Prevention of Electronic Crimes Ordinance, 2007 an ordinance

To make provision for prevention of the electronic crimes, WHEREAS it is expedient to prevent any

action directed against the confidentiality, integrity and availability of electronic system, networks and

data as well as the misuse of such system, networks and data by providing for the punishment of such

actions and to provide mechanism for investigation, prosecution and trial of offences and for matters

connected therewith or ancillary thereto; AND WHEREAS the National Assembly stands dissolved and

the President is satisfied that the circumstances exist which render it necessary to take immediate action;

Now, THEREFORE, in exercise of the powers conferred by clause (1) of Article 89 of the Constitution of

the Islamic Republic of Pakistan and in exercise of all powers enabling in that behalf, the president is

pleased to make and promulgate the following Ordinance: -

Short title, extent application and commencement. -

• This Ordinance may be called the Prevention of Electronic Crimes Ordinance, 2007.

• It extends to the whole of Pakistan.

• 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.

• It shall come into force at once.

OFFENCES AND PUNISHMENTS

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.

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.

Data damage

Whoever with intent to illegal gain or cause harm to the public or any person, damages any data is shall

be punished with imprisonment of either description for a term which may extend to three years, or with

fine, or with both.

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.

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.

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.

Misuse of electronic system or electronic device

a. 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:

b. 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.

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, or with both.

Misuse of encryption

Whoever for the purpose of commission of an offence or concealment of incriminating evidence,

knowingly and willfully encrypts any incriminating communication or data contained in electronic system

relating to that crime or incriminating evidence, commits the offence of misuse of encryption shall be

punished with imprisonment of either description for a term which may extend to five years, or with fine,

or with both.

Malicious code

a. 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:

b. 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.

Cyber stalking

a. Whoever with intent to coerce, intimidates, or harass any person uses computer, computer network,

internet, network site, electronic mail or any other similar means of communication to. -

• Communicate obscene, vulgar, profane, lewd, lascivious ,

• or indecent language, picture or image;

• make any suggestion or proposal of an obscene nature;

• threaten any illegal or immoral act;

• take or distribute pictures or photographs of any person

• without his consent or knowledge;

• display or distribute information in a manner that

• substantially increases the risk of harm or violence to any

• Other person commits the offence of cyber stalking.

b. Whoever commits the offence specified in sub-section (1) shall be punishable with imprisonment of

either description for a term which may extend to seven years or with fine not exceeding three hundred

thousand rupees, or with both:

Spamming

a. 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.

b. 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.

Spoofing. -

a. 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 spooling.

b. Whoever commits the offence of spooling 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.

Unauthorized interception. -

a. 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?

b. Whoever commits the offence of unauthorized interception described in subsection (1) shall be

punished with imprisonment of either description for a term which may extend to five years, or with fine

not exceeding five hundred thousand rupees, or with both.

Cyber terrorism. -

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 terrorist act commits the offence of cyber

terrorism.

Explanation1: 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.

Explanation2: For the purposes of this section the expression “terroristic act” includes, but is not limited

to, -

i. 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;

ii. Transmission or attempted transmission o a harmful program with the purpose of substantially

disrupting or disabling any computer network operated by the Government or any public entity;

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; o

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.

b. Whoever commits the offence of cyber terrorism and causes death of any person shall be punishable

with death or imprisonment for life, and with line 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.

Enhanced punishment for offences involving sensitive electronic systems. -

a. 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.

b. 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 was a sensitive electronic system.

Of abets, aids or attempts to commits offence

a. 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 this Ordinance shall be guilty

of that offence and shall be liable on conviction to the punishment provided for the offence.

b. Any person who attempts to commit an offence under this Ordinance shall be punished for a term

which may extend to oneha1f 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.

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 mean; 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.

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 he punished with fine not less than one

hundred thousand rupees or the amount involved in the offence whichever is the higher:

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.

Information And Communication Technologies Tribunal

31. Information and Communication Technologies Tribunal

a. As soon as possible after the commencement of this Ordinance, the Federal Government shall, by

notification in the official Gazette, constitute the Information and Communication Technologies Tribunal

whose principal seat shall be at Islamabad.

b. The Tribunal may hold its sittings at such place or places as the Federal Government may decide.

c. The Tribunal shall consist of a chairman and as many members as the Federal Government may

determine but not more than seven members.

d. The Chairman may constitute Benches of the Tribunal and unless otherwise directed by him a Bench

shall consist of not less than two members. A Bench shall exercise such powers and discharge such

functions as may be prescribed. There shall be established at least one Bench in each province.

e. The Federal Government shall appoint the Chairman and members of the Tribunal.

Saving Tribunal’s proceedings

No act or proceedings of the Tribunal shall be called in question in any manner on the ground merely of

any defect in the constitution of the Tribunal.

Right to legal representation

The parties in appeal may either appear in person or authorize one or more legal practitioners, and in case

of a corporate body any of its officers, to present the case before the Tribunal.

Appeal to Tribunals

Any person aggrieved by any of the following orders may, within fifteen days from the date of such order,

prefer an appeal to the Tribunal.

Appeal to High Court

Any person aggrieved by any decision or order of the Tribunal made under section 40 may prefer second

appeal to the respective High Court within thirty days from the date of the decision or order of the Tribunal.