Prevention of Electronic Crimes Act

Pakistan

Data Governance

Definitions of Data:

Data includes content data and traffic data

Main Focus of Document:

Provides regulatory measures for electronic crimes

Target Beneficiaries or Sectors:

Key Elements:

The key elements of this Act are detailed below:

- It extends to the whole of Pakistan;
- It shall apply to every citizen of Pakistan wherever he/she may be and also to every other person for the time being in Pakistan;
- It shall also apply to any act committed outside Pakistan by any person if the act constitutes an offence under this Act and affects a person, property, information system or data located in Pakistan.

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 a fine which may extend to fifty thousand rupees or with both.

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 a fine which may extend to one hundred thousand rupees or with both.

5. 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.

6. 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.

7. 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.

8. Glorification of an offence (l) whoever prepares or disseminates 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 activities of prescribed organizations or individuals or groups shall be punished with imprisonment for a term which may extend to seven years or with fine which may extend to ten million rupees or with both. Explanation: 'gloritication' includes depiction of any form of praise or celebration in a desirable manner.

9. Cyber terrorism Whoever commits or threatens to commit any, of the offences under sections 6, 7, 8 or 9, where the commission or threat is with the intent to: (a) coerce, intimidate, create a sense of fear, panic or insecurity in the government or the public or a section of the public or community or sector create a sense of fear or insecurity in society ; or (b) advance inter-faith, sectarian or ethnic hatred.

10A. Hate speech Whoever prepares or disseminates information through any information system or device that advances or is likely to advance inter-faith, sectarian or racial hatred, shall be punished with imprisonment for a term which may extend to seven years or with fine or with both.

11. Electronic forgery (1) Whoever interferes with or uses any information system, device or data, with the 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 inauthentic data with the intent that it be considered or acted upon for legal purpose or 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 three years, or with fine which may extend to two hundred and fifty thousand rupees or with both. (2) Whoever commits offence under sub-section (1) in relation to a critical infrastructure infomation system or data 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.

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 a fine which may extend to ten million rupees or with both.

13. Unauthorized uses of identity information (1) 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 a fine which may extend to five million rupees, or with both.

Data Data transfer or transmission Digital infrastructure Electronic crimes

Policy/regulation mirrored:

Countries: