Saint Lucia

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Version 16 March 2022

Table of contents

[reference to the provisions of the Budapest Convention]

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.

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

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

BUDAPEST CONVENTION	**DOMESTIC LEGISLATION**
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: 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; 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*;* c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; 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	**Computer Misuse Act (2011)** "computer" means a device that accepts information, in the form of digitalized data, and manipulates the information for some result based on a program or sequence of instructions on how the data is to be processed; "computer service" includes data processing and the storage or retrieval of data; "computer system" means a device or combination of devices, including input and output devices, except calculators which are not programmable, and capable of being used in conjunction with external files which contain computer programs, electronic instructions, input data and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions; "data" means— (a) information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose; and (b) representations of facts, information and concepts held in any removable storage medium; "record" means information that is inscribed, stored or otherwise fixed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form; "electronic record" means a record created, generated, sent, communicated, received or stored by electronic means and which can be read or perceived by a person or a computer system or other similar device; "service provider" means any person who provides an information and communication service, including telecommunication service; "information and communication service" means any service involving the use of information and communication technologies and telecommunication; "traffic data" means any data relating to a communication by means of a computer system and generated by the system that form part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	“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, other than traffic or other data, by which can be established— (a) the type of the communication service used, the technical provisions taken to use the communication service, and the period of the service; (b) the subscriber’s identity, postal or geographical address, telephone and other access number, billing and payment information, available on the basis of a service agreement or arrangement; or (c) any other information on the site of installation of a communication equipment available on the basis of a service agreement or arrangement; “subscriber” means a person using the services of a service provider; “access” in relation to any computer system, means instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the computer system; “damage” means, except for the purposes of section 31, any impairment to a computer system or the integrity or availability of data, a program or system, or information in a computer, that— (a) causes loss aggregating at least $10,000 in value, or such other amount as the Minister may, by Order published in the Gazette, prescribe except that any loss incurred or accrued more than one year after the date of the offence in question shall not be taken into account; (b) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment or care of a person; (c) causes or threatens physical injury or death to a person; or (d) threatens the public interest, public health or public safety; “electronic” in relation to technology, means technology- having electrical, digital, magnetic, wireless, optical, electromagnetic, biometric, photonic or similar capabilities; “function” includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system; “intercept” in relation to a function of a computer system, includes listening to, or recording a function of a computer system, or acquiring the substance, its meaning or purport of such a function; “telecommunication” means a transmission, emission or reception of signs, signals, writing, images, sounds or intelligence of any nature by wire, radio, optical or other electro-magnetic systems whether or not the signs, signals, writing, images, sounds or intelligence have been subjected to rearrangement, computation or other processes by any means in the course of the transmission, emission or reception;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Criminal Code (2004) **Chapter 2. Offences, Part 2. Offences against property, Sub-Part B. Forgery** **Section 267 (Computer Fraud)** (3) In this section— "computer" means any device for storing and processing information; "computer network" means the interconnection of 2 or more computers, whether geographically separated or in close proximity, or the interconnection of communication systems with a computer through terminals whether remote or local; "modification of the contents of a computer" includes the alteration of a programme or data held in a computer or any addition to the contents of a computer of a programme or data. **Interception of Communications Act (2005)** **Part V. Communication data** **Section 24 (Disclosure of communications data)** (1) For the purposes of this section — "designated person" means the Minister or person designated for the purposes of this section by the Minister by Order published in the Gazette; "traffic data" in relation to a communication, means any communication data — (a) identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted, and "data" in relation to a postal article, means anything written on the outside of the postal article; (b) identifying or selecting, or purporting to identify or select, apparatus through or by means of which the communication is or may be transmitted; (c) comprising signals for the actuation of — (i) apparatus used for the purposes of a telecommunications network for effecting, in whole or in part, the transmission of any communications; or (ii) any telecommunications network in which that apparatus is comprised; (d) identifying the data or other data as data comprised in or attached to a particular communication; or (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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	apparatus in which it is stored, and references to traffic data being attached to a communication include references to the data and the communication being logically associated with each other.
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	
Article 2 – Illegal access 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.	**Computer Misuse Act (2011)** **Section 5 (Unauthorized access to computer data)** (1) Subject to section 13 and subsections (3) and (4), a person shall not knowingly and without lawful authority, cause a computer system to perform any function for the purpose of securing access to any program or data held in that computer system or in any other computer system. (2) A person who contravenes subsection (1), commits an offence and is liable, on summary conviction— (a) in case of a first offence— (i) subject to subparagraph (ii), to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 3 months or to both, and (ii) where the computer system is damaged, impaired, or where data contained in the computer system is suppressed or modified, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 months, or to both; (b) in the case of a second or subsequent offence— (i) subject to subparagraph (ii), to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 6 months or to both, and (ii) where the computer system is damaged impaired, or where data contained in the computer system is suppressed or modified, to a fine not exceeding $50,000 or to imprisonment for a term not exceeding one year, or to both. (3) A person shall not be liable under subsection (1) if that person— (a) is the person with a right to control the operation or use of the computer system and exercises such right in good faith; (b) has the express or implied consent of the person empowered to authorize him or her to have such an access; (c) has reasonable grounds to believe that he or she had such consent as specified in paragraph (b);

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(d) is acting pursuant to measures that can be taken under Part 3; or (e) is acting in reliance of any statutory power arising under any enactment for the purpose of obtaining information, or of taking possession of, any document or other property. (4) An access by a person to a computer system is unauthorized if the person— (a) is not entitled or allowed to control access of the kind in question; and (b) does not have consent to the kind of access in question from any person who is entitled to give the consent. (5) For the purposes of this section, it is immaterial that the unauthorized access is not directed at— (a) any particular program or data; (b) a program or data of any kind; or (c) a program or data held in any particular computer system. **Section 6 (Access with intent to commit or facilitate commission of offence)** (1) A person shall not cause a computer system to perform any function for the purpose of securing access to any program or data held in a computer system, or in any other computer system with intent to commit an offence— (a) involving property, fraud, dishonesty or which causes bodily harm; and (b) which is punishable with imprisonment. (2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding one year. (3) For the purposes of this section, it is immaterial that the— (a) access referred to in subsection (1) is authorized or unauthorized; and (b) offence to which this section applies is committed at the same time when the access is secured or at any other time.
Article 3 – Illegal interception 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.	**Computer Misuse Act (2011)** **Section 7 (Unauthorized access to and interception of computer service)** (1) Subject to section 13 and subsection (4), a person shall not, by any means, knowingly— (a) secure access, without authority, to a computer system for the purpose of obtaining, directly or indirectly, any computer service; (b) intercept or cause to be intercepted, directly or indirectly, without authority, any function of, or any data within, a computer system; or (c) communicate directly or indirectly a number, code, password or other means of access to a computer system to any person other than a person

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	to whom he or she is duly authorized to communicate. (2) A person who contravenes subsection (1), commits an offence and is liable, on summary conviction— (a) in case of a first offence— (i) subject to subparagraph (ii), to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 months or to both, and (ii) where the computer system is damaged, impaired, or where data contained in the computer system is suppressed or modified, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 6 months; (b) in the case of a second or subsequent offence— (i) subject to subparagraph (ii), to a fine not exceeding $25,000 or to imprisonment for a term not exceeding one year or to both, and (ii) where the computer system is damaged impaired, or where data contained in the computer system is suppressed or modified, to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 18 months. (3) For the purpose of this section, it is immaterial that the unauthorized access or interception is not directed at— (a) any particular program or data; (b) a program or data of any kind; or (c) a program or data held in any particular computer system. (4) A person is not liable under subsection (1) if that person— (a) has the express or implied consent of both the person who sent the data and the intended recipient of that data; (b) is acting in reliance of any statutory power. **Interception of Communications Act (2005)** **Part II. Interception of Communications** **Section 3 (Prohibition of interception)** (1) Except as provided in this section, a person who intentionally intercepts a communication in the course of its transmission by means of a public postal service or a telecommunications network commits an offence, and on conviction on indictment, is liable to a fine not exceeding twenty thousand dollars or a term of imprisonment not exceeding four years, or to both.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 4 – Data interference 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. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Computer Misuse Act (2011)** **Section 8 (Unauthorized modification of computer material)** (1) Subject to section 13 and subsections (3) and (4), a person shall not do any act which he or she knows will cause an unauthorized modification of data held in a computer system for the purpose of— (a) impairing the operation of the computer system; (b) preventing or hindering access to any program or data held in any computer system; (c) impairing the operation of such program or reliability of the data; or (d) enhancing the operation of a computer system in order to secure unauthorized access to information in another computer system. (2) A person who contravenes subsection (1), commits an offence and is liable, on summary conviction— (a) in case of a first offence— (i) subject to subparagraph (ii), to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 months or to both, and (ii) where the computer system or access to any program or data held in a computer or the operation of any program or the reliability of data is suppressed, modified or otherwise impaired, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 6 months; (b) in the case of a second or subsequent offence— (i) subject to subparagraph (ii), to a fine not exceeding $25,000 or to imprisonment for a term not exceeding one year or to both, and (ii) where the computer system or access to any program or data held in a computer or the operation of any program or the reliability of data is suppressed, modified or otherwise impaired, to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 18 months. (3) A person is not liable under this section if that person is acting— (a) pursuant to measures that can be taken under Part 3; or (b) in reliance of any other statutory power. (4) For the purposes of this section, a modification is unauthorized if the person— (a) whose act causes it, is not the person entitled to determine whether the modification should be made; and (b) does not have the consent to cause or make the modification from a person who is entitled to give the consent.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Criminal Code (2004) **Chapter 2. Offences, Part 2. Offences against property, Sub-Part B. Forgery** **Section 267 (Computer Fraud)** (2) A modification of the contents of a computer is unauthorised— (a) if the person who causes it is not himself or herself entitled to determine whether the modification should be made; and (b) if the person does not have the consent of the person who is entitled to grant consent for the modification.
Article 5 – System interference 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	**Computer Misuse Act (2011)** **Section 9 (Damaging, and denying access to computer system)** (1) Subject to section 13, a person shall not, knowingly and without lawful authority, do any act which causes, directly or indirectly— (a) a degradation, failure, interruption or interference or obstruction of the operation of a computer system; (b) a denial of access to, or impairment of any program or data stored in, the computer system; (c) the data to be meaningless, useless or ineffective; (d) an obstruction, interruption, or interference with any person in the lawful use of data; or (e) the destruction or alteration of data. (2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 18 months or both and in the case of a subsequent conviction, to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 3 years or both. (3) Subsection (1) applies whether the person's act has a temporary or permanent effect.
Article 6 – Misuse of devices 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: a the production, sale, procurement for use, import, distribution or otherwise making available of: 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;	**Computer Misuse Act (2011)** **Section 10 (Unauthorized disclosure of password)** (1) Subject to section 13, a person shall not, knowingly and without lawful authority, disclose a password, access code, or any other means of gaining access to a program or data held in a computer system— (a) for any wrongful gain; (b) for any unlawful purpose; or (c) knowing that it is likely to cause prejudice to another person. (2) A person who contravenes subsection (1) commits an offence and is liable on

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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. 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. 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.	summary conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 months or both and in the case of a subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 6 months or both. **Section 11 (Unlawful possession of devices and data)** (1) A person shall not— (a) knowingly manufacture, or produce, sell, procure for use, import, distribute or otherwise make available, a computer system or any other device, designed or adapted primarily for the purpose of committing an offence under sections 5 to 10; (b) knowingly receive, or be in possession of, without sufficient excuse or justification, one or more of the devices referred to in paragraph (a); (c) have in his or her possession any data or program with the intention that the data or program is to be used by that person or another person, to commit or facilitate the commission of an offence under this Act. (2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding $200,000 or to imprisonment for a term not exceeding 5 years or both and in the case of a subsequent conviction, to a fine not exceeding $400,000 or to imprisonment for a term not exceeding 10 years or both. (3) For the purposes of subsection (1)(c), possession of any data or program includes having— (a) possession of a computer system or data storage device that holds or contains the data or program; (b) possession of a document in which the data or program is recorded; or (c) control of any data or program that is in the possession of another person.
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery 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	**Criminal Code (2004)** **Chapter 2. Offences, Part 2. Offences against property, Sub-Part B. Forgery** Section 267 (Computer fraud) 1. A person who, with intent to defraud or deceive - (a) alters, damages, destroys or otherwise manipulates data or programmes held in or used in connection with a computer or computer

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	network by adding to, erasing or otherwise altering the data or programme; or (b) does any act which causes an unauthorised modification of the contents of a computer or computer network; commits an offence and is liable on conviction on indictment to imprisonment for fifteen years. 2. A modification of the contents of a computer is unauthorised – (a) if the person who causes it is not himself or herself entitled to determine whether the modification should be made; and (b) if the person does not have the consent of the person who is entitled to grant consent for the modification. 3. In this section – "computer" means any device for storing and processing information; "computer network" means the interconnection of two or more computers, whether geographically separated or in close proximity, or the interconnection of communication systems with a computer through terminals whether remote or local; "modification of the contents of a computer" includes the alteration of a programme or data held in a computer or any addition to the contents of a computer of a programme or data.
Article 8 – Computer-related fraud 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: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**Computer Misuse Act (2011)** **Section 12 (Electronic fraud)** (1) Subject to section 13, a person shall not cause loss of property to another person by any— (a) input, alteration, deletion or suppression of data; or (b) interference with the functioning of a computer system; with intent to procure for himself or herself or another person, an advantage. (2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 18 months or both and in the case of a subsequent conviction, to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 3 years or both. **Section 13 (Offences involving protected computer systems)** (1) A person who is convicted of an offence under section 5, 7, 8, 9, 10 or 12, in the circumstances referred to in subsection (2) shall, in lieu of the punishment

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	prescribed in the section, be liable, on conviction, to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 3 years. (2) The punishment referred to in subsection (1) applies if the person who committed the offence knew, or ought reasonably to have known, at the material time, that the computer system, program or data is used directly in connection with, or is necessary for— (a) the security, defence or international relations of Saint Lucia; (b) the existence or identity of a confidential source of information relating to the enforcement of the criminal law; (c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or (d) the protection of public safety, including systems related to essential emergency services such as the police, civil defence and medical services. (3) For the purposes of any prosecution under this section, it is presumed that, until the contrary is proved, the accused has the requisite knowledge referred to in subsection (2) if there is, in respect of the computer system, program or data, an electronic or other warning stating that unauthorized access to that computer system, program, or data attracts the penalty under subsection (1). **Criminal Code (2004)** **Chapter 2. Offences, Part 2. Offences against property, Sub-Part B. Forgery** **Section 267 (Computer Fraud)** (1) A person who, with intent to defraud or deceive— (a) alters, damages, destroys or otherwise manipulates data or programmes held in or used in connection with a computer or computer network by adding to, erasing or otherwise altering the data or programme; or (b) does any act which causes an unauthorised modification of the contents of a computer or computer network; commits an offence and is liable on conviction on indictment to imprisonment for 15 years.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography	**Computer Misuse Act (2011)** **Section 14 (Indecent photographs of children)**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 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. 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.	(1) A person shall not, through a computer system— (a) take or permit to be taken or make, any indecent photograph or pseudo-photograph of a child; (b) distribute or show the indecent photograph or pseudo-photograph of a child; (c) have in his or her possession an indecent photograph or pseudo-photograph of a child, with a view to such photograph being distributed or shown by himself or herself or any other person; or (d) publish or cause to be published any advertisement likely to be understood as conveying that the advertiser distributes or shows such indecent photographs or pseudo-photographs, or intends to do so. (2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 18 months or both and in the case of a subsequent conviction, to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 3 years or both. (3) It is a defence to a charge under subsection (1) if the person establishes that the indecent photograph or pseudo-photograph is for a bona fide research, medical or law enforcement purpose. (4) Where the— (a) impression conveyed by the pseudo-photograph is that the person shown is a child; or (b) predominant impression conveyed is that the person shown is a child, not withstanding that some of the physical characteristics shown are those of an adult; the pseudo-photograph, is treated for the purposes of this Act as showing a child. (5) The Court before which a person is convicted of an offence under this section may, in addition to any penalty imposed, order— (a) the forfeiture of any apparatus, article or thing which is the subject matter of the offence or is used in connection with the commission of the offence; and (b) that the material subject matter of the offence be no longer stored on and made available through the computer system, or that the material be deleted. **Section 15 (Malicious communications)** (1) A person shall not use a computer to send a message, letter, electronic communication or article of any description that— (a) is indecent or obscene; (b) constitutes a threat; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(c) is menacing in character, with the intention to cause or being reckless as to whether he or she causes annoyance, inconvenience, distress or anxiety to the recipient or to any other person to whom he or she intends it or its contents to be communicated. (2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 months or both and in the case of a subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 6 months or both.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 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. 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. 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.	**Copyright (Amendment) Act (2015)** **Part 5. Infringements** **Section 32 (Infringement)** (1) The copyright in a protected work is infringed by any person who, not being the owner of the copyright and without the licence of the owner thereof— (a) in respect of the work, does, or authorises another unauthorised person to do, any of the acts mentioned in section 8, in relation to that work; (b) imports an article (otherwise than for his or her private and domestic use) into Saint Lucia which he or she knows or has reason to believe, is an infringing copy of the work; (c) in Saint Lucia, or on any ship or aircraft registered in Saint Lucia— (i) possesses in the course of business, (ii) sells, lets for hire, or by way of trade offers or exposes for sale or hire, or (iii) by way of trade exhibits in public, an article which he or she knows or has reason to believe, is an infringing copy of the work. (2) Subsection (1)(c) shall apply, in relation to the distribution of any article either— (a) for the purposes of trade; or (b) for other purposes, but only to such an extent as to affect prejudicially the owner of the copyright, as it applies in relation to the sale of an article.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) Copyright in a work is infringed by a person who, without the licence of the copyright owner— (a) makes; (b) imports into Saint Lucia; (c) possesses in the course of a business; or (d) sells or lets for hire or offers for sale or hire, an article specifically designed or adapted for making copies of that work, knowing or having reason to believe that it is to be used to make infringing copies. (4) Copyright in a work is infringed by a person who, without the licence of the copyright owner, transmits the work by means of a telecommunications system (otherwise than by broadcasting or inclusion in a cable programme service) knowing or having reason to believe that infringing copies of the work will be made by means of the reception of the transmission in Saint Lucia or elsewhere.
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 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. 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. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	
Article 12 – Corporate liability 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:	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	
Article 13 – Sanctions and measures 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. 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.	**Computer Misuse Act (2011)** **Section 23 (Order for compensation)** (1) A Court before which a person is convicted of an offence under this Act may make an order against that person for the payment by that person of a sum of money fixed by the Court by way of compensation to any person for any damage caused to his or her computer system, program or data by the offence in respect of which the sentence is passed. (2) A claim by a person for damages sustained by reason of the offence is deemed to have been satisfied to the extent of any amount which has been paid to him or her under an order for compensation, except that the order does not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order. (3) An order for compensation under this section is recoverable as a civil debt. (4) For the purposes of this section, a program or data held in a computer is deemed to be the property of the owner of the computer. **Section 24 (Forfeiture)** The Court before which a person is convicted of an offence under this Act may, in addition to any other penalty imposed, order the forfeiture of any apparatus, article or thing which is the subject matter of the offence or is used in connection with the commission of the offence.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Section 2 – Procedural law	
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: 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. 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. 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: 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, 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	
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
Article 16 – Expedited preservation of stored computer data 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. 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. 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.	**Computer Misuse Act (2011)** **Section 16 (Preservation order)** (1) Where a police officer or an authorized person has reasonable grounds to believe that data stored or processed by means of a computer system or other information communication technologies is vulnerable to loss or modification and where such data is required for the purposes of a criminal investigation or the prosecution of an offence, the Director of Public Prosecutions may apply ex parte to a Judge in Chambers on behalf of the police officer or authorized person for an order for the expeditious preservation of the data. (2) For the purposes of subsection (1), "data" includes traffic data and subscriber information. (3) An order made under subsection (1) remains in force— (a) until such time as may reasonably be required for the investigation of the offence; (b) where prosecution is instituted, until the final determination of the case; or (c) until such time as the Judge in Chambers determines or considers necessary.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 17 – Expedited preservation and partial disclosure of traffic data 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: 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. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Computer Misuse Act (2011)** **Section 17 (Disclosure of preserved data)** An authorized person may, for the purposes of a criminal investigation or the prosecution of an offence, apply ex parte to a Judge in Chambers for an order for the disclosure of— (a) any data subject to a preservation order under section 16, irrespective of whether one or more service providers were involved in the transmission of that data; (b) sufficient data referred to in paragraph (a) to identify the service providers and the path through which the data was transmitted; (c) the password enabling access to the data referred to in paragraph (a); or (d) the public key enabling the interpretation of data referred to in paragraph (a) that is in an asymmetric cryptosystem.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: 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 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. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 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: a the type of communication service used, the technical provisions taken thereto and the period of service;	**Computer Misuse Act (2011)** **Section 18 (Production order)** (1) Where the disclosure of data is required for the purposes of a criminal investigation or the prosecution of an offence, a police officer or an authorized person may ex parte apply to the Judge in Chambers for an order compelling any— (a) person to submit specified data in that person's possession or control, which is stored in a computer system; and (b) service provider offering its services to submit subscriber information in relation to such services in that service provider's possession or control. (2) Where any material to which an investigation relates consists of data stored in a computer system, disc, cassette, or on microfilm, or preserved by any mechanical or electronic device, the request is deemed to require the person to produce or give access to the material in a form in which the material can be taken away and in which the material is visible and legible. **Interception of Communications Act (2005)** **Part V. Communication data**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	**Section 24 (Disclosure of communications data)** (2) Where it appears to the designated person that a telecommunications provider is or may be in possession of, or capable of obtaining, any communications data, the designated person may, by notice in writing, require the telecommunications provider — (a) to disclose to an authorised officer all of the data in his or her possession or subsequently obtained by him or her, or (b) if the telecommunications provider is not already in possession of the data, to obtain the data and to disclose the data to an authorised officer. (3) A designated person shall not issue a notice under subsection (2) in relation to any communications data unless he or she is satisfied that it is necessary to obtain the data and to disclose the data to an authorised officer so disclose it. (4) A designated person shall not issue a notice under subsection (2) in relation to any communication data unless he or she is satisfied that it is necessary to obtain that data — (a) in the interests of national security; (b) for the purpose of preventing or detecting an offence specified in the Schedule where there are reasonable grounds to believe that such an offence is being or may be committed. (c) in the interests of public order; (d) in the interests of public morality; (e) in the interest of public health; (f) for the purpose in an emergency, of preventing death, injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or (4) A notice pursuant to this section shall state — (a) the communication data in relation to which it applies; (b) the authorised officer to whom the disclosure is to be made; (c) the manner in which the disclosure is to be made; (d) the matters falling within subsection (3) by reference to which the reference is issued; and (e) the date on which it is issued. (5) A notice pursuant to this section shall not require — (a) any communications data to be obtained after the end of the period of one month beginning on the date on which the notice is issued; or (b) the disclosure, after the end of such period, of any communications data not in the possession of the provider of the telecommunications service, or required to be obtained by him or her, during that period. (6) The provisions of sections 21 and 22 shall apply, with necessary modifications, in relation to the disclosure of data pursuant to a notice under to this section.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(7) Subject to subsection (8), a provider of a telecommunications service, to whom a notice is issued under this section, shall not disclose to any person the existence or operation of the notice, or any information from which such existence or operation could reasonably be inferred. (8) The disclosure referred to in subsection (7) may be made to— (a) an officer or agent of the service provider for the purpose of ensuring that the notice is complied with; or (b) an attorney-at-law for the purpose of obtaining legal advice or representation in relation to the notice; and a person referred to in paragraph (a) or (b) shall not disclose the existence or operation of the notice, except to the authorised officer specified in the notice for the purpose of — (i) ensuring that the notice is complied with, or obtaining legal advice or representation in relation to the notice, in the case of an officer or agent of the service provider; or (ii) giving legal advice or making representations in relation to the notice, in the case of an attorney-at-law. (9) A person shall not disclose any communications data obtained under this Act, except — (a) as permitted by the notice; (b) in connection with the performance of his or her duties; or (c) where if the Minister directs that the disclosure be made to a foreign Government or agency of a foreign Government where there exists between Saint Lucia and that foreign Government an agreement for the mutual exchange of that kind of information and the Minister considers it to be in the public interest that such disclosure be made. (10) A person who contravenes subsection (7), (8) or (9) of this section commits an offence and is liable, on summary conviction, to a fine not exceeding five thousand dollars or to a term of imprisonment for a term not exceeding one year or to both.
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: 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.	**Computer Misuse Act (2011)** **Section 19 (Powers of access, search and seizure for the purposes of investigation**) (1) Where a police officer or an authorized person has reasonable grounds to believe that stored data would be relevant for the purposes of an investigation or the prosecution of an offence, he or she may apply ex parte to a Judge in Chambers for the issue of a warrant to enter any premises to access, search and seize that data.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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: 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. 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. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	(2) The powers of the police officer or an authorized person under this section include the power to— (a) access, inspect, and check the operation of any computer system; (b) use or cause to be used any computer system to search any data contained in or available to the computer system; (c) access any information, code or technology which has the capability of transforming or unscrambling encrypted data contained or available to such computer system into readable and comprehensible format or text for the purpose of investigating any offence under this Act or any other offence which is disclosed in the course of the lawful exercise of the powers under this section; (d) require— (i) the person by whom or on whose behalf the police officer or authorized person has reasonable cause to suspect any computer system to which this section applies, (ii) any person having charge of or otherwise interfere with the operation of that computer system, to provide him or her with such reasonable technical, or other assistance as he or she may require for the purpose of paragraph (a); (e) require any person in possession of decryption information to grant him or her access to such decryption information necessary to decrypt data required for the purpose of investigating the offence; (f) seize or secure a computer system or any information and communication technologies medium; (g) make and retain a copy of data or information; (h) maintain the integrity of the relevant stored data or information; or (i) render inaccessible or remove the stored data or information from the computer system, or any information and communication technologies medium. (3) Where there are reasonable grounds to believe that a computer system or other device, would be relevant for the purposes of an investigation or the prosecution of an offence under this Act, a police officer or an authorized person may apply ex parte to a Judge in Chambers for the issue of a warrant to enter any premises to access, search and seize that computer system or other device. (4) Any computer system or other device seized under a warrant issued under subsection (3) may be retained until such time as is necessary for the investigation or prosecution of the offence for which the warrant was issued.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(5) A person who obstructs a police officer or an authorized person in the exercise of the police officer’s or authorized person’s powers under this section or who fails to comply with a request made by a police officer or an authorized person under this section commits an offence and is liable, on conviction, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 months or both. **Criminal Code (2004)** **Chapter 3. Procedures, Part 2. Search and Seizure** **Section 624 (Information for Search Warrant)** (1) A magistrate who is satisfied by information on oath that there are reasonable grounds for believing that there is in a building, ship, carriage, box, receptacle or place— (a) anything on or in respect of which any offence has been or is suspected to have been committed; (b) anything that there are reasonable grounds to believe will afford evidence with respect to the commission of an offence, or will reveal the whereabouts of a person who is believed to have committed an offence; or (c) anything that there are reasonable grounds to believe is intended to be used for the purpose of committing any offence against any person for which a person may be arrested without warrant; (d) any offence-related property, may at any time issue a warrant authorizing a police officer who is named in the warrant— (i) to search the building, receptacle or place for any such thing and to seize it, and (ii) bring the thing seized before the justice or some other magistrate to be dealt with by him or her according to law. (2) A person authorized under this section to search computer system in a building or place for data may— (a) use or cause to be used any computer system at the building or place in order to search any data contained in or available to the computer system; (b) reproduce or cause to be reproduced any data in the form of a print-out or other intelligible output; (c) seize the print-out or other output for examination or copying; and (d) use or cause to be used any copying equipment at the place to make copies of the data. (3) A person who is in possession or control of any building or place in respect of which a search is carried out under this section shall, on presentation of the warrant, permit the person carrying out the search—

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) to use or cause to be used any computer system at the building or place in order to search any data contained in or available to the computer system for data that the person is authorized by this section to search for; (b) to obtain a hard copy of the data and to seize it; and (c) to use or cause to be used any copying equipment at the place to make copies of the data. (4) A magistrate may issue a warrant in writing authorizing a police officer to, subject to this section, use any device or investigative technique or procedure or do any thing described in the warrant that would, if not authorized, constitute an unreasonable search or seizure in respect of a person or a person's property if— (a) the magistrate is satisfied by information on oath in writing that there are reasonable grounds to believe that an offence has been or will be committed and that information concerning the offence will be obtained through the use of the technique, procedure or device or the doing of the thing; (b) the magistrate is satisfied that it is in the best interests of the administration of justice to issue the warrant; and (c) there is no other provision in this Code or any other enactment that would provide for a warrant, authorization or order permitting the technique, procedure or device to be used or the thing to be done. (5) Nothing in subsection (4) shall be construed as to permit interference with the bodily integrity of any person. (6) A warrant issued under subsection (4) shall contain such terms and conditions as the magistrate considers advisable to ensure that any search or seizure authorized by the warrant is reasonable in the circumstances. (7) A warrant issued under subsection (4) that authorizes a police officer to observe, by means of a television camera or other similar electronic device, any person who is engaged in activity in circumstances in which the person has a reasonable expectation of privacy shall contain such terms and conditions as the judge considers advisable to ensure that the privacy of the person or of any other person is respected as much as possible. (8) A warrant issued under subsection (4) that authorizes a police officer to enter and search a place covertly shall require, as part of the terms and conditions referred to in subsection (6) that notice of the entry and search be given within any time after the execution of the warrant that the magistrate considers reasonable in the circumstances. (9) Where the magistrate who issues a warrant under subsection (4) or any other magistrate having jurisdiction to issue such a warrant is, on the basis of an affidavit submitted in support of an application to vary the period within which the notice referred to in subsection (8) is to be given, is satisfied that the interests of justice warrant the granting of the application, the magistrate may grant an

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	extension, or a subsequent extension, of the period, but no extension may exceed 3 years. (10) Where a police officer believes that it would be impracticable to appear personally before a magistrate to make an application for a warrant under this section, a warrant may be issued under this section on an information submitted by telephone or other means of telecommunication and, for that purpose, subsection (1) applies, with such modifications as the circumstances require, to the warrant.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: 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: 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. 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. 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. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Computer Misuse Act (2011)** **Section 20 (Collection of traffic data)** (1) Where a police officer or an authorized person has reasonable grounds to believe that any data would be relevant for the purposes of investigation and prosecution of an offence under this Act, he or she may apply ex parte to a Judge in Chambers for an order— (a) allowing the collection or recording of traffic data, associated with specified communications transmitted by means of any computer system; or (b) compelling a service provider, within its technical capabilities, to— (i) effect such collection and recording referred to in paragraph (a), or (ii) assist the police officer or authorized person, to effect such collection and recording. (2) An order made under subsection (1) remains in force— (a) until such time as may reasonably be required for the investigation of the offence; (b) where prosecution is instituted, until the final determination of the case; or (c) until such time as the Judge in Chambers determines or considers necessary.
Article 21 – Interception of content data	**Interception of Communications Act (2005)** **Part I. Preliminary** **Section 2 (Interpretation)**

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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: 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: 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, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 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. 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. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	"**intercept**" includes— (a) aural or other acquisition of the contents of a communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication; (b) monitoring a communication by means of a monitoring device; (c) viewing, examining, or inspecting the contents of a communication; and (d) diverting of any communication from its intended destination to any other destination; and "interception" shall be construed accordingly; **Part II. Interception of Communications** **Section 4 (Application for interception direction and unauthorised disclosure of application)** (7) Any person who discloses the existence of an application for an interception direction, other than to the authorised officer, commits an offence and is liable on conviction on indictment to a fine not exceeding $10,000 or to a term of imprisonment not exceeding 2 years or to both. **Section 5 (Issuance of interception direction)** (1) An interception direction shall be issued if a judge is satisfied, on the facts alleged in the application under section 4, that there are reasonable grounds to believe that— (a) obtaining the information sought under the interception direction is necessary— (i) in the interests of national security, (ii) in the interests of public order, (iii) in the interests of public morality, (iv) in the interests of public safety, (v) for the interest of public health, (vi) for the prevention or detection of any offence specified in the Schedule, where there are reasonable grounds to believe that such an offence has been, is being or may be committed… **Section 6 (Scope and form of interception direction)** (1) An interception direction shall be in the prescribed form and shall permit the authorised officer to — (a) intercept, at any place in Saint Lucia, any communication in the course of its transmission;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) secure the interception in the course of its transmission by means of a postal service or a public or private telecommunications network, of such communications as are described in the interception direction; and (c) secure the disclosure of the intercepted material obtained or required by the interception direction, and of related communications data. (2) An interception direction shall authorise the interception of — (a) communications transmitted by means of a postal service or a public or a private telecommunications network to or from — (i) one particular person specified or described in the interception direction; or (ii) one particular set of premises so specified and described; and (b) such other communications, if any as may be necessary in order to intercept communications falling within paragraph (a). (3) An interception direction shall specify the identity of the — (a) authorised officer on whose behalf the application is made pursuant to section 4, and the person who will execute the interception direction; (b) person, if known and appropriate, whose communication is to be intercepted; and (c) postal service provider or the telecommunication provider to whom the interception direction to intercept must be addressed, if applicable. (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. **Section 16 (Duty to provide assistance)** (1) A person who provides a public postal service or a telecommunications service by means of a public telecommunications network or a private telecommunications network shall take such steps as are necessary to facilitate the execution of an interception direction or an entry warrant, or both. (2) Where the authorised officer intends to seek the assistance of any person in executing an interception direction or an entry warrant or both, the judge shall, on the request of the Attorney General or the Director of Public Prosecutions, appearing on behalf of the authorised officer, direct appropriate persons to furnish information, facilities, or technical assistance necessary to accomplish the interception. (5) A person directed to provide assistance by way of information, facilities, or technical assistance pursuant to subsection (2), shall promptly comply in such a manner that the assistance is rendered— (a) as unobtrusively; and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) with the minimum interference to the services that such a person or entity normally provides to the party affected by the interception direction or entry warrant, as can reasonably be expected in the circumstances. **Section 18 (Exclusion of matters from legal proceedings)** (3) The persons referred to in subsection (2)(a) are— (a) any person to whom an interception direction or an entry warrant pursuant to this Act may be addressed; (d) any person providing a postal service or employed for the purposes of any business of providing a postal service; and (e) any person providing a telecommunications service or an employee for the purposes of any business of providing such a service. **Section 20 (Offence for unauthorised disclosure of interception)** (1) Where an interception direction or an entry warrant or both, has been issued or renewed, it shall be the duty of every person mentioned under section 18(3) to keep such information confidential— (a) the existence and the contents of the interception direction and the entry warrant; (b) the details of the issue of the interception direction and the entry warrant and of any renewal or modification of either; (c) the existence and the contents of any requirement to provide assistance with the giving effect to the interception direction or the entry warrant; (d) the steps taken under the interception direction or the entry warrant or of any such requirement; and (e) everything in the intercepted material together with any related communications data.
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	**Computer Misuse Act (2011)** **Section 4 (Application of the Act)** (1) This Act applies to an act done or an omission made— (a) in Saint Lucia; (b) on a ship or aircraft registered in Saint Lucia; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(c) by a national or citizen of Saint Lucia outside the territory of Saint Lucia, if the person's conduct would also constitute an offence under a law of the country where the offence was committed. (2) Where an offence under this Act is committed by a citizen or national of Saint Lucia in any place outside Saint Lucia, he or she may be dealt with as if the offence had been committed within Saint Lucia.
Article 23 – General principles relating to international co-operation The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes 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.	
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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 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. 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. 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. 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. 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. 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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	
Article 25 – General principles relating to mutual assistance 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. 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. 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. 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. 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 26 – Spontaneous information 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 Convention or might lead to a request for co-operation by that Party under this chapter. 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.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 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. 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. b The central authorities shall communicate directly with each other; 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; 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
Article 28 – Confidentiality and limitation on use 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. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: 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. 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. 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.	
Article 29 – Expedited preservation of stored computer data 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 2 A request for preservation made under paragraph 1 shall specify: 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. 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. 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. 5 In addition, a request for preservation may only be refused if: 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, *ordre public* or other essential interests. 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 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.	
Article 30 – Expedited disclosure of preserved traffic data 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. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: 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, *ordre public* or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data 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. 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. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or 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.	
Article 33 – Mutual assistance in the real-time collection of traffic data 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. 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.	
Article 34 – Mutual assistance regarding the interception of content data 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.	
Article 35 – 24/7 Network 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: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30;	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c the collection of evidence, the provision of legal information, and locating of suspects. 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. 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. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	
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.	

Back to the Table of Contents