President promulgates ordinance to prevent electronic crimes

ISLAMABAD, Nov 6 (APP): The President has promulgated the Prevention of Electronic Crimes Ordinance, 2008 (Ordinance No irrespective of his nationality or citizenship whatsoever or in any place outside or inside Pakistan, having detrimental effect on t

It shall come into force at once and shall be deemed to have taken effect on the 29th September, 2008.

Following is the text of the Ordinance:

WHEREAS it is expedient of prevent any action directed against the confidentiality, integrity and availability of electronic syste

AND WHEREAS THE the National Assembly is not in session and the President is satisfied that the circumstances exist which rer

NOW, THEREFORE, in exercise of the powers conferred by clause (1) of Article 89 of the Constitution of the Islamic Republic c

2. Definitions.- (1) In this Ordinance, unless there is anything repugnant in the subject or context,-

(a) "access" means gaining access to any electronic system or data held in an electronic system or by causing the electronic s

(b) "Authority" means the Pakistan Telecommunication Authority established under section 3 of the Pakistan Telecommunicatio

(c) "Code" means the Code of Criminal Procedure, 1898(Act V of 1898);

(d) "Constitution" means Constitution of the Islamic Republic of Pakistan;

(e) "data" means representations of information or of concepts that are being prepared or have been prepared in a form suitabl

including but not limited to computer program, text, images, sound, video and information within a database or electronic syster

(f) "decision of the Authority" means decision given, determination made or order passed by the Authority under any of the pı interim order passed by the Authority pending final decision;

(g) "Electronic Certification Accreditation Council" means the council established under section 18 of the Electronic Transactior

(h) "electronic" includes but not limited to electrical, digital, analogue, magnetic, optical, biochemical, electrochemical, electro

(i) "electronic device" means any hardware which performs one or more specific functions and operates on any form or combin

(j) "electronic mail message" means any data generated by an electronic system for a unique electronic mail address;

(k) "electronic mail address" means a destination, commonly expressed as a string of characters, consisting of a unique user o mail address which may be permanent, dynamic or disposable;

(1) "electronic system" means any electronic device or a group of interconnected or related devices, one or more of which, pur

(m) "encrypted data" means data which has been transformed or scrambled from its plain version or text to an unreadable or inc

(n) "function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, fr

(o) "Interpol" means International Criminal Police Organization;

(p) "offence" includes,-

(i) an offence punishable under this Ordinance;

(ii) an offence punishable under the laws mentioned in the Schedule ; or

(iii) any other offence punishable under any other law for the time being in force if committed through or by using any computer

(q) "plain version" means original data before it has been transformed or scrambled to an unreadable or incomprehensible format

(r) "rules" means rules made under this Ordinance; (s) "Schedule" means the

Schedule to this Ordinance;

(t) "sensitive electronic system" means 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, co

(iv) the protection of public safety including systems related to essential emergency services such as police, civil defence and r

(iv) the purpose declared as such by the Federal Government in accordance with the prescribed procedure ; or

(vi) containing any data or database protected as such, by any other laws.

(u) "service provider" includes but not limited to ,-

(i) a person acting as a service provider in relation to sending, receiving, storing or processing of electronic communication or

(ii) a person who owns, possesses, operates, manages or controls a public switched network or provides telecommunication se

(iii) any other person who processes or stores data on behalf of such electronic communication service or users of such service

(v) "subscriber information" means any information contained in any form that is held by a service provider, relating to subscrib

(i) the type of communication service used, the technical provisions taken thereto and the period of service;

✓ December, 2014
✓ November, 2014
✓ October, 2014
✓ September, 2014

(ii) the subscriber's identity, postal geographic, "electronic mail address, telephone and other access number, billing and payme

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

(w) "traffic data" means any data relating to a communication by means of an electronic system, generated by an electronic system tha

(x) "Tribunal" means the Information and Communication Technologies Tribunal constituted under section 31; and

(y) "unauthorized access" means access of any kind by any person to any electronic system or data held in an electronic syste

CHAPTER-II

OFFENCES AND PUNISHMENTS

3. Criminal access .- Whoever intentionally gains unauthorized access to the whole or any part of an electronic system or ele

4. Criminal data access,- Whoever intentionally causes any electronic system or electronic device to perform any function damage.- Whoever with intent to illegal gain or cause harm to the public or any person, damages any data shall be punished

Explanation .- For the purpose of this section the expression "data damage" includes but not limited to modifying, altering, delet

6. System damage.- Whoever with intent to cause damage to the public or any person interferes with or interrupts or obstruc of either description for a term which may extend to three years, or with fine or, with both.

Explanation .- For the purpose of this section the expression "services" include any kind of service provided through electronic s

7. Electronic fraud.- Whoever for wrongful gain interferes with or uses any data, electronic system or electronic device or inc with both.

8. Electronic forgery.- Whoever for wrongful gain interferes with data, electronic system or electronic device, with intent to unauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of the

9. Misuse of electronic system or electronic device.- (1) Whoever produces, possesses, sells, procures, transports, imports, di any part of an electronic system or electronic device is capable of being accessed or its functionality compromised or reverse e

Provided that the provisions of this section shall not apply to the authorized testing or protection of an electronic system for ar

(2) Whoever commits the offence described in sub-section (1) shall be punishable with imprisonment of either description for

10. Unauthorized access to code.- Whoever discloses or obtains any password, access as to code, system design or any othe years, or with fine, or with both.

11. Misuse of encryption.- Whoever for the purpose of commission of an offence or concealment of incriminating evidence, k years, or with fine, or with both.

12. Malicious code.- (1) Whoever willfully writes, offers, makes available, distributes or transmits malicious code through an ele

Provided that the provision of this section shall not apply to the authorized testing, research and development or protection of

Explanation,- For the purpose of this section the expression "malicious code" includes but not limited to a computer program or intervention including virus, worm or Trojan horse.

(2) Whoever commits the offence specified in sub-section (1) shall be punished with imprisonment of either description for a ter

13. Cyber stalking.- (1) Whoever with intent to coerce , intimidate, or harass any person uses computer, computer network, int

(a) communicate obscene, vulgar, profane, lewd, lascivious , or indecent language, picture or image;

(b) make any suggestion or proposal of an obscene nature;

(c) threaten any illegal or immoral act;

(d) take or distribute pictures or photographs of any person without his consent or knowledge; or

(e) display or distribute information in a manner that substantially increases the risk of harm or violence to any other person, c

(2) Whoever commits the offence specified in sub-section (1) shall be punishable with imprisonment of either description for a

Provided that if the victim of the cyber stalking under sub-section (1) is a minor the punishment may extend to ten years or wit

14. Spamming.- (1) Whoever transmits harmful, fraudulent, misleading, illegal or unsolicited electronic messages in bulk to any p offence of spamming as described in sub-section (1) shall be punishable with fine not exceeding fifty thousand rupees if he com

15. Spoofing.(I) Whoever establishes a website, or sends an electronic messagewith a counterfeit source intended to be believe in sub-section (1) shall be punished with imprisonment of either description for a term which may extend to three years, or with

16. Unauthorized interception.- (1) Whoever without lawful authority intercepts by technical means, transmissions of data to imprisonment of either description fora term which may extend to five years, or with fine not exceeding five hundred thousand

17. Cyber terrorism.- (1) Any person, group or organization who, with terroristic intent utilizes, accesses or causes to be acces

Explanation l.- For the purposes of this section the expression "terroristic intent" means to act with the purpose to alarm, fright

Explanation 2.- For the purposes of this section the expression "terroristic act" includes, but is not limited to,-

(a) altering by addition, deletion, or change or attempting to alter information that may result in the imminent injury, sickness,

(b) transmission or attempted transmission of a harmful program with the purpose of substantially disrupting or disabling any co

(c) aiding the commission of or attempting to aid the commission of an act of violence against the sovereignty of Pakistan, whe

(d) stealing or copying, or attempting to steal or copy, or secure classified information or data necessary to manufacture any f

(2) Whoever commits the offence of cyber terrorism and causes death of anyperson shall be punishable with death or imprison

in any other case he shall be punishable with imprisonment of either description for a term which may extend to ten years, or wi

18. Enhanced punishment for offences involving sensitive electronic systems.-(I) Whoever causes criminal access to any sensi exceeding one million rupees, or with both. (2) For the purposes of any prosecution under this section, it shall be presumed,

19. Of abets, aids or attempts to commits offence .- (1) Any person who knowingly and willfully abets the commission of or wh

(2) Any person who attempts to commit an offence under this Ordinance shall be punished for a term which may extend to one

Explanation.- For aiding or abetting an offence to be committed under this section, it is immaterial whether the offence has bee

20. Other offences.- Whoever commits any offence other than those expressly provided under this Ordinance, with the help of

or with both.

21. Offences by corporate body.- A corporate body shall be held liable for an offence under this Ordinance if the offence is com

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

Explanation.- For the purposes of this section corporate body, includes a body of persons incorporated under any law such as t

CHAPTER-III

PROSECUTION AND TRIAL OF OFFENCES

22. Offences to be compoundable and non-cognizable.- All offences under this Ordinance shall be compoundable, non-cognizabl

23. Prosecution and trial of offences.- (1) The Tribunal shall take cognizance of and try any offence under this Ordinance .

(2) In all matters with respect to which no procedure has been provided in this Ordinance or the rules made thereunder, the p

(3) All proceedings before the Tribunal shall be deemed to be judicial proceedings within the meanings of sections 193 and 228

24. Order for payment of compensation.- The Tribunal may, on awarding punishment of imprisonment or fine or both for commiss

Provided that the compensation awarded by the Tribunal shall not prejudice any right to a civil remedy for the recovery of dama

CHAPTER-IV

ESTABLISHMENT OF INVESTIGATION AND PROSECUTION AGENCIES

25. Establishment of investigation agencies and prosecution.- The Federal Government shall establish a specialized investigation

Provided that till such time any agency is so established, the investigation and prosecution of an offence shall be conducted in

Provided further that any police officer investigating an offence under this Ordinance may seek assistance of any special investi

26. Powers of officer.- (1) Subject to obtaining search warrant an investigation officer shall be entitled to,-

(a) have access to and inspect the operation of any electronic system;

(b) use or cause to be used any such electronic system to search any data contained in or available to such electronic system

(c) have access to or demand any information, code or technology which has the capability of retransforming or unscrambling e

(d) require any person by whom or on whose behalf, the investigating officer has reasonable cause to believe, any electronic s

(e) require any person having charge of, or otherwise concerned with the operation of such electronic system to provide him necessary to decrypt data required for the purpose of investigating any such offence.

Explanation.- Decryption information means information or technology that enables a person to readily retransform or unscramble

(2) The police officer may, subject to the proviso, require a service provider to submit subscriber information relating to such s

Provided that the investigating officer shall get prior permission to investigate any service provider from the licensing authority

(3) Any person who obstructs the lawful exercise of the powers under sub-sections (1) or (2) shall be liable to punishment with

27. Real-time collection of traffic data.- (1) The Federal Government may require a licensed service provider, within its existing means of an electronic system. (2) The Federal Government may also require the service provider to keep confidential the fac

28. Retention of traffic data,- (1) A service provider shall, within its existing or required technical capability, retain its traffic da

investigating officer when required. The Federal Government may extend the period to retain such date as and when deems app

(2) The service providers shall retain the traffic data under sub-section (1) by fulfilling all the requirements of data retention a

(3) Any person who contravenes the provisions of this section shall be punished with imprisonment for a term of six months, o

29. Trans-border access.- For the purpose of investigation the Federal Government or the investigation agency may

Government or international agency access publicly available electronic system or data notwithstanding the geographically locat

Provided that such access is not prohibited under the law of the foreign Government or the international agency:

Provided further that the investigating agency shall inform in writing the Ministry of Foreign Affairs of Government of Pakistan ar

CHAPTER - V

INTERNATIONAL COOPERATION

30. International cooperation.- (1) The Federal Government may cooperate with any foreign Government, Interpol o

it has, or establishes, reciprocal arrangements for the purposes of investigations or proceedings concerning offences related t interception of data.

(2) The Federal Government may, without prior request, forward to such foreign Government, Interpol or other international ag

information might assist the other Government or agency in initiating or carrying out investigations or proceedings concerning ar

(3) The Federal Government may require the foreign Government, Interpol or other international agency to keep the information

(4) The investigating agency shall, subject to approval of the Federal Government, be responsible for sending and answering re

(5) The Federal Government may refuse to accede to any request made by such foreign Government, Interpol or international a

(6) The Federal Government may postpone action on a request if such action would prejudice investigations of proceedings cor

Chapter - VI

INFORMATION AND COMMUNICATION TECHNOLOGIES TRIBUNAL

31. Information and Communication Technologies Tribunal .- (1) As soon as possible after the commencement of this Ordinance , the Fe

(2) The Tribunal may hold its sittings at such place or places as the Federal Government may decide.

(3) The Tribunal shall consist of a chairman and as many members as the Federal Government may determine but not more than sever

(4) The Chairman may constitute Benches of the Tribunal and unless otherwise directed by him a Bench shall consist of not less than t

(5) The Federal Government shall appoint the Chairman and members of the Tribunal.

32. Qualifications for appointment.- (1) A person shall not be qualified for appointment as Chairman unless he is, or has been, or is qua

(2) A person shall not be qualified for appointment as a member unless he -
(a) has for two years served as a District and Sessions Judge;
(b) has for a period of not less than ten years been an advocate of a High Court; or
(c) has special knowledge of legislation and professional experience of not less than ten years in the field of telecommunication an

33. Salary, allowances and other terms and conditions of services.- The salary, allowances, privileges and the other terms and conditio
34. Resignation and removal.- (1) The Chairman or a member of the Tribunal may, by writing under his hand addressed to the Federal G
Provided that the Chairman or a member shall, unless he is permitted by the Federal Government to relinquish his office sooner, contin
(2) The Chairman or a member of the Tribunal shall not be removed from his office before expiry of the term determined under section
(3) The Federal Government may, by rules, regulate the procedure for the investigation of misconduct or physical or mental incapacity
35. Saving Tribunal's proceedings.- No act or proceedings of the Tribunal shall be called in question in any manner on the ground merel
36. Employees of the Tribunal.- (1) The Federal Government shall provide the Tribunal with such employees as the Government may de

(2) The employees of the Tribunal shall perform their duties under general superintendence of the Chairman of the Tribunal.

(3) The salaries, allowances and other conditions of service of the employees of the Tribunal shall be such as may be prescribed by the

37. Right to legal representation.- The parties in appeal may either appear in person or authorize one or more legal practitioners,
38. Amicus curiae. - (1) The Tribunal may, if it so requires, be assisted in technical aspects in any case by an amicus curiae having know

(2) The Federal Government shall maintain a list of amicus curiae having relevant qualifications and experience.
(3) The Tribunal in consultation with the Federal Government shall determine the remuneration of the amicus curiae and the Tribunal m
39. Procedure and powers of Tribunal.- (1) Subject to the provisions of this Ordinance and the rules made thereunder, the Tribunal,--

(i) may, where it deems necessary, apply the procedures as provided in the Code or, as the case may be, in the Code of Civil Procedu
(ii) in the exercise of its civil jurisdiction, shall have powers vested in the civil court under the Code of Civil Procedure, 1908; and
(iii) in the exercise of its criminal jurisdiction, shall have the same powers as are vested in the Court of Session under the Code.

40. Appeal to Tribunals.- (1) Any person aggrieved by any of the following orders may, within fifteen days from the date of such order,

(a) any decision of the Authority; or
(b) any decision of the Electronic Certification Accreditation Council:
Provided that no appeal shall lie to the Tribunal from an order passed by the Authority or the Electronic Certification Accreditation Coun
(2) Any appeal against a decision of the Authority shall be accompanied by a court fee,-
(a) ten thousand rupees where the valuation of the subject matter in issue is not more than five million rupees;
(b) fifty thousand rupees where the valuation of the subject matter in issue is more than five million rupees but not more than ten milli
(c) one hundred thousand rupees where the valuation of the subject matter in issue is more than ten million rupees. if,

(3) The appeal filed before the Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and the Tribunal sha

41. Powers of Tribunal.- The Tribunal while hearing an appeal under section 40 shall have all the powers as are vested in the court of fi
42. Limitation".- The provisions of the Limitation Act, 1908 (IX of 1908), shall, mutatis mutandis , apply to the proceedings of Tribunal. 4

(1) any decision or order of the Tribunal made under section 40 may prefer second appeal to the respective High Court within thirty da
Provided that appeal under this clause shall lie only if the High Court grants leave to appeal;
(ii) an order of conviction passed by the Tribunal in respect of any offence under this Ordinance may prefer an appeal to the respect
(2) An appeal against an order of the Tribunal under section 40 or an order of sentence exceeding ten years shall be heard by the Divi
44. Civil court not to have jurisdiction.- No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter
45. Transitory proceedings.- (1) Until the establishment of the Tribunal all cases, proceedings and appeals, subject matter of which
(2) On the constitution of the Tribunal all cases, proceedings and appeals shall stand transferred to and be heard and disposed of by t
(3) On transfer of cases, proceedings and appeals under sub-section (2), the Tribunal shall proceed from the stage the proceedings ha

CHAPTER - VII MISCELLANEOUS

46. Ordinance to override other laws.- The provisions of this Ordinance shall have effect notwithstanding anything to the contrary
47. Power to amend Schedule.- The Federal Government may. by notification in the official Gazette, amend the Schedule so as to a
48. Powers to make rules. - (1) The Federal Government may , by notification in the official Gazette, make rules for carrying out pu
49. Removal of difficulties. - If any difficulty arises in giving effect to the provisions of this Ordinance, the Federal Government may

THE FIRST SCHEDULE

(See section 2(p)(ii))

1. The Electronic Transactions Ordinance, 2002 (LI of 2002).

2. The Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996).

3. The Telegraph Act, 1885 (XIII of 1885).
4. The Wireless Telegraphy Act, 1933 (XVII of 1933).

[Back]