Trinidad and Tobago

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 04/02/2022

[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:	Invited to accede

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 (10 November 2000)** **Part I. Preliminary** **Section 2 (Interpretation)** (1) In this Act— **"computer"** means an electronic, optical, electrochemical, or a magnetic, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such inter-connected or related devices, but does not include— (a) an automated typewriter or typesetter; (b) a portable hand held calculator; (c) a similar device which is non-programmable or which does not contain any data storage facility; or (d) such other device as the Minister may prescribe by Order; **"computer output" or "output"** means a statement or representation, whether in written, printed, pictorial, graphical or any other form, purporting to be a statement or representation of fact— (a) produced by a computer; or (b) accurately translated from a statement or representation so produced; **"computer service"** includes computer time, computer output, data processing and the storage or retrieval of a program or data; **"damage"** includes, except for the purpose of section 13, any impairment to a computer or the integrity or availability of any program or data held in a computer that—

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) causes loss aggregating at least ten thousand dollars in value, or such other larger amount as the Minister may prescribe by Order, except that any loss incurred or accrued more than one year after the date of the loss 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; **"data"** means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer; **"electronic, acoustic, mechanical or other device"** means any device or apparatus that is used or capable of being used to intercept any function of a computer; **"function"** includes logic, control, arithmetic, deletion, storage and retrieval, and communication or telecommunication to, from or within a computer; **"intercept"** includes, in relation to a function of a computer, listening to or recording a function of a computer, or acquiring the substance, meaning or purport thereof; **"program or computer program"** means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function. (2) For the purpose of this Act, access of any kind by any person to any program or data held in a computer is unauthorised or done without authority if— (a) he is not himself entitled to control access of the kind in question to the program or data; and (b) he does not have consent to access the kind of program or data in question from the person who is entitled to control access. **Cybercrime Bill (18 May 2017)** **Part I. Preliminary** **Section 4 (Interpretation)** In this Act – "computer data" means any representation of – (a) facts; (b) concepts;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(c) machine-readable code or instructions; or (d) information, including text, sound, image or video, that is in a form suitable for processing in a computer system and is capable of being sent, received or stored, and includes a program that can cause a computer system to perform a function; **"computer data storage medium"** means anything in which information is capable of being stored, or anything from which information is capable of being retrieved or reproduced, with or without the aid of any other article or device; "**computer program" or "program"** means data which represents instructions or statements that, when executed in a computer system, can cause the computer system to perform a function; **"computer system"** means a device or group of interconnected or related devices which follows a program or external instruction to perform automatic processing of information or electronic data; "**data message**" has the meaning assigned to it in the Electronic Transactions Act (Act No. 6 of 2011);
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 (10 November 2000)** **Part II. Offences** **Section 3 - Unauthorised access to computer program or data** (1) Subject to subsection (2), a person who knowingly and without authority causes a computer to perform any function for the purpose of securing access to any program or data held in that computer or in any other computer commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years and, in the case of a second or subsequent conviction, to a fine of thirty thousand dollars and to imprisonment for four years. (2) If any damage is caused as a result of an offence committed under subsection (1), the person convicted of the offence shall be liable to an additional fine of twenty thousand dollars and to imprisonment for three years. (3) For the purpose of this section, it is not material that the act in question is not directed at—

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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. (4) For the purpose of this section, a person secures or gains access to any program or data held in a computer if by causing the computer to perform any function he— (a) alters or erases the program or data; (b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held; (c) uses it; or (d) causes it to be output from the computer in which it is held, whether by having it displayed or in any other manner, and references to access to a program or data and to an intent to secure such access shall be read accordingly. (5) For the purpose of subsection (4)(c), a person uses a program if the function he causes the computer to perform— (a) causes the program to be executed; or (b) is itself a function of the program. (6) For the purpose of subsection (4)(d), the form in which any program or data is output, and in particular whether or not it represents a form in which, in the case of a program, it is capable of being executed or, in the case of data, it is capable of being processed by a computer, is immaterial. **Section 4 Access with intent to commit or facilitate commission of offence** (1) A person who knowingly causes a computer to perform any function for the purpose of securing access to any program or data held in that computer or in any other computer with intent to commit an offence— (a) involving property, fraud, dishonesty or which causes bodily harm; and (b) which is punishable on conviction by imprisonment for more than one year, commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years. (2) For the purpose of this section, it is immaterial whether— (a) the access referred to in subsection (1) is authorised or unauthorised; (b) the offence to which this section applies is (i) committed at the same time when the access is secured or at any other time; and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(ii) punishable summarily or indictably. **Cybercrime Bill (18 May 2017)** **Part II. Cybercrime Offences** **Section 5 Illegal access to a computer system** A person who, intentionally and without lawful excuse or justification, accesses a computer system or any part of a computer system, commits an offence and is liable – (a) on summary conviction to a fine of three hundred thousand dollars and imprisonment for three years; or (b) on conviction on indictment to a fine of five hundred thousand dollars and imprisonment for five years. **Section 6 Illegal remaining in a computer system** A person who, intentionally and without lawful excuse or justification, remains logged into a computer system or part of a computer system or continues to use a computer system commits an offence and is liable – (a) on summary conviction to a fine of one hundred thousand dollars and imprisonment for two years; or (b) on conviction on indictment to a fine of two hundred thousand dollars and imprisonment for three years.
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 (10 November 2000)** **Part II. Offences** **Section 6 Unauthorised use or interception of computer service** (1) Subject to subsection (2), a person who knowingly and without authority— (a) secures access to a computer for the purpose of obtaining, directly or indirectly, any computer service; (b) intercepts or causes to be intercepted, directly or indirectly, any function of any computer by means of an electromagnetic, acoustic, mechanical or other device; or (c) uses or causes to be used, directly or indirectly, a computer, or any other device for the purpose of committing an offence under paragraph (a) or (b), commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years and, in the case of a second or subsequent conviction, to a fine of thirty thousand dollars and to imprisonment for four years.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) If any damage is caused as a result of an offence under subsection (1), the person convicted of the offence shall be liable to an additional fine of twenty thousand dollars and to imprisonment for three years. (3) For the purpose of this section, it is immaterial that the unauthorised 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.
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 (10 November 2000)** **Part II. Offences** **Section 5 Unauthorised modification of computer program or data** (1) Subject to subsection (2), a person who does a direct or an indirect act without authority which he knows will cause an unauthorised modification of any program or data held in any computer commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years and, in the case of a second or subsequent conviction, to a fine of thirty thousand dollars and to imprisonment for four years. (2) If any damage is caused as a result of an offence committed under subsection (1), the person convicted of the offence shall be liable to an additional fine of twenty thousand dollars and to imprisonment for three years. (3) For the purpose of this section— (a) it is immaterial that the act in question is not directed at— (i) any particular program or data; (ii) a program or data of any kind; or (iii) a program or data held in any particular computer; (b) it is immaterial whether an unauthorised modification is, or is intended to be, permanent or merely temporary; (c) a modification of any program or data held in any computer takes place if, by the operation of any function of the computer concerned or any other computer— (i) any program or data held in any computer is altered or erased; (ii) any program or data is added to or removed from any program or data held in any computer; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(iii) any act occurs which impairs the normal operation of any computer, and any act which contributes towards causing such a modification shall be regarded as causing it. (4) Any modification referred to in this section is unauthorised if— (a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and (b) he does not have consent to the modification from the person who is so entitled. **Cybercrime Bill (18 May 2017)** **Part II. Cybercrime Offences** **Section 7 Illegal data interference** (1) A person who, intentionally and without lawful excuse or justification – (a) damages computer data or causes computer data to deteriorate; (b) deletes computer data; (c) alters computer data; (d) copies computer data to any computer data storage device or to a different location within the computer system; (e) moves computer data to a computer storage device or a different location within the computer system; (f) renders computer data meaningless, useless or ineffective; (g) obstructs, interrupts or interferes with the lawful use of computer data; (f) obstructs, interrupts or interferes with a person in his lawful use of computer data; or (g) denies access to computer data to a person who is authorised to access it, commits an offence. (2) A person who commits an offence under subsection (1), is liable – (a) on summary conviction to a fine of one hundred thousand dollars and imprisonment for two years; or (b) on conviction on indictment to a fine of two hundred thousand dollars and imprisonment for three years. **Section 8 Illegal acquisition of data**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(1) A person who intentionally and without lawful excuse or justification accesses a computer system without authorisation, or by exceeding authorised access, and obtains computer data commits an offence and is liable – (a) on summary conviction to a fine of one hundred thousand dollars and imprisonment for two years; or (b) on conviction on indictment to a fine of five hundred thousand dollars and imprisonment for three years. (2) A person who intentionally and without lawful excuse or justification receives or gains access to computer data knowing the same to have been stolen or obtained pursuant to sub-section (1) commits an offence and is liable – (a)on summary conviction to a fine of one hundred thousand dollars and imprisonment for two years; or (b)on conviction on indictment to a fine of five hundred thousand dollars and imprisonment for three years.
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 (10 November 2000)** **Part II. Offences** **Section 5 Unauthorised modification of computer program or data** (1) Subject to subsection (2), a person who does a direct or an indirect act without authority which he knows will cause an unauthorised modification of any program or data held in any computer commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years and, in the case of a second or subsequent conviction, to a fine of thirty thousand dollars and to imprisonment for four years. (2) If any damage is caused as a result of an offence committed under subsection (1), the person convicted of the offence shall be liable to an additional fine of twenty thousand dollars and to imprisonment for three years. (3) For the purpose of this section— (a) it is immaterial that the act in question is not directed at— (i) any particular program or data; (ii) a program or data of any kind; or (iii) a program or data held in any particular computer; (b) it is immaterial whether an unauthorised modification is, or is intended to be, permanent or merely temporary;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(c) a modification of any program or data held in any computer takes place if, by the operation of any function of the computer concerned or any other computer— (i) any program or data held in any computer is altered or erased; (ii) any program or data is added to or removed from any program or data held in any computer; or (iii) any act occurs which impairs the normal operation of any computer, and any act which contributes towards causing such a modification shall be regarded as causing it. (4) Any modification referred to in this section is unauthorised if— (a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and (b) he does not have consent to the modification from the person who is so entitled. **Section 7 Unauthorised obstruction of use or use of computer** (1) Subject to subsection (2), a person who knowingly and without authority— (a) interferes with, interrupts, or obstructs the lawful use of a computer; or (b) impedes, prevents access to, or impairs the usefulness or effectiveness of any program or data held in a computer, commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years and, in the case of a second or subsequent conviction, to a fine of thirty thousand dollars and to imprisonment for four years. (2) If any damage is caused as a result of an offence committed under subsection (1), the person convicted of the offence shall be liable to an additional fine of twenty thousand dollars and to imprisonment for three years. **Section 11 Causing a computer to cease to function** (1) A person who engages in conduct which causes a computer to cease to function permanently or temporarily and at the time he engages in that conduct he has— (a) knowledge that the conduct is unauthorised; (b) the requisite knowledge; and (c) the requisite intent, commits an offence and is liable on summary conviction to a fine of fifty thousand dollars and to imprisonment for ten years.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) For the purpose of subsection (1)— (a) "requisite knowledge" means knowledge that the conduct would or would be likely to cause a computer to cease to function permanently or temporarily; and (b) "requisite intent" means intent to cause a computer to cease to function and by so doing— (i) prevents or hinders access to the computer; or (ii) impair the operation of the computer, but the intent need not be directed at a particular computer. **Cybercrime Bill (18 May 2017)** **Part II. Cybercrime Offences** **Section 9 Illegal system interference** (1) A person who, intentionally and without lawful excuse or justification, hinders or interferes with a computer system commits an offence. (2) A person who, intentionally and without lawful excuse or justification, hinders or interferes with a person who is lawfully using or operating a computer system commits an offence. (3) A person who commits an offence under this section is liable – (a) on summary conviction to a fine of one hundred thousand dollars and imprisonment for two years; or (b) on conviction on indictment to a fine of three hundred thousand dollars dollars and imprisonment for three years.
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; 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	**Computer Misuse Act (10 November 2000)** **Part II. Offences** **Section 8 Unauthorised disclosure of access codes** (1) A person who knowingly and without authority discloses any password, access code or any other means of gaining access to any program or data held in a computer commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years and, in the case of a second or subsequent conviction, to a fine of thirty thousand dollars and to imprisonment for four years. (2) A person who knowingly and without authority discloses any password, access code or any other means of gaining access to any program or data held in a computer commits an offence if he did so— (a) for any unlawful gain, whether to himself or to another person; (b) for any unlawful purpose; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(c) knowing that it is likely to cause unlawful damage, is liable on summary conviction to a fine of thirty thousand dollars and to imprisonment for four years and, in the case of a second or subsequent conviction, to a fine of fifty thousand dollars and to imprisonment for five years. **Section 10 Unauthorised receiving or giving access to computer program or data** (1) A person who receives or is given access to any program or data held in a computer and who is not authorised to receive or have access to that program or data from another person, whether or not he knows that that person has obtained that program or data through authorised or unauthorised means, commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years. (2) A person who is authorised to receive or have access to any program or data held in a computer and who receives that program or data from another person knowing that that person has obtained that program or data through unauthorised means commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years. (3) A person who has obtained any program or data held in a computer through authorised means and gives that program or data to another person who he knows is not authorised to receive or have access to that program or data commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years. (4) A person who has obtained any program or data held in a computer through unauthorised means and gives that program or data to another person whether or not he knows that that other person is authorised to receive or have access to that program or data commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years. **Cybercrime Bill (18 May 2017)** **Part II. Cybercrime Offences** **Section 11 Illegal devices** (1) A person who – (a) produces, sells, procures for use, imports, exports, distributes or otherwise makes available or has in his possession – (i) a device, or computer program, that is designed or adapted for

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	the purpose of committing an offence under this Act; or (ii) a computer password, access code or similar data by which the whole or any part of a computer system, computer data storage device or computer data is capable of being accessed, with the intent that it be used for the purpose of committing an offence under this Act; or (b) intentionally and without lawful excuse or justification discloses a computer password, access code or similar data by which the whole or any part of a computer system, computer data storage device or computer data can be accessed - (i) for unlawful gain, whether for himself or another person; (ii) for an unlawful purpose; or (iii) knowing that it is likely to cause unlawful damage, commits an offence. (2) A person who commits an offence under subsection (1) is liable – (a) on summary conviction to a fine of two hundred thousand dollars and imprisonment for three years; or (b) on conviction on indictment to a fine of five hundred thousand dollars and imprisonment for five years. **Section 12 Unauthorised granting of access to computer data** (1) A person who, through authorised or unauthorised means, obtains or accesses computer data which— (a) is commercially sensitive or a trade secret; (b) relates to the national security of the State; or (c) is stored on a computer system and is protected against unauthorized access, and intentionally and without lawful excuse or justification grants access to or gives the computer data to another person, whether or not he knows that the other person is authorised to receive or have access to the computer data, commits an offence. (2) A person who commits an offence under this section is liable— (a) on summary conviction to a fine of two hundred thousand dollars and imprisonment for three years; and (b) on conviction on indictment to a fine of five hundred thousand dollars and imprisonment for five years.
Title 2 – Computer-related offences	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**Cybercrime Bill (18 May 2017)** **Part II. Cybercrime Offences** **Section 13 (Computer-related forgery)** (1) A person who, intentionally and without lawful excuse or justification inputs, alters, deletes or suppresses computer data, resulting in inauthentic data, with the intent that it be considered or acted upon as if it were authentic, regardless of whether or not the data is directly readable and intelligible, commits an offence and is liable – (a) on summary conviction to a fine of three hundred thousand dollars and imprisonment for three years; or (b) on conviction on indictment to a fine of five hundred thousand dollars and imprisonment for five years. (2) A person who commits an offence under subsection (1) by sending out multiple electronic mail messages from or through a computer system, is liable on conviction to a fine of two hundred thousand dollars and imprisonment for three years, in addition to the penalty set out in subsection (1).
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.	**Cybercrime Bill (18 May 2017)** **Part II. Cybercrime Offences** **Section 14 (Computer-related fraud)** (1) A person who, intentionally and without lawful excuse or justification – (a) inputs, alters, deletes or suppresses computer data; or (b) interferes with the functioning of a computer system, with the intent of procuring an economic benefit for himself or another person and thereby causes loss of, or damage to, property, commits an offence. (2) A person who commits an offence under subsection (1) is liable – (a) on summary conviction to a fine of one million dollars and imprisonment for five years; or (b) on conviction on indictment to a fine of two million dollars and imprisonment for ten years.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 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:	**Children Act (6 August 2012)** **Chapter 46:01 (as amended), Part VIII. Child pornography** **Section 3 Interpretation** (…)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	"**child"** means a person under the age of eighteen years. **"child pornography"** means a photograph, film, video or other visual representation, whether or not made by electronic, mechanical, artistic or other methods, that shows, for a sexual purpose— (a) a child engaging in explicit sexual activity or conduct; Act inconsistent with Constitution Short title and commencement Interpretation 126 No. 12 Children 2012 Chap. 16:01 Chap. 46:10 Enactment (b) a child in a sexually explicit pose; (c) parts of a child's body pasted to visual representations of parts of an adult's body or vice versa; or (d) parts of a child's body which have been rendered complete by computer generated images or by other methods of visual representation, but does not include any visual representation produced or reproduced for the purpose of education, counselling, the promotion of reproductive health or as part of a criminal investigation and prosecution or civil proceedings or in the lawful performance of a person's professional duties and functions; (…) **Section 40 Child pornography** (1) Subject to subsection (5), a person who knowingly – (a) makes or permits to be made any child pornography or copy thereof; (b) publishes, distributes, transmits or shows any child pornography; (c) publishes or causes to be published any advertisement likely to be understood as conveying that the advertiser distributes or shows any child pornography; (d) obtains access, through information and communication technologies, to child pornography; (e) has in his possession or control any child pornography; or (f) purchases, exchanges or otherwise receives any child pornography, commits an offence and is liable on conviction on indictment, to a fine of thirty thousand dollars and to imprisonment for ten years. (2) For the purposes of subsection (1), a person knowingly distributes child pornography, if he knowingly— (a) offers; or (b) transmits by any means including post, courier, electronic means or facsimile, child pornography to another person.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) Where a person is charged with an offence under subsection (1), it is a defence for him to prove that he had not himself seen the child pornography, or did not know, or did not have any cause to suspect it to be child pornography. (4) A person who is found in possession of child pornography is deemed to have known he was in possession of child pornography unless the contrary is proved, the burden of proof being on the accused. (5) A person who is— (a) a member of the Police Service established under the Police Service Act; (b) a member of the Prison Service established under the Prison Service Act; (c) a member of the Defence Force established under the Defence Act; (d) a member of Customs established under the Customs Act; (e) the Director of the Forensic Science Centre or any other officer designated by the Director of the Forensic Science Centre holding the office of Scientific Officer I or above; (f) any other officer employed by the State in the prevention, detection, investigation, or prosecution of an offence relating to child pornography; (g) a legal officer involved in the prosecution or defence of a case; (h) a teacher or counsellor in the execution of his duties for the purpose of education or counselling; or (i) any other person involved in the prosecution or defence of an offence relating to child pornography, does not commit an offence under subsection (1), if the act which would otherwise constitute an offence under that subsection is done by him in good faith, for the purpose of his official or professional duties.
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	Copyright Act **(Amended 5 of 2008)** **PART VII REMEDIES** **Section 31 Action by owner of rights for infringement**(1) Subject to this Act, infringements of rights of the owner of copyright or neighbouring rights shall be actionable in the Court at the suit of the owner of copyright or neighbouring rights; and in any action for such an infringement all such relief by way of damages, injunction, accounts or otherwise shall be available to the plaintiff as is available in any corresponding proceedings in respect of infringements of other proprietary rights.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(2) In an action for infringement of rights in respect of the construction of a building, no injunction or other order shall be made— (a) after the construction of the building has begun, so as to prevent it from being completed; or (b) so as to require the building, in so far as it has been constructed, to be demolished. **PART VIII OFFENCES** **Section 41 Penalties in respect of infringing copies of a work, performance, sound recording or broadcast** . (1) A person commits an offence who, without the licence of the copyright owner— (a) makes for sale or hire; (b) imports into Trinidad and Tobago otherwise than for his private and domestic use; (c) possesses in the course of a business with the intention of infringing the copyright in the work or neighbouring rights in the performance, sound recording or broadcast; (d) in the course of a business— (i) sells or lets for hire; (ii) offers or exposes for sale or hire; (iii) exhibits in public; (iv) distributes; or (e) distributes otherwise than in the course of a business in excess of three copies of, an article which is, and which he knows or has reason to believe is, an infringing copy of a copyright work, performance, sound recording or broadcast. (2) A person commits an offence who— (a) makes an article specifically designed or adapted for making copies of a particular copyright work, performance, sound recording or broadcast; or (b) has such an article in his possession, knowing or having reason to believe that it is to be used to make infringing copies for sale or hire or for use in the course of a business. (3) A person guilty of an offence under subsections (1) and (2) is liable on summary conviction to a fine of two hundred and fifty thousand dollars and imprisonment for ten years.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(4) The Magistrate before whom proceedings are brought against a person for an offence under this section may, if satisfied that at the time of his arrest or charge the person had in his possession, custody or control— (a) an infringing copy of a copyright work, performance, sound recording or broadcast in the case of a business; (b) an article specifically designed or adapted for making copies of a particular copyright work, performance, sound recording or broadcast, knowing or having reason to believe that it had been or was to be used to make infringing copies; or (c) any apparatus, implements or devices that may be used to commit or continue to commit an offence under this Act order that the infringing copy, article, apparatus, implements or devices be destroyed or delivered up to the copyright owner or to such other person as the Magistrate may direct.
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.	**Act relating to the trial and punishment of Accessories to and Abettors of Offences (17th March 1925)** **Section 2 Abettors in indictable offences** Any person who aids, abets, counsels or procures the commission of any indictable offence may be indicted, tried and punished as a principal offender. **Section 3 Abettors in summary offences** (1) Any person who aids, abets, counsels, or procures the commission of any offence punishable on summary conviction is liable to the same punishment as the principal offender, and may be proceeded against either with the principal offender or before or after his conviction, and either in the district in which the principal offender may be convicted or that in which the offence of aiding, abetting, counselling or procuring may have been committed. (2) Any person so aiding, abetting, counselling or procuring may be tried before any Magistrate or Justice having cognisance of the principal offence.
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	**Criminal Procedure (Corporations) Act (1st November 1961)**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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: 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 (10 November 2000)** **Part III. General Provisions** **Section 14 Order for payment of compensation** (1) The Court before which a person is convicted of any offence under this Act may make an order against him for the payment of a sum to be fixed by the Court by way of compensation to any person for any damage caused to that person's computer, program or data as a result of the offence for 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 under an order for compensation, but the order shall 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 purpose of this section, a program or data held in a computer is deemed to be the property of the owner of the computer. **Cybercrime Bill (18 May 2017)** **Part III. Enforcement**

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Section 29 Order for payment of additional fine (1) Where a person is convicted of an offence under this Act and the Court is satisfied that monetary benefits accrued to him as a result of the commission of the offence, the Court may order him to pay an additional fine in an amount equal to the amount of the monetary benefits. (2) Where damage is caused as a result of an offence under this Act, the person convicted of the offence is liable to an additional fine not exceeding the fine that the Court may impose for the commission of the offence that caused the damage. **Section 30 Order for payment of compensation** (1) Where a person is convicted of an offence under this Act, and the Court is satisfied that another person has suffered loss or damage because of the commission of the offence, it may, in addition to any penalty imposed under this Act, order the person convicted to pay a fixed sum as compensation to that other person for the loss or damage caused or likely to be caused, as a result of the commission of the offence. (2) An order made under subsection (1) shall be without prejudice to any other remedy which the person who suffered the damage may have under any other law. (3) The Court may make an order under this section of its own motion or upon application of a person who has suffered damage as a result of the commission of the offence. (4) A person who makes an application under subsection (3) shall do so before sentence is passed on the person against whom the order is sought. (5) For the purpose of this section, computer data held in an apparatus is deemed to be the property of the owner of the apparatus. **Section 31 Forfeiture Order** (1) Subject to subsection (2), where a person is convicted of an offence under this Act, the Court may order that any property – (a) used for, or in connection with; or (b) obtained as a result of, or in connection with, the commission of the offence, be forfeited to the State.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) Before making an order under subsection (1), the Court shall give an opportunity to be heard to any person who claims to be the owner of the property or who appears to the Court to have an interest in the property. (3) Property forfeited to the State under subsection (1) shall vest in the State— (a) if no appeal is made against the order, at the end of the period within which an appeal may be made against the order; or (b) if an appeal has been made against the order, on the final determination of the matter, where the decision is made in favour of the State. (4) Where property is forfeited to the State under this section, it shall be disposed of in the prescribed manner. **Section 32 Order for seizure and restraint** Where an ex parte application is made by the Director of Public Prosecutions to a Judge and the Judge is satisfied that there are reasonable grounds to believe that there is in any building, place or vessel, any property in respect of which a forfeiture order under section 31 has been made, the Judge may issue – (a) a warrant authorising a police officer to search the building, place or vessel for that property and to seize that property if found, and any other property in respect of which the police officer believes, on reasonable grounds, that a forfeiture order under section 31 may be made; or (b) a restraint order prohibiting any person from disposing of, or otherwise dealing with any interest in, the property, other than as may be specified in the restraint order.
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	**Evidence (Amendment) Act (25 February 2021)** **Chapter 7:02, Part 1A Police and Criminal Evidence, Division 5 Supplemental Provisions** **Section 14B Electronic evidence in criminal proceedings** (1) In any criminal proceedings, nothing in any written law or the common law shall apply to deny the admissibility of an electronic record in evidence on the sole ground that it is an electronic record. (2) Where a device or process is one that, or is of a kind that, ordinarily

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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	produces or accurately communicates an electronic record, the court shall presume that in producing or communicating that electronic record on the occasion in question, the device or process produced or accurately communicated the electronic record, unless evidence sufficient to raise doubt about the presumption is adduced. (3) The hearsay rule does not apply to a representation contained in a document recording an electronic communication so far as the representation is a representation as to— (a) the identity of the person from whom or on whose behalf the electronic communication was sent; (b) the date on which or the time at which the electronic communication was sent; or (c) the destination of the electronic communication or the identity of the person to whom the electronic communication was addressed. (4) Any person seeking to admit an electronic record in any criminal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is that which it is purported to be. (5) Where it is intended to prove the authenticity of an electronic record as evidence, it is permissible to have the evidence of the expert relating to the authenticity of an electronic record presented in the form of a certificate.
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other	**Trinidad and Tobago (Constitution) Order in Council 1962** **CHAPTER 1. THE RECOGNITION AND PROTECTION OF HYMAN RIGHTS AND FUNDAMENTAL FREEDOMS** **Section 1. Recognition and declaration of rights and freedoms** It is hereby recognised and declared that in Trinidad and Tobago there have existed and shall continue to exist without discrimination by reason of race, origin, colour, religion orsex, the following human rights and fundamental freedoms, namely: (a) the right of the individual to life, liberty, security of the person and enjoyment of property, and the right not to be deprived thereof except by due process of law; (b) the right of the individual to equality before the law and the protection of the law;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(c) the right of the individual to respect for his private and family life; (d) the right of the individual to equality of treatment from any public authority in the exercise of any functions; (e) the right to join political parties and to express political views; (f) the right of a parent or guardian to provide a school of his own choice for the education of his child or ward; (g) freedom of movement; (h) freedom of conscience and religious belief and observance; (i) freedom of thought and expression; (j) freedom of association **Section 2. Protection of rights and freedoms** Subject to the provisions of sections 3, 4 and 5 of this Constitution, no law shall abrogate, abridge or infringe or authorise the abrogation, abridgment or infringement of any of the rights and freedoms hereinbefore recognised and declared and in particular no Act of Parliament shall— (a) authorise or effect the arbitrary detention, imprisonment or exile of any person; (b) impose or authorise the imposition of cruel and unusual treatment or punishment; (c) deprive a person who has been arrested or detained— (i) of the right to be informed promptly and with sufficient particularity of the reason for his arrest or detention; (ii) of the right to retain and instruct without delay a legal adviser of his own choice and to hold communication with him; (iii) ofthe right to be brought promptly before an appropriate judicial authority; (iv) of the remedy by way of habeas corpus for the determination of the validity of his detention and for his release if the detention is not lawful; (d) authorise a court, tribunal, commission, board or other authority to compel a person to give evidence if he is denied legal representation or protection against self-crimination; (e) deprive a person of the right to a fair hearing in accordance with the principles of fundamental justice for the determination of his rights and obligations;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(f) deprive a person charged with a criminal offence of the right to be presumed innocent until proved guilty according to law in a fair and public hearing by an independent and impartial tribunal, or of the right to reasonable bail without just cause; (g) deprive a person of the right to the assistance of an interpreter in any proceedings in which he is involved or in which he is a party or a witness, before a court, commission, board or other tribunal, if he does not understand or speak the language in which such proceedings are conducted; or (h) deprive a person of the right to such procedural provisions as are necessary for the purpose of giving effect and protection to the aforesaid rights and freedoms.
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. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Cybercrime Bill (18 May 2017)** **Part III. Enforcement** **Section 25 Expedited preservation** (1) A Magistrate may, if satisfied on an ex parte application by a police officer of the rank of Superintendent or above, that there are grounds to believe that computer data that is reasonably required for the purpose of a criminal investigation is vulnerable to loss or modification, authorise the police officer to require a person in control of the computer data, by notice in writing, to preserve the data for such period not exceeding ninety days as is stated in the notice. (2) A Magistrate may, on an ex parte application by a police officer of the rank of Superintendent or above, authorise an extension of the period referred to in subsection (1) by a further specified period not exceeding ninety days.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Cybercrime Bill (18 May 2017)** **Part III. Enforcement** **Section 27 Disclosure of traffic data** If a Magistrate is satisfied on the basis of information on oath by a police officer, that there are reasonable grounds to believe that computer data stored in an apparatus is reasonably required for the purpose of a criminal investigation into a data message, he may require a person to disclose sufficient traffic data about the data message to identify – (a) the internet service provider; or (b) the path, through which the data message was transmitted.
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; 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;	**Cybercrime Bill (18 May 2017)** **Part III. Enforcement** **Section 24 Production order** If a Magistrate is satisfied on the basis of information on oath by a police officer that computer data, a printout or other information is reasonably required for the purpose of a criminal investigation or criminal proceedings, the Magistrate may order – (a) a person in Trinidad and Tobago who is in control of an apparatus, to produce from the apparatus computer data or a printout or other intelligible output of the computer data; or (b) an internet service provider in Trinidad and Tobago to produce information about a person who subscribes to, or otherwise uses his service.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	
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. 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.	**Computer Misuse Act (10 November 2000)** **Part III. General Provisions** **Section 16 Power of police officer to access computer program or data** (1) This section applies to a computer which a police officer or an authorised person has reasonable cause to suspect is or has been in use in connection with any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section. (2) Where a Magistrate is satisfied by information on oath given by a police officer that there are reasonable grounds for believing that an offence under this Act has been or is about to be committed in any place and that evidence that such an offence has been or is about to be committed is in that place, he may issue a warrant authorising any police officer to enter and search that place, including any computer, using such reasonable force as is necessary. (3) A warrant issued under this section may also direct an authorised person to accompany any police officer executing the warrant and remains in force for twenty-eight days from the date of its issue. (4) In executing a warrant under this section, a police officer may seize any computer, data, program, information, document or thing if he reasonably believes that it is evidence that an offence under this Act has been or is about to be committed. **Cybercrime Bill (18 May 2017)** **Part III. Enforcement** **Section 21 Search and seizure** (1) Where a Magistrate is satisfied on the basis of information on oath by a police officer that there is reasonable ground to believe that there is in a place an apparatus or computer data – (a) that may be material as evidence in proving an offence under this Act; or (b) that has been acquired by a person as a result of an offence under this Act, he may issue a warrant authorizing a police officer, with such assistance as may be necessary, to enter the place to search for and seize the apparatus or computer data.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) If a police officer who is undertaking a search under this section has reasonable grounds to believe that – (a) the computer data sought is stored in another apparatus; or (b) part of the computer data sought is in another place within Trinidad and Tobago, and such computer data is lawfully accessible from, or available to the first apparatus, he may extend the search and seizure to that other apparatus or other place. (3) In the execution of a warrant under this section, a police officer may, in addition to the powers conferred on him by the warrant – (a) activate an onsite computer system or computer data storage media; (b) make and retain a copy of computer data; (c) remove computer data in a computer system or render it inaccessible; (d) take a printout of the output of computer data; (e) impound or similarly secure a computer system or part of it or a computer data storage medium; or (f) remove a computer system or computer data storage medium from its location. (4) A police officer who undertakes a search under this section shall secure any apparatus and maintain the integrity of any computer data that is seized. (5) For the purpose of this section, "apparatus" includes – (a) a computer system or part of a computer system; or (b) a computer data storage medium. **Section 22 (Assistance)** (1) A person who has knowledge about the functioning of an apparatus, or measures applied to protect computer data, that is the subject of a search warrant shall, if requested by the police officer authorised to undertake the search, assist the officer by – (a) providing information that facilitates the undertaking of the search for and seizure of the apparatus or computer data sought; (b) accessing and using an apparatus to search computer data which is stored in, or lawfully accessible from, or available to, that apparatus; (c) obtaining and copying computer data; or (d) obtaining an intelligible output from an apparatus in such a format that is admissible for the purpose of legal proceedings.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) A person who fails to comply with this section commits an offence and is liable on summary conviction to a fine of one hundred thousand dollars and imprisonment for one year.
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.	**Part III. Enforcement** **Cybercrime Bill (18 May 2017)** **23. Order for removal or disablement of data** If a Magistrate is satisfied on the basis of information on oath by a police officer that an internet service provider or any other entity with a domain name server is storing, transmitting or providing access to information in contravention of this Act or any other written law, the Magistrate may order the internet service provider or other entity with a domain name server to remove, or disable access to, the information.
Article 21 – Interception of content data 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:	**Part III. Enforcement** **Cybercrime Bill (18 May 2017)** **23. Order for removal or disablement of data** If a Magistrate is satisfied on the basis of information on oath by a police officer that an internet service provider or any other entity with a domain name server is storing, transmitting or providing access to information in contravention of this Act or any other written law, the Magistrate may order the internet service provider or other entity with a domain name server to remove, or disable access to, the information

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Interception of Communications (Amendment) Act (18 June 2020)** **Chapter. 15:08** **Section 9 (Amendment Section 8)** (1) Subject to this section, an authorised officer may apply ex parte to a Judge for a warrant authorising the person named in the warrant— (a) authorising the person named in the warrant— (i) to intercept, in the course of their transmission by means of a public or private telecommunications network, such communications as are described in the warrant; and (ii) to disclose the intercepted communication to such persons and in such manner as may be specified in the warrant; (b) authorising the person named in the warrant to obtain stored communication from a telecommunications service provider and to disclose the stored communication to such persons and in such manner as may be specified in the warrant; or (c) authorising the person named in the warrant to obtain stored data and to disclose the stored data to such persons and in such manner as may be specified in the warrant.”;
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and	**Computer Misuse Act (10 November 2000)** **Part III. General Provisions** **Section 12 Territorial scope of offences under this Act** (1) Subject to subsection (2), this Act shall have effect in relation to any person, whatever his nationality or citizenship, outside as well as within the State, and where an offence under this Act is committed by a person in any place outside of the State, he may be dealt with as if the offence had been committed within the State. (2) For the purpose of subsection (1), this Act shall apply if, for the offence in question— (a) the accused was in the State at the material time; (b) the computer, program or data was in the State at the material time; or (c) the damage occurred within the State, whether or not paragraph (a) or (b) applies

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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	**Section 13 Jurisdiction of court** (1) A Court shall have jurisdiction to hear and determine all offences committed under this Act. (2) A summary Court shall have jurisdiction to hear and determine any offence, except an offence under section 9, if— (a) the accused was within the magisterial district at the time when he committed the offence; (b) any computer containing any program or data which the accused used was within the magisterial district at the time when he committed the offence; or (c) the damage occurred within the magisterial district, whether or not paragraph (a) or (b) applies. **Cybercrime Bill (18 May 2017)** **Part III. Enforcement** **Section 20 Jurisdiction** (1) A Court in Trinidad and Tobago shall have jurisdiction in respect of an offence under this Act where the act constituting the offence is carried out – (a) wholly or partly in Trinidad and Tobago; (b) by a citizen of Trinidad and Tobago, whether in Trinidad and Tobago or elsewhere; or (c) by a person on board a vessel or aircraft registered in Trinidad and Tobago. (2) For the purpose of subsection (1)(a), an act is carried out in Trinidad and Tobago if – (a) the person is in Trinidad and Tobago at the time when the act is committed; (b) a computer system located in Trinidad and Tobago or computer data on a computer data storage device located in Trinidad and Tobago is affected by the act; or (c) the effect of the act, or the damage resulting from the act, occurs within Trinidad and Tobago. (3) Subject to subsection (1), a Summary Court has jurisdiction to hear and determine any offence under this Act, if –

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) the accused was within the magisterial district at the time when he committed the offence; (b) a computer system, containing any computer program or computer data which the accused used, was within the magisterial district at the time when he committed the offence; or (c) damage occurred within the magisterial district, whether or not paragraph (a) or (b) applies.
Chapter III – International co-operation	
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.	No specific provisions found
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 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.	**Extradition (Commonwealth and Foreign Territories) Act (1985)** **Chapter 12:04, Part III. Extradition from Trinidad and Tobago** **Section 6 Extraditable offences** (1) For the purpose of this Act, an offence in respect of which a person is accused or has been convicted in a declared Commonwealth territory, or a declared foreign territory, is an extraditable offence if— (a) it is an offence against the law of that territory which is punishable under the law with death or imprisonment for a term of not less than twelve months; (b) the conduct of the person would constitute an offence against the law of Trinidad and Tobago if it took place in Trinidad and Tobago, or in the case of an extra-territorial offence, if it took place in corresponding circumstances outside Trinidad and Tobago, and would be punishable under the law of Trinidad and Tobago with death or imprisonment for a term of not less than twelve months; and (c) in the case of a declared foreign territory, extradition for that offence is provided for by a treaty between Trinidad and Tobago and that territory.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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	(2) For the purpose of this section, in determining whether an offence against the law of a declared Commonwealth territory, or a declared foreign territory, is an offence against the law of Trinidad and Tobago, any special intent, state of mind or special circumstances of aggravation which may be necessary to constitute that offence under the law of Trinidad and Tobago shall be disregarded. (3) For greater certainty, it is not relevant whether the conduct referred to in subsection (1) is named, defined or characterised by the declared Commonwealth territory, or the declared foreign territory, in the same way as it is in Trinidad and Tobago. (4) An offence constituted by conduct, whether in Trinidad and Tobago or not, that is of a kind over which Contracting States to an international Convention to which Trinidad and Tobago is a party are required by that Convention to establish jurisdiction, and which jurisdiction Trinidad and Tobago has so established, is an extraditable offence for the purpose of this Act.
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.	**Mutual Assistance in Criminal Matters Act (2004)** **CHAP. 11:24, Part II. Requests by Trinidad and Tobago to Commonwealth countries for assistance** **Section 7 Assistance in obtaining evidence** Where there are reasonable grounds to believe that evidence or information relevant to any criminal proceedings may be obtained, if, in a Commonwealth country— (a) evidence is taken from any person;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(b) information is provided; (c) judicial records, official records or other records, or documents or other articles are produced or examined; (d) samples of any matter or thing are taken, examined or tested; (e) any building, place or thing is viewed or photographed, a request may be transmitted requesting that assistance be given by that country in so obtaining the evidence or information. **Section 8 Assistance in locating or identifying person** Where there are reasonable grounds to believe that a person who— (a) is or might be concerned in or affected by; or (b) could give or provide evidence or assistance relevant to, any criminal proceedings, is in a Commonwealth country, a request may be transmitted requesting that assistance be given by that country in locating that person or, if his identity is unknown, in identifying and locating him. **Section 9 Assistance in obtaining article or thing, by search and seizure** Where there are reasonable grounds to believe that an article or thing is in a Commonwealth country and would, if produced, be relevant to any criminal proceedings, a request may be transmitted requesting that assistance be given by that country in obtaining, by search and seizure, if necessary, the article or thing. **Section 10 Assistance in arranging attendance of person** Where there are reasonable grounds to believe that a person in a Commonwealth country could give or provide evidence or assistance relevant to any criminal proceedings, a request may be transmitted requesting that assistance be given by that country in arranging the attendance of the person in Trinidad and Tobago to give or provide such evidence or assistance but such attendance may be secured only with the signed consent of that person.
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.	**Mutual Assistance in Criminal Matters Act (2004)** **Article 7 Confidentiality and Restricting Evidence and Information** 1. The Requested Party shall, to any extent requested, keep confidential a request for assistance, its contents and any supporting documents, and the fact of granting such assistance except to the extent that disclosure is necessary to execute the request. If the request cannot be executed without breaching confidentiality, the Requested Party shall so inform the Requesting Party which shall then determine the extent to which it wishes the request to be executed.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	2. The Requesting Party shall, if so requested, keep confidential any evidence and information provided by the Requested Party, except to the extent that its disclosure is necessary for the proceeding described in the request.
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. 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.	No specific provision found.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency,	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Mutual Assistance in Criminal Matters Act (2004)** **CHAP. 11:24, Part II. Requests by Trinidad and Tobago to Commonwealth countries for assistance** **Section 16 (Restriction on use of evidence, etc.)** Any — (a) evidence or information obtained or, as the case may be, given or provided, by any person pursuant to a request made in section 7, 10, 12 or 14; or (b) article or thing obtained pursuant to a request made in section 9, shall be used, by or on behalf of Trinidad and Tobago, only for the purposes of, or in connection with, the criminal proceedings to which the request relates, unless the Commonwealth country, to which the request was made, consents to it being otherwise used by or on behalf of Trinidad and Tobago.
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 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;	No specific provision found.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Interception of Communications Act (2010)** **Chapter. 15:08, Part II. Interception of Communication** **Section 18. Disclosure of communications data** (…) (2) Where it appears to the authorised officer that a person providing a telecommunications service is or may be in possession of, or capable of obtaining, any communications data, the authorised officer may, by notice in writing, require the provider— (a) to disclose to an authorised officer all of the data in his possession or subsequently obtained by him; or (b) if the provider is not already in possession of the data, to obtain the data and so disclose it. (3) An authorised officer shall not issue a notice under subsection (2) in relation to any communications data unless he has obtained a warrant under section 8 or 11. (4) A notice under subsection (2) shall state— (a) the communications 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 by reference to which the notice is issued; and (e) the date on which it is issued. (5) Sections 13 and 14 shall apply, with the necessary modifications, to the disclosure of data pursuant to a notice issued under this section. (6) Subject to subsection (7), 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.
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.	No specific provision found.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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.	No specific provision found.
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.	No specific provision found.
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.	No specific provision found.
Article 35 – 24/7 Network	No specific provision found.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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; 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