Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Version 23 February 2010

Cybercrime legislation – country profile

PAKISTAN

This profile has been prepared within the framework of the Council of Europe's capacity building projects on cybercrime in view of sharing information and assessing the current state of implementation of the Convention on Cybercrime under domestic legislation. It does not necessarily reflect official positions of the country covered or of the Council of Europe.

Comments may be sent to:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe, Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

Country:	**Pakistan**
Signature of Convention:	No
Ratification/accession:	No
Provisions of the Convention	***Corresponding provisions/solutions in national legislation*** *(pls quote or summarise briefly; pls attach relevant extracts as an appendix)*
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;	**Electronic Transactions Ordinance, 2002** ("**ETO**"): 2. **Definitions**.—(1) In this Ordinance, unless there is anything repugnant in the subject or context,— (1) "electronic" includes electrical, digital, magnetic, optical, biometric, electro-chemical, wireless or electromagnetic technology;

b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	(m) "electronic document" includes documents, records, information, communications or transactions in electronic form; (o) "information" includes text, message, data, voice, sound, database, video, signals, software, computer programs, codes including object code and source code; (p) "information system" means an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing information; (q) "integrity" means, in relation to an electronic document, electronic signature or advanced electronic signature, the electronic document, electronic signature or advanced electronic signature that has not been tampered with, altered or modified since a particular point in time; (r) "intermediary" means a person acting as a service provider in relation to the sending, receiving, storing or processing of the electronic communication or the provision of other services in relation to it; (s) "network service provider" means a person who owns, possesses, operates, manages or controls a public switched network or provides telecommunication services; (x) "security procedure" means a procedure which : (i) is agreed between parties; (ii) is implemented in the normal course by a business and which is reasonably secure and reliable ; or (iii) in relation to a certificate issued by a certification service provider, is specified in its certification practice statement; for establishing the authenticity or integrity, or both, of any electronic document, which may require the use of algorithms or codes, identifying words and numbers, encryption, answer back or acknowledgment procedures, software, hardware or similar security devices;

	Prevention of Electronic Crimes Ordinance, 2009 ("**PECO**") Definitions.- (1) In this Ordinance, unless there is anything repugnant in the subject or context,- (a) "access" means gaining access to any electronic system or data held in an electronic system or by causing the electronic system to perform any function to achieve that objective; (b) "Authority" means the Pakistan Telecommunication Authority established under section 3 of the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996); (c) "Code" means the Code of Criminal Procedure, 1898(Act V of 1898); (d) "Constitution" means Constitution of the Islamic Republic of Pakistan; (e) "data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in an electronic system including but not limited to computer program, text, images, sound, video and information within a database or electronic system; (f) "decision of the Authority" means decision given, determination made or order passed by the Authority under any of the provisions of the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996) on any matter relating to one or more licensed operators pursuant to the powers conferred upon the Authority by any other law, rule, regulation or directive for the time being in force which includes any interim order passed by the Authority pending final decision; (g) "Electronic Certification Accreditation Council" means the council established under section 18 of the Electronic Transaction Ordinance, 2002 (LI of 2002); (h) "electronic" includes but not limited to electrical, digital, analogue, magnetic, optical, biochemical, electrochemical, electromechanical,electromagnetic, radio electric or wireless technology;

	(i) "electronic device" means any hardware which performs one or more specific functions and operates on any form or combination of electrical energy; (j) "electronic mail message" means any data generated by an electronic system for a unique electronic mail address; (k) "electronic mail address" means a destination, commonly expressed as a string of characters, consisting of a unique user or group name or mailbox, commonly referred to as the local part, and a reference to an internet or intranet domain, commonly referred to as the domain part, whether or not displayed, to which an electronic mail message can be sent or delivered or originated from and includes an electronic mail address which may be permanent, dynamic or disposable; (1) "electronic system" means any electronic device or a group of interconnected or related devices, one or more of which, pursuant to a program or manual or any external instruction, performs automatic processing of information or data and may also include a permanent, removable or any other electronic storage medium; (m) "encrypted data" means data which has been transformed or scrambled from its plain version or text to an unreadable or incomprehensible format and is recoverable by an associated decryption or decoding technique, regardless of the technique utilized for such transformation or scrambling and irrespective of the medium in which such data occurs or can be found for the purposes of protecting such data; (n) "function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within an electronic system; (o) "Interpol" means International Criminal Police Organization; (p) "offence" includes,- (i) an offence punishable under this Ordinance; (ii) an offence punishable under the laws mentioned in the Schedule ; or (iii) any other offence punishable under any other law for the time being in force

	if committed through or by using any computer, electronic system, electronic means or electronic device as a means or tool; (q) "plain version" means original data before it has been transformed or scrambled to an unreadable or incomprehensible format or after it has been recovered by using any decryption or decoding technique; (r) "rules" means rules made under this Ordinance; (s) "Schedule" means the Schedule to this Ordinance; (t) "sensitive electronic system" means an electronic system used directly in connection with or necessary for,- (i) the security, defence or international relations of Pakistan; (ii) the existence or identity of a confidential source of information relating to the enforcement of criminal law; (iii) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, courts, public transportation, public key infrastructure, payment systems infrastructure or e-commerce infrastructure ; (iv) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services ; (iv) the purpose declared as such by the Federal Government in accordance with the prescribed procedure ; or (vi) containing any data or database protected as such, by any other laws. (u) "service provider" includes but not limited to ,- (i) a person acting as a service provider in relation to sending, receiving, storing or processing of electronic communication or the provision of other services in relation to electronic communication through any electronic system; (ii) a person who owns, possesses, operates, manages or controls a public switched network or provides telecommunication services; or (iii) any other person who processes or stores data on behalf of such electronic communication service or users of such service; (v) "subscriber information" means any information contained in any form that is held by a service provider, relating to subscriber's services other'than traffic

	data and by which can be established,- (i) the type of communication service used, the technical provisions taken thereto and the period of service; (ii) the subscriber's identity, postal geographic, "electronic mail address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; or (iii) any other information on the site of the installation of communication equipment, ¦ available on the basis of the service agreement or arrangement; (w) "traffic data" means any data relating to a communication by means of an electronic system, generated by an electronic 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; (x) "Tribunal" means the Information and Communication Technologies Tribunal constituted under section 31; and (y) "unauthorized access" means access of any kind by any person to any electronic system or data held in an electronic system or electronic device, without authority or in excess of authority, if he is not himself entitled to control access of the kind in question to the electronic system or electronic device, or data and he does not have consent to such access from any person, so entitled.
Chapter II – Measures to be taken at the national level ***Section 1 – Substantive criminal law***	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**Electronic Transactions Ordinance, 2002 ("ETO"):** 36. Violation of privacy of information.—Any person who gains or attempts to gain access to any information system with or without intent to acquire the information contained therein or to gain knowledge of such information, whether or not he is aware of the nature or contents of such information, when he is not authorised to gain access, as aforesaid, shall be guilty of an offence under this Ordinance punishable with

	either description of a term not exceeding seven years, or fine which may extend to one million rupees, or with both. [Repealed by PECO 2009] 37. Damage to information system, etc.—(1) Any person who does or attempts to do any act with intent to alter, modify, delete, remove, generate, transmit or store any information through or in any information system knowingly that he is not authorised to do any of the foregoing, shall be guilty of an offence under this Ordinance. (2) Any person who does or attempts to do any act with intent to impair the operation of, or prevent or hinder access to, any information contained in any information system, knowingly that he is not authorised to do any of the foregoing, shall be guilty of an offence under this Ordinance. (3) The offences under sub-section (1) and (2) of this section will be punishable with either description of a term not exceeding seven years or fine which may extend to one million rupees, or with both. **Prevention of Electronic Crimes Ordinance, 2009 ("PECO")** **3. Criminal access** .- Whoever intentionally gains unauthorized access to the whole or any part of an electronic system or electronic device with or without infringing security measures, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine not exceeding three hundred thousand rupees, or with both. **4. Criminal data access**.- Whoever intentionally causes any electronic system or electronic device to perform any function for the purpose of gaining unauthorized access to any data held in any electronic system or electronic device or on obtaining such unauthorized access shall be punished with imprisonment of either description for a term which may extend to three years,

	or with fine or with both. **10. Unauthorized access to code.-** Whoever discloses or obtains any password, access as to code, system design or any other means of gaining access to any electronic system or data with intent to obtain wrongful gain, do reverse engineering or cause wrongful loss to any person or for any other unlawful purpose shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.
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.	**16. Unauthorized interception.-** (1) Whoever without lawful authority intercepts by technical means, transmissions of data to, from or within an electronic system including electromagnetic emissions from an electronic system carrying such data commits the offence of unauthorized interception. (2) Whoever commits the offence of unauthorized interception described in sub-section (1) shall be punished with imprisonment of either description fora term which may extend to five years, or with fine not exceeding five hundred thousand rupees, or with both.
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**5. Data damage.**- Whoever with intent to illegal gain or cause harm to the public or any person, damages any data shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both. Explanation .- For the purpose of this section the expression "data damage" includes but not limited to modifying, altering, deleting, deterioration, erasing, suppressing, changing location of data or making data temporarily or permanently unavailable, halting electronic system, choking the networks or affecting the reliability or usefulness of data. **12. Malicious code.**- (1) Whoever willfully writes, offers, makes available, distributes or transmits malicious code through an electronic system or electronic device, with intent to cause harm to any electronic system or resulting in the corruption, destruction, alteration, suppression, theft or loss of data commits the offence of malicious code: Provided that the provision of this section shall not apply to the authorized testing, research and development or protection of an electronic system for any lawful purpose.

	Explanation,- For the purpose of this section the expression "malicious code" includes but not limited to a computer program or a hidden function in a program that damages data or compromises the electronic system's performance or uses the electronic system resources without proper authorization, with or without attaching its copy to a file and is capable of spreading over electronic system with or without human intervention including virus, worm or Trojan horse. (2) Whoever commits the offence specified in sub-section (1) shall be punished with imprisonment of either description for a term which may extend to five years, or with fine or with both. **17. Cyber terrorism.**- (1) Any person, group or organization who, with terroristic intent utilizes, accesses or causes to be accessed a computer or computer network or electronic system or electronic device or by any available means, and thereby knowingly engages in or attempts to engage in a terroristic act commits the offence of cyber terrorism. Explanation l.- For the purposes of this section the expression "terroristic intent" means to act with the purpose to alarm, frighten, disrupt, harm, damage, or carry out an act of violence against any segment of the population, the Government or entity associated therewith. Explanation 2.- For the purposes of this section the expression "terroristic act" includes, but is not limited to,- (a) altering by addition, deletion, or change or attempting to alter information that may result in the imminent injury, sickness, or death to any segment of the population; (b) transmission or attempted transmission of a harmful program with the purpose of substantially disrupting or disabling any computer network operated by the Government or any public entity; (c) aiding the commission of or attempting to aid the commission of an act of violence against the sovereignty of Pakistan, whether or not the commission of such act of violence is actually completed; or (d) stealing or copying, or attempting to steal or copy, or secure classified information or data necessary to manufacture any form of chemical, biological or nuclear weapon, or any other weapon of mass destruction. (2) Whoever commits the offence of cyber terrorism and causes death of anyperson shall be punishable with death or imprisonment for life, and with fine and

	in any other case he shall be punishable with imprisonment of either description for a term which may extend to ten years, or with fine not less than ten-million rupees, or with both
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	**6. System damage.**- Whoever with intent to cause damage to the public or any person interferes with or interrupts or obstructs the functioning, reliability or usefulness of an electronic system or electronic device by inputting, transmitting, damaging, deleting, altering, tempering, deteriorating or suppressing any data or services or halting electronic system or choking the networks shall be punished with imprisonment of either description for a term which may extend to three years, or with fine or, with both. Explanation .- For the purpose of this section the expression "services" include any kind of service provided through electronic system. **12. Malicious code**.- (1) Whoever willfully writes, offers, makes available, distributes or transmits malicious code through an electronic system or electronic device, with intent to cause harm to any electronic system or resulting in the corruption, destruction, alteration, suppression, theft or loss of data commits the offence of malicious code: Provided that the provision of this section shall not apply to the authorized testing, research and development or protection of an electronic system for any lawful purpose. Explanation,- For the purpose of this section the expression "malicious code" includes but not limited to a computer program or a hidden function in a program that damages data or compromises the electronic system's performance or uses the electronic system resources without proper authorization, with or without attaching its copy to a file and is capable of spreading over electronic system with or without human intervention including virus, worm or Trojan horse. (2) Whoever commits the offence specified in sub-section (1) shall be punished with imprisonment of either description for a term which may extend to five years, or with fine or with both.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:	**4. Criminal data access**.- Whoever intentionally causes any electronic system or electronic device to perform any function for the purpose of gaining unauthorized access to any data held in any electronic system or electronic device or on obtaining such unauthorized access shall be punished with

a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	imprisonment of either description for a term which may extend to three years, or with fine or with both. **9. Misuse of electronic system or electronic device.**- (1) Whoever produces, possesses, sells, procures, transports, imports, distributes or otherwise makes available an electronic system or electronic device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established under this Ordinance or a password, access code, or similar data by which the whole or any part of an electronic system or electronic device is capable of being accessed or its functionality compromised or reverse engineered , with the intent that it be used for the purpose of committing any of the offences established under this Ordinance, is said to commit offence of misuse of electronic system or electronic devices: Provided that the provisions of this section shall not apply to the authorized testing or protection of an electronic system for any lawful purpose. (2) Whoever commits the offence described in sub-section (1) shall be punishable with imprisonment of either description for a term which may extend to three years, or with fine, or with both.
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A	**8. Electronic forgery.**- Whoever for wrongful gain interferes with data, electronic system or electronic device, with intent to cause damage or injury to the public or to any person, or to make any illegal claim or title or to cause any person to part with property or to enter into any express or implied contract, or with intent to commit fraud by any input, alteration, deletion, or suppression of data, resulting in unauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of the fact that the

Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	data is directly readable and intelligible or not shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine or with both. **14. Spamming.**- (1) Whoever transmits harmful, fraudulent, misleading, illegal or unsolicited electronic messages in bulk to any person without the express permission of the recipient, or causes any electronic system to show any such message or involves in falsified online user account registration or falsified domain name registration for commercial purpose commits the offence of spamming. (2) Whoever commits the offence of spamming as described in sub-section (1) shall be punishable with fine not exceeding fifty thousand rupees if he commits this offence of spamming for the first time and for every subsequent commission of offence of spamming he shall be punished with imprisonment of three months or with fine, or with both. **15. Spoofing.**(l) Whoever establishes a website, or sends an electronic message with a counterfeit source intended to be believed by the recipient or visitor or its electronic system to be an authentic source with intent to gain unauthorized access or obtain valuable information which later can be used for any unlawful purposes commits the offence of spoofing. (2) Whoever commits the offence of spoofing specified in sub-section (1) shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**7. Electronic fraud.**- Whoever for wrongful gain interferes with or uses any data, electronic system or electronic device or induces any person to enter into a relationship or with intent to deceive any person, which act or omission is likely to cause damage or harm to that person or any other person shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine, or with both.
Title 3 – Content-related offences	

Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	**Pakistan Penal Code Act 1860:** **292. Sale, etc., of obscene books, etc.** **Whoever--** (a) sells, lets to hire, distributes, publicly exhibits or in any manner puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation, makes, produce or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatever, or (b) imports, exports or conveys any obscene object of any of the purposes aforesaid, or knowing or having reason to believe that such object will be sold, let to hire, distributed or publicly exhibited or in any manner put into circulation, or (c) takes part in or receives profits from any business in the course of which he knows or has reason to believe that any such obscene objects are, for any of the purposes aforesaid, make, produced, purchased, kept, imported, exported, conveyed, publicly exhibited or in any manner put into circulation, or (d) advertises or makes known by any means whatsoever that any person is engaged or is ready to engage in any act which is an offence under this section, or that any such obscene object can be procured from or through any person, or (e) offers or attempts to do any act which is an offence under this section, [shall be punished with imprisonment of either description for a term which may extend to three months, or with fine, or with both. Exception. This section does not extend to any book, pamphlet, writing, drawing or painting kept or used bona fide for religious purposes or any representation sculptured, engraved, painted or otherwise represented on or in any temple, or on any car used for the conveyance of idols, or kept or used for any religious purpose. **293. Sale, etc., of obscene objects to young person.** Whoever sells, lets to hire, distributes, exhibits or circulates to any person under the age of twenty years any such obscene object as is referred to in the last preceding section, or offers or attempts so to do, shall be punished with imprisonment of either description for a term which may extend to six months, or with fine, or with both.

	294. Obscene acts and songs. Whoever, to the annoyance of others, (a) does any obscene act in any public place, or (b) sings, recites or utters any obscene songs, balled or words, in or near any public place, shall be punished with imprisonment of either description for a term which may extend to three months, or with fine, or with both. This needs to be read in conjunction with the provisions of section 3 the Electronic Transactions Ordinance 2002 and section 20 of the Prevetion of Electronic Crimes Ordinance, 2009: **ETO 2002** **3. Legal recognition of electronic forms**.—No document, record, information, communication or transaction shall be denied legal recognition, admissibility, effect, validity, proof or enforceability on the ground that it is in electronic form and has not been attested by any witness. **PECO:** **20. Other offences**.-Whoever commits any offence, other than those expressly provided under this Ordinance, with the help of computer, electronic system, electronic device or any other electronic means shall be punished, in addition to the punishment provided for that offence, with imprisonment of either description for a term which may extend to two years, or with fine not exceeding two hundred thousand rupees. or with both.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic	**Copyright Ordinance, 1962:** 2. Definitions. In this Ordinance, unless there is any thing repugnant in the subject or context:- (p) "literary work" includes works on humanity, religion, social and physical

Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	sciences, tables "compilations and **computer programmes, that is to say programmes recorded on any disc, tape, perforated media or other information storage device, which, if fed into or located in a computer or computer-based equipment is capable of reproducing any information**" **66. Offenses of infringement of copyright or other rights conferred by this Ordinance Any person who knowingly infringes or abets the infringement of.** (a) the copyright in a work, or (b) any other right conferred by this Ordinance, shall be punishable with imprisonment which may extend to three years, or with fine which may extend to one hundred thousand rupees" or with both 66 (A), 66(B), 66(C), and 66(D), Explanation. Construction of a building or other structure which infringes or which, if completed, would infringe the copyright in some other work, shall not be an offence under this section. **66A. Penalty for publishing collections or compendiums of work which have been adapted, translated or modified in any manner without the authority of the owner of the copyright.** Any person who knowingly publishes, or causes to be published, a collection or compendium of works which have been adapted, translated or modified in any manner without the authority of the owner of the copyright in the original works, or who fraudulently employs a title which tends to mislead the public or create confusion with another work published earlier, shall be punishable with imprisonment which may extend to three years, or with fine which may extend to one hundred thousand rupees. or with both. **66B. Penalty for unauthorised reproduction or distribution of counterfeit copies of sound recording and cinematographic work.** Any person who unauthorisedly makes or distributes counterfeit of sound recording and cinematographic work for the purpose of business, profit or gain

	shall be publishable with imprisonment which may extend to three years, or with fine which may extend to one hundred thousand rupees, or with both. **66C. Penalty for exploitation and appropriation of recording or audio-visual work intended for private use.** Any person who for the purpose of business, profit or gain, exploits or appropriates any sound recording or audio-visual work intended for private use, shall be punishable with imprisonment which may extend to three years, or with fine which may extend to one hundred thousand rupees, or with both. **66D. Penalty for making copies or reproduction in excess of those authorised by the copyright owner or his successor in title.** Any person who produces or causes to be produced, copies or reproductions in excess or the number authorised by the copyright owner or his successor in title. shall be punishable with imprisonment which may extend to three years or with fine which may extend to one hundred thousand rupees or with both. **66E. Penalty of unauthorized rental of cinematographic works and computer programmes**, -- any person who, without authorization of the copyright owner or his licensee rents out the original or copies of the cinematographic works or computer programmes, shall be punishable with imprisonment which may extend to three year or with fine which may extend to one hundred thousand rupees or with both. **70B. Enhanced fine in the case of subsequent offences.** Where any person convicted for an offence punishable under section 66, 66A, 66B, 66C, 66D, or 70A, is again convicted for the same offence, the said section shall have effect as if for the words "one hundred thousand" therein the words "two hundred thousand" were substituted.
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when	**19. Of abets, aids or attempts to commits offence .-** (1) Any person who knowingly and willfully abets the commission of or who aids to commit or does any act preparatory to or in furtherance of the commission of any offence under

committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	this Ordinance shall be guilty of that offence and shall be liable on conviction to the punishment provided for the offence. (2) Any person who attempts to commit an offence under this Ordinance shall be punished for a term which may extend to one-half of the longest term of imprisonment provided for that offence. Explanation.- For aiding or abetting an offence to be committed under this section, it is immaterial whether the offence has been committed or not.
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	**21. Offences by corporate body.**- A corporate body shall be held liable for an offence under this Ordinance if the offence is committed on its instructions or for its benefit. The corporate body shall be punished with fine not less than one hundred thousand rupees or the amount involved in the offence whichever is the higher: Provided that such punishment shall not absolve the criminal liability of the natural person who has committed the offence. Explanation.- For the purposes of this section corporate body, includes a body of persons incorporated under any law such as trust, waqf, an association, a statutory body or a company.
Article 13 – Sanctions and measures 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary	**18. Enhanced punishment for offences involving sensitive electronic systems**.-(l) Whoever causes criminal access to any sensitive electronic system in the course of the commission of any of the offences established under this Ordinance shall, in addition to the punishment prescribed for that offence, be punished with imprisonment of either description for a term which may extend to ten years, or with fine not exceeding one million rupees, or with both. (2) For the purposes of any prosecution under this section, it shall be presumed, until contrary is proved, that the accused had the requisite knowledge that it

sanctions.	was a sensitive electronic system.
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	**20. Other offences.**- Whoever commits any offence other than those expressly provided under this Ordinance, with the help of computer electronic system, electronic device or any other electronic means shall be punished, in addition to the punishment provided for that offence, with imprisonment of either description for a term which may extend to two years, or with fine not exceeding two hundred thousand rupees, or with both.

Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	[No specific provisions in PECO but the FIA in practice acts upon authorization of a judicial magistrate. [Specifics should be defined as PECO is turned into act
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.	**28. Retention of traffic data**,- (1) A service provider shall, within its existing or required technical capability, retain its traffic data minimum for a period of ninety days and provide that data to the investigating agency or the investigating officer when required. The Federal Government may extend the period to retain such date as and when deems appropriate. (2) The service providers shall retain the traffic data under sub-section (1) by fulfilling all the requirements of data retention and its originality as provided under sections 5 and 6 of the Electronic Transaction Ordinance, 2002 (LI of 2002). (3) Any person who contravenes the provisions of this section shall be punished with imprisonment for a term of six months, or with fine, or with both.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form	**26. Powers of officer.**-(I) Subject to obtaining search warrant an investigation officer shall be entitled to,- (a) have access to and inspect the operation of any electronic system; (b) use or cause to be used any such electronic system to search any data contained in or available to such electronic system; (c) have access to or demand any information, code or technology which has the capability of retransforming or unscrambling encrypted data contained or available to such electronic system into readable and comprehensible format or plain version; (d) require any person by whom or on whose behalf, the investigating officer has reasonable cause to believe, any electronic system has been used; (e) require any person having charge of, or otherwise concerned with the operation of such electronic system to provide him reasonable technical and

that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	other assistance as he may require for the purposes of clauses (a), (b) and (c); and (f) require any person who is in possession of decryption information of under investigation electronic system, device or data to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence. Explanation.-Decryption information means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable form and from cipher text to its plain text. (2) The police officer may, subject to the proviso, require a service provider to submit subscriber information relating to such services in respect of a person under investigation in that service provider's possession or control necessary for the investigation of the offence: Provided the investigating officer shall get prior permission to investigate any service provider from the licensing authority where prior permission of the licensing authority is required under any law to investigate the licensed service provider. (3) Any person who obstructs the lawful exercise of the powers under sub-sections (I) or (2) shall be liable to punishment with imprisonment of either description for a term which may extend to one year, or with fine not exceeding one hundred thousand rupees, or with both.
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 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	*There are no legislative provisions that specifically provide for Search and Seizure of computer data.* ***PECO 2009:*** 25. Establishment of investigation agencies and prosecution.-The Federal Government shall establish a specialized investigation and prosecution cell within Federal Investigation Agency to investigate and prosecute the offences under this Ordinance: Provided that till such time any agency is so established, the investigation and prosecution of an offence shall be conducted in accordance with the provisions of

grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	the Code: Provided further that any police officer investigating an offence under this Ordinance may seek assistance of any special investigation agency for any technical in put, collection and preservation of evidence. *Code of Criminal Procedure, 1898 (Act V of 1898) to read in conjunction with section 3 of the Electronic Transactions Ordinance, 2002:* **77. (1) Warrants to whom directed.-** A warrant so arrest shall ordinarily be directed to one or more police officers, but any Court issuing officer is immediately available, direct it to any other persons or persons and such persons shall executed the same. (2) Warrants to several persons. When a warrant is directed to more officers or persons than one; it may be executed by all, or by any one or more, of them. **79. Warrant directed to police officer**.- A warrant directed or other person executing a warrant of arrest shall notify the substances thereof to the person to be arrested, and, if so required, shall show him the warrant. 80. Notification of substance of warrant.- The police officer or other person executing a warrant of arrest shall notify the substance thereof to the person to be arrested, and, if so required, shall show him the warrant. **B. -Search-warrants** **96. When search warrant may be issued.-**(1) Where any Court has reason to believe that a person to whom a summons or order under section 94 or a requisition under section 95, sub-section (1), has been or might be addressed, will not or would not produce the documents or thing as required by such summons or requisition. or where such documents or thing is not known to the Court to be in the possession of any person. or where the Court considers that the purposes of any inquiry, trial or other proceedings under this Code will be served by a general search or inspection,

	it may issue a search-warrant; and the person to whom such warrant is directed, may search or inspect in accordance therewith and the provisions hereinafter contained. **99. Disposal of things found in search beyond jurisdiction.-** When in the execution of a search-warrant at any place beyond the local limits of the jurisdiction of the Court which issued the same, any of the things for which search is made, are found, such things, together with list of the same prepared under the provisions hereinafter contained, shall be immediately taken before the Court issuing the warrant, unless such place is nearer to the Magistrate having jurisdiction therein than to such Court, in which case the list and things shall be immediately taken before such Magistrate; and unless there by good cause to the contrary, such Magistrate shall make an order authorizing them to be taken to such Court. **99A. Power to declare certain publications forfeited and to issue search-warrants for the same.-** (1) Where--- (a) any newspaper, or book as defined in the 6[West Pakistan Press and Publications Ordinance, 1963, or any other law relating to press and publications for the time being in force,] or (b) any document, wherever printed, appears to the Provincial Government to contain any reasonable or seditious matter or any matter which is prejudicial to national integration or any matter which promotes or is intended to promote feelings of enmity or hatred between different classes of the citizens of Pakistan or which is deliberately and maliciously intended to outrage the religious feelings of any such class by insulting the religion or the religious beliefs of that class 7[or any matter of the nature referred to in clause (ii) of sub-section (1) of section 24 of the West Pakistan Press and Publications Ordinance, 1963,] that is to say, any matter the publication of which is punishable under section 123-A or section 124A or section 153A or section 295A 7[or Section 298A or section 298B or Section 298C] of the

	Pakistan Penal Code, the Provincial Government may, by notification in the official Gazette, stating the grounds of its opinion declare every copy of the issue of the newspaper containing such matter, and every copy of such book or other document to be forfeited to Government, and thereupon any police officer may seize the same wherever found in Pakistan and any Magistrate may be warrant authorize any police officer not below the rank of sub-inspector to enter upon and search for the same in any premises where any city of such issue or any such book or other document may be or may be reasonably suspected to be. (2) In sub-section (1) "document" includes also any painting, drawing or photograph, or other visible representation. **102. Persons incharge of closed place to allow search.-** (1) Wherever any place liable to search or inspection under this Chapter is closed, any person residing on, or being incharge of such place shall, on demand of the officer or other person executing the warrant, and on production of the warrant, allow him free ingress thereto, and afford all reasonable facilities for a search therein. (2) If ingress into such place cannot be so obtained, the officer or other person executing the warrant may proceed in manner provided by section 48. (3) Where any person in or about such place is reasonably suspected of concealing about his person any article for which search should be made, such person may be searched. If such person is a woman, the directions of section 52 shall be observed. **103. Search to be made in presence of witnesses. -**(1) Before making a search under this Chapter, the officer or other person about to make it shall call upon two

	or more respectable inhabitants of the locality in which the place to be searched is situate to attend and witness the search and may issue an order in writing to them or any of them so to do. (2) The search shall be made in their presence, and a list of all things seized in the course of such search and of the places in which they are respectively found shall be prepared by such officer or other person and signed by such witnesses but no person witnessing a search under this section shall be required to attend the Court as a witness of the search unless specially summoned by it. (3) Occupant of place searched may attend. The occupant of the place searched, or some person in his behalf, shall in every instance be permitted to attend during the search, and a copy of the list prepared under this section, signed by the said witnesses, shall b e delivered to such occupant or person at his request. (4) When any person is searched under section 102, sub-section (3), a list of all things taken possession of shall be prepared, and a copy thereof shall be delivered to such person at his request. (5) Any person who, without reasonable cause, refuses or neglects to attend any witness a search under this section, when called upon to do so by an order in writing delivered or tendered to him, shall be deemed to have committed an offence under section 18 of the Pakistan Penal Code. **104. Power to impound document, etc., produced**.- Any Court may, if it thinks fit impound any document or thing produced before it under this Code. **105. Magistrate may direct search in his presence.-** Any Magistrate may direct a search to be made in his presence of any place for the search of which he is competent to issue a search-warrant.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:	**27. Real-time collection of traffic data.-** (1) The Federal Government may require a licensed service provider, within its existing or required technical capability, to collect or record through the application of technical means or to

a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	co-operate and assist any law enforcement or intelligence agency in the collection or recording of traffic data or data, in real-time, associated with specified communications transmitted by means of an electronic system. (2) The Federal Government may also require the service provider to keep confidential the fact of the execution of any power provided for in this section and any information relating to it.
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: ito collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may	**Pakistan Telecommunication (Re-organization) Act, 1996** **54. National Security.—**(1) Notwithstanding anything contained in any law for the time being in force, in the interest of national security or in the apprehension of any offence, the Federal Government may authorise any person or persons to intercept calls and messages or to trace calls through any telecommunication system. (2) During a war or hostilities against Pakistan by any foreign power or internal aggression or for the defense or security of Pakistan, the Federal Government shall have preference and priority in telecommunication system over any licensee. (3) Upon proclamation of emergency by the President, the Federal

instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	Government may suspend or modify all or any order or licences made or issued under this Act or cause suspension of operation, functions or services of any licensee for such time as it may deem necessary. Provided that the Federal Government may compensate any licensee whose facilities or services are affected by any action under this sub-section. **PECO [check: "traffic data or data"]** **27. Real-time collection of traffic data.-** (1) The Federal Government may require a licensed service provider, within its existing or required technical capability, to collect or record through the application of technical means or to co-operate and assist any law enforcement or intelligence agency in the collection or recording of traffic data or data, in real-time, associated with specified communications transmitted by means of an electronic system. (2) The Federal Government may also require the service provider to keep confidential the fact of the execution of any power provided for in this section and any information relating to it.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its	**Electronic Transactions Ordinance, 2002** **32. Application to acts done outside Pakistan.** The provisions of this Ordinance shall apply notwithstanding the matters being the subject hereof occurring outside Pakistan, in so far as they are directly or indirectly connected to, or have an effect on or bearing in relation to persons, information systems or events within the territorial jurisdiction of Pakistan.cv **PECO 2009**: **1. Short title, extent application and commencement**.-(I) This Ordinance may be called the Prevention of Electronic Crimes Ordinance, 2009. (2) It extends to the whole of Pakistan. (3) It shall apply to every person who commits an offence under this Ordinance irrespective of his nationality or citizenship whatsoever or in any place outside or inside Pakistan, having detrimental effect on the security of Pakistan or its nationals or national harmony or any property or any electronic system or data located in Pakistan or any electronic system or data capable of being connected, sent to, used by or with any electronic system in Pakistan.

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

on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.	

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and	

requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the	

execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:	

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

similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	

Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	**29. Trans-border access.-** For the purpose of investigation the Federal Government or the investigation agency may, without the permission of any foreign Government or international agency access publicly available electronic system or data notwithstanding the geographically location of such electronic system or data, or access or receive, through an electronic system, data located in foreign country or territory, if it obtains the lawful and voluntary consent of the person who has the lawful authority to disclose it: Provided that such access is not prohibited under the law of the foreign Government or the international agency: Provided further that the investigating agency shall inform in writing the Ministry of Foreign Affairs of Government of Pakistan and other relevant agencies as the case may be about the investigation conducted under this section.
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a	

similar domestic case.	
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2,	

Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	