

CYBER LAWS IN PAKISTAN

Lesson # 7

Cyber Laws in Pakistan


- ▶ There are different laws, promulgated in Pakistan.
- ▶ These laws not only deal with crime of Internet
- ▶ These deal with all dimensions related to computer & networks.
- ▶ Two of them are most known.
- ▶ They are:
 - Electronic Transaction Ordinance 2002
 - Electronic / Cyber Crime Bill 2007

Electronic Transaction Ordinance 2002




Electronic Transaction Ordinance 2002

Overview

- ▶ The Electronic Transactions Ordinance (ETO), 2002, was the first IT-relevant legislation created by national lawmakers.
 - ▶ Protection for Pakistani e-Commerce locally and globally.
 - ▶ Protect Pakistan's critical infrastructure
 - ▶ It is heavily taken from foreign law related to cyber crime.
- 


Pre-ETO 2002

- ▶ No recognition of electronic documentation
 - ▶ No recognition of electronic records
 - ▶ No recognition of evidential basis of documents/records
 - ▶ Failure to authenticate or identify digital or electronic signatures or forms of authentication
 - ▶ No online transaction system on legal basis.
 - ▶ Electronic Data & Forensic Evidence not covered.
 - ▶ No Rules for all of these ...
- 

POST ETO 2002




Post ETO 2002

- ▶ Electronic Documentation & Records recognized
 - ▶ Electronic & Digital forms of authentication & identification
 - ▶ Messages through email, fax, mobile phones, Plastic Cards, Online recognized.
- 

ETO 2002


Sections

- There are 43 sections in this ordinance
 - It deals with following 8 main areas relating to e-Commerce.
 - Recognition of Electronic Documents
 - Electronic Communications
 - Web Site
 - Digital Signatures Certification Providers
 - Stamp Duty
 - Attestation, certified copies
 - Jurisdiction
 - Offences
- 

VIOLATION OF PRIVACY INFORMATION




36. Violation of privacy information

- ▶ Gains or attempts to gain access
 - ▶ To any information system with or without any purpose
 - ▶ To acquire the information unauthorized
 - ▶ Imprisonment 7 years
 - ▶ Fine Rs. 1 million
- 

DAMAGE TO INFORMATION SYSTEM



37. Damage to information system

- ▶ Alter, modify, delete, remove, generate, transmit or store information
 - ▶ Create hindrance in information access
 - ▶ knowingly when not authorized to do so
 - ▶ Imprisonment 7 years
 - ▶ Fine Rs. 1 million
- 

OFFENCES TO BE NON-BAIL ABLE

38. Offences to be non-bail able

- ▶ All offences under this Ordinance shall be non-bail able, compoundable and cognizable.

PROSECUTION AND TRAIL OF OFFENCES




39. Prosecution and trial of offences

- ▶ No Court inferior to the Court of Sessions shall try any offence under this Ordinance.


Electronic/Cyber Crime Bill 2007



Overview

- ▶ “Prevention of Electronic Crimes Ordinance, 2007” is in force now
 - ▶ It was promulgated by the President of Pakistan on the 31st December 2007
 - ▶ The bill deals with the electronic crimes included:
 - Cyber terrorism
 - Data damage
 - Electronic fraud
 - Electronic forgery
 - Unauthorized access to code
 - Cyber stalking
 - Cyber Spamming/spoofing
- 

Electronic/Cyber Crime Bill 2007

- ▶ It will apply to every person who commits an offence, irrespective of his nationality or citizenship.
 - ▶ It gives exclusive powers to the Federal Investigation Agency (FIA) to investigate and charge cases against such crimes.
- 

Electronic/Cyber Crime Bill 2007

Punishments


- ▶ Every respective offence under this law has its distinctive punishment which can be imprisonment or/and fine.

Sections

Data Damage:

- ▶ Whoever with intent to illegal gain or cause harm to the public or any person, damages any data, shall come under this section.

Punishment:


- ▶ 3 years
 - ▶ 3 Lac
- 

Electronic/Cyber Crime Bill 2007

Electronic fraud:

- ▶ People for illegal gain get in the way or use any data, electronic system or device or with intent to deceive any person, which act or omissions is likely to cause damage or harm.

Punishment:

- ▶ 7 years
 - ▶ 7 Lac
- 

Electronic/Cyber Crime Bill 2007

Electronic Forgery:

- ▶ Whoever for unlawful gain interferes with data, electronic system or device, with intent to cause harm or to commit fraud by any input, alteration, or suppression of data, resulting in unauthentic data that it be considered or acted upon for legal purposes as if it were authentic

Punishment:

- ▶ 7years
 - ▶ 7 Lac
- 

Electronic/Cyber Crime Bill 2007

Malicious code:

- ▶ Whoever willfully writes, offers, makes available, distributes or transmits malicious code through an electronic system or device, with intent to cause harm to any electronic system or resulting in the theft or loss of data commits the offence of malicious code.

Punishment:


- ▶ 5 years
 - ▶ 5 Lac
- 

Electronic/Cyber Crime Bill 2007

Cyber stalking:

- ▶ Whoever with intent to harass any person uses computer, computer network, internet, or any other similar means of communication to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, picture or image.
- ▶ Threaten any illegal or immoral act
- ▶ Take or distribute pictures or photographs of any person without his knowledge
- ▶ Commits the offence of cyber stalking.

Punishment:


- ▶ 3 Years
 - ▶ 3 Lac
- 

Electronic/Cyber Crime Bill 2007

Spamming:

- ▶ Illegal electronic messages to any person without the permission of the recipient.

Punishment:

- ▶ 6 month
 - ▶ 50,000
- 

Electronic/Cyber Crime Bill 2007

Spoofing:

- ▶ Whoever establishes a website, or sends an electronic message with a fake 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

Punishment:


- ▶ 3 Years
 - ▶ 3 Lac
- 

Offence	Imprisonment (years)	Fine
Criminal Access	3	3 Lac
Criminal Data Access	3	3 Lac
Data Damage	3	3 Lac
System Damage	3	3 Lac
Electronic Fraud	7	7 Lac
Electronic Forgery	7	7 Lac
Misuse of Device	3	3 Lac
Unauthorized access to code	3	3 Lac
Malicious code	5	5 Lac
Defamation	5	5 Lac
Cyber stalking	3	3 Lac
Cyber Spamming	6 months	50,000
Spoofing	3	3 Lac
Pornography	10	-----
Cyber terrorism	Life	10 Million


CRITICISM



Criticism

- ▶ There are seemingly 21 'cyber' issues covered in this Bill
 - ▶ It may seem to cover all aspects of the new digital era.
 - ▶ But detailed look shows quite the contrary.
 - ▶ Practically in all issues the government has gone the extra mile to reinvent a new definition, significantly deviating from the internationally accepted norms.
- 

Criticism

- ▶ There seems to be an elaborate play of words within the document
 - ▶ allow room for the regulating body (FIA) to confuse and entrap the innocent people
 - ▶ The FIA, has been given complete and unrestricted control to arrest and confiscate material as they feel necessary
 - ▶ A very dangerous supposition
 - ▶ Safeguards and Protection
- 

Criticism

▶ One example of the hideous nature of the bill:

- The Government has literally attempted to insert a new word in the English language.
- The word TERRORISTIC is without doubt a figment of their imagination vocabulary
- Hence they attempt to define the word, quite literally compounding the problem at hand
- They have actually defined what real-life terrorism might be
- But fail to explain what they mean by the word Cyber in cyber terrorism.
- the concern is that there happens to be no clear-cut explanation on how a Cyber Terrorism crime is committed.

Why we must know Cyber Laws?

- ▶ Which specific laws apply to Organization.
 - ▶ By law, which information assets need to be protected?
 - ▶ Organizational Policies and Rules
- 