arrested or detained shall be entitled-</p> <p>(a) to be informed promptly, and in any case no later than forty- eight hours after such arrest or detention, in a language he un- derstands, of the reasons for his arrest or detention;</p> <p>(b) to communicate without delay and in private with a legal prac- titioner of his choice and, in the case of a minor, with his par- ents or guardian, and to have adequate opportunity to give instructions to a legal practitioner of his choice;</p> <p>(c) to be informed immediately upon his arrest of his rights under paragraph (b) of this subsection; and</p> <p>(d) to the remedy by way of habeas corpus for determining the validity of his detention.</p> <p>(3) Any person who is arrested or detained-</p> <p>(a) for the purpose of bringing him before a court in execution of the order of a court; or</p>
--	---

	<p>(b) upon reasonable suspicion of his having committed, or being about to commit, a criminal offence under any law, and who is not released, shall be brought before a court without undue delay and in any case not later than seventy-two hours after such arrest or detention.</p> <p>(4) Where any person is brought before a court in execution of the order of a court in any proceedings or upon suspicion of his having committed or being about to commit an offence, he shall not be thereafter further held in custody in connection with those proceedings or that offence save upon the order of a court.</p> <p>(5) If any person arrested or detained as mentioned in subsection (3)(b) of this section is not tried within a reasonable time, then without prejudice to any further proceedings that may be brought against him, he shall, unless he is released, be entitled to bail on reasonable conditions.</p> <p>(6) Any person who is unlawfully arrested or detained by any other person shall be entitled to compensation therefor from that other person or from any other person or authority on whose behalf that other person was acting:</p> <p>Provided that no person shall be liable for any act done in the performance of a judicial function for which he would not be liable apart from this subsection.</p> <p>(7) For the purposes of subsection (1)(a) of this section a person charged before a court with a criminal offence in respect of whom a special verdict has been returned that he was guilty of the act or omission charged but was insane when he did the act or made the omission shall be regarded as a person who has been convicted of a criminal offence and the detention of a person in consequence of such a verdict shall be regarded as detention in execution of the order of a court.</p> <p>Section 6 Protection of Law</p> <p>(2) If any person is charged with a criminal offence, then, unless the charge is withdrawn, the case shall be afforded a fair hearing within a reasonable time by an independent and impartial court established by law.</p> <p>(3) Every person who is charged with a criminal offence-</p> <p>(a) shall be presumed to be innocent until he is proved or has pleaded guilty;</p> <p>(b) shall be informed as soon as reasonably practicable, in a language that he understands, of the nature and particulars of the offence charged;</p>
--	---

	<p>(c) shall be given adequate time and facilities for the preparation of his defence;</p> <p>(d) shall be permitted to defend himself before the court in person or, at his own expense, by a legal practitioner of his own choice;</p> <p>(e) shall be afforded facilities to examine in person or by his legal representative the witnesses called by the prosecution before the court, and to obtain the attendance and carry out the examination of witnesses to testify on his behalf before the court on the same conditions as those applying to witnesses called by the prosecution; and</p> <p>(f) shall be permitted to have without payment the assistance of an interpreter if he cannot understand the language used at the trial,</p> <p>and except with his own consent the trial shall not take place in his absence unless he so conducts himself as to render the continuance of the proceedings in his presence impracticable and the court has ordered him to be removed and the trial to proceed in his absence:</p> <p>Provided that the trial may take place in his absence in any case in which it is so provided by a law under which he is entitled to adequate notice of the charge and the date, time and place of the trial and to a reasonable opportunity of appearing before the court.</p> <p>(4) A person shall not be held to be guilty of a criminal offence on account of any act or omission that did not, at the time it took place, constitute such an offence, and no penalty shall be imposed for any criminal offence that is severer in degree or description than the maximum penalty that might have been imposed for that offence at the time when it was committed.</p> <p>(5) A person who shows that he has been tried by a competent court for a criminal offence and either convicted or acquitted shall not again be tried for that offence or for any other criminal offence of which he could have been convicted at the trial for that offence, save upon the order of a superior court in the course of appeal or review proceedings relating to the conviction or acquittal.</p> <p>(6) A person who is tried for a criminal offence shall not be compelled to give evidence at the trial.</p> <p>Section 12 Protection of freedom of expression:</p> <p>(I) Except with his own consent, a person shall not be hindered in the enjoyment of his freedom of expression, including freedom to hold opinions without</p>
--	--

	<p>interference, freedom to receive ideas and information without interference, freedom to communicate ideas and information without interference (whether the communication be to the public generally or to any person or class of persons) and freedom from interference with his correspondence.</p> <p>(2) Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes reasonable provision-</p> <p>(a) that is required in the interests of defence, public safety, public order, public morality or public health;</p> <p>(b) that is required for the purpose of protecting the reputations, rights and freedoms of other persons or the private lives of persons concerned in legal proceedings, preventing the disclosure of information received in confidence, maintaining the authority and independence of the courts or regulating the administration or the technical operation of telephone, telegraphy, posts, wireless broadcasting, television or other means of communication, public exhibitions or public entertainments;</p> <p>or</p> <p>(c) that imposes restrictions on officers in the public service that are required for the proper performance of their functions.</p> <p>Section 14 Protection of right to privacy</p> <p>(1) A person shall not be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. The private and family life, the home and the personal correspondence of every person shall be respected.</p> <p>(2) Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision of the kind specified in subsection (2) of section 9 of this Constitution.</p>
<p>Article 16 – Expedited preservation of stored computer data</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.</p>	<p>Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto (Cybercrime Act, 2020)</p> <p>Section 27. - Expedited Preservation Order</p> <p>(1) A Judge, if satisfied on an ex-parte application by the Director of Public Prosecution, or a police officer of the rank of Superintendent or above that there</p>

<p>2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>are reasonable grounds to believe that computer data or traffic data that is reasonably required for the purpose of a criminal investigation, under this Act or any other law, is vulnerable to loss or modification, may make an order requiring a person in possession or control of computer data or traffic data to preserve and maintain the integrity of the computer data or traffic data for a period not exceeding ninety days.</p> <p>(2) A Judge, on an ex-parte application by the Director of Public Prosecution or a police officer of the rank of Superintendent or above, may order an extension of the period referred to in subsection (1) by a further specified period of ninety days or more but not exceeding one year on a special case by case basis.</p> <p>Section 30. - Offence to disclose confidential information</p> <p>(1) A person who is the subject of an Order under this Act shall not disclose to any other person–</p> <ul style="list-style-type: none"> (a) the fact that an Order was made; (b) the details of the Order; (c) anything done pursuant to the Order; or (d) any compute or traffic data, subscriber information or other information collected or recorded pursuant to the Order under this Act. <p>(2) Sub-section (1) shall not apply to any actions between a service provider and any other person permitted under any law, or performed for the benefit of investigating or prosecuting an alleged offender.</p> <p>(3) A person who without lawful excuse or justification, fails to comply with the requirements under sub-section (1), commits an offence and is liable on summary conviction to a fine of five thousand dollars and to a term of imprisonment for three years.</p>
<p>Article 17 – Expedited preservation and partial disclosure of traffic data</p> <p>1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:</p> <ul style="list-style-type: none"> a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 	<p>Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto (Cybercrime Act, 2020)</p> <p>Section 19 - Ex-parte, application for Storage Direction</p> <p>(1) The Director of Public Prosecutions or Head of Prosecution Branch may in the prescribed form, make an <i>ex parte</i> application for a Storage Direction.</p> <p>(2) An application under sub-section (1), shall–</p> <ul style="list-style-type: none"> (a) be accompanied by an affidavit in support and attested to by the investigating police officer declaring the following– <ul style="list-style-type: none"> (i) the name of the investigating police officer; (ii) the facts or allegations giving rise to the application, including the alleged offence;

<p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<ul style="list-style-type: none"> (iii) sufficient information for the Court to make a determination on whether to grant or refuse the application; (iv) the ground on which the application is made; (v) full particulars of all facts and circumstances alleged, including– <ul style="list-style-type: none"> (aa) where practical, a description of the nature and location of the facilities or computer from, or the premises at, which the traffic data and subscriber information are to be intercepted; and (bb) the basis for believing that evidence relating to the ground on which the application is made will be obtained during the life/period of the Storage Direction; (vi) where applicable– <ul style="list-style-type: none"> (aa) whether other investigative procedures were applied and whether they failed to produce the required evidence; (bb) the reason why any other investigative procedures may be unlikely to succeed if applied, or are likely to be too dangerous to apply in order to obtain the required evidence; (vii) the requested duration of the Storage Direction; (viii) whether any previous application was made for a Storage Direction in respect of the person, facility or premises, and the status of that other application; (ix) where applicable, a description of the computer system to be targeted; and (x) any other relevant directives issued by a Court in relation to the matter. <p>(3) Where a serious offence is being, has been or is likely to be committed for the benefit of, or at the direction of, or in association with, a person, a group of persons or syndicate involved in organised crime or groups classified as criminal gangs, an application for a Storage Direction, shall not require the grounds under section 22(1)(a).</p> <p>(4) Where a Storage Direction is based on the ground of national security, the application shall be accompanied by written authorisation by Minister.</p> <p>(5) Records relating to an application for a Storage Direction, renewal or modification of a Storage Direction, shall immediately upon the determination of the matter, be–</p> <ul style="list-style-type: none"> (a) sealed by the Court; and (b) kept in the custody of the Court, in a place that is not accessible to the public, or in any other place as the Court determines fit. <p>(6) The records under sub-section (5) may be unsealed upon an order by the Court for the following purpose only–</p>
--	--

	<p>(a) on an application for a further Storage Direction, in relation to the same matter; or</p> <p>(b) for a renewal of a Storage Direction.</p> <p>Section 20. - Scope and form of Storage Direction</p> <p>(1) A Storage Direction shall direct the named service provider to–</p> <p>(a) keep stored, at any place in Belize accurate records of–</p> <p>(i) the traffic data and subscriber information of any person, facility or premises;</p> <p>(ii) any computer system; or</p> <p>(iii) any communication in the course of its transmission;</p> <p>(b) store the traffic data for the period of time as stated in the Storage Direction; and</p> <p>(c) submit the stored traffic data and subscriber information to a named police officer.</p> <p>(2) A Storage Direction shall specify–</p> <p>(a) the manner in which the data is to be stored and submitted to the police officer; and</p> <p>(b) any other conditions or restrictions that relate to the traffic data.</p> <p>(3) A Storage Direction may contain any ancillary provisions as may be necessary to secure its implementation in accordance with the provisions of this Act.</p> <p>Section 22. - Application for a Storage Direction or Search and Seizure Warrant</p> <p>(1) A Court shall issue a Storage Direction or a Search and Seizure Warrant, where it is satisfied that the facts deponed there is reasonable grounds to believe that–</p> <p>(a) obtaining the information sought is necessary in the interest of–</p> <p>(i) national security;</p> <p>(ii) public order;</p> <p>(iii) public safety;</p> <p>(iv) public health;</p> <p>(v) preventing, detecting, investigating or prosecuting an offence under this Act or any other law; or</p> <p>(vi) giving effect to the provisions of any mutual legal assistance request or in circumstances appearing to the Court to be equivalent to those in which he would issue a Storage Direction under sub-paragraph (v); and</p> <p>(b) other procedures–</p> <p>(i) have not been or are unlikely to be successful in obtaining the information sought;</p> <p>(ii) are too dangerous to adopt in the circumstances; or</p> <p>(iii) are impractical having regard to the urgency of the case; or</p>
--	--

	<p>(c) it would be in the best interest of the administration of justice to issue the Storage Direction.</p> <p>(2) In considering an application under sub-section (1), the Court may require the applicant to furnish the Court with any further information as it deems necessary.</p>
<p>Article 18 – Production order</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:</p> <p>a a person in its territory to submit specified computer data in that person’s possession or control, which is stored in a computer system or a computer-data storage medium; and</p> <p>b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider’s possession or control.</p> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p> <p>3 For the purpose of this article, the term “subscriber information” means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:</p> <p>a the type of communication service used, the technical provisions taken thereto and the period of service;</p> <p>b the subscriber’s identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;</p> <p>c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.</p>	<p>Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto (Cybercrime Act, 2020)</p> <p>Section 26. - Production Order</p> <p>(1) The Director of Public Prosecutions or Head Prosecution Branch may, in the prescribed form, make an ex-parte application to the Court for a Production Order.</p> <p>(2) An application under sub-section (1), shall be accompanied by an affidavit in support and attested to by the investigating police officer declaring the following–</p> <p>(a) the name of the investigating police officer;</p> <p>(b) the facts or allegations giving rise to the application, including the alleged offence;</p> <p>(c) full particulars of all facts and circumstances alleged by the applicant, including–</p> <p>(i) where practical, a description of the nature and location of the facilities or computer from, or the premises at, which the application relates; and</p> <p>(ii) the basis for believing that evidence relating to the ground on which the application is made will be obtained if the Production Order is granted;</p> <p>(d) where applicable–</p> <p>(i) whether other investigative procedures were applied and whether they failed to produce the required evidence; or</p> <p>(ii) the reason why any other investigative procedures may be unlikely to succeed if applied, or are likely to be too dangerous to apply in order to obtain the required evidence;</p> <p>(iii) the requested duration of the Order;</p> <p>(iv) whether any previous application was made for a Production Order in respect of the same person, facility or premises, and the status of that other application; and</p> <p>(v) any other relevant directives issued by a Court in relation to the matter.</p> <p>(3) A Court shall issue a Production Order, where it is satisfied that computer data or traffic data, a printout or other information is reasonably required for the</p>

	<p>purpose of a criminal investigation or criminal proceedings under this Act or any other law.</p> <p>(4) A Production Order may direct–</p> <ul style="list-style-type: none"> (a) a person in Belize who is in possession or control of a computer system or computer data storage medium, to produce, from the computer system or computer data storage medium, specified computer data or a printout or other intelligible output of the computer data; or (b) a service provider in Belize to produce traffic data relating to information transmitted from a subscriber through a computer system or from other relevant persons, or subscriber information about a person who uses the service, and give it to a specified person within a specified period.
<p>Article 19 – Search and seizure of stored computer data</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:</p> <ul style="list-style-type: none"> a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. <p>2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:</p> <ul style="list-style-type: none"> a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 	<p>Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto (Cybercrime Act, 2020)</p> <p>Section 21. - Ex-Parte application for Search and Seizure Warrant</p> <p>(1) The Director of Public Prosecutions or Head Prosecution Branch may in the prescribed form, make an ex-parte application for Search and Seizure Warrant.</p> <p>(2) An application under sub-section (1), shall–</p> <ul style="list-style-type: none"> (a) be accompanied by an affidavit in support and attested to by the investigating police officer declaring the following– <ul style="list-style-type: none"> (i) the name of the investigating police officer; (ii) that there is reasonable grounds for suspecting that– <ul style="list-style-type: none"> (aa) an offence under this Act or any other law has been or is about to be committed, in a specified place; and (bb) evidence that the offence has been or is about to be committed, is in the specified place; (iii) the facts or allegations giving rise to the application, including the alleged offence; (iv) sufficient information for the Court to make a determination on whether to grant or refuse the application; (v) the ground on which the application is made; (vi) full particulars of all facts and circumstances alleged, including– <ul style="list-style-type: none"> (aa) where practical, a description of the nature and location of the facilities or computer from, or

<p>4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.</p> <p>5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>the premises at, which the traffic data and subscriber information are to be intercepted; and</p> <p>(bb) the basis for believing that evidence relating to the ground on which the application is made will be obtained during the duration of the Search and Seizure Warrant;</p> <p>(vii) where applicable–</p> <p>(aa) whether other investigative procedures were applied and whether they failed to produce the required evidence; or</p> <p>(bb) the reason why any other investigative procedures may be unlikely to succeed if applied, or are likely to be too dangerous to apply in order to obtain the required evidence;</p> <p>(viii) The requested duration of the Search and Seizure Warrant;</p> <p>(ix) whether any previous application was made for a Search and Seizure Warrant in respect of the person, facility or premises, and the status of that other application;</p> <p>(x) where applicable, a description of the computer system to be targeted; and</p> <p>(xi) any other relevant directives issued by a Court in relation to the matter.</p> <p>(3) A Search and Seizure Warrant shall specify the place, or evidence to which it relates and authorise a police officer, with any assistance as the police officer deems necessary, to–</p> <p>(a) enter and search any place; or</p> <p>(b) to access, seize and secure any evidence, including any computer system or computer data.</p> <p>(4) A police officer who executes a Search and Seizure Warrant under this section shall, secure the computer system or data and maintain the integrity of the data seized.</p> <p>(5) In addition to any powers of a Search and Seizure Warrant under this section, a police officer when executing a Search and Seizure Warrant, has the following additional powers including–</p> <p>(a) to activate an onsite computer system;</p> <p>(b) inspect and check the operation of a computer system or computer data;</p> <p>(c) to make and retain a copy of computer data;</p> <p>(d) to remove computer data from a computer system or render the computer system inaccessible;</p> <p>(e) to take a printout of computer data; or</p>
---	---

	<p>(f) to impound or similarly secure a computer system or any part of the system.</p> <p>(6) Any evidence seized under a Search and Seizure Warrant, including any computer system or data shall be valid for a period of ninety days and may, on an application to a Judge in Chambers, be extended for a further period of not more than one year.</p> <p>(7) Upon the expiration of the period stated under sub-section (6), or when the evidence seized is no longer required, the evidence shall immediately be returned to the person to whom the Search and Seizure Warrant was addressed.</p> <p>(8) Where a serious offence is being, has been or is likely to be committed for the benefit of, or at the direction of, or in association with, a person, a group of persons or syndicate involved in organised crime or groups classified as criminal gangs, an application for a search and seizure warrant, shall not require the grounds under section 22(1)(a).</p> <p>(9) Where a Search and Seizure Warrant is based on the ground of national security, the application shall be accompanied by written authorisation by Minister.</p> <p>Section 22. - Application for a Storage Direction or Search and Seizure Warrant</p> <p>(1) A Court shall issue a Storage Direction or a Search and Seizure Warrant, where it is satisfied that the facts deponed there is reasonable grounds to believe that—</p> <ul style="list-style-type: none"> (a) obtaining the information sought is necessary in the interest of— <ul style="list-style-type: none"> (i) national security; (ii) public order; (iii) public safety; (iv) public health; (v) preventing, detecting, investigating or prosecuting an offence under this Act or any other law; or (vi) giving effect to the provisions of any mutual legal assistance request or in circumstances appearing to the Court to be equivalent to those in which he would issue a Storage Direction under sub-paragraph (v); and (b) other procedures— <ul style="list-style-type: none"> (i) have not been or are unlikely to be successful in obtaining the information sought; (ii) are too dangerous to adopt in the circumstances; or (iii) are impractical having regard to the urgency of the case; or (c) it would be in the best interest of the administration of justice to issue the Storage Direction. <p>(2) In considering an application under sub-section (1), the Court may require the applicant to furnish the Court with any further information as it deems necessary.</p>
--	--

	<p>Section 25. - Assistance</p> <p>(1) A person with knowledge about the functioning of a computer system or computer data storage medium, or security measures applied to protect computer data, that is the subject of a Search and Seizure Warrant shall, if requested, assist the police officer who is executing the search, by–</p> <ul style="list-style-type: none"> (a) providing any information, about the computer system, computer data or storage medium sought, that may facilitate the execution of the Search and Seizure Warrant; (b) accessing and using the computer system or computer data storage medium to search computer data which is stored in, or lawfully accessible from or available to, that computer system or computer data storage medium; (c) obtaining and copying computer data; or (d) obtaining an intelligible output from a computer system or computer data storage medium in such a format that is admissible for the purpose of legal proceedings. <p>(2) A person who fails, without lawful excuse or justification, to comply with the requirements under sub-section (1), commits an offence and is liable on summary conviction to a fine of three thousand dollars and to a term of imprisonment for one year.</p>
<p>Article 20 – Real-time collection of traffic data</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:</p> <ul style="list-style-type: none"> a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: <ul style="list-style-type: none"> i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. <p>2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.</p>	<p>Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto (Cybercrime Act, 2020)</p> <p>Section 30. - Offence to disclose confidential information</p> <p>(1) A person who is the subject of an Order under this Act shall not disclose to any other person–</p> <ul style="list-style-type: none"> (a) the fact that an Order was made; (b) the details of the Order; (c) anything done pursuant to the Order; or (d) any compute or traffic data, subscriber information or other information collected or recorded pursuant to the Order under this Act. <p>(2) Sub-section (1) shall not apply to any actions between a service provider and any other person permitted under any law, or performed for the benefit of investigating or prosecuting an alleged offender.</p> <p>(3) A person who without lawful excuse or justification, fails to comply with the requirements under sub-section (1), commits an offence and is liable on summary conviction to a fine of five thousand dollars and to a term of imprisonment for three years.</p>

<p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	
<p>Article 21 – Interception of content data</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:</p> <p>a collect or record through the application of technical means on the territory of that Party, and</p> <p>b compel a service provider, within its existing technical capability:</p> <p> i to collect or record through the application of technical means on the territory of that Party, or</p> <p> ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.</p> <p>2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p><u>Interception of Communication Act, 2002</u> CAP. 229:01 Revised edition 2011</p> <p>Section 5. Application for interception direction, etc.</p> <p>(1) An authorised officer who wishes to obtain an interception direction pursuant to the provisions of this Act shall request the Director of Public Prosecutions to make an application ex parte to a Judge in chambers on his behalf.</p> <p>(2) An application referred to in subsection (1) of this section shall be in the prescribed form and shall be accompanied by an affidavit deposing the following,</p> <p>(a) the name of the authorised officer on behalf of whom the application is made;</p> <p>(b) the facts or allegations giving rise to the application;</p> <p>(c) sufficient information for a Judge to issue an interception direction;</p> <p>(d) the ground referred to in section 6 (1) of this Act on which the application is made;</p> <p>(e) full particulars of all the facts and the circumstances alleged by the authorised officer on whose behalf the application is made including,</p> <p> (i) if practical, a description of the nature and location of the facilities from which or the premises at which the communication is to be intercepted; and</p> <p> (ii) the basis for believing that evidence relating to the ground on which the application is made will be obtained through the interception;</p> <p>(f) if applicable, whether other investigative procedures have been applied and failed to produce the required evidence or the reason why other investigative procedures reasonably appear to be unlikely to succeed if applied, or are likely to be too dangerous to apply in order to obtain the required evidence;</p> <p>(g) the period for which the interception direction is required to be issued;</p> <p>(h) whether any previous application has been made for the issuing of an interception direction in respect of the same person, the same facility or</p>

	<p>the same premises specified in the application and, if such previous application exists, shall indicate the current status of that application; and</p> <p>(i) if applicable, a description of the communication equipment to be intercepted;</p> <p>(j) any other directives issued by the Judge.</p> <p>(3) Subsection (2)(d) of this section, shall not apply in respect of an application for the issuing of an interception direction on a ground referred to in section 6(1) (a) of this Act, if a serious offence has been or is being or will probably be committed for the benefit of, or at the direction of, or in association with, a person, a group of persons or syndicate involved in organised crime or groups classified as criminal gangs.</p> <p>(4) Where an interception direction is applied for on the grounds of national security, the application from the authorised officer shall be accompanied by a written authorisation signed by the Minister authorising the application on that ground.</p> <p>(5) Subject to subsection (6) of this section, the records relating to an application for an interception direction or the renewal or modification thereof shall be,</p> <p>(a) placed in a packet and sealed by the Judge to whom the application is made immediately on determination of the application; and</p> <p>(b) kept in the custody of the court in a place to which the public has no access or such place as the Judge may authorise.</p> <p>(6) The records referred to in subsection (5) of this section may be opened if a Judge so orders only,</p> <p>(a) for the purpose of dealing with an application for further authorisation; or</p> <p>(b) for renewal of an authorisation.</p> <p>Section 6. Issuance of interception direction</p> <p>(1) An interception direction shall be issued if a Judge is satisfied, on the facts alleged in the application pursuant to section 5 of this Act, that there are reasonable grounds to believe that,</p> <p>(a) obtaining the information sought under the interception direction is necessary in the interests of,</p> <p>(i) national security;</p> <p>(ii) public order;</p> <p>(iii) public safety; or</p> <p>(iv) public health;</p> <p>(v) preventing, detecting, investigating, or prosecuting any offence specified in the Issuance of interception direction.</p>
--	--

	<p>Schedule, where there are reasonable grounds to believe that such an offence has been, is being or may be committed; or</p> <p>(vi) giving effect to the provisions of any mutual legal assistance agreement in circumstances appearing to the Judge to be equivalent to those in which he would issue an interception direction by virtue of subparagraph</p> <p>(v); and</p> <p>(b) other procedures,</p> <p>(i) have not been or are unlikely to be successful in obtaining the information sought to be acquired by means of the interception direction;</p> <p>(ii) are too dangerous to adopt in the circumstances; or</p> <p>(iii) having regard to the urgency of the case are impracticable; and</p> <p>(c) it would be in the best interests of the administration of justice to issue the interception direction.</p> <p>(2) A Judge considering an application may require the authorised officer to furnish such further information as he deems necessary.</p> <p>Section 7. Scope and form of interception direction</p> <p>(1) An interception direction shall be in the prescribed form and shall permit the authorised officer to,</p> <p>(a) intercept, at any place in Belize, any communication in the course of its transmission;</p> <p>(b) secure the interception in the course of its transmission by means of a postal service or a public or private communication network, of such communication as are described in the interception direction; and</p> <p>(c) secure the disclosure of the intercepted material obtained or required by the interception direction, and of related communication data.</p> <p>(2) An interception direction shall authorise the interception of,</p> <p>(a) communication transmitted by means of a postal service or a public and private communication network to or from,</p> <p>(i) the person specified in the interception direction;</p> <p>(ii) the premises so specified and described; or</p> <p>(iii) the set of communication equipment so specified and described; and</p> <p>(b) such other communication, if any as may be necessary in order to intercept communication falling within paragraph (a).</p> <p>(3) An interception direction shall specify the identity of the,</p>
--	--

	<p>(a) authorised officer on whose behalf the application is made pursuant to section 5 of this Act, and the person who will execute the interception direction;</p> <p>(b) person, if known and appropriate, whose communication is to be intercepted; and</p> <p>(c) postal service provider or the communication provider to whom the interception direction to intercept must be addressed, if applicable.</p> <p>(4) An interception direction may contain such ancillary provisions as are necessary to secure its implementation in accordance with the provisions of this Act. (5) An interception direction issued pursuant to this section may specify conditions or restrictions relating to the interception of communications authorised therein.</p> <p>Section 8. Duration and renewal of interception</p> <p>(1) An interception direction shall cease to have effect at the end of the relevant period, but may be renewed at any time before the end of that period, on an application made pursuant to subsection (2) of this section.</p> <p>(2) A Judge may renew the interception direction before the expiration of the relevant period, upon an application for the renewal of an interception direction being made by the Director of Public Prosecutions on behalf of an authorised officer, if satisfied that the renewal of the interception direction is justified.</p> <p>(3) An application for the renewal of an interception direction under subsection (2) of this section shall be in the prescribed form and shall be accompanied by an affidavit deposing to the circumstances relied on as justifying the renewal of the interception direction.</p> <p>(4) If at any time before the end of the periods referred to in subsections (1) and (2) of this section, it appears to the authorised officer to whom the interception direction is issued, or a person acting on his behalf, that an interception direction is no longer necessary, he shall make an application to the Court for the cancellation of the interception direction and the court may cancel the interception direction.</p> <p>(5) For the purposes of this section “relevant period” means a period of up to six months as specified by the Judge beginning with the date of the issuance of the interception direction or, in the case of an interception direction that has been renewed, the date of its latest renewal.</p>
--	--

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

- a in its territory; or
- b on board a ship flying the flag of that Party; or
- c on board an aircraft registered under the laws of that Party; or
- d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto ([Cybercrime Act, 2020](#))

Section 43. – Jurisdiction

A Court in Belize shall have jurisdiction in respect of an offence under this Act where the act constituting the offence is carried out–

- (a) wholly or in substantial part within its territory;
- (b) against the status of persons, or interests in things, present within its territory;
- € outside its territory but has or is intended to have substantial effect within its territory;
- (d) against the activities, interests, status, or relations of its nationals outside as well as within its territory; and
- € outside its territory by persons not its nationals that is directed against the security of the state or against a limited class of other state interests.

Chapter III – International co-operation

Article 24 – Extradition

1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

B Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No.

Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto ([Cybercrime Act, 2020](#))

Section 39. - Extradition

The offences described in this Act shall be deemed to be extraditable offences and the Extradition Act shall apply.

<p>24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.</p> <p>2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.</p> <p>3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.</p> <p>4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.</p> <p>5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.</p> <p>6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.</p> <p>7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.</p> <p>B The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure</p>	<p>The rules on extradition of criminals are contained in the Extradition Act (Chapter 112). Belize has entered into bilateral agreements on extradition with United States, Guatemala and Mexico.</p>
<p>Article 25 – General principles relating to mutual assistance</p>	<p>Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of</p>

<p>1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.</p> <p>2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.</p> <p>3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.</p> <p>4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.</p> <p>5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.</p>	<p>the offences of cybercrime; and to provide for matters connected therewith or incidental thereto (Cybercrime Act, 2020)</p> <p>Section 37. - Mutual Legal Assistance For the purposes of international cooperation, the Mutual Legal Assistance Act shall apply.</p> <p>Belize is not part of the Inter-American Convention on Mutual Assistance in Criminal Matters.</p> <p>Belize has entered into bilateral agreements on mutual legal assistance on criminal matters with:</p> <ul style="list-style-type: none"> (1) The United States, which operates under the Mutual Legal Assistance in Criminal Matters Act (Revised on 2011); and (2) Caribbean Treaty on Mutual Legal Assistance in Serious Crimes Matters Act Chapter 17:05
<p>Article 26 – Spontaneous information</p> <p>1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this</p>	<p>Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto (Cybercrime Act, 2020)</p> <p>Section 38. - Spontaneous information (1) The Central Authority may, concerning the possible commission of any offence under this Act, and without prior request, forward to foreign government or</p>

<p>Convention or might lead to a request for co-operation by that Party under this chapter.</p> <p>2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.</p>	<p>international agency information obtained within the framework of an investigation when it considers that the disclosure of the information might assist the foreign government or international agency in initiating or carrying out investigations or proceedings concerning criminal offences under its own law or applicable laws or might lead to a request for mutual legal assistance under this Act.</p> <p>(2) The Central Authority may request that the information provided under sub-section (1) be kept confidential or only used subject to conditions.</p> <p>(3) Where the information provided cannot kept confidential, the Central Authority may determine if the spontaneous information should be shared.</p>
<p>Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements</p> <p>1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.</p> <p>2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.</p> <p>b The central authorities shall communicate directly with each other;</p> <p>c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;</p> <p>d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.</p> <p>3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.</p> <p>4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:</p> <p>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or</p> <p>b it considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.</p>	<p>This article is covered by the Mutual Legal Assistance and International Cooperation Act of 2014.</p>

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

<p>Article 28 – Confidentiality and limitation on use</p> <p>1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.</p> <p>2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:</p> <ul style="list-style-type: none"> a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. <p>3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.</p> <p>4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.</p>	
<p>Article 29 – Expedited preservation of stored computer data</p> <p>1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.</p> <p>2 A request for preservation made under paragraph 1 shall specify:</p> <ul style="list-style-type: none"> a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 	

<p>3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.</p> <p>4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.</p> <p>5 In addition, a request for preservation may only be refused if:</p> <ul style="list-style-type: none"> a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests. <p>6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.</p> <p>4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.</p>	
<p>Article 30 – Expedited disclosure of preserved traffic data</p> <p>1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.</p>	

<p>2 Disclosure of traffic data under paragraph 1 may only be withheld if:</p> <p>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or</p> <p>b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.</p>	
<p>Article 31 – Mutual assistance regarding accessing of stored computer data</p> <p>1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.</p> <p>2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.</p> <p>3 The request shall be responded to on an expedited basis where:</p> <p>a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or</p> <p>b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.</p>	
<p>Article 32 – Trans-border access to stored computer data with consent or where publicly available</p> <p>A Party may, without the authorisation of another Party:</p> <p>a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or</p> <p>b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.</p>	<p>Law no. 32 of 2020 - AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto (Cybercrime Act, 2020)</p> <p>Section 40. - Transborder access to computer data with consent or when unsecured and publicly available</p> <p>It shall not be an offence under this Act for any foreign government or any person to, without the authorisation of the Government of Belize or any person–</p> <p>(a) access open source stored computer data, regardless of where the data is located, if the computer data is not subjected to security measures; or</p> <p>(b) access or receive stored computer data located in Belize, if the foreign government or person obtains the consent of the person who has the authority to disclose the data through that computer system.</p>
<p>Article 33 – Mutual assistance in the real-time collection of traffic data</p>	

<p>1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.</p> <p>2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.</p>	
<p>Article 34 – Mutual assistance regarding the interception of content data</p> <p>The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.</p>	
<p>Article 35 – 24/7 Network</p> <p>1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:</p> <ul style="list-style-type: none"> a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. <p>2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.</p> <p>b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.</p> <p>3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.</p>	

Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	