Center for Global & Strategic Studies

Islamabad

Cyber Crimes And Laws To Prevent It

By Mr. Waqar Mirza, Research Intern at Center for Global & Strategic Studies (CGSS), Islamabad

Published on 28th July 2020

Pakistan is a relatively novel country in the evolving cyber world. Rapid development of information technology is transforming our society and its institutions. It has wide range of implications on every aspect of life and has directly or indirectly affected almost all sectors of the society. Many electronic crimes which are still prevailing in Pakistan are not covered under any legal boundary, including the recently enacted

PECA Act 2016 does not cover many of the existing crimes. The availability of computers and the internet connections, provide unprecedented opportunities to communicate and learn in Pakistan. However, some individuals do exploit the power of the internet for illegal purposes. Thus, we can say that Pakistan is not free from cyber-attack problems.

Online activities

a. Social networking
b. Internet suffering
c. Audio video interactions
d. Communication
e. Entertainment
f. Online shopping
g. Maps, GPS
h. Online education
i. Online auction
j. Information sharing
k. Medical assistance
l. Online games

Cyber Crime

Activity in which computers or networks are a tool, a target, or a place of criminal activity. Cybercrime also refers to use of a computer as an instrument to further illegal objectives. It also includes the traditional crimes in which computers or networks are used to enable the illicit activities.

Examples

a. Committing fraud
b. Violating privacy
c. Stealing identities
d. Hacking
e. Cyber Defamation
f. Credit card frauds
g. Threatening emails
h. Online banking frauds

Cyber Laws

Cyber laws are defined as the legal framework related to the use of communications technology, particularly "cyberspace", i.e. the internet. It is an intersection of many legal fields.

www.cgss.com.pk
info@cgss.com.pk

Cyber Laws in the World

a. Electronic Transmission Act
b. Electronic Commerce Act
c. Electronic Commission Acct
d. Information and Technology Act
e. Information Communication Act

Cyber Laws in Pakistan

The law on cybercrime is a relatively new one in the Pakistani legal system and most of it has been derived from laws being practiced in other countries. Following are the cyber laws in Pakistan.

a. Electronic Transaction Ordinance (ETO) 2002
b. Prevention of Electronic Crimes Ordinance (PECA) 2007
c. Prevention of Electronic Crimes Act (PECA) 2016

Pakistan's Electronic Transaction Ordinance (ETO) 2002

The ETO was the first IT-relevant legislation created by national lawmakers. It was a solid foundation for legal sanctity and protection for Pakistani e-Commerce locally and globally. It laid the foundation for a unique legal infrastructure. President Pervez Musharraf on September 11 promulgated the Electronic Transactions Ordinance 2002.

It was enacted to provide recognition and facilitation of documents, records, information, communications and transactions in electronic form etc.

Pre- ETO scenario

Before ETO there was no recognition of electronic documentation, electronic records and electronic data. The forensic evidence was not covered. There was not any proper rule or regulation to regulate electronic flow of information and no online transaction could be legally binding.

Post-ETO scenario

a. Electronic and Digital forms of authentication and identification given legal sanctity
b. Electronic Documentation and records recognized
c. Message through e-mail, fax, mobile phones, plastic card were online recognized.

Electronic Transaction Ordinance (ETO) 2002

There are 43 sections in this ordinance. It deals with the cases like recognition of electronic documents, electronic communications, digital signature regime and its evidential consequences, stamp duty, attestation, notarization and certified copies and web site and digital signatures certification providers.

Important sections are

Section	Crime	Crime Detail	Imprisonment	Fine
36	Violation of privacy of information	Gain or attempt to gain access to any information with or without intention	7 years	1 million
37	Damage to information system	Alter, modified, delete, remove, generate, transmit or store information or prevent or hinder access to information	7 years	1 million

All the offences mentioned in ETO 2002 are non-bail able, compound able and cognizable (section 38). And no Court inferior to the Court of Session shall try any offence under this Ordinance (section 39).

Prevention of Electronic Crime Ordinance (PECO) 2007

It was promulgated in June 2007. It deals with the electronic crimes like, cyber terrorism, data damage, electronic fraud, electronic forgery, cyber spamming/spoofing, cyber stalking and unauthorized access to code. It imparts penalties from six months imprisonment to capital punishment for 17 types of cybercrimes. It gives exclusive powers to the Federal Investigation Agency (FIA) to investigate and charge cases against such crimes.

Prevention of Electronic Crimes Act (PECA) 2016

There are total 55 sections in PECA. It is in operation from August-2016 to till now. The 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. It also deals with new offences like illegal access of data, DOS AND DDOS attacks, electronic forgery and electronic fraud and cyber terrorism. It also support cybercrime bill 2007. The legislation provides more investigative powers which were unavailable before like:

a. Production orders for electronic evidence,
b. Electronic evidence preservation order, partial disclosure of traffic data,
c. Search and seizure of digital forensic evidence using technological means and
d. Real time collection of data under certain circumstances and other enabling power which are necessary to effectively investigate cybercrime cases.

Every respective offence has distinctive punishment which can be imprisonment or fine.

Offence	Imprisonment	Fine (PKR)
Cyber terrorism	Life	10 million
Pornography	10 years	3 lacs
Electronic fraud	7 years	7 lacs
Electronic forgery	7 years	7 lacs

Malicious code	5	5 lacs
Defamation	5	5 lacs
Criminal access	3	3 lacs
Criminal data access	3	3 lacs
Data damage	3	3 lacs
System damage	3	3 lacs
Misuse of device	3	3 lacs
Unauthorized access to code	3	3 lacs
Cyber stalking	3	3 lacs
Cyber spamming	6 months	50,000

Legal authorities doing against cybercrimes

In 2002, FIA formed a specialized wing for investigating information and Communication Technology (ICT) related crimes. This wing is commonly known as the

National Response Centre for Cyber Crimes (NR3C). This wing of the FIA has state of the art Digital Forensic Laboratories managed by highly qualified Forensic Experts and is specialized in Computer and Cell Phone Forensics, cyber/electronic crime, investigation, information System Audits and Research and Development. Officers of the NR3C carry out training for officers of Police and other Law Enforcement Agencies of Pakistan.

FIA REPORT FOR THE YEAR 2019 (January 06, 2020)

The Federal Investigation Agency (FIA) has issued a report for the year 2019 in which 15,038 cases of cybercrime were registered. According to the report cases like absconders, illegally operating telephone exchanges, gangs involved in buying and selling via fake credit cards and harassment of housewives and girls in Punjab's educational institutes via Facebook and WhatsApp were registered.

Cybercrime prevention tips

To secure your smart phones, online banking, Facebook, Wi-Fi and browsing, FIA provides following tips:

a. Never share your PASSWORDS
b. Never reveal your PERSONAL INFORMATION
c. Always keep social media profiles PRIVATE
d. Report inappropriate/ abusive contents
e. Never communicate with strangers

f. Always LOG OFF before you leave

g. Always use secure connection

How to lodge a complaint

a. Cyber rescue helpline 9911

b. www.nr3c.gov.pk

c. complaints@fia.gov.pk

d. help@nr3c.gov.pk

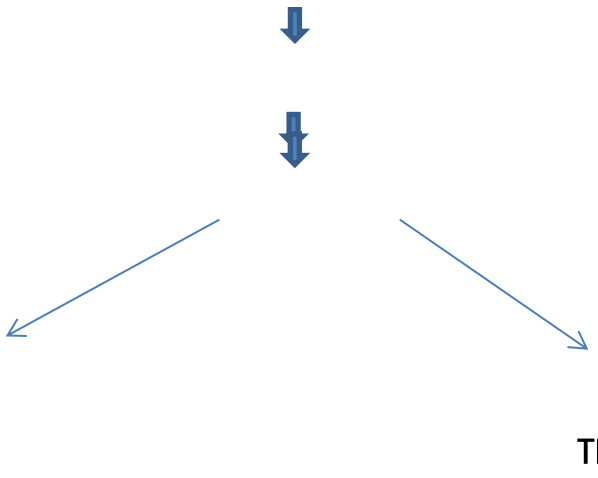
Procedure after complaint

Complaint

Inquiry

FIR

INVESTIGATION



BAIL TRIAL

Ratio of reporting

Only 5% reports are lodged every year and 95% cases are not reported.

Reasons

a. Difficult investigation process
b. Delays in judicial proceeding
c. Ill repute

Conclusion

There are many challenges to control cybercrimes in Pakistan. Several attempts are in process to make cyber laws more affective in Pakistan. To prevent these crimes education and public awareness is necessary. Due to lack of awareness of existing cybercrimes in Pakistan, people are facing many problems. Even the law enforcement agencies face challenges due to the complex nature of these crimes. A proper understanding of such crimes in needed to control them. Without knowing them, we cannot make proper laws to punish the criminals. New tools for enforcing laws on the use of internet is necessary. Online consumer protection legislation should be introduced to protect the online consumer and online business industry. Illegal purchase and sale of goods on the internet shall also be prohibited and penalized. There is a dire need to get the information as early as possible for the investigation purposes. If the telecommunication industry is not providing latest data and detail of

it, then it will make very difficult for law enforcement agencies to investigate the crime expeditiously.