Federal Investigation Agency (FIA)
Council of Europe
Microsoft

Cybercrime training workshop, Islamabad, Pakistan, February 2010

Cybercrime legislation in Pakistan

Alexander Seger / Zahed Jamil

Alexander Seger
Council of Europe,
Strasbourg, France
Tel +33-3-9021-4506
alexander.seger@coe.int

www.coe.int/cybercrime

1

Budapest Convention on Cybercrime

www.coe.int/cybercrime

- Criminalising conduct
- Investigative tools
- International cooperation

Elaborated by Council of Europe (2001) but any country can accede

Council of Europe
www.coe.int
Created 1949 – 47 Member States
Human Rights – Democracy – Rule of Law

Council of Europe

Legislation on cybercrime 2

2

1 Definition of terms

Council of Europe

Defining key terms in legislation:

- "Computer system"
- "Computer data"
- "Service provider"
- "Traffic data"

3

Article 1 of the Convention on Cybercrime:

4

Council of Europe

- "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

- "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

- "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

- "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

4

Legislation in Pakistan: Prevention of Electronic Crimes Ordinance (PECO), 2009

1 Definition of terms

(1) Definitions

5

(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

(l) "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;

(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;

(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;

Council of Europe

Legislation on cybercrime

5

2 Substantive Criminal Law

Legislation to deal with – as a minimum:

- **Illegal access to a computer system** ("hacking", circumventing password protection, key-logging, exploiting software loopholes etc)
- **Illegal interception** (violating privacy of data communication)
- **Data interference** (malicious codes, viruses, trojan horses etc)
- **System interference** (hindering the lawful use of computer systems)
- **Misuse of devices** (tools to commit cyber-offences)
- **Computer-related forgery** (similar to forgery of tangible documents)
- **Computer-related fraud** (similar to real life fraud)
- **Child pornography**
- **Infringement of copyright and related rights**

Criminalising specific techniques/technologies or conduct?

Council of Europe

Legislation on cybercrime 6

6

Budapest Convention and corresponding provisions in Pakistan legislation – Substantive law

Budapest Convention	Pakistan Legislation
Art 2 Illegal access	PECO 3. Criminal access , 4. Criminal data access and 10. Unauthorized access to code
Art 3 Illegal interception	PECO 16. Unauthorized interception
Art 4 System interference	PECO 5. Data damage, 12. Malicious code, 17. Cyber terrorism [?]
Art 5 Data interference	PECO 6. System damage, 12.
Art 6 Misuse of devices	PECO 9. Misuse of electronic system or electronic device
Art 7 Computer-related forgery	PECO 8. Electronic forgery, 14. Spamming, 15. Spoofing
Art 8 Computer-related fraud	7. Electronic fraud
Art 9 Child pornography	-
Art 10 Infringement of copyright and related rights	Copyright Ordinance, 1962

7

Article 2 of the Convention: illegal access

- Establish as criminal offences under 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.

8

Pakistan – PECO 2009

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 of the Convention: illegal interception

- **Establish as criminal offences under 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.**

Pakistan – PECO 2009

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 of the Convention: data interference

- **Establish as criminal offences under domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.**
- **A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.**

Pakistan – PECO 2009

2 Substantive criminal law

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.

Pakistan – PECO 2009

2 Substantive criminal law

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 I.- 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 any person 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 of the Convention: system interference

- Establish as criminal offences under 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.

Pakistan – PECO 2009

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.-

Article 6 - Misuse of devices

1 Establish as criminal offences under domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Pakistan – PECO 2009

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.

Article 7 - Computer-related forgery

- Establish as criminal offences under domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Pakistan – PECO 2009

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 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.

Pakistan – PECO 2009

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.

Pakistan – PECO 2009

15. Spoofing.(I) 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

Council of Europe

➢Establish as criminal offences under 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.

Pakistan – PECO 2009

Council of Europe

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.

Article 9 - Child pornography

1 Establish as criminal offences 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.

Article 9 - Child pornography

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 – Pakistan Penal Code Act 1860: In combination with 20. PECO

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

293. Sale, etc., of obscene objects to young person

Article 10 - Copyright and related rights

1 Establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 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.

Pakistan – Copyright Ordinance, 1962: 2 Substantive criminal law

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 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,

hall 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),

Council of Europe

29

3 Procedural Law

Council of Europe

Legislation to provide for – as a minimum:

- **Expedited preservation of stored computer data**
- **Expedited preservation and partial disclosure of traffic data**
- **Production order**
- **Search and seizure of stored computer data**
- **Real-time collection of traffic data**
- **Interception of content data**
- **Procedural safeguards**

30

Budapest Convention and corresponding provisions in Pakistan legislation – Procedural law

Budapest Convention	Pakistan Legislation
Art 14 Scope of procedural provisions	PECO 20. Other offences ETO 2002 3. Legal recognition of electronic forms
Art 16 Expedited preservation of stored computer data	PECO 28. Retention of traffic data
Art 17 Expedited preservation and partial disclosure of traffic data	
Art 18 Production order	PECO 26. Powers of officer
Art 19 Search and seizure of stored computer data	PECO Art 25. Establishment of investigation agencies and prosecution CPC, ETO 2002
Art 20 Real-time collection of traffic data	PECO 27. Real-time collection of traffic data
Art 21 Interception of content data	Telecommunication (Re-organization) Act, 1996, Art 54. National Security, PECO 27[?]

31

3 Procedural law

Article 14 – Scope of procedural provisions

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.

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.

Council of Europe

Legislation on cybercrime 32

32

Pakistan legislation

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.

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.

Article 15 - Conditions and safeguards

1 Each Party shall ensure that ... the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Article 16 of the Convention – Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

Pakistan legislation - PECO

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.

[Can a service provider or a person be ordered to preserve specific data?]

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

37

Article 18 - Production order

1 ...measures to empower 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.

3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

38

Pakistan legislation - PECO

26. Powers of officer.-(l) 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 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.

Pakistan legislation - PECO

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 (l) 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 Measures to ensure that where authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

Article 19 - Search and seizure of stored computer data

3 Measures to empower 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 Measures to empower 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.

Pakistan legislation

PECO

Art 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 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.

Art 26 (see above)

Pakistan legislation

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
(2) Warrants to several persons.

79. Warrant directed to police officer
B. --- Search-warrants
96. When search warrant may be issued.
99. Disposal of things found in search beyond jurisdiction
99A. Power to declare certain publications forfeited and to issue search-warrants for the same.-
102. Persons incharge of closed place to allow search
103. Search to be made in presence of witnesses
104. Power to impound document, etc.
105. Magistrate may direct search in his presence

Article 20 - Real-time collection of traffic data

1 measures to empower competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 measures 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.

Pakistan legislation – PECO

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.

Article 21 - Interception of content data

1 Measures, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or

ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Measures 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.

Pakistan Legislation

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 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.

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.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution

Article 22 – Jurisdiction

3 Procedural law

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.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution

Article 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.

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.

4 International Cooperation

Chapter III of the Convention - International cooperation

Section 1 – General principles

- **Art 23 General principles on international cooperation**
- **Art 24 Principles related to extradition**
- **Art 25 Principles related to mutual legal assistance**
- **Art 26 Spontaneous information**
- **Art 27 MLA in the absence of applicable international instruments**
- **Art 28 Confidentiality and limitation on use**

Pakistan Legislation - PECO

30. International cooperation.- (1) The Federal Government may cooperate with any foreign Government, Interpol or any other international agency with whom it has, or establishes, reciprocal arrangements for the purposes of investigations or proceedings concerning offences related to electronic system and data, or for the collection of evidence in electronic form of an offence or obtaining expeditious preservation and disclosure of traffic data or data by means of an electronic system or real-time collection of traffic data associated with specified communications or interception of data.

(2) The Federal Government may, without prior request, forward to such foreign Government, Interpol or other international agency, any information obtained from its own investigations if it considers that the disclosure of such information might assist the other Government or agency in initiating or carrying out investigations or proceedings concerning any offence.

(3) The Federal Government may require the foreign Government, Interpol or other international agency to keep the information provided confidential or use it subject to some conditions.

(4) The investigating agency shall, subject to approval of the Federal Government, be responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

(5) The Federal Government may refuse to accede to any request made by such foreign Government, Interpol or international agency if the request concerns an offence which is likely to prejudice its sovereignty, security, public order or other essential interests.

(6) The Federal Government may postpone action on a request if such action would prejudice investigations of proceedings conducted by its investigation agency

Chapter III - International cooperation 4 International cooperation
Section 2 – Specific provisions

Art 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.

Art 30 - Expedited disclosure of preserved computer data

4 International cooperation

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.

Council of Europe

Legislation on cybercrime 55

55

Art 31 - Mutual assistance regarding accessing stored computer data

4 International cooperation

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.

Council of Europe

Legislation on cybercrime 56

56

Art 32 - Trans-border access to stored computer data (public/with consent)

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.

Pakistan Legislation - PECO

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.

Art 33 - Mutual assistance in real-time collection of traffic data

Council of Europe

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.

59

Art 34 - Mutual assistance regarding interception of content data

Council of Europe

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.

60

Art 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.