

Table of contents

Version 10 August 2023

[reference to the provisions of the Budapest Convention]

Chapter I – Use of terms

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

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Article 2 – Illegal access

Article 3 – Illegal interception

Article 4 – Data interference

Article 5 – System interference

Article 6 – Misuse of devices

Article 7 – Computer-related forgery

Article 8 – Computer-related fraud

Article 9 – Offences related to child pornography

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

Article 11 – Attempt and aiding or abetting

Article 12 – Corporate liability

Article 13 – Sanctions and measures

Section 2 – Procedural law

Article 14 – Scope of procedural provisions

Article 15 – Conditions and safeguards

Article 16 – Expedited preservation of stored computer data

Article 17 – Expedited preservation and partial disclosure of traffic data

Article 18 – Production order

Article 19 – Search and seizure of stored computer data

Article 20 – Real-time collection of traffic data

Article 21 – Interception of content data

Section 3 – Jurisdiction

Article 22 – Jurisdiction

Chapter III – International co-operation

Article 24 – Extradition

Article 25 – General principles relating to mutual assistance

Article 26 – Spontaneous information

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

Article 28 – Confidentiality and limitation on use

Article 29 – Expedited preservation of stored computer data

Article 30 – Expedited disclosure of preserved traffic data

Article 31 – Mutual assistance regarding accessing of stored computer data

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

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

Article 34 – Mutual assistance regarding the interception of content data

Article 35 – 24/7 Network

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

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

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
<p>Article 1 – “Computer system”, “computer data”, “service provider”, “traffic data”:</p> <p>For the purposes of this Convention:</p> <p>a “computer system” means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;</p> <p>b “computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;</p> <p>c “service provider” means:</p> <p>i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and</p> <p>ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;</p> <p>d “traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service</p>	<p>The Information Technology Act, 2000 (amended 2008)</p> <p>Art 2. Definitions</p> <p>(l) “computer system” means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;</p> <p>(o) “data” means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;</p> <p>Art 69B. Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security</p> <p>(4) [...] Explanation: For the purposes of this section, [...] (ii) “traffic data” means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
<p>Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.</p>	<p>The Information Technology Act, 2000 (amended 2008)</p> <p>Art 43 Penalty and Compensation for damage to computer, computer system, etc (Amended vide ITAA-2008) If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network - (a) accesses or secures access to such computer, computer system or computer network or computer resource</p> <p>Art 66 Computer Related Offences (Substituted vide ITAA 2008) If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to two three years or with fine which may extend to five lakh rupees or with both. Explanation: For the purpose of this section,- a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code; b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code</p>
<p>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.</p>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>Article 4 – Data interference</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.</p> <p>2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.</p>	<p>The Information Technology Act, 2000 (amended 2008)</p> <p>Art 43 Penalty and Compensation for damage to computer, computer system, etc (Amended vide ITAA-2008)</p> <p>If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network -</p> <p>d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;</p> <p>(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;</p> <p>(j) steal, conceal, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;</p> <p>[he shall be liable to pay damages by way of compensation to the person so affected.]</p> <p>Explanation.- For the purposes of this section,-</p> <p>i) "computer contaminant" means any set of computer instructions that are designed-(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or(b) by any means to usurp the normal operation of the computer, computer system, or computer network;</p> <p>(ii) "computer data-base "means are presentation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;</p> <p>(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;</p> <p>(iv) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.</p> <p>(v) "computer source code" means the listing of programme, computer commands, design and layout and programme analysis of computer resource in any form.]</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>Art 66 Computer Related Offences (Substituted vide ITAA 2008)</p> <p>If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to two three years or with fine which may extend to five lakh rupees or with both.</p> <p>Explanation: For the purpose of this section,-</p> <p>a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code;</p> <p>b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code</p>
<p>Article 5 – System interference</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data</p>	<p>The Information Technology Act, 2000 (amended 2008)</p> <p>Art 43 Penalty and Compensation for damage to computer, computer system, etc (Amended vide ITAA-2008)</p> <p>If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, –</p> <p>(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;</p> <p>d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;</p> <p>(e) disrupts or causes disruption of any computer, computer system or computer network;</p> <p>Explanation.–For the purposes of this section,–</p> <p>i) "computer contaminant" means any set of computer instructions that are designed–(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or(b) by any means to usurp the normal operation of the computer, computer system, or computer network;</p> <p>(ii) "computer data-base "means are presentation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;</p> <p>(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;</p> <p>(iv) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.</p> <p>(v) "computer source code" means the listing of programme, computer commands, design and layout and programme analysis of computer resource in any form.]</p> <p>Art 66 Computer Related Offences (Substituted vide ITAA 2008) If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to two three years or with fine which may extend to five lakh rupees or with both. Explanation: For the purpose of this section, - a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code; b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code</p> <p>Art 65. Tampering with computer source documents. Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both. Explanation. - For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.</p>
<p>Article 6 – Misuse of devices</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:</p> <p>a the production, sale, procurement for use, import, distribution or otherwise making available of:</p> <p>i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;</p>	<p>The Information Technology Act, 2000 (amended 2008)</p> <p>Art 43. Penalty and Compensation for damage to computer, computer system, etc (Amended vide ITAA-2008) If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network - (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under;</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and</p> <p>b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.</p> <p>2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.</p> <p>3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.</p>	<p>Art 66C Punishment for identity theft. (Inserted Vide ITA 2008)</p> <p>Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.</p>
Title 2 – Computer-related offences	
<p>Article 7 – Computer-related forgery</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.</p>	<p>The Information Technology Act, 2000 (amended 2008)</p> <p>Art 66C Punishment for identity theft. (Inserted Vide ITA 2008)</p> <p>Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.</p> <p>Art 66D Punishment for cheating by personation by using computer resource (Inserted Vide ITA 2008)</p> <p>Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>Art 73 Penalty for publishing electronic Signature Certificate false in certain particulars</p> <p>(1) No person shall publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that</p> <p>(a)the Certifying Authority listed in the certificate has not issued it; or</p> <p>(b)the subscriber listed in the certificate has not accepted it; or</p> <p>(c)the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation</p> <p>(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.</p>
<p>Article 8 – Computer-related fraud</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:</p> <p style="padding-left: 40px;">a any input, alteration, deletion or suppression of computer data;</p> <p style="padding-left: 40px;">b any interference with the functioning of a computer system,</p> <p>with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.</p>	<p>The Information Technology Act, 2000 (amended 2008)</p> <p>Art 43. Art 43 Penalty and Compensation for damage to computer, computer system, etc (Amended vide ITAA-2008)</p> <p>If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network -</p> <p>(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,</p> <p>Art 66C Punishment for identity theft. (Inserted Vide ITA 2008)</p> <p>Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.</p> <p>Art 66D Punishment for cheating by personation by using computer resource (Inserted Vide ITA 2008)</p> <p>Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>Art 74 Publication for fraudulent purpose Whoever knowingly creates, publishes or otherwise makes available a Electronic Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.</p>
Title 3 – Content-related offences	
<p>Article 9 – Offences related to child pornography</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:</p> <ol style="list-style-type: none"> 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. <p>2 For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:</p> <ol style="list-style-type: none"> 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 <p>3 For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.</p> <p>4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.</p>	<p>The Information Technology Act, 2000 (amended 2008)</p> <p>Art 67B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form. Whoever,-</p> <ol style="list-style-type: none"> (a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or (c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or (d) facilitates abusing children online or (e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees: Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form- <ol style="list-style-type: none"> (i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or (ii) which is kept or used for bona fide heritage or religious purposes <p>Explanation: For the purposes of this section, "children" means a person who has not completed the age of 18 years.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Title 4 – Offences related to infringements of copyright and related rights	
<p>Article 10 – Offences related to infringements of copyright and related rights</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.</p> <p>3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party’s international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.</p>	<p>The Information Technology Act, 2000 (amended 2008)</p> <p>Art 81 Act to have Overriding effect The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force. Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act 1957 or the Patents Act 1970 (Inserted Vide ITAA 2008).</p>
Title 5 – Ancillary liability and sanctions	
<p>Article 11 – Attempt and aiding or abetting</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.</p>	<p>The Information Technology Act, 2000 (amended 2008)</p> <p>Art 84B Punishment for abetment of offences (Inserted Vide ITA-2008) Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.</p> <p>3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.</p>	<p>of such abetment, be punished with the punishment provided for the offence under this Act.</p> <p>Explanation: An Act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.</p> <p>Art 84C Punishment for attempt to commit offences (Inserted Vide ITA-2008) Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both.</p>
<p>Article 12 – Corporate liability</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:</p> <ul style="list-style-type: none"> a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. <p>2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.</p> <p>3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.</p> <p>4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.</p>	<p>The Information Technology Act, 2000 (amended 2008)</p> <p>Art 85 Offences by Companies.</p> <p>(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a Company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly: Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.</p> <p>(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.</p> <p>Explanation-For the purposes of this section</p> <ul style="list-style-type: none"> (i) "Company" means any Body Corporate and includes a Firm or other Association of individuals; and (ii)"Director", in relation to a firm, means a partner in the firm

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>Article 13 – Sanctions and measures</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.</p> <p>2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.</p>	<p>The Information Technology Act, 2000 (amended 2008)</p> <p>Art 66 Computer Related Offences (Substituted vide ITAA 2008) If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to two three years or with fine which may extend to five lakh rupees or with both. Explanation: For the purpose of this section,- a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code; b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code</p> <p>Art 66A Punishment for sending offensive messages through communication service, etc. (Introduced vide ITAA 2008) Any person who sends, by means of a computer resource or a communication device,- a) any information that is grossly offensive or has menacing character; or b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device, c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008) shall be punishable with imprisonment for a term which may extend to two three years and with fine. Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message</p> <p>Art 66B Punishment for dishonestly receiving stolen computer resource or communication device (Inserted Vide ITA 2008) Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>Art 66E. Punishment for violation of privacy. (Inserted Vide ITA 2008) Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both</p> <p>Explanation.-For the purposes of this section—</p> <p>(a)—transmitll means to electronically send a visual image with the intent that it be viewed by a person or persons;</p> <p>(b)—capturell, with respect to an image, means to videotape, photograph, film or record by any means;</p> <p>(c)—private areall means the naked or undergarment clad genitals, pubic area, buttocks or female breast;</p> <p>(d)—publishesll means reproduction in the printed or electronic form and making it available for public;</p> <p>(e)—under circumstances violating privacyll means circumstances in which a person can have a reasonable expectation that—</p> <p>(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or</p> <p>(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place</p> <p>Art 66F.Punishment for cyber terrorism</p> <p>(1) Whoever,-</p> <p>(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –</p> <p>(i) denying or cause the denial of access to any person authorized to access computer resource; or</p> <p>(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or</p> <p>(iii) introducing or causing to introduce any Computer Contaminant. and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or</p> <p>(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorized access, and by means of such</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.</p> <p>(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life’.</p> <p>Art 67A Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form (Inserted vide ITAA 2008)Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.</p> <p>Exception: This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-(i)the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art, or learning or other objects of general concern; or(ii) which is kept or used bona fide for religious purposes</p> <p>Art 67C Preservation and Retention of information by intermediaries</p> <p>(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.</p> <p>(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.</p> <p>Art 68 Power of Controller to give directions (Amended Vide ITAA 2008)(1)The Controller may, by order, direct a Certifying Authority or any employee of such</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.(2)Any person who intentionally or knowingly (Inserted vide ITAA 2008) fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or to both.</p> <p>Art 69A Power to issue directions for blocking for public access of any information through any computer resource (1) Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource. (2) The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed. (3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.</p> <p>Art 70 Protected system (Amended Vide ITAA-2008) (1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system. Explanation: For the purposes of this section, "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety. (Substituted vide ITAA-2008) (2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1) (3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.</p> <p>(4) The Central Government shall prescribe the information security practices and procedures for such protected system. (Inserted vide ITAA 2008)</p> <p>Art 71 Penalty for misrepresentation Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.</p> <p>Art 71 Penalty for misrepresentation Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.</p> <p>Art 72 Breach of confidentiality and privacy Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.</p> <p>Art 72A Punishment for Disclosure of information in breach of lawful contract (Inserted vide ITAA-2008)Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>Art 84B Punishment for abetment of offences (Inserted Vide ITA-2008) Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act. Explanation: An Act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.</p> <p>Art 84C Punishment for attempt to commit offences (Inserted Vide ITA-2008) Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both.</p>
Section 2 – Procedural law	
<p>Article 14 – Scope of procedural provisions</p> <p>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.</p> <p>2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:</p> <ul style="list-style-type: none"> a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. <p>3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.</p>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:</p> <ul style="list-style-type: none"> i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, <p>that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21</p>	
<p>Article 15 – Conditions and safeguards</p> <p>1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.</p> <p>2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, <i>inter alia</i>, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.</p> <p>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.</p>	
<p>Article 16 – Expedited preservation of stored computer data</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the</p>	<p>The Information Technology Act, 2000 (amended 2008)</p> <p>Art 29 Access to computers and data.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.</p> <p>2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>(1) Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorized by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this chapter made there under has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.(Amended vide ITAA 2008)</p> <p>(2) For the purposes of sub-section (1), the Controller or any person authorized by him may, by order, direct any person in charge of, or otherwise concerned with the operation of the computer system, data apparatus or material, to provide him with such reasonable technical and other assistant as he may consider necessary.</p> <p>Art 67C Preservation and Retention of information by intermediaries</p> <p>(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.</p>
<p>Article 17 – Expedited preservation and partial disclosure of traffic data</p> <p>1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:</p> <p>a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and</p> <p>b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.</p> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>Information Technology (Intermediary Guidelines) Rules, 2011</p> <p>Art 3(7) When required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorised for investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing stating clearly the purpose of seeking such information or any such assistance.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>Article 18 – Production order</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:</p> <p>a a person in its territory to submit specified computer data in that person’s possession or control, which is stored in a computer system or a computer-data storage medium; and</p> <p>b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider’s possession or control.</p> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p> <p>3 For the purpose of this article, the term “subscriber information” means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:</p> <p>a the type of communication service used, the technical provisions taken thereto and the period of service;</p> <p>b the subscriber’s identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;</p> <p>c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.</p>	<p>The Information Technology Act, 2000 (amended 2008)</p> <p>Art 28 Power to investigate contraventions.</p> <p>2) The Controller or any officer authorized by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 and shall exercise such powers, subject to such limitations laid down under that Act</p> <p>Art 58 Procedure and Powers of the Cyber Appellate Tribunal</p> <p>(2) The Cyber Appellate Tribunal shall have, for the purposes of discharging their functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely –</p> <p>(b) requiring the discovery and production of documents or other electronic records.</p> <p>Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.</p>
<p>Article 19 – Search and seizure of stored computer data</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:</p> <p>a a computer system or part of it and computer data stored therein; and</p> <p>b a computer-data storage medium in which computer data may be stored</p> <p>in its territory.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system</p>	<p>The Information Technology Act, 2000 (amended 2008)</p> <p>Art 76 Confiscation</p> <p>Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation:</p> <p>Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:</p> <ul style="list-style-type: none"> a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. <p>4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.</p> <p>5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit.</p>
<p>Article 20 – Real-time collection of traffic data</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:</p> <ul style="list-style-type: none"> a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: <ul style="list-style-type: none"> i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. <p>2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may</p>	<p>The Information Technology Act, 2000 (amended 2008)</p> <p>Art 69B Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security</p> <p>(1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.</p> <p>(2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating , transmitting, receiving or storing such traffic data or information.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.</p> <p>(4) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.</p> <p>Explanation: For the purposes of this section,</p> <p>(i) "Computer Contaminant" shall have the meaning assigned to it in section 43</p> <p>(ii) "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.</p>
<p>Article 21 – Interception of content data</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:</p> <p>a collect or record through the application of technical means on the territory of that Party, and</p> <p>b compel a service provider, within its existing technical capability:</p> <p> i to collect or record through the application of technical means on the territory of that Party, or</p> <p> ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.</p> <p>2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>The Information Technology Act, 2000 (amended 2008)</p> <p>Art 69 Powers to issue directions for interception or monitoring or decryption of any information through any computer resource (Substituted Vide ITAA 2008)</p> <p>(1) Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.</p> <p>(2) The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed</p> <p>(3) The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub section (1), extend all facilities and technical assistance to –</p> <p>(a) provide access to or secure access to the computer resource containing such information; generating, transmitting, receiving or storing such information; or</p> <p>(b) intercept or monitor or decrypt the information, as the case may be; or</p> <p>(c) provide information stored in computer resource.</p> <p>(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Section 3 – Jurisdiction	
<p>Article 22 – Jurisdiction</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:</p> <ol style="list-style-type: none"> 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. <p>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.</p> <p>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.</p> <p>4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.</p> <p>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.</p>	<p>The Information Technology Act, 2000 (amended 2008)</p> <p>Art 1. Short Title, Extent, Commencement and Application</p> <p>(2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention hereunder committed outside India by any person</p> <p>Art 75 Act to apply for offence or contraventions committed outside India</p> <p>(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.</p> <p>(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.</p>
Chapter III – International co-operation	
<p>Article 24 – Extradition</p> <p>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.</p>	

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

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure</p>	
<p>Article 25 – General principles relating to mutual assistance</p> <p>1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.</p> <p>2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.</p> <p>3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.</p> <p>4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.</p> <p>5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.</p>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>Article 26 – Spontaneous information</p> <p>1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.</p> <p>2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.</p>	
<p>Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements</p> <p>1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.</p> <p>2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.</p> <p>b The central authorities shall communicate directly with each other;</p> <p>c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;</p> <p>d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.</p>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.</p> <p>4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:</p> <p>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or</p> <p>b it considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.</p> <p>5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).</p> <p>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</p>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>request to the competent national authority and inform directly the requesting Party that it has done so.</p> <p>d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.</p> <p>e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.</p>	
<p>Article 28 – Confidentiality and limitation on use</p> <p>1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.</p> <p>2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:</p> <p>a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or</p> <p>b not used for investigations or proceedings other than those stated in the request.</p> <p>3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.</p> <p>4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.</p>	
<p>Article 29 – Expedited preservation of stored computer data</p> <p>1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the</p>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.</p> <p>2 A request for preservation made under paragraph 1 shall specify:</p> <ul style="list-style-type: none"> a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. <p>3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.</p> <p>4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.</p> <p>5 In addition, a request for preservation may only be refused if:</p> <ul style="list-style-type: none"> a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests. <p>6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so</p>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>inform the requesting Party, which shall then determine whether the request should nevertheless be executed.</p> <p>4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.</p>	
<p>Article 30 – Expedited disclosure of preserved traffic data</p> <p>1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.</p> <p>2 Disclosure of traffic data under paragraph 1 may only be withheld if:</p> <p>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or</p> <p>b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.</p>	
<p>Article 31 – Mutual assistance regarding accessing of stored computer data</p> <p>1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.</p> <p>2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.</p> <p>3 The request shall be responded to on an expedited basis where:</p> <p>a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or</p> <p>b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.</p>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>Article 32 – Trans-border access to stored computer data with consent or where publicly available</p> <p>A Party may, without the authorisation of another Party:</p> <p>a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or</p> <p>b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.</p>	
<p>Article 33 – Mutual assistance in the real-time collection of traffic data</p> <p>1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.</p> <p>2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.</p>	<p>The Information Technology Act, 2000 (amended 2008)</p> <p>Art 69 Powers to issue directions for interception or monitoring or decryption of any information through any computer resource (Substituted Vide ITAA 2008)</p> <p>(1) Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.</p> <p>(2) The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed</p> <p>(3) The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub section (1), extend all facilities and technical assistance to –</p> <p>(a)provide access to or secure access to the computer resource containing such information; generating, transmitting, receiving or storing such information; or</p> <p>(b)intercept or monitor or decrypt the information, as the case may be; or</p> <p>(c)provide information stored in computer resource.</p> <p>(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>Article 34 – Mutual assistance regarding the interception of content data</p> <p>The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.</p>	<p>The Information Technology Act, 2000 (amended 2008)</p> <p>Art 69 Powers to issue directions for interception or monitoring or decryption of any information through any computer resource (Substituted Vide ITAA 2008)</p> <p>(1) Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.</p> <p>(2) The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed</p> <p>(3) The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub section (1), extend all facilities and technical assistance to –</p> <p>(a) provide access to or secure access to the computer resource containing such information; generating, transmitting, receiving or storing such information; or</p> <p>(b) intercept or monitor or decrypt the information, as the case may be; or</p> <p>(c) provide information stored in computer resource.</p> <p>(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.</p>
<p>Article 35 – 24/7 Network</p> <p>1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:</p> <p>a the provision of technical advice;</p> <p>b the preservation of data pursuant to Articles 29 and 30;</p> <p>c the collection of evidence, the provision of legal information, and locating of suspects.</p>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.</p> <p>b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.</p> <p>3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.</p>	
<p>Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.</p>	