The law dealing with cyber crimes in Pakistan is Prevention of Electronic Crimes Act, 2016 ("**Act**") which is applicable to every citizen of Pakistan wherever he may be and to every other person who is stationed in Pakistan for the time being.

The law address to following types of cyber crimes under the Act:

1. **Access or interfere** the data or information system and copying or transmission of data; (Section 3, 4 and 5 of the Act).
2. Unauthorized **access**, unauthorized **copying**, unauthorized **transmitting** or unauthorized **interfering** with the critical infrastructure OR threaten to commit any of the aforesaid offences with an intention to coerce, intimidate, create a sense of fear, panic, insecurity or public or community/society (Sections 6, 7 and 8 of the Act).
3. Prepare or disseminate information through any information system or device with the intent to **glorify an offence relating to terrorism**, or any person convicted of a crime relating to terrorism OR threaten to commit any of the aforesaid offences with an intention to coerce, intimidate, create a sense of fear, panic, insecurity or public or community/society (Section 9 of the Act).
4. Whosoever prepares or disseminates any **Hate Speech**, information that invites **motivation of people to fund or recruits for terrorism** through any information system or device (Sections 11 & 12 of the Act).
5. **Electronic forgery** and **electronic fraud** committed by interfering with any information system, device or data with the intent to cause damage or injury to the public; or to make any illegal claim; or title or to cause any person to part with property; or to enter into a contract; to commit fraud; alteration, deletion or suppression of data etc. (Sections 13 & 14 of the Act).
6. An act to **manufacture, generate, adapt, export, supply**, **offer** to supply or **import** any information system, data or device, with an 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. (Section 15 of the Act).
7. Unauthorized **use of another person's identity** information or to obtain, sell, possess or transmit such information. (Sections 16 of the Act).
8. **Issuance of SIM** (subscriber identity module); R-IUM (re-useable identification module); or UICC (universal integrated circuit) or any other module designed for authenticating users to establish connection with the network and to be used in cellular mobile, wireless phone or other digital devices without obtaining and verification of the subscriber's antecedents. (Section 17 of the Act).
9. **Dignity of Natural Person**: Public exhibit or display or transmission of any information knowingly that such information is false and intimidate or harm the reputation or privacy of a natural person through an information system. (Section 20 of the Act).
10. **Modesty of Natural Person**:, Intentional and public display or exhibition or transmission of any information which superimposes a photograph over any sexually explicit image or video of a natural person; includes a photograph in sexually explicit conduct of a natural person; intimates a natural person with sexual act; sexually explicit image or video of a natural person; or entices or induces a natural person to engage in sexually explicit act; through an information system to harm a natural person or his reputation, take revenge, create hatred or blackmail a natural person. (Section 21 of the Act).
11. **Child Pornography**: Produce, offer or make available, distribute or transmit through an information system or to procure for himself or for any other person or without lawful justification possesses material in an information system any material which contain the elements of child pornography. (Section 22 of the Act).
12. Writing, offering, making available, distributing or transmitting **malicious code** through an information system with an intent to cause harm to any information system or data resulting

in the corruption, destruction, alteration suppression, theft or loss of information system. (Section 23 of the Act).

13. Doing **Cyber Stalking** with an intent to coerce or intimidate or harass any person by using information system, information system network, internet website, electronic mail or any similar means of communication. The term Cyber Stalking includes: **(a)** foster personal interaction repeatedly to a person who clearly indicates a disinterest from the stalker; **(b)** monitor the internet, electronic mail, text message or any other form of electronic communication of another person; **(c)** watch or spy upon a person in a manner that results in fear of violence or serious alarm or distress in mind of such persons; and **(d)** take photograph or make video of a person and display or distribute such video in a manner without his consent that harms a person. (Section 24 of the Act).
14. **Spamming**: A person commits the offence of spamming who with an intent transmits harmful, fraudulent, misleading, illegal or unsolicited information to any person without permission of the recipient or who causes any information system to show any such information for wrongful gain. (Section 25 of the Act).