

Electronic Crimes Act 2004

A

Bill

to provide for punishment of the electronic crimes and for matters connected therewith or incidental thereto;

Whereas it is expedient to deter action directed against the confidentiality, integrity and availability of electronic system, networks and data as well as the misuse of such system, networks and data by providing for the punishment of such conduct and providing for sufficient powers to effectively combat such offences and to facilitate their detection, investigation and prosecution and for matters ancillary thereto;

It is hereby enacted as follows : -

CHAPTER I

PRELIMINARY

1. **Short title, extent and commencement:**— (1) This Act may be called the Electronic Crimes Act 2004.
 - (2) It shall extend to the whole of Pakistan.
 - (3) It shall come into force at once.
2. **Territorial scope of offences under this Act.**— Every person shall be liable to punishment under this Act for every act or omission contrary to the provisions thereof, if:
 - (a) the offence was committed in Pakistan;
 - (b) any act of preparation towards the offence or any part of the offence was committed in Pakistan, or where any result of the offence has had an effect in Pakistan;
 - (c) the offence was committed by a Pakistani national or a person resident or carrying out business in Pakistan or visiting Pakistan or staying in transit in Pakistan;
 - (d) the offence was committed in relation to or connected with an electronic system or data in Pakistan or capable of being connected, sent to, used by or with any electronic system in Pakistan; or

(e) the offence was committed by any person, of any nationality or citizenship whatsoever or in any place outside or inside Pakistan, having an effect on the security of Pakistan or its nationals or having universal application under international law, custom and usage.

3. **Definitions:**— (1) In this Act, unless the context otherwise requires –

- (a) “access” means gaining access to any electronic system or data held in an electronic system by causing the electronic system to perform any function to achieve that objective;
- (b) “corporation” for the purposes of Section 25 means a body of persons incorporated under any law such as trust, waqf, association, statutory body, company including joint venture or consortium;
- (c) “cyber stalking” means criminal intimidation, insult and annoyance through electronic system as defined in Chapter XXII of the Pakistan Penal Code (XLV of 1860);
- (d) “damage” includes modifying, altering, deleting, erasing, suppressing, changing location of data or making data temporarily unavailable, halting electronic system or choking the networks;
- (e) “data ” means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in an electronic system including computer programme, text, images, sound, video and information within a database or electronic system;
- (f) “decryption information” means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable and incomprehensible format to its plain version;
- (g) “defamation” means defamation as defined in Section 499 of the Pakistan Penal code (XLV of 1860);
- (h) “electronic” includes electrical, digital, magnetic, optical, biometric, electro-chemical, wireless or electromagnetic technology;
- (i) “electronic crime” means any offence committed through or by using any electronic system or means and includes offences established under this Act;
- (j) “electronic system” means any electronic system, device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data and includes a permanent, removeable or any other electronic storage medium;

- (k) “encrypted data” means data which has been transformed or scrambled from its plain version to an unreadable or incomprehensible format, regardless of the technique utilized for such transformation or scrambling and irrespective of the medium in which such data occurs or can be found for the purposes of protecting such data;
- (l) “spoofing” means establishing a website or sending an electronic message with a counterfeit source intended to be believed by the recipient or visitor or its electronic system to be an authentic source;
- (m) “function” includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within an electronic system;
- (o) “Interpol” means International Criminal Police Organisation;
- (p) “malicious code” means a computer program or a hidden function in a program that infects data or compromises the electronic system’s performance or uses the electronic system resources without proper authorization, with or without attaching its copy to a file and is capable of spreading over electronic system with or without human intervention including virus, worm or Trojan horse.
- (r) “plain version” means original data before or after it has been transformed or scrambled to an unreadable or incomprehensible format;
- (s) “sensitive electronic system” is an electronic system used directly in connection with or necessary for—
- (i) the security, defence or international relations of Pakistan;
 - (ii) the existence or identity of a confidential source of information relating to the enforcement of criminal law;
 - (iii) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, courts, public transportation or public key infrastructure;
 - (iv) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services ; or
 - (v) the purpose declared as such by the Federal Government in the official Gazette; or
 - (vi) containing any data or database protected as such, by any other law.
- (s) “service provider” means,—

- (t) a person acting as a service provider in relation to the sending, receiving, storing or processing of the electronic communication or the provision of other services in relation to electronic communication through any electronic system;
- (ii) a person who owns, possesses, operates, manages or controls a public switched network or provides telecommunication services; or
- (iii) any other person that processes or stores data on behalf of such electronic communication service or users of such service;
- (t) “subscriber information” means any information contained in any form that is held by a service provider, relating to subscribers of its services other than traffic data and by which can be established:—
 - (i) the type of communication service used, the technical provisions taken there to and the period of service;
 - (ii) the subscriber’s identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; or
 - (iii) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.
- (u) “other offence” means an offence made punishable under any law for the time being in force;
- (v) “traffic data” means any data relating to a communication by means of an electronic system, generated by an electronic system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service; and
- (w) “unauthorized access” means access of any kind by any person to any electronic system or data held in an electronic system, without authority or in excess of authority, if he is not himself entitled to control access of the kind in question to the electronic system, or data and he does not have consent to such access from any person, so entitled.

4. **Criminal access** — (1) Whoever gains unauthorized access to the whole or any part of an electronic system with or without infringing security measures, with intent to infringe privacy or commit further offence is said to commit the offence of criminal access.

(2) Whoever commits the offence of criminal access shall be punished with imprisonment of either description for a term which may extend to two years, or with fine not exceeding three hundred thousand rupees or with both.

5. **Criminal data access.**— (1) Whoever intentionally causes electronic system to perform any function for the purpose of gaining unauthorized access to any data held in any electronic system is said to commit the offence of criminal data access.

(2) Whoever commits the offence of criminal data access shall be punished with imprisonment of either description for a term which may extend to three years, or with fine or with both.

6. **Data damage.**— (1) Whoever with intent to cause damage to the public or any person, damages any data is said to commit the offence of data damage.

(2) Whoever commits the offence of data damage shall be punished with imprisonment of either description for a term which may extend to three years, or with fine or with both.

7. **System damage.**— (1) Whoever with intent to cause damage to the public or any person interferes with or interrupts or obstructs the functioning, reliability or usefulness of an electronic system by inputting, transmitting, damaging or deteriorating any data is said to commit system damage.

(2) Whoever commits the offence of system damage shall be punished with imprisonment of either description for a term which may extend to three years, or with fine or with both.

8. **Electronic fraud.**— (1) Whoever for gain interferes with data or electronic system to induce any person to enter into a relationship or with intent to deceive any person, which act or omission is likely to cause damage or harm to that person or any other person, commits electronic fraud.

(2) Whoever commits the offence of electronic fraud shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine or with both.

9. **Electronic forgery.**— (1) Whoever for gain interferes with data or electronic system, with intent to cause injury to the public or to any person, or to support any 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, commits electronic forgery, regardless of the fact that the data is directly readable and intelligible or not.

(2) Whoever commits the offence of electronic forgery shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine or with both.

10. **Misuse of devices.**— (1) Whoever produces, possesses, sells, procures, imports, distributes or otherwise makes available a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established under this Act or a password, access code, or similar data by which the whole or any part of an electronic system is capable of being accessed, with the intent that it be used for the purpose of committing any of the offences established under this Act, is said to commit offence of misuse of devices.

Provided that this Section shall not extend to a case where the production, possession, sale, procurement, import, distribution or otherwise making available of a device is not primarily for the purpose of committing an offence established under this Act but is for other lawful purposes, such as, for the authorized testing or protection of an electronic system.

(2) Whoever commits the offence of misuse of devices shall be punished with imprisonment of either description for a term which may extend to three years, or with fine or with both.

11. **Unauthorized access to code.**— (1) Whoever discloses or obtains any password, access code or any other means of gaining access to any electronic system or data with intent to obtain wrongful gain or inflict wrongful loss to any person or for any other unlawful purpose, commits offence of unauthorized access to code.

(2) Whoever commits the offence of unauthorized access to code shall be punished with imprisonment of either description for a term which may extend to three years, or with or with both.

12. **Misuse of encryption.**— (1) Whoever for the purpose of commission of an offence or concealment of incriminating evidence, knowingly and willfully encrypts any incriminating communication or data contained in electronic system relating to that crime or incriminating evidence, commits the offence of misuse of encryption.

(2) Whoever commits the offence of misuse of encryption shall be punished with imprisonment of either description for a term which may extend to five years, or with fine or with both.

13. **Malicious code.**— (1) Whoever writes, offers, makes available, distributes or transmits malicious code through an electronic system is said to commit the offence of malicious code.

(2) Whoever commits the offence of malicious code shall be punished with imprisonment of either description for a term which may extend to five years, or with fine or with both.

14. **Cyber stalking.**— Whoever commits the offence of cyber stalking shall be punished with imprisonment of either description for a term which may extend to three years or with fine not exceeding three hundred thousand rupees or with both.

15. **Spamming.**— Whoever transmits, without the express permission of the recipient, unsolicited electronic messages in bulk to any person or causes any electronic system to show an unsolicited message, for commercial purposes shall be guilty of spamming.

(2) Whoever commits the offence of spamming shall be punished with fine not exceeding fifty thousand rupees if he commits this offence of spamming for the first time and if the same person who commits the offence of spamming again then for every subsequent commission of offence of spamming he shall be punished with imprisonment of three months or with fine not exceeding one hundred thousand rupees or with both. .

16. **Spoofing.**— Whoever does spoofing or uses other device to attract or solicit people or electronic systems for the purpose of gaining unauthorized access to commit further offence or obtain their valuable information which later can be used for unlawful purposes, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine not exceeding three hundred thousand rupees or with both.

17. **Unauthorized interception.**— (1) Whoever without lawful authority intercepts by technical means, non-public transmissions of data to, from or within an electronic system, including electromagnetic emissions from an electronic system carrying such data, commits unauthorized interception.

(2) Whoever commits the offence of unauthorized interception shall be punished with imprisonment of either description for a term which may extend to five years, or with fine not exceeding five hundred thousand rupees or with both.

18. **Cyber Terrorism.**— (1) Whoever in furtherance of any criminal objective commits a premeditated, attack against electronic systems or data, which results in death of any person or causes extreme financial harm, shall be guilty of cyber terrorism.

(2) Whoever commits the offence of cyber terrorism and causes death of any person shall be punished with death or imprisonment for life and in case of causing extreme financial harm shall be liable for imprisonment of either description for a term which may extend to ten years, or with fine not less than ten million rupees or with both.

19. **Waging cyber war.**— Whoever lodges offensive against any electronic system declared by Government of Pakistan as sensitive electronic system, disables communication system and energy facilities or systems or attempts to do so, shall be punished with death, or imprisonment for life and shall also be liable to fine.

20. **Enhanced punishment for offences involving sensitive electronic systems.**—

(1) Whoever obtains criminal access to any sensitive electronic system in the course of the commission of any of the offences established under this Act shall, in addition to the punishment prescribed in those sections, be punished with imprisonment of either description for a term which may extend to ten years, or with fine not exceeding one million rupees or with both.

(2) For the purposes of any prosecution under this section, it shall be presumed, until contrary is proved, that the accused has the requisite knowledge that it was a sensitive electronic system.

21. **Attempt and aiding or abetting.**— (1) Any person who abets the commission of or who aids to commit or does any act preparatory to or in furtherance of the commission of any offence under this Act shall be guilty of that offence and shall be liable on conviction to the punishment provided for the offence.

Provided that any person who attempts to commit an offence under this Act shall be punished for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence, or with both

(2) For aiding or abetting an offence to be committed under this section, it is immaterial whether the act in question took place or not.

22. **Other offences.**— Whoever commits any offence other than those established under this Act, with the help of an electronic system shall be punished, in addition to the punishment provided for that crime, with imprisonment of either description for a term which may extend to two years, or with fine not exceeding two hundred thousand rupees or with both

23. **Corporate liability.**— A corporation shall be held liable for a criminal offence committed on its instructions or for its benefit. The corporation shall be punished with fine not less than one hundred thousand rupees.

Provided that such punishment shall not absolve the criminal liability of the natural person, who has committed the offence.

24. **Offences to be compoundable and cognizable.**—All offences under this Act shall be compoundable and non-cognizable and bailable except the offences the punishment of which are ten years imprisonment or more.

25. **Prosecution and trial of offences.**—No Court inferior to the Court of Sessions shall take cognizance of and try any offence under this Act. For the procedure of investigation and trial Cr. P. C will be applicable on this Act Mutatis Mutandis

26. **Order for payment of compensation.**— The court while awarding punishment may make an order for the payment of a sum to be fixed by the court by way of compensation to any person for any damage caused to his electronic system or data by the offence, for which the punishment is awarded. The compensation so awarded shall be recoverable as arrears of land revenue.

Provided that the compensation awarded by the court shall not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation awarded.

27. **Special investigating agency for electronic crimes.**—The Federal Government immediately after the commencement of this Act shall constitute a special investigating agency or designate any existing agency or its cell to investigate the electronic crimes and prosecute the offenders under this Act.

28. **Saving for investigations by police officers.**— Nothing in this Act shall prohibit a police officer from lawfully conducting investigations, pursuant to his powers conferred under any law for the time being in force, for an offence not mentioned in this Act but enlisted in Pakistan Penal Code or in the Schedule of any other law, notwithstanding, the fact that computer or any electronic system has been used as mean or tool to commit that offence.

Provided where any police officer so investigate a crime he shall seek assistance of the Special Agency for any technical in-put, collection and preservation of evidence and the investigation will jointly be conducted by the police officer not below the rank of Sub-Inspector and an officer of the Special Agency.

Explanation: **A** posts a defamatory statement on a website against **B**, having good reason to believe that the matter in the statement is defamatory for **B**. **A** commits a crime under section 501 of Pakistan Penal Code and a police office is competent to investigate the matter.

29. **Power of investigating officer to access electronic system and data.**— (1) An Investigating officer, for the purpose of investigating any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section, after obtaining search warrant and subject to the terms of the warrant, shall —

- (a) be entitled at any time to —
 - (i) have access to and inspect the operation of any electronic system;
 - (ii) use or cause to be used any such electronic system to search any data contained in or available to such electronic system; or
 - (iii) have access to any information, code or technology which has the capability of retransforming or unscrambling encrypted data contained or available to such electronic system into readable and comprehensible format or plain version;

- (b) be entitled to require —
 - (i) the person by whom or on whose behalf, the investigating officer has reasonable cause to believe, any electronic system is or has been used; or
 - (ii) any person having charge of, or otherwise concerned with the operation of, such electronic system,

to provide him with such reasonable technical and other assistance as he may require for the purposes of clause (a); or

- (c) be entitled to require any person in possession of decryption information to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence.

(2) The Investigating Officer may also require a service provider to submit subscriber information relating to such services in respect of the person or persons under investigation in that service provider's possession or control necessary for the investigation of that offence.

(3) Any person who obstructs the lawful exercise of the powers under sub-section (1) or fails to comply with a request made under the said sub-section shall be liable to be punished with imprisonment of either description for a term which may extend to one year, or with fine not exceeding one hundred thousand rupees or with both.

29. **Real-time collection of traffic data.**— (1) The Federal Government may compel a service provider, within its existing or required technical capability to collect or record through the application of technical means or to co-operate and assist any law enforcement or intelligence agency in the collection or recording of traffic data or data, in real-time, associated with specified communications transmitted by means of a electronic system.

(2) The Federal Government may also require the service provider to keep confidential the fact of the execution of any power provided for in this section and any information relating to it.

30. **Trans-border access.**— The Federal Government or its authorized agency may, without the permission of any foreign government or international agency access publicly available electronic system or data, regardless of where the electronic system or data is located geographically or access or receive, through an electronic system, data located in foreign country or territory, if it obtains the lawful and voluntary consent of the person who has the lawful authority to disclose it.

Provided such access is not prohibited under the law of the foreign government or the international agency .

31. **International co-operation.**— (1) The Federal Government may co-operate with any foreign government, Interpol or any other international agency with whom it has or establishes reciprocal arrangements for the purposes of investigations or proceedings concerning criminal offences related to electronic system and data, or for the collection of evidence in electronic form of a criminal offence or obtaining expeditious preservation and disclosure of traffic data or data by means of a electronic system or real-time collection of traffic data associated with specified communications or interception of data.

(2) The Federal Government may without prior request forward to such foreign government, Interpol or other international agency, any information obtained from its own investigations if it considers that the disclosure of such information might assist the other government or agency in initiating or carrying out investigations or proceedings concerning the criminal offences.

(3) The Federal Government may require such foreign government, Interpol or other international agency to keep the information provided confidential or use it subject to some conditions.

(4) The Federal Government immediately after the commencement of this Act shall nominate any agency or authority responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

(5) The Federal Government may refuse to accede to any request made by such foreign government, Interpol or international agency if the request concerns an offence which it considers a political offence or an offence connected with a political offence, or that execution of the request is likely to prejudice its sovereignty, security, *order public* or other essential interests.

(6) The Federal Government may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

32. Amendment of Ordinance LI of 2002.—(1) In the Electronic Transactions Ordinance, 2002 (LI of 2002), Sections 36 and 37 shall be omitted.

33. Overriding effect.— The provisions of this Act shall apply notwithstanding anything to the contrary contained in any other law for the time being in force.

34. Powers to make rules.- The Federal Government shall , by notification in the official Gazette, make special rules for investigation procedure, collection and preservation of evidence relating to an electronic crime apart from and in addition to procedure already prescribed in the Code of Criminal Procedure of Pakistan and which is applicable on this Act *Mutatis Mutendis*.

35. Removal of difficulties.- The Federal Government may, by notification in the official Gazette , make provisions for removal of difficulties in a manner not inconsistent with the provision of this Act.