Canada

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Version 01 May 2020

Table of contents

[reference to the provisions of the Budapest Convention]

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

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

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

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	**Criminal Code** **342.1** computer data means representations, including signs, signals or symbols, that are in a form suitable for processing in a computer system; (données informatiques) computer password means any computer data by which a computer service or computer system is capable of being obtained or used; (mot de passe) computer program means computer data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function; (programme d'ordinateur) computer service includes data processing and the storage or retrieval of computer data; (service d'ordinateur) computer system means a device that, or a group of interconnected or related devices one or more of which, (a) contains computer programs or other computer data, and (b) by means of computer programs, (i) performs logic and control, and (ii) may perform any other function; (ordinateur)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	data[Repealed, 2014, c. 31, s. 16] electro-magnetic, acoustic, mechanical or other device means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing; (dispositif électromagnétique, acoustique, mécanique ou autre) function includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system; (fonction) intercept includes listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof; (intercepter) traffic means, in respect of a computer password, to sell, export from or import into Canada, distribute or deal with in any other way. (trafic)
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.	
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	**Criminal Code** **Interception of Communications** **184** (1) Every person who, by means of any electro-magnetic, acoustic, mechanical or other device, knowingly intercepts a private communication is

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	guilty of (a) an indictable offence and liable to imprisonment for a term of not more than five years; or (b) an offence punishable on summary conviction. Marginal note:Saving provision (2) Subsection (1) does not apply to (a) a person who has the consent to intercept, express or implied, of the originator of the private communication or of the person intended by the originator thereof to receive it; (b) a person who intercepts a private communication in accordance with an authorization or pursuant to section 184.4 or any person who in good faith aids in any way another person who the aiding person believes on reasonable grounds is acting with an authorization or pursuant to section 184.4; (c) a person engaged in providing a telephone, telegraph or other communication service to the public who intercepts a private communication, (i) if the interception is necessary for the purpose of providing the service, (ii) in the course of service observing or random monitoring necessary for the purpose of mechanical or service quality control checks, or (iii) if the interception is necessary to protect the person’s rights or property directly related to providing the service; (d) an officer or servant of Her Majesty in right of Canada who engages in radio frequency spectrum management, in respect of a private communication intercepted by that officer or servant for the purpose of identifying, isolating or preventing an unauthorized or interfering use of a frequency or of a transmission; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(e) a person, or any person acting on their behalf, in possession or control of a computer system, as defined in subsection 342.1(2), who intercepts a private communication originating from, directed to or transmitting through that computer system, if the interception is reasonably necessary for (i) managing the quality of service of the computer system as it relates to performance factors such as the responsiveness and capacity of the system as well as the integrity and availability of the system and data, or (ii) protecting the computer system against any act that would be an offence under subsection 342.1(1) or 430(1.1).
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.	**Criminal Code** **Mischief in relation to computer data** **430** (1.1) Everyone commits mischief who wilfully (a) destroys or alters computer data; (b) renders computer data meaningless, useless or ineffective; (c) obstructs, interrupts or interferes with the lawful use of computer data; or (d) obstructs, interrupts or interferes with a person in the lawful use of computer data or denies access to computer data to a person who is entitled to access to it.
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	
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	**Criminal Code** **Unauthorized use of computer** **342.1** (1) Everyone is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years, or is guilty of an offence punishable on

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	summary conviction who, fraudulently and without colour of right, (a) obtains, directly or indirectly, any computer service; (b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system; (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or under section 430 in relation to computer data or a computer system; or (d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c).
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Criminal Code** **Identity fraud** **403** (1) Everyone commits an offence who fraudulently personates another person, living or dead, (a) with intent to gain advantage for themselves or another person; (b) with intent to obtain any property or an interest in any property; (c) with intent to cause disadvantage to the person being personated or another person; or (d) with intent to avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice. Marginal note:Clarification (2) For the purposes of subsection (1), personating a person includes pretending to be the person or using the person's identity information — whether by itself or in combination with identity information pertaining to any person — as if it pertains to the person using it. Marginal note:Punishment (3) Everyone who commits an offence under subsection (1) (a) is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years; or (b) is guilty of an offence punishable on summary conviction.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography	**Criminal Code**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	**Definition of child pornography** **163.1** (1) In this section, child pornography means (a) a photographic, film, video or other visual representation, whether or not it was made by electronic or mechanical means, (i) that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity, or (ii) the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region of a person under the age of eighteen years; (b) any written material, visual representation or audio recording that advocates or counsels sexual activity with a person under the age of eighteen years that would be an offence under this Act; (c) any written material whose dominant characteristic is the description, for a sexual purpose, of sexual activity with a person under the age of eighteen years that would be an offence under this Act; or (d) any audio recording that has as its dominant characteristic the description, presentation or representation, for a sexual purpose, of sexual activity with a person under the age of eighteen years that would be an offence under this Act. Marginal note:Making child pornography (2) Every person who makes, prints, publishes or possesses for the purpose of publication any child pornography is guilty of an indictable offence and liable to imprisonment for a term of not more than 14 years and to a minimum punishment of imprisonment for a term of one year. Marginal note:Distribution, etc. of child pornography

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) Every person who transmits, makes available, distributes, sells, advertises, imports, exports or possesses for the purpose of transmission, making available, distribution, sale, advertising or exportation any child pornography is guilty of an indictable offence and liable to imprisonment for a term of not more than 14 years and to a minimum punishment of imprisonment for a term of one year. Marginal note:Possession of child pornography (4) Every person who possesses any child pornography is guilty of (a) an indictable offence and is liable to imprisonment for a term of not more than 10 years and to a minimum punishment of imprisonment for a term of one year; or (b) an offence punishable on summary conviction and is liable to imprisonment for a term of not more than two years less a day and to a minimum punishment of imprisonment for a term of six months. Marginal note:Accessing child pornography (4.1) Every person who accesses any child pornography is guilty of (a) an indictable offence and is liable to imprisonment for a term of not more than 10 years and to a minimum punishment of imprisonment for a term of one year; or (b) an offence punishable on summary conviction and is liable to imprisonment for a term of not more than two years less a day and to a minimum punishment of imprisonment for a term of six months. Marginal note:Interpretation (4.2) For the purposes of subsection (4.1), a person accesses child pornography who knowingly causes child pornography to be viewed by, or transmitted to, himself or herself.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Marginal note:Aggravating factor (4.3) If a person is convicted of an offence under this section, the court that imposes the sentence shall consider as an aggravating factor the fact that the person committed the offence with intent to make a profit. Marginal note:Defence (5) It is not a defence to a charge under subsection (2) in respect of a visual representation that the accused believed that a person shown in the representation that is alleged to constitute child pornography was or was depicted as being eighteen years of age or more unless the accused took all reasonable steps to ascertain the age of that person and took all reasonable steps to ensure that, where the person was eighteen years of age or more, the representation did not depict that person as being under the age of eighteen years. Marginal note:Defence (6) No person shall be convicted of an offence under this section if the act that is alleged to constitute the offence (a) has a legitimate purpose related to the administration of justice or to science, medicine, education or art; and (b) does not pose an undue risk of harm to persons under the age of eighteen years. Marginal note:Question of law (7) For greater certainty, for the purposes of this section, it is a question of law whether any written material, visual representation or audio recording advocates or counsels sexual activity with a person under the age of eighteen years that would be an offence under this Act.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	**Criminal Code** **Forgery of Trademarks and Trade Descriptions** **406** For the purposes of this Part, every one forges a trademark who (a) without the consent of the proprietor of the trademark, makes or reproduces in any manner that trademark or a mark so nearly resembling it as to be calculated to deceive; or (b) falsifies, in any manner, a genuine trademark. R.S., 1985, c. C-46, s. 4062014, c. 20, s. 366(E) Previous Version Marginal note:Offence 407 Every one commits an offence who, with intent to deceive or defraud the public or any person, whether ascertained or not, forges a trademark. R.S., 1985, c. C-46, s. 4072014, c. 20, s. 366(E) Previous Version Marginal note:Passing off 408 Every one commits an offence who, with intent to deceive or defraud the public or any person, whether ascertained or not, (a) passes off other wares or services as and for those ordered or required; or (b) makes use, in association with wares or services, of any description that is false in a material respect regarding (i) the kind, quality, quantity or composition, (ii) the geographical origin, or (iii) the mode of the manufacture, production or performance of those wares or services.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	R.S., 1985, c. C-46, s. 4081992, c. 1, s. 60(F) Marginal note:Instruments for forging trademark 409 (1) Every one commits an offence who makes, has in his possession or disposes of a die, block, machine or other instrument designed or intended to be used in forging a trademark. Marginal note:Saving (2) No person shall be convicted of an offence under this section where he proves that he acted in good faith in the ordinary course of his business or employment. R.S., 1985, c. C-46, s. 4092014, c. 20, s. 366(E) Previous Version Marginal note:Other offences in relation to trademarks 410 Every one commits an offence who, with intent to deceive or defraud, (a) defaces, conceals or removes a trademark or the name of another person from anything without the consent of that other person; or (b) being a manufacturer, dealer, trader or bottler, fills any bottle or siphon that bears the trademark or name of another person, without the consent of that other person, with a beverage, milk, by-product of milk or other liquid commodity for the purpose of sale or traffic.
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,	**Criminal Code** **PART XIII** **Attempts — Conspiracies — Accessories** **463** Except where otherwise expressly provided by law, the following provisions apply in respect of persons who attempt to commit or are accessories after the fact to the commission of offences: (a) every one who attempts to commit or is an accessory after the fact to the commission of an indictable offence for which, on conviction, an accused is liable to be sentenced to imprisonment for life is guilty of an indictable offence and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
paragraph 2 of this article.	liable to imprisonment for a term not exceeding fourteen years; (b) every one who attempts to commit or is an accessory after the fact to the commission of an indictable offence for which, on conviction, an accused is liable to imprisonment for fourteen years or less is guilty of an indictable offence and liable to imprisonment for a term that is one-half of the longest term to which a person who is guilty of that offence is liable; (c) every one who attempts to commit or is an accessory after the fact to the commission of an offence punishable on summary conviction is guilty of an offence punishable on summary conviction; and (d) every one who attempts to commit or is an accessory after the fact to the commission of an offence for which the offender may be prosecuted by indictment or for which he is punishable on summary conviction (i) is guilty of an indictable offence and liable to imprisonment for a term not exceeding a term that is one-half of the longest term to which a person who is guilty of that offence is liable, or (ii) is guilty of an offence punishable on summary conviction. R.S., 1985, c. C-46, s. 463R.S., 1985, c. 27 (1st Supp.), s. 591998, c. 35, s. 120 Marginal note:Counselling offence that is not committed 464 Except where otherwise expressly provided by law, the following provisions apply in respect of persons who counsel other persons to commit offences, namely, (a) every one who counsels another person to commit an indictable offence is, if the offence is not committed, guilty of an indictable offence and liable to the same punishment to which a person who attempts to commit that offence is liable; and (b) every one who counsels another person to commit an offence punishable on summary conviction is, if the offence is not committed, guilty of an offence

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	punishable on summary conviction. R.S., 1985, c. C-46, s. 464R.S., 1985, c. 27 (1st Supp.), s. 60 Marginal note:Conspiracy 465 (1) Except where otherwise expressly provided by law, the following provisions apply in respect of conspiracy: (a) every one who conspires with any one to commit murder or to cause another person to be murdered, whether in Canada or not, is guilty of an indictable offence and liable to a maximum term of imprisonment for life; (b) every one who conspires with any one to prosecute a person for an alleged offence, knowing that they did not commit that offence, is guilty of (i) an indictable offence and liable to imprisonment for a term of not more than 10 years or an offence punishable on summary conviction, if the alleged offence is one for which, on conviction, that person would be liable to be sentenced to imprisonment for life or for a term of not more than 14 years, or (ii) an indictable offence and liable to imprisonment for a term of not more than five years or an offence punishable on summary conviction, if the alleged offence is one for which, on conviction, that person would be liable to imprisonment for less than 14 years; (c) every one who conspires with any one to commit an indictable offence not provided for in paragraph (a) or (b) is guilty of an indictable offence and liable to the same punishment as that to which an accused who is guilty of that offence would, on conviction, be liable; and (d) every one who conspires with any one to commit an offence punishable on summary conviction is guilty of an offence punishable on summary conviction. (2) [Repealed, 1985, c. 27 (1st Supp.), s. 61] Marginal note:Conspiracy to commit offences

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) Every one who, while in Canada, conspires with any one to do anything referred to in subsection (1) in a place outside Canada that is an offence under the laws of that place shall be deemed to have conspired to do that thing in Canada. Marginal note:Idem (4) Every one who, while in a place outside Canada, conspires with any one to do anything referred to in subsection (1) in Canada shall be deemed to have conspired in Canada to do that thing.
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
criminal or non-criminal sanctions or measures, including monetary sanctions.	
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its	**Criminal Code** **Preservation order — computer data** 487.013 (1) On ex parte application made by a peace officer or public officer, a justice or judge may order a person to preserve computer data that is in their possession or control when they receive the order. Marginal note:Conditions for making order (2) Before making the order, the justice or judge must be satisfied by information on oath in Form 5.002 (a) that there are reasonable grounds to suspect that an offence has been or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	will be committed under this or any other Act of Parliament or has been committed under a law of a foreign state, that the computer data is in the person's possession or control and that it will assist in the investigation of the offence; and (b) that a peace officer or public officer intends to apply or has applied for a warrant or an order in connection with the investigation to obtain a document that contains the computer data. Marginal note:Offence against law of foreign state (3) If an offence has been committed under a law of a foreign state, the justice or judge must also be satisfied that a person or authority with responsibility in that state for the investigation of such offences is conducting the investigation.
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.	
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	**Criminal Code** **General production order** 487.014 (1) Subject to sections 487.015 to 487.018, on ex parte application made by a peace officer or public officer, a justice or judge may order a person to produce a document that is a copy of a document that is in their possession

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	or control when they receive the order, or to prepare and produce a document containing data that is in their possession or control at that time. Marginal note:Conditions for making order (2) Before making the order, the justice or judge must be satisfied by information on oath in Form 5.004 that there are reasonable grounds to believe that (a) an offence has been or will be committed under this or any other Act of Parliament; and (b) the document or data is in the person's possession or control and will afford evidence respecting the commission of the offence. Marginal note:Form (3) The order is to be in Form 5.005. Marginal note:Limitation (4) A person who is under investigation for the offence referred to in subsection (2) may not be made subject to an order. 2004, c. 3, s. 72014, c. 31, s. 20 Previous Version Marginal note:Production order to trace specified communication 487.015 (1) On ex parte application made by a peace officer or public officer for the purpose of identifying a device or person involved in the transmission of a communication, a justice or judge may order a person to prepare and produce a document containing transmission data that is related to that purpose and that is, when they are served with the order, in their possession or control. Marginal note:Conditions for making order (2) Before making the order, the justice or judge must be satisfied by

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	information on oath in Form 5.004 that there are reasonable grounds to suspect that (a) an offence has been or will be committed under this or any other Act of Parliament; (b) the identification of a device or person involved in the transmission of a communication will assist in the investigation of the offence; and (c) transmission data that is in the possession or control of one or more persons whose identity is unknown when the application is made will enable that identification. Marginal note:Form (3) The order is to be in Form 5.006. Marginal note:Service (4) A peace officer or public officer may serve the order on any person who was involved in the transmission of the communication and whose identity was unknown when the application was made (a) within 60 days after the day on which the order is made; or (b) within one year after the day on which the order is made, in the case of an offence under section 467.11, 467.12 or 467.13, an offence committed for the benefit of, at the direction of or in association with a criminal organization, or a terrorism offence. Marginal note:Limitation (5) A person who is under investigation for the offence referred to in subsection (2) may not be made subject to an order. Marginal note:Report

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(6) A peace officer or public officer named in the order must provide a written report to the justice or judge who made the order as soon as feasible after the person from whom the communication originated is identified or after the expiry of the period referred to in subsection (4), whichever occurs first. The report must state the name and address of each person on whom the order was served, and the date of service. 2004, c. 3, s. 72014, c. 31, s. 20 Previous Version Marginal note:Production order — transmission data 487.016 (1) On ex parte application made by a peace officer or public officer, a justice or judge may order a person to prepare and produce a document containing transmission data that is in their possession or control when they receive the order. Marginal note:Conditions for making order (2) Before making the order, the justice or judge must be satisfied by information on oath in Form 5.004 that there are reasonable grounds to suspect that (a) an offence has been or will be committed under this or any other Act of Parliament; and (b) the transmission data is in the person’s possession or control and will assist in the investigation of the offence. Marginal note:Form (3) The order is to be in Form 5.007. Marginal note:Limitation (4) A person who is under investigation for the offence referred to in subsection (2) may not be made subject to an order.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	2004, c. 3, s. 72014, c. 31, s. 20 Previous Version Marginal note:Production order — tracking data 487.017 (1) On ex parte application made by a peace officer or public officer, a justice or judge may order a person to prepare and produce a document containing tracking data that is in their possession or control when they receive the order. Marginal note:Conditions for making order (2) Before making the order, the justice or judge must be satisfied by information on oath in Form 5.004 that there are reasonable grounds to suspect that (a) an offence has been or will be committed under this or any other Act of Parliament; and (b) the tracking data is in the person's possession or control and will assist in the investigation of the offence. Marginal note:Form (3) The order is to be in Form 5.007. Marginal note:Limitation (4) A person who is under investigation for the offence referred to in subsection (2) may not be made subject to an order. 2004, c. 3, s. 72014, c. 31, s. 20 Previous Version Marginal note:Production order — financial data 487.018 (1) On ex parte application made by a peace officer or public officer, a justice or judge may order a financial institution, as defined in section 2 of the Bank Act, or a person or entity referred to in section 5 of the Proceeds of Crime

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(Money Laundering) and Terrorist Financing Act, to prepare and produce a document setting out the following data that is in their possession or control when they receive the order: (a) either the account number of a person named in the order or the name of a person whose account number is specified in the order; (b) the type of account; (c) the status of the account; and (d) the date on which it was opened or closed. Marginal note:Identification of person (2) For the purpose of confirming the identity of a person who is named or whose account number is specified in the order, the order may also require the institution, person or entity to prepare and produce a document setting out the following data that is in their possession or control: (a) the date of birth of a person who is named or whose account number is specified in the order; (b) that person’s current address; and (c) any previous addresses of that person. Marginal note:Conditions for making order (3) Before making the order, the justice or judge must be satisfied by information on oath in Form 5.004 that there are reasonable grounds to suspect that (a) an offence has been or will be committed under this or any other Act of Parliament; and (b) the data is in the possession or control of the institution, person or entity

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	and will assist in the investigation of the offence. Marginal note:Form (4) The order is to be in Form 5.008. Marginal note:Limitation (5) A financial institution, person or entity that is under investigation for the offence referred to in subsection (3) may not be made subject to an order.
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	**Criminal Code** **Information for search warrant** **487** Operation of computer system and copying equipment (2.1) A person authorized under this section to search a computer system in a building or place for data may (a) use or cause to be used any computer system at the building or place to search any data contained in or available to the computer system; (b) reproduce or cause to be reproduced any data in the form of a print-out or other intelligible output; (c) seize the print-out or other output for examination or copying; and (d) use or cause to be used any copying equipment at the place to make copies of the data. Marginal note:Duty of person in possession or control (2.2) Every person who is in possession or control of any building or place in respect of which a search is carried out under this section shall, on presentation of the warrant, permit the person carrying out the search

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(a) to use or cause to be used any computer system at the building or place in order to search any data contained in or available to the computer system for data that the person is authorized by this section to search for; (b) to obtain a hard copy of the data and to seize it; and (c) to use or cause to be used any copying equipment at the place to make copies of the data. **487.01** (1) A provincial court judge, a judge of a superior court of criminal jurisdiction or a judge as defined in section 552 may issue a warrant in writing authorizing a peace officer to, subject to this section, use any device or investigative technique or procedure or do any thing described in the warrant that would, if not authorized, constitute an unreasonable search or seizure in respect of a person or a person's property if (a) the judge is satisfied by information on oath in writing that there are reasonable grounds to believe that an offence against this or any other Act of Parliament has been or will be committed and that information concerning the offence will be obtained through the use of the technique, procedure or device or the doing of the thing; (b) the judge is satisfied that it is in the best interests of the administration of justice to issue the warrant; and (c) there is no other provision in this or any other Act of Parliament that would provide for a warrant, authorization or order permitting the technique, procedure or device to be used or the thing to be done.
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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: 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	**Criminal Code** **Interception of Communications** **Marginal note:Interception** **184** (1) Every person who, by means of any electro-magnetic, acoustic, mechanical or other device, knowingly intercepts a private communication is guilty of (a) an indictable offence and liable to imprisonment for a term of not more than five years; or (b) an offence punishable on summary conviction. Marginal note:Saving provision

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(2) Subsection (1) does not apply to (a) a person who has the consent to intercept, express or implied, of the originator of the private communication or of the person intended by the originator thereof to receive it; (b) a person who intercepts a private communication in accordance with an authorization or pursuant to section 184.4 or any person who in good faith aids in any way another person who the aiding person believes on reasonable grounds is acting with an authorization or pursuant to section 184.4; (c) a person engaged in providing a telephone, telegraph or other communication service to the public who intercepts a private communication, (i) if the interception is necessary for the purpose of providing the service, (ii) in the course of service observing or random monitoring necessary for the purpose of mechanical or service quality control checks, or (iii) if the interception is necessary to protect the person's rights or property directly related to providing the service; (d) an officer or servant of Her Majesty in right of Canada who engages in radio frequency spectrum management, in respect of a private communication intercepted by that officer or servant for the purpose of identifying, isolating or preventing an unauthorized or interfering use of a frequency or of a transmission; or (e) a person, or any person acting on their behalf, in possession or control of a computer system, as defined in subsection 342.1(2), who intercepts a private communication originating from, directed to or transmitting through that computer system, if the interception is reasonably necessary for (i) managing the quality of service of the computer system as it relates to performance factors such as the responsiveness and capacity of the system as well as the integrity and availability of the system and data, or (ii) protecting the computer system against any act that would be an offence

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	under subsection 342.1(1) or 430(1.1). Marginal note:Use or retention (3) A private communication intercepted by a person referred to in paragraph (2)(e) can be used or retained only if (a) it is essential to identify, isolate or prevent harm to the computer system; or (b) it is to be disclosed in circumstances referred to in subsection 193(2). R.S., 1985, c. C-46, s. 1841993, c. 40, s. 32004, c. 12, s. 42019, c. 25, s. 64 Previous Version Marginal note:Interception to prevent bodily harm 184.1 (1) An agent of the state may intercept, by means of any electro-magnetic, acoustic, mechanical or other device, a private communication if (a) either the originator of the private communication or the person intended by the originator to receive it has consented to the interception; (b) the agent of the state believes on reasonable grounds that there is a risk of bodily harm to the person who consented to the interception; and (c) the purpose of the interception is to prevent the bodily harm. Marginal note:Admissibility of intercepted communication (2) The contents of a private communication that is obtained from an interception pursuant to subsection (1) are inadmissible as evidence except for the purposes of proceedings in which actual, attempted or threatened bodily harm is alleged, including proceedings in respect of an application for an authorization under this Part or in respect of a search warrant or a warrant for the arrest of any person. Marginal note:Destruction of recordings and transcripts (3) The agent of the state who intercepts a private communication pursuant to

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	subsection (1) shall, as soon as is practicable in the circumstances, destroy any recording of the private communication that is obtained from an interception pursuant to subsection (1), any full or partial transcript of the recording and any notes made by that agent of the private communication if nothing in the private communication suggests that bodily harm, attempted bodily harm or threatened bodily harm has occurred or is likely to occur. Definition of agent of the state (4) For the purposes of this section, agent of the state means (a) a peace officer; and (b) a person acting under the authority of, or in cooperation with, a peace officer. 1993, c. 40, s. 4 Marginal note:Interception with consent 184.2 (1) A person may intercept, by means of any electro-magnetic, acoustic, mechanical or other device, a private communication where either the originator of the private communication or the person intended by the originator to receive it has consented to the interception and an authorization has been obtained pursuant to subsection (3). Marginal note:Application for authorization (2) An application for an authorization under this section shall be made by a peace officer, or a public officer who has been appointed or designated to administer or enforce any federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament, ex parte and in writing to a provincial court judge, a judge of a superior court of criminal jurisdiction or a judge as defined in section 552, and shall be accompanied by an affidavit, which may be sworn on the information and belief of that peace officer or public officer or of any other peace officer or public officer, deposing to the following matters: (a) that there are reasonable grounds to believe that an offence against this or any other Act of Parliament has been or will be committed;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) the particulars of the offence; (c) the name of the person who has consented to the interception; (d) the period for which the authorization is requested; and (e) in the case of an application for an authorization where an authorization has previously been granted under this section or section 186, the particulars of the authorization. Marginal note:Judge to be satisfied (3) An authorization may be given under this section if the judge to whom the application is made is satisfied that (a) there are reasonable grounds to believe that an offence against this or any other Act of Parliament has been or will be committed; (b) either the originator of the private communication or the person intended by the originator to receive it has consented to the interception; and (c) there are reasonable grounds to believe that information concerning the offence referred to in paragraph (a) will be obtained through the interception sought. Marginal note:Content and limitation of authorization (4) An authorization given under this section shall (a) state the offence in respect of which private communications may be intercepted; (b) state the type of private communication that may be intercepted; (c) state the identity of the persons, if known, whose private communications are to be intercepted, generally describe the place at which private communications may be intercepted, if a general description of that place can be

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	given, and generally describe the manner of interception that may be used; (d) contain the terms and conditions that the judge considers advisable in the public interest; and (e) be valid for the period, not exceeding sixty days, set out therein. Marginal note:Related warrant or order (5) A judge who gives an authorization under this section may, at the same time, issue a warrant or make an order under any of sections 487, 487.01, 487.014 to 487.018, 487.02, 492.1 and 492.2 if the judge is of the opinion that the requested warrant or order is related to the execution of the authorization.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence,	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; 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

Back to the Table of Contents