Sri Lanka

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Version 27.03.2020

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:	28/05/2015

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 CRIME ACT, No. 24 OF 2007** **Interpretation** 38. In this Act, unless the context otherwise requires, — "computer" means an electronic or similar device having information processing capabilities; "storage medium" means any [electronic or similar device] from which information is capable of being reproduced, with or without the aid of any other article or device; "computer programme" means a set of instructions expressed in words, codes, schemes or any other form, which is capable when incorporated in a medium that the computer can read, of causing a computer to perform or achieve a particular task ; "computer system" means a computer or group of interconnected computers, including the internet; "document" includes an electronic record; "electronic record" means, information, record or data generated, stored, received or sent in an electronic form or microfilm, or by any other similar means; "function" in relation to a computer, includes logic, control or carrying out of an arithmetical process, deletion, storage and retrieval and communication to or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	within a computer; "information" includes data, text, images, sound, codes, computer programmes, databases or microfilm; "service provider" means — (a) a public or private entity which provides the ability for its customers to communicate by means of a computer system; and (b) any other entity that processes or stores computer data or information on behalf of that entity or its customers; "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; "traffic data" means data — (a) that relates to the attributes of a communication by means of a computer system; (b) data generated by a computer system that is part of a service provider; and (c) which shows communications origin, destination, route, time, data, size, duration or details of subscriber information.
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	**COMPUTER CRIME ACT, No. 24 OF 2007** **PART I - COMPUTER CRIME** **Securing unauthorised access to a computer an offence.** 3. Any person who intentionally does any act, in order to secure for himself or for any other person, access to —

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
to another computer system.	(a) any computer ; or (b) any information held in any computer, knowing or having reason to believe that he has no lawful authority to secure such access, shall be guilty of an offence and shall on conviction be liable to a fine not exceeding one hundred thousand rupees, or to imprisonment of either description for a term which may extend to five years, or both such fine and imprisonment. Doing any act to secure unauthorised access in order to commit an offence 4. Any person who intentionally does any act, in order to secure for himself or for any other person, access to — (a) any computer ; or (b) any information held in any computer, knowing or having reason to believe that he has no lawful authority to secure such access and with the intention of committing an offence under this Act or any other law for the time being in force, shall be guilty of an offence and shall on conviction be liable to a fine not exceeding two hundred thousand rupees or to imprisonment of either description for a term which may extend to five years or to both such fine and imprisonment. Explanation 1— for the purposes of paragraph (a) the mere turning on of a computer is sufficient. Explanation 2 — for the purposes of paragraph (b) — (a) there should be an intention to secure any programme or data held in any computer; (b) the access intended to be secured, should be unauthorised;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(c) it is not necessary to have access directed at any particular programme, data or computer.
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 CRIME ACT, No. 24 OF 2007** **Illegal interception of data an offence.** 8. Any person, who, knowingly or without lawful authority intercepts — (a) any subscriber information or traffic data or any communication, to, from or within a computer ; or (b) any electromagnetic emissions from a computer that carries any information, shall be guilty of an offence and shall on conviction be liable to a fine not less than one hundred thousand rupees and not exceeding three hundred thousand rupees or to imprisonment of either description for a term not less than six months and not exceeding three years, or to both such fine and imprisonment.
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 CRIME ACT, No. 24 OF 2007** **Causing a computer to perform a function without lawful authority an offence.** 5. Any person who, intentionally and without lawful authority causes a computer to perform any function knowing or having reason to believe that such function will result in unauthorised modification or damage or potential damage to any computer or computer system or computer programme shall be guilty of an offence and shall on conviction be liable to a fine not exceeding three hundred thousand rupees or to imprisonment of either description for as term which may extend to five years or to both such fine and imprisonment. **Illustrations** For any unauthorised modification or damage or potential damage to any computer or computer system or computer programme to take place, any one of the following may occur: —

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) impairing the operation of any computer, computer system or the reliability of any data or information held in any computer; or (b) destroying, deleting or corrupting, or adding, moving or altering any information held in any computer; (c) makes use of a computer service involving computer time and data processing for the storage or retrieval of data; (d) introduces a computer program which will have the effect of malfunctioning of a computer or falsifies the data or any information held in any computer or computer system. Explanation- for the purposes of paragraphs (a) to (d) above, it is immaterial whether the consequences referred to therein were of a temporary or permanent nature.
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	**See Section 5 of the Computer Crime Act, No. 24 of 2007 above.** **COMPUTER CRIME ACT, No. 24 OF 2007** **Offences committed against national security &c.** 6. (1) Any person who intentionally causes a computer to perform any function, knowing or having reason to believe that such function will result in danger or imminent danger to — (a) national security ; (b) the national economy ; or (c) public order, shall be guilty of an offence and shall on conviction be punishable with imprisonment of either description for a term not exceeding five years. (2) In a prosecution for an offence under paragraphs (a) or (c) of subsection (1), a Certificate under the hand of the Secretary to the Ministry of the Minister

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	in charge of the subject of Defence or, in a prosecution for an offence under paragraph (b) of subsection (1), a Certificate under the hand of the Secretary to the Ministry of the Minister in charge of the subject of Finance, stating respectively, that the situation envisaged in subsection (1) did in fact exist in relation to national security or public order, or the national economy, as the case may be, shall be admissible in evidence and shall be prima facie evidence of the facts stated therein.
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 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.	**COMPUTER CRIME ACT, No. 24 OF 2007** **Dealing with data &c., unlawfully obtained an offence.** 7. Any person who, knowing or having reason to believe that any other person has without lawful authority obtained information from a computer or a storage medium of a computer,— (a) buys, receives, retains, sells, or in any manner deals with ; or (b) offers to buy or sell, or in any manner deals with ; or (c) downloads, uploads, copies or acquires the substance or meaning of, any such information shall be guilty of an offence and shall on conviction be liable to a fine not less than one hundred thousand rupees and not exceeding three hundred thousand rupees or to imprisonment of either description for a term not less than six months and not exceeding three years, or to both such fine and imprisonment. Explanation — For the purposes of sections 9 and 10 — (a) It is immaterial that the offender had authority to access the computer or had authority to perform the function; (b) The offender need not have intended to cause or have had the knowledge that he is likely to cause, loss or damage to any particular person or institution.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Using of illegal devices an offence. 9. Any person who, without lawful authority produces, sells, procures for use, imports, exports, distributes or otherwise makes available — (a) any device, including a computer or computer program; (b) a computer password, access code or similar information by which the whole or any part of a computer is capable of being accessed, with the intent that it be used by any person for the purpose of committing an offence under this Act shall be guilty of an offence and shall on conviction be liable to a fine not less than one hundred thousand rupees and not exceeding three hundred thousand rupees or to imprisonment of either description for a term not less than six months and not exceeding three years, or to both such fine and imprisonment. **Unauthorised disclosure of information enabling access to a service, an offence.** 10. Any person who, being entrusted with information which enables him to access any service provided by means of a computer, discloses such information without any express authority to do so or in breach of any contract expressed or implied, shall be guilty of an offence and shall on conviction be liable to a fine not less than one hundred thousand rupees and not exceeding three hundred thousand rupees or to imprisonment of either description for a term not less than six months and not exceeding three years or to both such fine and imprisonment.
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	.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	
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.	**PAYMENT DEVICES FRAUDS ACT, No. 30 OF 2006** **Printed on the Order of Government [Certified on 12th September, 2006]** An Act to Prevent the Possession and Use of unauthorised or Counterfeit Payment Devices; to Create Offences Connected with the Possession or Use of Unauthorised Payment Devices; To Protect Persons Lawfully Issuing And Using Such Payment Devices ; To Make Provision For The Investigation, Prosecution And Punishment Of Offenders; and to Provide for Matters Connected therewith or Incidental Thereto 3. (1) Any person who — (a) possesses or has in the control or custody of such person without lawful authority, equipment used for the making or altering of payment devices including an embossing, encoding or skimming device; (b) without lawful authority, tampers with any payment device or card making or altering equipment or any equipment used for acceptance or processing of payment devices or implants foreign objects including chips, data or voice recording devices, to record transaction data; (c) uses without lawful authority a phone listening device or other similar device, including any voice or data recording device, for the purpose of capturing authorization data passing through the acquirer’s point of sale networks or automated teller machine network; (d) being an employees of an Issuer or its processors or is a service provider, provides any cardholder information or full track data to unauthorized individuals, groups or syndicates without the payment device holder’s authority or permission;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(e) possesses or has in his control or custody, any unauthorised or counterfeit payment device; (f) makes a fraudulent application for a payment device or a fraudulent merchant application; (g) uses, produces or trafficks in one or more unauthorised or counterfeit payment devices; (h) uses an unauthorized payment device or a payment device without obtaining permission therefor from either its, Issuer or holder; (i) generates, valid payment device account numbers, using account generating software for the purpose of utilizing such account numbers for committing an offence under this or any other written law; (j) furnishes for the purpose of obtaining goods or services, information contained in any payment device by telephone, facsimile, email internet or other mode of telecommunication or by voice or through the postal service, without the authority or permission of the holder of the payment device and induces the person receiving the information to accept the information for the supply of goods or services; (k) makes multiple imprints of a transaction record, sales invoice or similar document, thereby making it appear that the payment device holder has entered into transactions other than those which such payment device holder had lawfully contracted for; (l) knowing that a payment device is unauthorised or counterfeit, accepts such unauthorised or counterfeit payment device as a mode of payment for goods or services; (m) submits without being an affiliated merchant, an order to collect from the Issuer of the payment device, such transaction record, sales invoice or similar

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	document through an affiliated merchant who connives therewith, or under the false pretence of being an affiliated merchant, presents for collection such transaction record, sales invoice or similar document; (n) alters or causes another person to alter, without the payment device holder's authority or permission, any amount or other information appearing on the sales invoice; (o) accepts as a mode of payment, a payment device or information imprinted on the payment device, for the purpose of dishonestly gaining a financial advantage; (p) writes, or causes to be written on sales invoices, approval numbers from the Issuer of the payment device, which is proof of the fact of approval, where in fact no such approval was given, or where, if approval was actually given what is written is deliberately different therefrom; (q) has in such person's possession, without authority from the payment device holder or the Issuer, any material such as invoices, carbon paper or any other medium, on which the payment device is written, printed, embossed or otherwise indicated; (r) obtains money or goods through the use of a payment device, with intent to defraud; or (s) induces, entices, permits or in any manner allows another person, for consideration or otherwise, to commit or engage in any of the acts specified in the preceding paragraphs of this section, shall be guilty of an offence under this Act. (2) A person guilty of an offence under this Act shall, on conviction after trial before the High Court — (i) in the case of an offence under paragraphs (a), (b). (c), (d), (e), (g), (h), (i),

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(j) or (r) be liable to a term of imprisonment not exceeding ten years or to a fine not exceeding rupees five hundred thousand or to both such imprisonment and fine; (ii) in the case of an offence under paragraphs (k) or (q) be liable to a term of imprisonment not exceeding five years or to a fine not exceeding two hundred thousand rupees or to both such imprisonment and fine; (iii) in the case of an offence under paragraphs (f), (l), (m), (n), (o) or (p) be liable to a term of imprisonment not exceeding three years or to a fine not exceeding one hundred thousand rupees or to a fine which may extend to five times the value of the money obtained by the commission of the act constituting the offence or the financial advantage gained, consequent to the commision of the act constituting the offence, whichever is higher, or to both such imprisonment and fine; (iv) in the case of an offence under paragraph (s) be liable to one and half times the punishment prescribed for the offence which the offender induces, entices, permits or allows another person to commit.
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: 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.	**Penal Code** **Obscene publication, exhibition&c. relating to children. [§2,22 of 1995.]** 286A.(1) Any person who - (a) hires, employs, assists, persuades, uses, induces or coerces, any child to appear or perform, in any obscene or indecent exhibition or show or to pose or model for, or to appear in, any obscene or indecent photograph or film or who sell or distributes, or otherwise publishes, or has in his possession, any such photograph or film; or (b) being the parent, guardian or person having the custody of, a child, causes or allows such child to be employed, or to participate, in any obscene or indecent exhibition or show or to pose or model for, or to appear in, any such photograph or film as is referred to in paragraph (a);

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(c) (i) takes, or assists in taking of any indecent photograph of a child; or (ii) distributes or shows any such photograph or any publication containing such photograph; (iii) has in his possession for distribution or showing, any such photograph or publication; iv) publishers or cause to be published, any such photograph or publishes or causes to be published, any advertisement capable of conveying the message that the advertiser or person named in the advertisement distributes or shows any such photograph or publication or intends to do so commits of obscene publication and exhibition relating to children and shall on conviction be punished with imprisonment of either description for a term not less than two years and not exceeding ten years and may also be punished with fine. 2) Any person who, being a developer of photographs or films, discovers that any photograph or film given to him for developing is an indecent or obscene photograph or a film of a child, shall, forthwith on such discovery, inform the officer in charge of the nearest police station that he has in his possession, such photograph or film. (3) Whoever being a developer of photographs or films acts in contravention of the provisions of subsection (2) shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.) (4) in this section - "child " means a person under eighteen years of age; and "film" includes any form of video recording **Penal Code (Amendment) Act, No. 16 Of 2006**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Insertion of new sections 286B and 286C in the principal enactment. 3. The following new sections are hereby inserted immediately after section 286A of the principal enactment and shall have effect as sections 286B and 286c of such enactment : — "Duty of person providing service by computer to prevent sexual abuse of a child. 286B. (1) A person who provides a service by means of a computer shall take all such steps as are necessary to ensure that such computer facility is not used for the commission of an act constituting an offence relating to the sexual abuse of a child. (2) A person referred to in subsection (1) who has knowledge of any such computer facility referred to in subsection (1) being used for the commission of an act constituting an offence relating to the sexual abuse of a child, shall forthwith inform the officer in charge of the nearest police station of such fact and give such information as may be in his possession with regard to such act and the identity of the alleged offender. (3) A person who contravenes the provisions of subsections (1) or (2) shall be guilty of an offence and shall on conviction be liable to imprisonment of either description for a term not exceeding two years or to a fine or to both such imprisonment and fine. (4) In this section, "child" means a person under eighteen years of age. **Penal Code (AMENDMENT) ACT, No. 16 OF 2006** **Duty to inform of use of premises for child abuse.** 286C. (1) Any person who, having the charge, care, control or possession of any premises, has knowledge of such premises being used for the commission of an act constituting the abuse of a child, shall forthwith inform the officer in charge of the nearest police station of such fact.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) Any person referred to in subsection (1) who fails to inform the officer in charge of the nearest police station of the fact that such premises is being used for the commission of an act constituting the abuse of a child shall be guilty of an offence and shall on conviction be liable to imprisonment of either description for a term not exceeding two years or to a fine or to both such imprisonment and fine. "Trafficking. 360C. (1) Whoever — (a) buys, sells or barters or instigates another person to buy, sell or barter any person or does anything to promote, facilitate or induce the buying, selling or bartering of any person for money or other consideration; (b) recruits, transports, transfers, harbours or receives any person or does any other act by the use of threat, force, fraud, deception or inducement or by exploiting the vulnerability of another for the purpose of securing forced or compulsory labour or services, slavery, servitude, the removal of organs, prostitution or other forms of sexual exploitation or any other act which constitutes an offence under any law ; c) recruits, transports, transfers, harbours or receives a child or does any other act whether with or without the consent of such child for the purpose of securing forced or compulsory labour or services, slavery, servitude or the removal of organs, prostitution or other forms of sexual exploitation, or any other act which constitutes an offence under any law, shall be guilty of the offence of trafficking. (2) Any person who is guilty of the offence of trafficking shall on conviction be punished with imprisonment of either description for a term not less than two years and not exceeding twenty years and may also be punished with fine and where such offence is committed in respect of a child, be punished with imprisonment of either description for a term not less than three years and not exceeding twenty years and may also be punished with fine. (3) In this section, —

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	"child" means a person under eighteen years of age; Soliciting a child. 360E. (1) Whoever, whether within Sri Lanka or from outside Sri Lanka solicits by whatever means — (a) a person under eighteen years of age; or (b) any person believing such person to be under eighteen years of age, for the purpose of sexual abuse of a child, commits the offence of soliciting a child and shall on conviction be liable to imprisonment of either description for a term not exceeding ten years or to a fine, or to both such imprisonment and fine."
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	**Intellectual Property Act, No. 36 Of 2003** An Act to Provide for the Law Relating to Intellectual Property and for an Efficient Procedure for the Registration, Control and Administration thereof to Amend The Customs Ordinance (Chapter 235) and the High Court of The Provinces (Special) Provisions Act, No. 10 Of 1996; and to Provide for Matters Connected Therewith or Incidental Thereto 22. (1) Any person who infringes or is about to infringe any of the rights protected under this Part may be prohibited from doing so by way of an injunction and be liable to damages. The owner of such rights is entitled to seek such other remedy as the court may deem fit. (2) (a) The Court shall have power and jurisdiction — (i) to grant such injunctions to prohibit the commission of any act of, infringement or the continued commission of such acts of infringment of any right protected under this Part; (ii) to order the impounding of copies of works or sound recordings suspected of

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	being made sold, rented or imported without the authorization of the owner of any right protected under this Part where the making, selling, renting or importation of copies is subject to such authorization, as well as the impounding of the packaging of, the implements that could be used for the making of, and the documents, accounts or business papers, referring to, such copies. (b) The Court shall in addition have the jurisdiction to order the payment by the infringer, of damages for the loss suffered as a consequence of the act of infringement, as well as the payment of expenses caused by the infringement, including legal costs. The amount of damages shall be fixed taking into account inter alia, the importance of the material and moral prejudice suffered by the owner of the right, as well as the importance of the infringer's profits attributable to the infringement. Where the infringer did not know or had no reasonable cause to know that he or it was engaged in infringing activity, the court may limit damages to the profits of the infringer attributable to the infringement or to pre established damages. (c) The Court shall have the authority to order the destruction or other reasonable manner of disposing of copies made in infringement of any right protected under this Part if available and their packaging outside the channels of commerce in such a manner as would avoid harm to the owner of the rights, unless he requests otherwise. The provisions of this section shall not be applicable to copies and their packaging which were acquired by a third party in good faith. (d) Where there is a danger that implements may be used to commit or continue to commit acts of infringement, the Court shall, whenever and to the extent that it is reasonable, order their destruction or other reasonable manner of disposing of the same outside the channels of commerce in such a manner as to minimize the risks of further infringements, including surrender to the owner of the rights. (e) Where there is a danger that acts of infringement may be continued, the court shall make such orders as may be necessary prevent such acts being committed. (f) The provisions of Chapter XXXV of this Act relating to infringement and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	remedies shall apply, mutatis mutandis, to rights protected under this Part. (g) Any person who infringes or attempts to infringe any of the rights protected under this Part shall be guilty of an offence and on conviction be liable to any penalty as provided for in Chapters XXXVIII and XLI of the Act. (3) (a) The Director-General may on an application being made in the prescribed form and manner by a person aggrieved by any of his rights under this Part being infringed or in any other manner affected, and after such inquiry as he thinks fit determine any question that may be necessary or expedient to determine in connection with such application and such decision shall be binding on the parties subject to the provisions of paragraph (b) of this subsection. (b) Any person aggrieved by the decision of the Director-General may make an appeal to the Court and unless the Court issues an interim order staying the operation of the decision of the Director-General, such decision shall continue to be in force until the matter is decided by the Court. 23. (1) The following acts shall be considered unlawful and in the application of section 22 shall be assimilated to infringements of the rights of the owner of copyright :— (i) the manufacture or importation for sale or rental of any device or means specifically designed or adapted to circumvent any device or means intended to prevent or restrict reproduction of a work or to impair the quality of copies made (the latter device or means hereinafter referred to as "copy protection or copy management device or means"); (ii) the manufacture or importation for sale or rental of any device or means that is susceptible to enable or assist the reception of an encrypted program, which is broadcast or otherwise communicated to the public, including reception by satellite, by those who are not entitled to receive the program. (2) In the application of section 22, any illicit device and means mentioned in subsection (1) of this section shall be assimilated to infringing copies of works.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) The owner of copyright in a work shall also be entitled to the damages for infringement provided for in section 22 where — (a) authorized copies of the work have been made and offered for sale or rental in an electronic form combined with a copy protection or copy management device or means, and a device or means specifically designed or adapted to circumvent the said device or means, made or imported for sale or rental ; (b) the work is authorised for inclusion in an encrypted program, broadcast or otherwise communicated to the public, including by satellite, and a device or means enabling or assisting the reception of the program by those who are not entitled to receive the program made or imported, for sale or rental.
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.	**COMPUTER CRIME ACT, No. 24 OF 2007** **Attempts to commit offence** 11. Any person who attempts to commit an offence under sections 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 and 14 of this Act or to cause such an offence to be committed, shall be guilty of an offence and shall on conviction be liable to a fine not exceeding one half of the maximum fine provided for each of such offences, or to imprisonment of either description for a term not exceeding one half of the maximum term provided for each of such offences, or to both such fine and imprisonment. **Abetment of an offence.** 12. (1) Any person who abets the commission of an offence under this Act shall be guilty of the offence of abetment and shall on conviction — (a) if the offence abetted is committed in consequence of the abetment, be liable to the same punishment as is provided for the offence; and (b) if the offence is not committed in consequence of the abetment, be liable — (i) where the maximum fine or term of imprisonment is provided for, to a fine not exceeding one fourth of the maximum fine provided for the offence or to

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	imprisonment of either description for a term not exceeding one fourth of the maximum term provided for the offence, or to both such fine and imprisonment; and (ii) where the maximum fine or imprisonment is not provided for or the maximum term of imprisonment is life, to a fine not exceeding two hundred and fifty thousand rupees or to imprisonment of either description for a term not exceeding five years, or to both such fine and imprisonment. (2) The term 'abet' shall have the same meaning as in sections 100 and 101 of the Penal Code (Chapter 19) and the provisions of sections 101A, 103, 104, 105, 106 and 107 of the Penal Code (Chapter 19) shall mutatis mutandis apply in relation to the abetment of any offence under this Act. **Conspiring to commit an offence.** 13. (1) Any person who conspires to commit an offence under this Act shall be guilty of an offence and shall, on conviction be liable to be punished with the punishment prescribed for abetting the commission of that offence. (2) The term "conspire" shall have the same meaning as in subsection (2) of section 113A of the Penal Code (Chapter 19) and the provisions of that section shall mutatis mutandis apply in relation to conspiracy to commit any offence under this Act.
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	**COMPUTER CRIME ACT, No. 24 OF 2007** **Offences by bodies of persons.** 30. Where an offence under this Act is committed by a body of persons, then if that body of person is — (a) a body corporate, every director and officer of that body corporate; or (b) a firm, every partner of that firm; or (b) a firm, every partner of that firm; or (c) a body unincorporated other than a firm, every officer of that body responsible for its management and control, shall be deemed to be guilty of

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	such offence: Provided that no such person shall be deemed to be guilty of such offence if he proves that such offence was committed without his knowledge or that he exercised all due diligence to prevent the commission of such 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 CRIME ACT, No. 24 OF 2007** **Compensation to be awarded for loss or damage consequent to an offence.** 14. (1) Where a person is convicted of an offence under this Act, and where it is established that as a result of the commission of such offence — (a) loss or damage was caused to any person or institution; or (b) monetary gain accrued to the offender or any other person, the court shall, in addition to any other punishment that may be imposed on the offender, make order for the payment by the offender — (i) of compensation, to the person or institution that incurred loss or damage; or (ii) of a sum equivalent to the value of the monetary gain so accrued, to the State, as the case may be. (2) An order made under subsection (1) for payment, shall be enforced as if such order was a decree entered by the District Court in favour of the person or institution which suffered the loss or damage or the State, as the case may be. (3) A Certificate under the hand of an expert containing a record of the quantum of compensation as computed by the victim and a statement whether in the opinion of the expert, the quantum of compensation is proportionate to the loss or damage caused or the monetary value of the gain accrued shall be admissible in evidence and shall be prime facie proof of the facts stated therein. (4) An order under subsection (1) for the payment of compensation in favour of

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	any person shall not debar or prejudice any right of that person to a civil remedy for the recovery of damages : Provided however that the time limit specified in the Prescription Ordinance (Chapter 68) for the commencement of any action relating to a civil remedy, shall, for the purposes of this Act, be computed only from the date on which an order under subsection (1) is made.
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	**COMPUTER CRIME ACT, No. 24 OF 2007** **PART II - INVESTIGATIONS** **Offences under this Act to be investigated under the provisions of the Code of Criminal Procedure.** 15. Except as otherwise provided by this Act, all offences under this Act shall be investigated, tried or otherwise dealt with in accordance with the provisions of the Code of Criminal Procedure Act, No. 15 of 1979. **Offence under the Act to be cognizable offence.** 16. Every offence under this Act shall be a cognizable offence within the meaning of, and for the purpose of, the Code of Criminal Procedure Act, No. 15 of 1979. **Appointment of a panel of experts.** 17. (1) The Minister in charge of the subject of Science and Technology may, in consultation with the Minister in charge of the subject of Justice, appoint by Order published in the Gazette any public officer having the required qualification and experience in electronic engineering or software technology (hereinafter referred to as "an expert") to assist any police officer in the investigation of an offence under this Act. (2) For the purposes of this section "expert" includes - (a) any member of the staff of any University who possesses the prescribed qualification and, who is nominated by the Vice-Chancellor of the relevant

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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	University; (b) any public institution which in the opinion of the relevant University possesses the prescribed qualification and is nominated by the Vice-Chancellor of such University: Provided that where an "expert" cannot be identified in terms of paragraph (a) or (b) above the Minister may, in consultation with the Vice-Chancellor of the relevant University appoint any other institution which satisfies the prescribed qualification; (c) University shall mean any University established under the Universities Act, No. 16 of 1978. (3) The qualifications and experience (having regard to the specific areas of expertise in electronic engineering or software technology) required to be fulfilled by an officer appointed under subsection (1) and the manner and mode of appointment and the conditions of appointment of such officer shall be as prescribed by regulations. (4) For the purpose of an investigation under this Act, an expert called upon to assist any police officer shall, have the power to — (a) enter upon any premises along with a police officer not below the rank of a sub-inspector; (b) access any information system, computer or computer system or any programme, data or information held in such computer to perform any function or to do any such other thing; (c) require any person to disclose any traffic data; (d) orally examine any person; (e) do such other things as may be reasonably required, for the purposes of this Act.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(5) An expert shall be paid such remuneration as may be determined by the Minister in consultation with the Minister in charge of the subject of Finance. (6) An expert may be called upon to assist any police officer in the investigation of an offence under this Act and it shall be duty of the officer to render all such assistance as may be required for the purposes of such investigation. Where any proceedings have been commenced consequent to the findings of an investigation, it shall be the duty of the officer to make available for the purposes of such proceedings, any information, data, material or other matter that may be obtained by him in the course of such investigation. **Jurisdiction.** 25. The jurisdiction to hear, try and determine all offences under this Act shall be vested with the High Court : Provided however that where the provisions of the Extradition Law, No. 8 of 1977 is applicable in relation to the commission of an offence under this Act, the High Court holden at Colombo shall have exclusive jurisdiction to hear, try and determine such offence. **Proof of document issued by an expert or a Police Officer.** 26. (1) Every document duly signed and issued by an expert or a police officer, as the case may be, and duly authenticated by an expert in the prescribed manner, shall be admissible in evidence and shall be prima facie evidence of the facts stated therein. (2) for the purposes, of this section the expression "document" shall include a certificate, declaration, information, data, report or any other similar document.
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	**COMPUTER CRIME ACT, No. 24 OF 2007** **Powers of search and seizure with warrant** 18. (1) An expert or a police officer may, for the purposes of an investigation under this Act under the authority of a warrant issued in that behalf by a Magistrate on application made for such purpose, —

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(i) obtain any information including subscriber information and traffic data in the possession of any service provider; (ii) intercept any wire or electronic communication including subscriber information and traffic data, at any stage of such communication. (2) Notwithstanding the provisions of subsection (1), an expert or a police officer may without a warrant exercise all or any of the powers referred to in that subsection, if — (a) the investigation needs to be conducted urgently; and (b) there is a likelihood of the evidence being lost, destroyed, modified or rendered inaccessible; and (c) there is a need to maintain confidentiality regarding the investigation. **Rights of certain persons arrested for offences under this Act.** 34. Where a person who is not a citizen of Sri Lanka is arrested for an offence under this Act, such person shall be entitled — (a) to communicate without delay, with the nearest appropriate representative of the State of which he is a national or which is otherwise entitled to protect his rights or if he is a stateless person, with the nearest appropriate representative of the State in the territory of which he was habitually resident ; and (b) to be visited by a representative of that State ; and (c) be informed of his rights under paragraphs (a) and (b).
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.	**COMPUTER CRIME ACT, No. 24 OF 2007** **Preservation of information.** 19. (1) Where an expert or a police officer is satisfied that any information stored in a computer is reasonably required for the purposes of an investigation under this Act and that there is a risk that such information may be lost, destroyed, modified or rendered inaccessible, he may by written notice require

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	the person in control of such computer or computer system to ensure that the information be preserved for such period not exceeding seven (07) days as may be specified in such notice. (2) On an application made to a Magistrate having jurisdiction, the period for which the information is to be preserved may be extended for such further period, which in the aggregate shall not exceed upto ninety days. **Confidentiality of information obtained in the course of an investigation.** 24. (1) Every person engaged in an investigation under this Act shall maintain strict confidentiality with regard to all information as may come to his knowledge in the course of such investigations and he shall not disclose to any person or utilize for any purpose whatsoever any information so obtained other than in the discharge of his duties under this Act. (2) Every service provider from whom any information has been requested or obtained and any person to whom a written notice has been issued for the preservation of any information shall maintain strict confidentiality in relation to such information and the fact that such information has been requested, obtained or required to be preserved, and shall not make any disclosure in regard to such matters other than with lawful authority. (3) A service provider shall not be held liable under the civil or criminal law for the disclosure of any data or other information for the purposes of an investigation under this Act. (4) Any person who contravenes the provisions of subsections (1) and (2) shall commit an offence and shall on conviction be liable to a fine not exceeding three hundred thousand rupees or to imprisonment of either description for a term not exceeding two years or to both such fine and imprisonment.
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	**See article 18 and 19 of the Computer Crime Act, No. 24 of 2007 above.**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	**COMPUTER CRIME ACT, No. 24 OF 2007** **Powers of search and seizure with warrant.** 18. (1) An expert or a police officer may, for the purposes of an investigation under this Act under the authority of a warrant issued in that behalf by a Magistrate on application made for such purpose, — (i) obtain any information including subscriber information and traffic data in the possession of any service provider; (ii) intercept any wire or electronic communication including subscriber information and traffic data, at any stage of such communication. (2) Notwithstanding the provisions of subsection (1), an expert or a police officer may without a warrant exercise all or any of the powers referred to in that subsection, if — (a) the investigation needs to be conducted urgently; and (b) there is a likelihood of the evidence being lost, destroyed, modified or rendered inaccessible; and (c) there is a need to maintain confidentiality regarding the investigation. (3) The provisions of sections 36, 37 and 38 of the Code of Criminal Procedure Act, No. 15 of 1979 shall not apply in relation to the arrest of a person for an

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	offence under this Act. (4) The Minister may by regulation prescribe the manner in which and the procedures required to be followed in respect of, the retention and interception of data and information including traffic data, for the purposes of any investigation under this Act. **Duty to assist investigation** 23. (1) Any person who is required to make any disclosure or to assist in an investigation under this Act, shall comply with such requirement. (2) A person who obstructs the lawful exercise of the powers conferred on an expert or a police officer or fails to comply with such request made by such expert or police officer during an investigation shall be guilty of an offence and shall on conviction be liable to a fine not exceeding two hundred thousand rupees or to imprisonment of either description for a period not less than one year and not exceeding two years or to both such fine and imprisonment.
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 CRIME ACT, No. 24 OF 2007** **Powers of search and seizure with warrant.** 18. (1) An expert or a police officer may, for the purposes of an investigation under this Act under the authority of a warrant issued in that behalf by a Magistrate on application made for such purpose, — (i) obtain any information including subscriber information and traffic data in the possession of any service provider; (ii) intercept any wire or electronic communication including subscriber information and traffic data, at any stage of such communication. (2) Notwithstanding the provisions of subsection (1), an expert or a police officer may without a warrant exercise all or any of the powers referred to in that subsection, if —

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(a) the investigation needs to be conducted urgently; and (b) there is a likelihood of the evidence being lost, destroyed, modified or rendered inaccessible; and (c) there is a need to maintain confidentiality regarding the investigation. (3) The provisions of sections 36, 37 and 38 of the Code of Criminal Procedure Act, No. 15 of 1979 shall not apply in relation to the arrest of a person for an offence under this Act. (4) The Minister may by regulation prescribe the manner in which and the procedures required to be followed in respect of, the retention and interception of data and information including traffic data, for the purposes of any investigation under this Act. **Preservation of information** 19. (1) Where an expert or a police officer is satisfied that any information stored in a computer is reasonably required for the purposes of an investigation under this Act and that there is a risk that such information may be lost, destroyed, modified or rendered inaccessible, he may by written notice require the person in control of such computer or computer system to ensure that the information be preserved for such period not exceeding seven (07) days as may be specified in such notice. (2) On an application made to a Magistrate having jurisdiction, the period for which the information is to be preserved may be extended for such further period, which in the aggregate shall not exceed up to ninety days. **Normal use of computer not to be hampered.** 20. Every police officer and every expert who conducts any search, inspection or does any other thing in the course of an investigation, shall make every

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	endeavour to ensure that the ordinary course of legitimate business for which any computer may be used is not hampered by such search, inspection or investigation and shall not seize any computer, computer system or part thereof, if such seizure will prejudice the conduct of the ordinary course of business for which the computer is used, unless — (a) it is not possible to conduct the inspection on the premises where such computer, computer system or part thereof is located; or (b) seizure of such computer, computer system or part thereof is essential to prevent the commission of the offence or the continuance of the offence or to obtain custody of any information which would otherwise be lost, destroyed, modified or rendered inaccessible. **Power of police officer to arrest, search and seize.** 21. (1) Any police officer may, in the course of an investigation under this Act, exercise powers of arrest, search, or seizure of any information accessible within any premises, in the manner provided for by law: Provided that a police officer making an arrest without a warrant of person suspected of committing an offence under this Act, shall without unnecessary delay and within twentyfour hours of such arrest, exclusive of the time taken for the journey from the place of arrest to the presence of the Magistrate, produce such person before the Magistrate of the Court nearest to the place that the suspect is arrested. (2) No police officer shall access any computer for the purpose of an investigation under this Act unless the Inspector General of Police has certified in writing that such police officer possesses adequate knowledge and skill in the field of information communication technology and is thereby possessed of the required expertise to perform such a function. **Police officer to record and afford access to seized data.**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	22. (1) Where any item or data has been seized or rendered inaccessible in the course of an investigation, the police officer conducting the search shall issue a complete list of such items and data including the date and time of such seizure or of rendering it inaccessible to the owner or person in charge of the computer or computer system. (2) Subject to the provisions of subsection (3), a police officer may upon application made by the owner or person in control of the computer or computer system, permit a person nominated by such owner or person to issue such person a copy of such data. (3) A police officer shall not grant permission or give such copies under subsection (2) if it appears that such permission would be prejudicial to any criminal investigation or proceeding.
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	**See Article 18, 23 and 24 of the Computer Crime Act, No. 24 of 2007 above.**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	**See Article 18, 23 and 24 of the Computer Crime Act, No. 24 of 2007 above.**
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	**COMPUTER CRIME ACT, No. 24 OF 2007** **Application of this Act** 2. (1) The provisions of this Act shall apply where —

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	(a) a person commits an offence under this Act while being present in Sri Lanka or outside Sri Lanka; (b) the computer, computer system or information affected or which was to be affected, by the act which constitutes an offence under this Act, was at the material time in Sri Lanka or outside Sri Lanka; (c) the facility or service, including any computer storage, or data or information processing service, used in the commission of an offence under this Act was at the material time situated in Sri Lanka or outside Sri Lanka; or (d) the loss or damage is caused within or outside Sri Lanka by the commission of an offence under this Act, to the State or to a person resident in Sri Lanka or outside Sri Lanka. **Presumptions.** 31. For the purposes of the application of the provisions of the Penal Code (Chapter 19) in relation to an offence committed under this Act — (a) an offence under this Act committed outside the territory of Sri Lanka shall be deemed to have been committed in Sri Lanka; and (b) any information referred to in this Act shall be deemed to be property.
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	**COMPUTER CRIME ACT, No. 24 OF 2007** **Amendment of the Schedule to the Extradition Law, No. 8 of 1977.** 27. The Schedule to the Extradition Law, No. 8 of 1977 is hereby amended by the insertion immediately before Part B thereof, of the following new item :— "(49) An offence committed in terms of the Computer Crimes Act, No. 24 of 2007."

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	**COMPUTER CRIME ACT, No. 24 OF 2007** **Assistance to Convention States &c.** 35. (1) The provisions of the Mutual Assistance in Criminal Matters Act, No. 25 of 2002 shall, wherever it is necessary for the investigation and prosecution of an offence under this Act, be applicable in respect of the providing of assistance as between the Government of Sri Lanka and other States who are either Commonwealth countries specified by the Minister by Order under section 2 of the aforesaid Act or Non-Commonwealth countries with which the Government of Sri Lanka entered into an agreement in terms of the aforesaid Act. (2) In the case of a country which is neither a Commonwealth country specified by the Minister by Order under section 2 of the aforesaid Act nor a Non-Commonwealth country with which the Government of Sri Lanka entered into an agreement in terms of the aforesaid Act, then it shall be the duty of the Government to afford all such assistance to, and may through the Minister request all such assistance from, a convention country, as may be necessary for the investigation and prosecution of an offence under this Act (including assistance relating to the taking of evidence and statements, the serving of process and the conduct of searches). (3) The grant of assistance in terms of this section may be made subject to such terms and conditions as the Minister thinks fit. **Offences under this Act, not to be political offences &c., for the purposes of the Extradition Law.** 36. Notwithstanding anything in the Extradition Law, No. 8 of 1977, an offence specified in the Schedule to that Law and in this Act, shall for the purposes of that law be deemed not to be an offence of a political character or an offence connected with a political offence or an offence inspired by political motives, for the purposes only of the extradition of any person accused or convicted of any such offence, as between the Government of Sri Lanka and any requesting State, or of affording assistance to a requesting State under section 35.
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except	**COMPUTER CRIME ACT, No. 24 OF 2007** **Assistance to Convention States &c** 35. (1) The provisions of the Mutual Assistance in Criminal Matters Act, No. 25 of 2002 shall, wherever it is necessary for the investigation and prosecution of an offence under this Act, be applicable in respect of the providing of assistance as between the Government of Sri Lanka and other States who are either Commonwealth countries specified by the Minister by Order under section 2 of the aforesaid Act or Non-Commonwealth countries with which the Government of Sri Lanka entered into an agreement in terms of the aforesaid Act. (2) In the case of a country which is neither a Commonwealth country specified by the Minister by Order under section 2 of the aforesaid Act nor a Non-Commonwealth country with which the Government of Sri Lanka entered into an agreement in terms of the aforesaid Act, then it shall be the duty of the Government to afford all such assistance to, and may through the Minister request all such assistance from, a convention country, as may be necessary for the investigation and prosecution of an offence under this Act (including assistance relating to the taking of evidence and statements, the serving of process and the conduct of searches). (3) The grant of assistance in terms of this section may be made subject to such terms and conditions as the Minister thinks fit.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the 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.	**See Article 35 of the Computer Crime Act, No. 24 OF 2007 ~~below.~~** **Mutual Assistance in Criminal Matters (Amendment) Act, no. 24 of 2018** 3. Section 3 of the principal enactment is hereby repealed and the following section substituted therefor:– 3. (1) The object of this Act is to facilitate the provision and obtaining by Sri

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so 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	Lanka of assistance in criminal and related matters, including- (d) the provision and obtaining of evidence, documents, other articles or information; (l) the tracing of crimes committed via internet, information communications technology, cloud computing, blockchain technology and other computer networks including the trading in of any digital currencies; (n) the expedited preservation of stored computer data and expedited disclosure of preserved traffic data and data retention; (p) the use of documentary evidence obtained in a specified country through specific authorization to be made admissible in a judicial proceeding; and (q) the admissibility and applicability of evidence led from a specified country through video conferencing technology **"PART VIIA** **EXPEDITED PRESERVATION OF STORED DATA IN RELATION TO COMPUTER CRIMES** **Relevant Secretary to a Ministry to make order to preserve data** 20A. Where the Central Authority is of the opinion that expedited preservation is required of stored computer data or traffic data, the Central Authority shall inform the Secretary to the Ministry of the Minister assigned the relevant subject to make an order for the expedited preservation of stored computer data or traffic data, as the case may be, or to both such data, for the period specified under section. **Period of preservation of data.** 20B. All data for which an order is made under section 20A shall be preserved for a minimum period of six years. **Mode of preservation.** 20C. (1) Records of data preserved under this Part shall be maintained in a manner and form that will enable an institution to immediately comply with the request for information in the form in which it is requested. (2) A copy of the record may– (a) be kept in a machine readable form to conveniently obtain a print thereof; (b) be kept in an electronic form, to enable a readable copy to be readily obtained and an electronic signature of the person who keeps the records is inserted for purposes of verification; (c) where necessary, entail freezing of the stored computer data; or (d) be updated, if

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	necessary. **Release of preserved data.** 20D. (1) Preserved data shall be released for the purpose of criminal investigation or judicial proceedings on a request duly made by the appropriate authority for such period as specified in the request. (2) Every order made under section 20A shall lapse on the expiry of the time period specified under section 20B or on the expiry of the period specified in the request. (3) Where in the course of granting a request to preserve traffic data concerning a specific communication, the Central Authority is informed that a service provider in another country was involved in the transmission of the communication, the Central Authority shall instruct the relevant competent authority to disclose, such amount of traffic data as is sufficient to identify that service provider and the path through which the communication was transmitted, prior to receipt of the request for production. **Production of stored computer data.** 20E. Subject to any written law on admissibility of computer data and notwithstanding the provisions of Part VI of this Act, upon the request of an appropriate authority of a specified country or specified organization, for computer data or information to investigate the criminal matter, the Magistrate may issue an order to enable the production of– (a) specified computer data in the possession or control of a person stored in a computer system or a computer data storage medium; and (b) the necessary subscriber information in the possession or control of a service provider. **Search and seizure of computer data.** 20F. (1) Upon the request by an appropriate authority of a specified country or specified organization, a warrant may be issued under section 15, mutatis mutandis, to search or otherwise access any computer system or part thereof as well as any computer storage medium in which computer data may be stored. (2) The search warrant issued by the Magistrate within whose jurisdiction such computer or computer system is believed to be located, may authorize the police officer or any other designated person, where necessary, to– (a) seize or otherwise secure a computer system or part thereof, or a computer data storage medium; (b) make and retain a copy of that computer data; (c)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	maintain the integrity of the relevant stored computer data; and (d) render inaccessible or remove that computer data in the accessed computer system.”.
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.	**See Article 35 of the Computer Crime Act, No. 24 OF 2007 ~~below.~~**
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	**See Article 35 of the Computer Crime Act, No. 24 OF 2007 ~~below.~~** Powers of search and seizure with warrant. 18. (1) An expert or a police officer may, for the purposes of an investigation under this Act under the authority of a warrant issued in that behalf by a Magistrate on application made for such purpose, — (i) obtain any information including subscriber information and traffic data in the possession of any service provider; (ii) intercept any wire or electronic communication including subscriber information and traffic data, at any stage of such communication. (2) Notwithstanding the provisions of subsection (1), an expert or a police officer may without a warrant exercise all or any of the powers referred to in that subsection, if— (a) the investigation needs to be conducted urgently; and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) there is a likelihood of the evidence being lost, destroyed, modified or rendered inaccessible; and (c) there is a need to maintain confidentiality regarding the investigation. (3) The provisions of sections 36, 37 and 38 of the Code of Criminal Procedure Act, No. 15 of 1979 shall not apply in relation to the arrest of a person for an offence under this Act. (4) The Minister may by regulation prescribe the manner in which and the procedures required to be followed in respect of, the retention and interception of data and information including traffic data, for the purposes of any investigation under this Act. **Preservation of information** 19. (1) Where an expert or a police officer is satisfied that any information stored in a computer is reasonably required for the purposes of an investigation under this Act and that there is a risk that such information may be lost, destroyed, modified or rendered inaccessible, he may by written notice require the person in control of such computer or computer system to ensure that the information be preserved for such period not exceeding seven (07) days as may be specified in such notice. (2) On an application made to a Magistrate having jurisdiction, the period for which the information is to be preserved may be extended for such further period, which in the aggregate shall not exceed up to ninety days.
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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**COMPUTER CRIME ACT, No. 24 OF 2007** **Assistance to Convention States &c.** 35. (1) The provisions of the Mutual Assistance in Criminal Matters Act, No. 25 of 2002 shall, wherever it is necessary for the investigation and prosecution of an offence under this Act, be applicable in respect of the providing of assistance as between the Government of Sri Lanka and other States who are either Commonwealth countries specified by the Minister by Order under section 2 of the aforesaid Act or Non-Commonwealth countries with which the Government of Sri Lanka entered into an agreement in terms of the aforesaid Act. (2) In the case of a country which is neither a Commonwealth country specified by the Minister by Order under section 2 of the aforesaid Act nor a Non-Commonwealth country with which the Government of Sri Lanka entered into an agreement in terms of the aforesaid Act, then it shall be the duty of the Government to afford all such assistance to, and may through the Minister request all such assistance from, a convention country, as may be necessary for the investigation and prosecution of an offence under this Act (including assistance relating to the taking of evidence and statements, the serving of process and the conduct of searches). (3) The grant of assistance in terms of this section may be made subject to such terms and conditions as the Minister thinks fit. Offences under this Act, not to be political offences &c., for the purposes of the Extradition Law.
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.	See Article 35 of the Computer Crime Act, No. 24 OF 2007 above.
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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