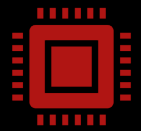
Cyber Laws in Pakistan

Legal regulations and frameworks related to cybersecurity and digital activities in Pakistan

Cybercrime



Activity in which computers or networks are a tool, a target, or a place of criminal activity

Cyber-crime also stated as any use of a computer as an instrument to further illegal ends, such as:

Hacking, malware attacks, phishing, identity theft, online fraud, cyberbullying, DoS attacks, Cyber Espionage, Online Copyright Infringement

Cybercrimes

- Hacking: Unauthorized access to computer systems or networks
- Malware attacks: Distributing malicious software (viruses, ransomware, etc.)
- Phishing: Deceptive attempts to obtain sensitive information, such as passwords or credit card details, by posing as trustworthy.
- Identity theft: Stealing someone's personal information to commit fraud
- Online fraud: Engaging in fraudulent activities on the internet
- Cyberbullying: Harassment, intimidation, or threatening behavior carried out online
- Dos attacks: Overloading a system, network, or website to make it unavailable to users
- Cyber espionage: Illegally accessing and stealing sensitive information for political, economic, or military purposes.
- Online copyright infringement: Unauthorized distribution or reproduction of copyrighted materials online.

Cyber LAWS

It refers to the legal regulations and frameworks related to cybersecurity and digital activities

It is an intersection of many legal fields, like: Intellectual property, privacy etc.

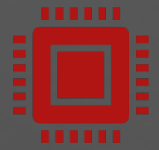
Cyber laws is an attempt to apply laws designed for the physical world to human activity on the Internet

Cyber LAWS in the world

Electronic Commerce Act (Ireland)

Electronic Transactions Act (UK, USA, Australia, New Zealand, Singapore)

Electronic Transactions Ordinance (Hong Kong)



Information Technology Act (India)

Information Communication Technology Act Draft (Bangladesh)

Cyber LAWS in pakistan

- Electronic Transaction Ordinance 2002
- Pakistan Electronic Crime Ordinance 2007 - Expired
- Prevention of Electronic Crimes Act, 2016

ELECTRONIC TRANSACTION ORDINANCE 2002

Overview:

The Electronic Transactions Ordinance (ETO), 2002, was the first IT-relevant legislation created by national lawmakers

A first step and a solid foundation for legal sanctity and protection for Pakistani e-Commerce locally and globally

Laid the foundation for comprehensive Legal Infrastructure

It is heavily taken from foreign law related to cyber-crime

https://pakistancode.gov.pk/pdffiles/administratordbc98dd49f2df3b1d07bb986dcceb9a3.pdf

ETO 2002

Sections

- There are 43 sections in this ordinance
- It deals with following 8 main areas relating to e- Commerce which are:
  - Recognition of Electronic Documents (e.g., pdf)
  - Electronic Communications (e.g., email, text messages)
- Web Site & Digital Signatures Certification Providers
  - Stamp Duty (a type of tax imposed on certain legal documents and transactions)
  - Attestation, notarization (Notarization is an official process that adds a layer of security and verification to important documents and transactions).

ETO 2002

Important Sections are:

- 36. Violation of privacy information
  - gains or attempts to gain access
  - to any information system with or without intent
  - to acquire the information
  - Gain Knowledge
  - Imprisonment 7 years
  - Fine Rs. 1 million

ETO 2002

- 37. Damage to information system, etc.
  - alter, modify, delete, remove, generate, transmit or store information
  - to impair the operation of,
  - or prevent or hinder access to, information
  - knowingly not authorized
  - Imprisonment 7 years
  - Fine Rs. 1 million

Cyber crime

38. Offences to be non-bailable, compoundable and cognizable

- All offences under this Ordinance shall be non-bailable, compoundable and cognizable.

39. Prosecution and trial of offences

- No Court inferior to the Court of Sessions shall try any offence under this Ordinance. ETO 2002

POST ETO 2002

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

Pakistan Electronic Crime Ordinance 2007

http://pklegal.org/pdf/Prevention-of-Electronic-Crimes-Ordinance-2007-(PECO2007).pdf

ELECTRONIC/CYBER CRIME BILL 2007

- OVERVIEW
  - PECO (Pakistan Electronic Crime Ordinance) was promulgated by Musharraf in 2007. Since it was an ordinance, it lapsed in 2009.
  - There was huge uproar against it because innocent people can be charged and framed. It gave excessive powers to FIA (Federal Investigation Agency).
- 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 offers penalties ranging from six months imprisonment to capital punishment for 17 types of cyber crimes
- It applied to every person who commits an offence, irrespective of his nationality or citizenship
- It gave exclusive powers to the Federal Investigation Agency (FIA) to investigate and charge cases against such crimes

Prevention of Electronic Crimes Act, 2016

PREVENTION OF ELECTRONIC CRIMES ACT PECA 1/2

- National Assembly enacted the PECA to provide a comprehensive legal framework to define various kinds of electronic crimes, mechanisms for investigation, prosecution and adjudication in relation to electronic crimes
- Supports Cyber Crime Bill 2007
- The legislation established new offences including
  - illegal access of data (hacking)
  - DOS and DDOS attacks
  - electronic forgery and electronic fraud
  - CYBER TERRORISM

PREVENTION OF ELECTRONIC CRIMES ACT PECA 2/2

- The legislation provides new investigative powers that were unavailable before, such as:
  - production orders for electronic evidence,
  - electronic evidence preservation order,
  - partial disclosure of traffic data,

PUNISHMENTS

- Under this law there are defined punishment for the offence
- Every respective offence under this law has its distinctive punishment which can be imprisonment or fine

OFFENCES AND PUNISHMENTS

- **Section 3:- Unauthorized access to information system or data.-**
  - Whoever with dishonest intention gains unauthorized access to any information system or data shall be punished with imprisonment for a term which may extend to **three months or with a fine** which may extend to fifty thousand rupees or with both.
- **Section 4:- Unauthorized copying or transmission of data.-** Whoever with dishonest intention and without authorization copies or otherwise transmits or causes to be transmitted any data shall be punished with imprisonment for a term which may extend to **six months**, or with fine which may extend to one hundred thousand rupees or with both.

OFFENCES AND PUNISHMENTS

- **Section 5:- Interference with information system or data.-**
  - Whoever with dishonest intention interferes with or damages or causes to be interfered with or damages any part or whole of an information system or data shall be punished with imprisonment, which may extend to two years, or with a fine, which may extend to five hundred thousand rupees or with both.

- **Section 6:- Unauthorized access to critical infrastructure information system or data.-**
  - Whoever with dishonest intention gains unauthorized access to any critical infrastructure information system or data shall be punished with imprisonment, which may extend to three years, or with a fine, which may extend to one million rupees, or with both.

OFFENCES AND PUNISHMENTS

- **Section 7:- Unauthorized copying or transmission of critical infrastructure data.-**
  - Whoever, with dishonest intention and without authorization, copies or otherwise transmits or causes to be transmitted any critical infrastructure data shall be punished with imprisonment for a term which may extend to five years or with a fine which may extend to five million rupees or with both.

- **Section 8:- Interference with critical infrastructure information system or data**.-
  - Whoever with dishonest intention interferes with or damages, or causes to be interfered with or damaged, any part or whole of a critical information system or data, shall be punished with imprisonment which may extend to seven years or with a fine which may extend to ten million rupees or with both.

OFFENCES AND PUNISHMENTS

- **Section 9:- Glorification of an offense and hate speech.-**
  - Whoever prepares or disseminates information, through any information system or device, with the intent to glorify an offense and the person accused or convicted of a crime relating to terrorism or activities of proscribed organizations shall be punished with imprisonment for a term which may extend to **five years** or with fine which may extend to ten million rupees or with both.

OFFENCES AND PUNISHMENTS

- **Section 10:- Cyber terrorism.**
  - Whoever commits or threatens to commit any of the offenses under sections 6, 7, 8, or 9, where the commission or threat is with the intent to
  - (a) coerce (force someone to do something against their will), create a sense of fear, panic, or insecurity in the Government or the public or a section of the public or community or sect or create a sense of fear or insecurity in society; or
  - (b) advance inter-faith, sectarian, or ethnic hatred,
  - shall be punished with imprisonment of either description for a term extending to fourteen years or with a fine extending to fifty million rupees or with both.

OFFENCES AND PUNISHMENTS

- **Section 11:- Electronic forgery**.-
  - Whoever interferes with or uses any information system, device, or data with the intent to cause damage or injury to the public or any person, 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, even though the data is directly readable and intelligible or not, shall be punished with imprisonment of either description for a term which may extend to **three years**, or with fine which may extend to two hundred and fifty thousand rupees or with both.

- **Section 12:- Electronic fraud.**-
  - Whoever with the intent for wrongful gain interferes with or uses any information system, device or data or induces any person to enter into a relationship or deceives 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 for a term which may extend to **two years** or with fine which may extend to ten million rupees or with both.

OFFENCES AND PUNISHMENTS

- **Section 13:- Making, obtaining, or supplying device for use in offence.-**
  - Whoever produces, makes, generates, adapts, exports, supplies, offers to supply or imports for use any information system, data or device, with the intent to be used or believing that it is primarily to be used to commit or to assist in the commission of an offence under this Act shall, without prejudice to any other liability that he may incur in this behalf, be punished with imprisonment for a term which may extend to **six months** or with fine which may extend to fifty thousand rupees or with both.
- **Section 14:- Unauthorized use of identity information.-**
  - Whoever obtains, sells, possesses, transmits or uses another person's identity information without authorization shall be punished with imprisonment for a term which may extend to **three years** or with fine which may extend to five million rupees, or with both.

OFFENCES AND PUNISHMENTS

- **Section 15:- Unauthorized issuance of SIM cards etc.-**
  - Whoever sells or otherwise provides a subscriber identity module (SIM) card ,or other portable memory chip designed to be used in cellular mobile or wireless phones for transmitting information without obtaining and verification of the subscriber's antecedents in the mode and manner for the time being approved by the Authority shall be punished with imprisonment for a term which may extend to **three years** or with fine which may extend to five hundred thousand rupees or with both.
- **Section 16:- Tampering, etc., of communication equipment.-**
  - Whoever unlawfully or without authorization changes, alters, tampers with or re-programs the unique device identifier of any communication equipment, including a cellular or wireless handset, and starts using or marketing such device for transmitting and receiving information shall be punished with imprisonment, which may extend to **three years** or with fine which may extend to one million rupees or with both.

OFFENCES AND PUNISHMENTS

- **Section 17:- Unauthorized interception.-**
  - Whoever withdishonest intention commits unauthorized interception by technical means shall be punished with imprisonment of either description for a term which may extend to **two years** or with fine which may extend to five hundred thousand rupees or with both.

- **Section 18:- Offences against dignity of natural person.-**
  - Whoever intentionally and publicly exhibits or displays or transmits any information through any information system, which he knows to be false, and intimidates or harms the reputation or privacy of a natural person, shall be punished with imprisonment for a term which may extend to **three years** or with fine which may extend to one million rupees or with both:

OFFENCES AND PUNISHMENTS

- **Section 19:- Offences against modesty of a natural person and minor.-**
  - 1. Whoever intentionally and publicly exhibits or displays or transmits any information
    - (a) superimposes a photograph of the face of a natural person over any sexually explicit image or video, or
    - (b) distorts the face of a natural person or includes a photograph or a video of a natural person in sexually explicit conduct or
    - (c) threatens a natural person with any sexual act or any sexually explicit image or video of a natural person or
    - (d) cultivates, entices, or induces a natural person to engage in a sexually explicit act,
  - through an information system to harm a natural person or his reputation, or to take revenge, or to create hatred or to blackmail, shall be punished with imprisonment for a term which may extend to **seven years or with a fine which may extend to five million rupees or with both**.

OFFENCES AND PUNISHMENTS

- **Section 20:- Malicious code.-**
  - Whoever willfully and without authorization writes, offers, makes available, distributes or transmits malicious code through an information system or device, with intent to cause harm to any information system or data resulting in the corruption, destruction, alteration, suppression, theft or loss of the information system or data shall be punished with imprisonment for a term which may extend to **two years** or with fine which may extend to one million rupees or with both.

OFFENCES AND PUNISHMENTS

- **Section 21:- Cyber stalking.-**
  - Whoever commits the offense specified in sub-section (1) shall be punished with imprisonment for a term which may extend to **one year** or with a fine which may extend to one million rupees or with both:
- **Section 22:- Spamming.-**
  - Whoever commits the offense of spamming as described in sub-section (1) or engages in direct marketing in violation of sub-section (2) for the first time shall be punished with a fine not exceeding fifty thousand rupees, and for every subsequent violation shall be punished with imprisonment for a term which may extend to **three months** or with fine which may extend to one million rupees or with both.

OFFENCES AND PUNISHMENTS

- **Section 23:- Spoofing.-**
  - Whoever commits spoofing shall be punished with imprisonment for a term which may extend to **three years** or with fine which may extend to five hundred thousand rupees or with both.

Thank you