PEC Bill As Modified by Expert Committee Constituted by National Assembly Standing Committee

An Act to make provisions for securing electronic material against unauthorized access, transmission or modification, and cyber fraud and for connected purposes.

CHAPTER I

PRELIMINARY

1. Short title, extent, application and commencement.- (1) This Act may be called the Prevention of Electronic Crimes Act, 2015.

(2) It extends to the whole of Pakistan.

(3) It shall apply to every citizen of Pakistan whenever he may be, and also to every other person for the time being in Pakistan.

(4) It shall come into force at once.

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

(a) "act" includes

i) a series of acts or omissions contrary to the provisions of this Act; or

ii) causing an act to be done by a person either directly or through an automated information system or automated mechanism or self-executing, adaptive or autonomous device, and whether having temporary or permanent impact;

(b) "Access to data" means gaining control or ability to read, use, copy, modify or delete any data held in or generated by any device or information system;

(c) "Access to information system" means gaining control or ability to use any part or whole of an information system whether or not through infringing any security measure;

(d) "Authority" means the Pakistan Telecommunication Authority established under Pakistan Telecommunication (Re-organization) Act. 1996 (XVII of 1996);

(e) "Authorisation" means authorisation by law or the person empowered to make such authorisation under the law

(f) "Authorised officer" means an officer of the designated investigation agency authorised to perform any function on behalf of the investigation agency by or under this Act;

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

(h) "content data" means any representation of fact, information or concept for processing in an information system including source code or a program suitable to cause an information system to perform a function;

(i) "Court" means the Court of Sessions competent to try offenses, issue warrants and pass orders under this Act;

(j) "critical infrastructure" includes:

(i) the infrastructure, publicly or privately owned and controlled, so vital to the functioning of the State that its incapacitation disrupts or adversely affects the national security, economy, public order, supplies, services, health, safety or matters incidental or related thereto or

(ii) any other infrastructure so designated by the Government as critical infrastructure;

(k) "critical infrastructure information system or data" means an information system, program or data that supports or performs a function with respect to a critical infrastructure;

(l) "damage to an information system" means any unauthorised change in the ordinary working of an information system that impairs its performance, access, output or change in location whether temporary or permanent and with or without causing any change in the system;

(m) "data" includes content data and traffic data;

(n) "data damage" means alteration, deletion, deterioration, erasure, relocation, suppression, of data or making data temporarily or permanently unavailable;

(o) "device" includes-

(i) physical device or article:

(ii) any electronic or virtual tool that is not in physical form;

(iii) a password, access code or similar data, in electronic or other form, by which the whole or any part of an information system is capable of being accessed; or

(iv) automated, self-executing, adaptive or autonomous devices, programs or information systems;

(p) "electronic" includes electrical, digital, magnetic, optical, biometric, electrochemical, electromechanical, wireless or electromagnetic technology;

(q) "fraudulently" shall have the meaning assigned to it in section 25 of the Pakistan Penal Code, 1860.

(r)"Government" means the Federal Government.

(s) "identity information" means information, in any form whatsoever, whether presently existing or which may emerge in future with the advent of modern devices and technology, used alone or in combination with other information, which may authenticate or identify an individual or an information system and enable access to any data or information system;

(t) "information" includes text, message, data, voice, sound, database, video, signals, software, computer programs, codes including object code and source code;

(u) "information system" means an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing any information;

(v) "integrity" means, in relation an electronic document, electronic signature or advanced electronic signature, the electronic document, electronic signature or advanced electronic signature that has not been tampered with, altered or modified since a particular point in time;

(w) "interference with information system or data" means and includes an unauthorised act in relation to an information system or data that may disturb its normal working or form with or without causing any actual damage to such system or data.

(x) "investigation agency" means the law enforcement agency established by or designated under this Act;

(y)"minor" means, notwithstanding anything contained in any other law, any person who has not completed the age of eighteen years.

(aa) "offence" means an offence punishable under this Act;

(bb) "rules" means rules made under this Act;

(cc) "seize" with respect to an information system or data includes taking possession of such system or data or making and retaining a copy of the data;

(dd) "service provider" includes a person who:

(i) acts as a service provider or intermediary in relation to sending, receiving, storing, processing or distribution of any electronic communication or the provision of other services in relation to electronic communication through an information system;

(ii) owns, possesses, operates, manages or controls a public switched network or provides telecommunication services; or

(iii) processes or stores data on behalf of electronic communication service providers mentioned in (i) and (ii) above or users of such electronic communication service.

(ee) "subscriber information" means any information held in any form by a service provider relating to a subscriber other than traffic.- data;

(ff) "traffic data" includes data relating to a communication indicating its origin, destination, route, time, size, duration or type of service;

(gg) "unauthorised access" means deliberate access to an information system or data without

(i) legal right or authorisation and in disregard for absence of such legal right or authorization, or

(ii) in violation of the terms and conditions of the authorization granted by the person entitled to grant such authorisation.

(hh) "unauthorised interception'' shall mean in relation to an information system or data, any deliberate interception without legal right or authorisation:

(3) Unless context provides otherwise, any other expression used in this Act or rules framed thereunder but not defined in the Act, shall have meanings assigned to the expression in the Pakistan Penal Code, 1860 (XLV of 1860), the Code of Criminal Procedure. 1898 (V of 1898) and the Qanoon-e-Shahadat Order, 1984 (X of 1984), as the case may be.

CHATPER II

OFFENCES AND PUNISHMENTS

3. Unauthorised access to information system or data.- (1) Whoever with malicious intent gains unauthorised access to any information system or data shall be punished with fine up to one fifty thousand rupees or with both.

4. Unauthorised copying or transmission of data.- Whoever with malicious intent and without authorisation accesses and copies or otherwise transmits or causes to be transmitted any data shall be punished with fine up to one hundred thousand rupees or with both.

5. Interference with information system or data.- Whoever with malicious intent interferes with and/or damages or causes to be interfered with or damage any part or whole of an information system or data shall be punished with imprisonment which may extend to two years or with fine up to five hundred thousand rupees or with both.

6. Unauthorised access to critical infrastructure information system or data:- Whoever with malicious intent gains unauthorised access to any critical infrastructure information system or data shall be punished with imprisonment which may extend to three years or with fine up to one million rupees or with both.

7. Unauthorised copying or transmission of critical infrastructure data.- Whoever with malicious intent and without authorisation copies or otherwise transmits or causes to be transmitted any critical infrastructure data shall he punished with imprisonment for a term which may extend to five years, or with fine up to five million rupees or with both.

8. Interference with critical infrastructure information system or data.- Whoever with malicious intent interferes with or damages, or causes to be interfered with or damage, any part or whole of a critical information system, or data , shall be punished with imprisonment which may extend to seven years or with fine up to ten million rupees or with both.

9. Incitement, Glorification of terrorism and hate speech. Whoever with malicious intent prepares or disseminates information, through any information system or device to:-

(a) incite an act of terrorism;

(b) glorify and support terrorism or activities of proscribed organizations; or

(c) advance religious, ethnic or sectarian hatred

shall be punished with imprisonment for a term which may extend to five years or with fine up to ten million rupees or with both.

Explanation: ‘‘Glorification’’ includes depiction of any form of praise or celebration in a desirable manner.

10. Cyber terrorism. Whoever with malicious intent commits or attempts to commit any of the offences under sections 6, 7 and 8 of this Act, where the commission or attempt is to:-

(a) coerce, intimidate, overawe or create a sense of fear, panic or insecurity in the Government or the public or a section of the public or community or sect or create a sense of fear or insecurity in society; or (b) advance religious, ethnic or sectarian discord,

shall be punished with imprisonment of either description for a term which may extend to fourteen years or with fine up to fifty million rupees or with both.

11. Electronic forgery.- (1) Whoever with malicious intent for wrongful gain interferes with or uses any information system, device or data, 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 unauthentic data with the intent that it be considered or acted upon for legal purposes 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 up to two hundred and fifty thousand rupees or both with.

(2) Whoever commits offence under sub-section (1) in relation to a critical infrastructure information system or data shall be punished with imprisonment for a term which may extend to seven years or with fine up to five million rupees or with both.

12. Electronic fraud:- Whoever with malicious 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 fine up to ten million rupees, or with both.

13. Making, obtaining, or supplying device for use in offence.- Whoever with malicious intent produces, makes, generates, adapts, exports, supplies, offers to supply or imports for use any information system, data or device, primarily to be used to commit or to assist in the commission of an offence under this Act shall, without prejudice to any other liability that he may incur in this behalf, be punished with imprisonment for a term which may extend to 6 months or with fine up to fifty thousand rupees or with both.

14. Unauthorized use of identity information.-(1) whoever with malicious intent, fraudulently 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 fine up to five million rupees, or with both.

(2) Any person whose identity information is wrongfully obtained, sold, possessed, used or transmitted may apply to the Authority for securing, destroying, blocking access or preventing transmission of identity information referred to in sub-section (1) and the Authority on receipt of such application may take due and reasonable measures to protect the best interest of the aggrieved person for securing,

destroying or preventing transmission of such identity information, pursuant to the provisions of this Act.

(3) The Authority shall make bylaws for carrying out purposes referred to in sub-section (2) pursuant to provisions of this Act.

15. Unauthorized interception.- whoever with malicious intent commits unauthorized interception by technical means of:-

(a) any electronic transmission that is not intended to be and is not open to the public from or within an information System, or

(b) electro magnetic emissions from an information system that are carrying data shall be punished with imprisonment of either description for a term which may extend to two years or with fine up to five hundred thousand rupees or with both.

16. Unauthorized issuance of SIM cards etc.- Whoever with malicious intent sells or otherwise provides subscriber identity module (SIM) card, re-usable identification module (R-IUM) or other portable memory chip designed to be used in cellular mobile or wireless phone for transmitting information without obtaining and verification of the subscriber`s antecedents in the mode and manner for the time being approved by the Authority shall be punished with imprisonment for a term which may extend to three years or with fine up to five hundred thousand rupees or both.

17. Tampering etc. of communication equipment.- Whoever with malicious intent or without authorization of the Authority changes, alters, tampers with or re-programs unique device identifier of any communication equipment including a cellular or wireless handset and starts using or marketing such device for transmitting and receiving Intelligence shall be punished with imprisonment which may extend to three years or with fine up to one million rupees or both;

Provided that the Authority shall frame bylaws under the provisions of this Act to enable persons, including individuals, companies and research organizations, to seek prior permission from the Authority to change, alter or re-program unique device identifier of any communication equipment for any legitimate purpose.

Explanation: A "unique device identifier" is an electronic equipment identifier which is unique to a mobile wireless communication device.

18. Offences against dignity of natural person.- (1) When a person with malicious intent through an information system,

(a) produces, offers and makes available, distributes or transmits, procures or solicits, or possesses sexually explicit images of a natural person, or

(b) produces, offers and makes available, distributes or transmits, procures or solicits or possesses an image, photograph or video of a natural person in sexually explicit conduct or intimidates or threatens a natural person with production, distribution or transmission of such material, or

(c) cultivates, entices or induces a minor to engage in a sexually explicit act or in a lewd manner that is offensive to the privacy of the minor,

shall be punished with imprisonment for a term up to three years which may extend up to six years in relation to a minor or with fine up to ten million rupees or both.

(2) Anyone, including the guardian of the aggrieved minor, may apply to the Authority for passing of such orders for removal, destruction or blocking access to such information referred to in sub-section (1) and the Authority on receipt of such application may take due and reasonable measures to protect the best interest of the aggrieved person for securing, destroying or preventing transmission of such information, pursuant to the provisions of this Act.

(3) The Authority shall make bylaws for carrying out purposes referred to in sub-section (2) pursuant to provisions of this Act.

19. Malicious code.- Whoever with malicious intent without authorization writes, offers, makes available, distributes or transmits malicious code through an information system or device, with intent to cause harm to any information system or data resulting, in the corruption, destruction, alteration, suppression, theft or loss of the information system or data shall be punished with imprisonment for a term which may extend to two years or with fine up to one million rupees or both.

Explanation.- For the purpose of this section the expression "malicious code" includes a computer program or a hidden function in a program that damages an information system or data or compromises the performance of such system or availability of data or uses it without proper authorisation.

20. Spamming.- (1) Whoever with malicious intent transmits unsolicited information in bulk repeatedly to any recipient who has expressly unsubscribed from receiving such bulk information, commits the offence of spamming.

Explanation.- "Unsolicited information in bulk" does not include (i) marketing authorized under the law, or (ii) information that has not been specifically unsubscribed by the recipient.

(2) A person engaged in direct marketing shall provide the option to the recipient of direct marketing to block or subscribe such marketing.

(3) Whoever commits the offence of spamming as described in sub-section (1) or engages in direct marketing in violation of sub-section (2), for the first time, shall he punished with fine not exceeding fifty thousand rupees and for every subsequent violation shall he punished with fine up to five hundred thousand rupees.

21. Legal recognition of offences committed in relation to information system.- (1) Notwithstanding anything contained in any other law for the time being in force, an offence under this Act or any other law shall not be denied legal recognition and enforcement for the sole reason of such offence being committed in relation to, or through the use of an information system.

(2) References to "property" in any law creating an offence in relation to or concerning property, shall include information system and data.

22. Pakistan Penal Code 1860 to apply.- The provisions of the Pakistan Penal Code 1860 (XLV of 1860), to the extent not inconsistent with anything provided in this Act, shall apply to the offences provided in this Act.

CHAPTER III

ESTABLISHMENT OF INVESTIGATION AND PROSECUTION AGENCY AND PROCEDURAL POWERS FOR INVESTGATION

23. Establishment of investigation agency.- (1) The Federal Government shall establish or designate a law enforcement agency as the investigation agency for the purposes of investigation of offences under this Act.

(2) Unless otherwise provided for under this Act, the investigation agency and the authorised officer shall in all matters follow the procedure laid down in the Code to the extent that it is not inconsistent with any provision of this Act.

(3) Notwithstanding provisions of any other law, the Federal Government shall make rules for appointment and promotion in the investigation agency including undertaking of specialized courses in digital forensics, information technology, computer science and other related matters for training of the officers and staff of the investigation agency, and all authorized officers exercising powers or performing functions pursuant to this Act shall have received prior training in digital forensics, information technology or computer science, in such terms as may be prescribed.

24. Establishment of forensic laboratory.- (1) The Federal Government shall establish an autonomous forensic laboratory, independent of the investigation agency, to provide expert opinion before the Court or for the benefit of the investigation agency in relation to electronic evidence collected for purposes of investigation and prosecution of offences under this Act.

(2) Notwithstanding provisions of any other law, the Federal Government shall make rules, *inter alia*, for management and oversight of the forensic laboratory, adequate training of its staff, and provision of required resources for discharge of its functions.

25. No warrant, arrest, search, seizure or other power not provided for in the Act.- (1) Only an authorised officer of the investigation agency shall have the powers to investigate an offence under this Act and no search and seizure of information or system or arrest of person shall be affected except upon grant of warrant by the Court:

Provided that the Federal Government or the Provincial Government may, as the case may be, constitute one or more joint investigation teams headed by the authorised officer of the designated investigation agency and comprising officers of any other law enforcement agency for investigation of offence pursuant to the provisions of this Act.

26. Expedited preservation of data.- (1) Upon an application by an authorized officer that demonstrates to the satisfaction of the Court that-

(a) data stored in any information system or by means of an information system, is reasonably required for the purposes of a criminal investigation; and

(b) there is a risk or vulnerability that the data may be modified, lost, destroyed or rendered inaccessible,

the Court may, by written notice given to a person in control of the information system, require that person to ensure that the data specified in the notice be preserved and the integrity thereof is maintained for a period not exceeding ninety days as specified in the notice:

(2) The period provided in sub-section (1) for preservation of data may be extended by the Court if so deemed necessary upon receipt of an application from the authorised officer in this behalf.

(3) The person in control of the information system shall only be responsible to preserve the data specified-

(a) for the period of the preservation and maintenance of integrity specified in the notice or for any extended period permitted by the Court; and

(b) where it is technically and practically possible to preserve the data and maintain its integrity.

(4) Any person, including a service provider and an authorized officer, who, while providing services under the terms of lawful contract or otherwise in accordance with law, has secured access to any material or data containing personal information about another person, discloses such material to any other person, except when required by law, without the consent of the person concerned or in breach of a lawful contract, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain, or compromises its integrity and confidentiality, shall be punished with imprisonment for a term which may extend to three years or with fine up to one million rupees or with both.

27. Retention of traffic data.---(1) A service provider shall, within its existing technical capability, retain its traffic data up to a period of 90 days or such lesser period as the Authority may notify from time to time and provide such traffic data to the designated investigation agency or the authorised officer pursuant to provisions of Section 30.

(2) The service providers shall retain the traffic data under sub section (1) by fulfilling all the requirements of data retention and its originality as provided under sections 5 and 6 of the Electronic Transaction Ordinance, 2002 (LI of 2002).

(3) Any person, including a service provider and an authorized officer, who, while providing services under the terms of lawful contract or otherwise in accordance with law, has secured access to any material or data containing personal information about another person, discloses such material to any other person, except when required by law, without the consent of the person concerned or in breach of a lawful contract, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain, or compromises its integrity and confidentiality, shall be punished with imprisonment for a term which may extend to three years or with fine up to one million rupees or with both.

28. Warrant for search or seizure.- (1) Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that there may be in a specified place an information system, data, device or storage medium of a specified kind that-

(a) may reasonably be required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence in proving a specifically identified offence made out under this Act; or

(b) has been acquired by a person as a result of the commission of an offence,

the Court may after recording reasons issue a warrant which shall authorise an officer of the designated investigation agency, with such assistance as may be necessary to enter in the presence of a judicial magistrate the specified place and to search the specified premises and specified information system, data, device or storage medium relevant to the offence identified in the application and access, seize or similarly secure the specified information system, data or other articles relevant to the offence identified in the application.

(2) The application under subsection (1) shall in addition to substantive grounds and reasons also:

(a) explain why it is believed the material sought will be found on the premises to be searched; and

(b) why the purpose of a search may be frustrated or seriously prejudiced unless an investigating officer arriving at the premises can secure immediate entry to them;

(3) No court shall issue any warrant to enter and search any specific premises, information system, data, device or other articles, unless satisfied that consequent upon the particulars of the offence referred to in the application, there are reasonable grounds for believing that it is necessary to search the specific premises, information system, data, device or other articles in order to find the material sought.

29. Warrant for disclosure of traffic data.- (1) Upon an application by an authroised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that specified data stored in an information system is reasonably required for the purpose of a criminal investigation or criminal proceedings with respect to an offence made out under this Act, the Court may, after recording reasons, order that a person in control of the information system or traffic data, to disclose sufficient traffic data about a specified communication to identify-

(a) the service providers; and

(b) the path through which provide such traffic data or access to such traffic data to the authorised officer.

(2) The period of a warrant issued under sub-section (1) may be extended if, on an application, a Court authorises an extension for a further period of time as may be specified by the Court.

(3) The application under sub-section (1) shall in addition to substantive grounds and reasons also explain why it is believed the traffic data sought will be available with the person in control of the information system.

30. Warrant for acquisition of information or data other than traffic data.- (1) Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that specified data stored in an information system is reasonably required for the purpose of a criminal investigation or criminal proceedings with respect to an offence made out under this Act, the Court may, after recording reasons, order that a person in control of the information system or data, to disclose sufficient data about a specified communication to identify-

(2) The application under sub-section (1) shall in addition to substantive grounds and reasons also explain why it is believed the data sought will be available with the person in control of the information system.

31. Warrants for arrest.– (1) No person shall be arrested or detained with respect to or in connection with any offence under this Act unless a warrant for arrest has been issued by the Court under this section.

(2) Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that a specified person identified in the application has committed or participated in the commission of an offence under this Act, the Court may, after recording reasons, issue a warrant which shall authorise an authorized officer, with such assistance as may be necessary, to arrest the person identified in the application.

(3) The application under sub-section (1) shall in addition to substantive grounds and reasons also explain why it is reasonably believed that the person identified in the application committed or participated in the commission of an offence under this Act.

(4) No court shall issue any warrant to arrest any person unless satisfied that consequent upon the particulars of the offence referred to in the application, there are reasonable grounds for believing that the person identified in the application has committed an offence under this Act.

(5) No person arrested under this Act shall be denied the right of access and presence of his advocate before and during any questioning.

32. Powers of an authorised officer;- (1) Subject to provisions of this Act, an authorised officer shall have the powers to -

(a) subject to grant of a warrant, have access to and inspect the operation of any specified information system;

(b) subject to grant of a warrant, use or cause to be used any specified information system to search any specified data contained in or available to such system;

(c) subject to grant of a warrant, obtain and copy only relevant data, use equipment to make copies and obtain an intelligible output from an information system;

(d) subject to grant of a warrant, require any person by whom or on whose behalf, the authorised officer has reasonable cause to believe, specified information system has been used to grant access to any data within an information system within the control of such person; and

(e) subject to the grant of a warrant, require any person having charge of or otherwise concerned with the operation of any information system to provide him reasonable technical and other assistance as the authorised officer may require for investigation of an offence under this Act;

Provided, that these powers shall not empower an authorized officer to compel a suspect or an accused to provide decryption information, or to incriminate himself or provide or procure information or evidence or be a witness against himself;

Explanation.- Decryption information means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable form and from ciphered data to intelligible data.

(2) In exercise of the power of search and seizure of any information system, program or data the authorized officer at all times shall-

(a) act with proportionality;

(b) take all precautions to maintain the integrity of the information system and confidentiality of data in respect of which a warrant for search or seizure has been issued;

(c) not disrupt or interfere with the integrity or miming and operation of any information system or data that is not the subject of the offences identified in the application for which a warrant for search or seizure has been issued;

(d) avoid disruption to the continued legitimate business operations and the premises subjected to search or seizure under this Act; and

(e) avoid disruption to any information system, program or data not connected with the information system that is not the subject of the offences identified in the application for which a warrant has been issued or is not necessary for the investigation of the specified offence in respect of which a warrant has been issued.

(3) When seizing or securing any information system or data, the authroised officer shall make all efforts to use technical measures while maintaining its integrity and chain of custody and shall only seize an information system, data, device or articles, in part or in whole, as a last resort, for sufficient reasons that do not make it possible under the circumstances to use such technical measures or where use of such technical measures by themselves would not be sufficient to maintain the integrity and chain of custody of the data being seized.

33. Dealing with seized data.- (1) If data has been seized or similarly secured, following a search or a seizure under Section 29 the authorised officer who undertook the search shall, at the time of the search or as soon as practicable after the search with respect to the data seized-

(a) make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and

(b) give a copy of that list to-

(i) the occupier of the premises; or
(ii) the person in control of the information system; or
(iii) a person having any legal right to the data.

(2) at the time of the search and in any event not later than twenty-four hours following the seizure, the authorised officer shall-

(a) permit a person who had the custody or control of the information system or someone acting on their behalf to access and copy data on the information system; or

(b) give the person a copy of the data.

(3) Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that giving the access or providing the copies-

(a) would constitute a criminal offence; or

(b) would prejudice-

(i) the investigation in connection with which the search was carried out;
(ii) another on going investigation; or
(iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations.

the Court may, after recording reasons, through written notification allow the authorised officer not to provide access or copies

(4) The Court may, on the application of:

(a) the occupier of the premises; or

(b) the person in control of the information system, or

(c) a person with any legal right to the data,
on being shown sufficient cause, order that a copy be provided to such a person.

(5) The costs associated with the exercise of rights under sub-sections (2) and (4) shall be borne by the person exercising these rights.

(6) Any person, including a service provider and an authorized officer, who, while providing services under the terms of lawful contract or otherwise in accordance with law, has secured access to any material or data containing personal information about another person, discloses such material to any other person, except when required by law, without the consent of the person concerned or in breach of a lawful contract, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain, or compromises its integrity and confidentiality, shall be punished with imprisonment for a term which may extend to three years or with fine up to one million rupees or with both.

34. Dealing with seized physical information systems.-(1) If an information has been physically seized or similarly secured, following a search or a seizure under section 29, the authorized officer who undertook the search must, at the time of the search or in any event no later than twenty-four hours after the seizure, with respect to the physical information systems seized,-

(a) make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and

(b) give a copy of that list to-

(i) the occupier of the premises; or
(ii) the person in control of the information system; or
(iii) a person with any legal right to the data.

(2) Subject to sub-section (3), on request, an authorized officer must, at the time of the search or as soon as practicable after the search,-

(a) permit a person who had the custody or control of the information system, or someone acting on their behalf to access and copy data on the information system; or

(b) give the person a copy of the data.

(3) Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that giving the access or providing the copies-

(a) would constitute a criminal offence; or

(b) would prejudice-

(i) the investigation in connection with which the search was carried out; or
(ii) another on going investigation; or
(iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations.

the Court may, after recording reasons, through written notification allow the authorised officer not to provide access or copies

(4) The Court may on the application of-

(a) the occupier of the premises; or

(b) the person in control of the information system, or

(c) a person with any legal right to the data,
on being shown sufficient cause, order that a copy be provided to such a person.

(5) The costs associated with the exercise of rights under sub-sections (2) and (4) shall be borne by the person exercising these rights.

(6) Any person, including a service provider and an authorized officer, who, while providing services under the terms of lawful contract or otherwise in accordance with law, has secured access to any material or data containing personal information about another person, discloses such material to any other person, except when required by law, without the consent of the person concerned or in breach of a lawful contract, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain, or compromises its integrity and confidentiality, shall be punished with imprisonment for a term which may extend to three years or with fine up to one million rupees or with both.

35. Power to manage information and issue directions for removal or blocking of access of any information through any information system: (I) The Authority is empowered to manage information and issue directions for removal or blocking of access of any information through any information system. The Authority may direct any service provider, to remove any information or block access to such intelligence, if it considers it necessary in the interest of the glory of Islam or the integrity, security

or defence of Pakistan or any part thereof, friendly relations with foreign states, public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offence under this Act.

(2) The Authority shall prescribe rules for adoption of standards and procedure to manage information, block access and entertain complaints.

(3) Until such procedure and standards are prescribed, the Authority shall exercise its powers under this Act or any other law for the time being in force in accordance with the directions issued by the Federal Government not inconsistent with the provisions of this Act.

(NOTE: THIS CHANGE IS RECOMMENDED BY ISPAK & P@SHA, WHO WILL BE SUBMITTING A PROCEDURE AS AN ADDENDUM. ALL OTHER GROUPS ARE OF THE VIEW THAT THIS SECTION SHOULD BE OMITTED IN ITS ENIRETY).

36. Limitation of liability of service providers.- (1) No service provider shall he subject to any civil and criminal liability, unless it is established that the service provider had specific actual knowledge and intent to proactively and positively participate, and not merely through omission or failure to act, and thereby facilitated, aided or abetted the use by any person of any information system, service, application, online platform or telecommunication system maintained, controlled or managed by the service provider in connection with a contravention of this Act or rules made thereunder or any other law for the time being in force:

Provided that the burden to prove that a service provider had specific actual knowledge, and willful intent to proactively and positively participate in any act that gave rise to any civil or criminal liability shall he upon the person alleging such facts and no interim or final orders, or directions shall he issued with respect to a service provider by any investigation agency or Court unless such facts have so been proved and determined:

Provided further that such allegation and its proof shall clearly identify with specificity the content, material or other aspect with respect to which civil or criminal liability is claimed including but not limited to unique identifiers such as the Account Identification (Account II)), Uniform Resource Locator (URL), Top Level Domain (TLD), Internet Protocol Addresses (11) Addresses), or other unique identifier and clearly state the statutory provision and basis of the claim.

(2) No service provider shall under any circumstance be liable under this Act, rules made thereunder or any other law for maintaining and making available the provision of their service in good faith.

(3) No service provider shall he subject to any civil or criminal liability as a result of informing a subscriber, user or end-users affected by any claim, notice or exercise of any power under this Act, rules made thereunder Or any other law

Provided that the service provider, for a period not exceeding fourteen days, shall keep confidential and not disclose the existence of any investigation or exercise of any power under this Act when a notice to this effect is served by Court upon an application by an authorised officer, that demonstrates there is reasonable cause for such confidentiality and the Court shall only authorize an extension beyond fourteen days for a specified period upon an application by an authorized officer, after it is satisfied that reasonable cause for such extension exists .

(4) No service provider shall he liable under this Act, rules made thereunder or any other law for the disclosure of any data or other information that the service provider discloses only to the extent of the provisions of this Act.

(5) No service provider shall he under any obligation to proactively monitor, make inquiries about material or content hosted, cached, routed, relayed, conduit, transmitted or made available by such intermediary or service provider.

37. Immunity against disclosure of information relating to security procedure.—(1) Subject to sub-section (2), no person shall be compelled to disclose any password, key or other secret information exclusively within his private knowledge, which enables his use of the security procedure or advanced electronic signature.

(2) Subject to the right against self-incrimination under sub-section (2) of section 161 of the Code and Article 13 (2) of the Constitution, sub-section (1) shall not confer any immunity where such information is used for the commission of any offence under this Act, rules made thereunder or any other law.

38. Inadmissibility of seized evidence.- (1) Any evidence seized or similarly secured through any violation or failure to comply with any of the provisions of this Act shall have the effect of tainting the evidence seized and such evidence shall not be admissible before any Court or authority for any purpose in the relevant proceedings or any other proceedings.

(2) No evidence shall be accessed, searched, seized or similarly secured unless it is relevant to the offence identified in the application and the warrant issued which shall superficially identify the particular evidence to be searched or seized is issued.

(3) An application to declare evidence inadmissible for the purposes of sub-section (1) or for any other reason may be moved at any time during the criminal proceedings whether during the stage of inquiry, investigation, trial, before judgment or in appeal.

39. Real-time collection and recording of traffic data.- (1) If a Court is satisfied on the basis of information furnished by an authorised officer that there are reasonable grounds to believe that the content of any specifically identified electronic communication is reasonably required for the purposes of a specific criminal investigation, the Court may order, with respect to traffic data held by or passing through a service provider within its jurisdiction, and where financially and technically possible for the service provider, to have that intermediary or service provider collect or record traffic data in real-time associated with only the specified communications and related to or connected with only the person under investigation transmitted by means of an information system and disclose only the specified traffic data:

Provided that such real-time collection or recording shall not he ordered for a period beyond what is absolutely necessary and in any event for not more than seven days.

(2) Notwithstanding anything contained in any law to the contrary the information so collected under sub-section (1) shall be admissible in evidence.

(3) The period of real-time collection or recording may be extended beyond seven days if, on an application, the Court authorises an extension for a further specified period of time.

(4) The application under sub-sections (1) and (2) shall in addition to substantive grounds and reasons also-

(a) explain why it is believed the data sought will be available with the person in control of an information system;

(b) identify and explain with specificity the type of information likely to be found on such information system;

(c) identity and explain with specificity the identified offence made out under this Act in respect of which the warrant is sought;

(d) if authority to seek real-time collection or recording on more than one occasion is needed, explain why, and how many further disclosures are needed to achieve the purpose for which the warrant is to be issued;

(e) what measures shall be taken to prepare and ensure that the real-time collection or recording is carried out whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information of an person not part of the investigation;

(f) why the investigation may be frustrated or seriously prejudiced unless the real time collection or recording is permitted; and

(g) why to achieve the purpose for which the warrant is being applied, real time collection or recording by the person in control of the information system is necessary.

(5) Any person, including a service provider and an authorized officer, who, while providing services under the terms of lawful contract or otherwise in accordance with law, has secured access to any material or data containing personal information about another person, discloses such material to any other person, except when required by law, without the consent of the person concerned or in breach of a lawful contract, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain, or compromises its integrity and confidentiality, shall be punished with imprisonment for a term which may extend to three years or with fine up to one million rupees or with both.

CHAPTER IV

INTERNATIONAL COOPERATION

40. International cooperation.- (1) The Federal Government may on receipt of request, extend such cooperation to any foreign Government, 24 x 7 network, any foreign agency or any international organization or agency for the purposes of investigations or proceedings concerning offences related to information systems, electronic communication or data or for the collection of evidence in electronic form relating to an offence or obtaining expeditious preservation and disclosure of data by means of an information system or real-time collection of data associated with specified communications or interception of data pursuant to the provisions of this Act.

(2) The Federal Government may, at its own, forward to a foreign Government, 24 x 7 network, any foreign agency or any international agency or organization any information obtained, pursuant to the

provisions of this Act, from its own investigations if it considers that the disclosure of such information might assist the other Government, agency or organization etc., as the case be in initiating or carrying out investigations or proceedings concerning any offence.

(3) The Federal Government shall require the foreign Government, 24 x 7 network, any foreign agency or any international agency to keep the information provided confidential and use it strictly for purposes mentioned in sub-section (1) of this section.

(4) The Federal Government shall be responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

Provided that the Federal Government when receiving or making a request for mutual assistance:

a) Shall make and receive requests for mutual assistance through the agency established or designated under this Act

b) Require the requesting government to make a request through the designated agency under its domestic law

c) Ensure that when making or receiving a request for mutual assistance the necessary particulars are fulfilled, relating inter alia to:

i) the name, address and any other relevant particulars identifying the agency making the request;

ii) the specific data to which the request pertains, or its controller;

iii) the purpose of the request

d) The requesting agency, which has received information in reply to its own request for mutual assistance, shall not use that information for purposes other than those specified in the request for assistance

e) Persons belonging to or acting on behalf of the designated authority shall be bound by appropriate obligations of secrecy or confidentiality with regard to that information

(5) The Federal Government may refuse to accede to any request made by a foreign Government, 24 x 7 network, any foreign agency or any international organization or agency if the request concerns an offence which may prejudice Pakistanʾs national interests including its sovereignty, security, public order or an ongoing investigation or trial.

CHAPTER — V

PROSECUTION AND TRIAL OF OFFENCES

41. Offences to be compoundable and non-cognizable.- (1) All offences under this Act, except the offences section 10 of this Act, and abetment thereof, shall be non-cognizable, bailable and compoundable.

(2) Offences under section 10 and abetment thereof shall he non-bailable and non-compoundable.

42. Cognizance and trial of offences. (1) The Federal Government, in consultation with the Chief Justice of respective High Court, shall designate Presiding Officers of the Courts to try offences under this Act at such places as deemed necessary.

(2) The Federal Government shall, in consultation with the Chief Justice of respective High Court, arrange for special training to be conducted by an entity notified by the Federal Government for training on computer sciences, cyber forensics, electronic transactions and data protection.

(3) Prosecution and trial of an offence under this Act committed by a minor shall he conducted under the Juvenile Justice System Ordinance, 2000.

(4) To the extent not inconsistent with the provisions of this Act, the investigation agency and the prosecutors shall follow the procedure laid down under the Code of Criminal Procedure 1898 (V of 1898) and the Qanoon-e-Shahadat Order 1984 (President's Order No. 10 of 1984).

43. Order for payment of compensation.- (1) The Court may, in addition to award of any punishment including fine under this Act, make an order for payment of compensation to the victim for any damage or loss caused and 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 so awarded.

44. Supply of statements and documents to the accused.- (1) In all cases, copies of the entire investigation file, documents related to any proceeding or investigation and all evidence, including all exculpatory facts and evidence shall be supplied free of cost to the accused not later than fourteen days before the commencement of the trial.

45. Description of offence to be mentioned with specificity.-The Court shall, when taking into consideration in a proceeding or mentioning any section of this Act in any document, including but not limited to any proceeding for issuance of warrant, bail, framing of charge or trial or any other proceeding with respect to or involving this Act, shall not merely consider and mention the section of the offence in question but shall also consider and specify the sub-section, clause and sub clause to identify exactly which offence is being referred to.

46. Preliminary assessment.- (1) Upon the lodging of a report under section 155 of the Code, and again upon the filing of the interim investigation report under section 173 (1) of the Code, the Court shall, without the need for any application for such preliminary assessment to be filed, no later than the following day make a preliminary assessment under subsections (2) and (3) respectively, as to whether an offence is made out against the accused and whether there is a likelihood of conviction based upon the facts placed on record and shall as the Court may deem appropriate:

(a) discharge the accused;

(b) if an accused is not in custody and:

(i) the case is of further enquiry, order that no arrests be made unless the Court is satisfied that based upon the facts placed on record an offence is made out against the accused and there is a likelihood of conviction; or

(ii) if the Court is satisfied that based upon the facts placed on record an offence is made out against the accused and there is a likelihood of conviction, proceed with the matter without prejudice to the right of any accused including his right to seek bail;

(c) if an accused is in custody and:

(i) the case is of further enquiry, order that the accused be released without bail subject to any future possibility of arrests if the Court is subsequently satisfied that based upon the facts placed on record an offence is made out against the accused and there is a likelihood of conviction; or

(ii) if the Court is satisfied that based upon the facts placed on record an offence is made out against the accused and there is a likelihood of conviction, proceed with the matter without prejudice to the right of any accused including his right to seek bail:

Provided that any assessment under this section shall only be tentative and shall be without prejudice to future determinations of the Court with respect to any further proceedings, including but not limited to bail, acquittal, framing of charge, or trial.

(2) The presence of the accused shall not be necessary for any proceeding, hearing or determination under this section.

47. Right to pre-arrest bail.- (1) Any person whether an accused or apprehending that he may be arrested for a commission of an offence under this Act, whether or not nominated or named in any report under section 154, 155 or 173 of the Code shall have the right to seek bail and any court of competent jurisdiction shall have the power to grant him bail.

(2) Notwithstanding proceedings having taken place under subsection (1), any person whether an accused or apprehending that he may be arrested for a commission of an offence under this Act, whether or not nominated or named in any report under section 154, 155 or 173 of the Code shall have the right to move an application for another preliminary proceeding under subsection (1) at any stage of the case whether during the stage of inquiry, investigation, trial, before judgment or in appeal.

48. Pre-arrest bail when person outside Pakistan.- (1) When a person present outside the territorial limits of Pakistan comes to have knowledge of any circumstance under subsection (1) or (2) of section 42 and apprehends that he may be arrested upon his return to Pakistan for an offence under this Act, he shall have the right to seek bail or protective bail before any Court of competent jurisdiction without the need for his personal attendance and to be represented and appear by and through his pleader.

(2) The Court may at its discretion make such order as to provide such a person with assurance and protection on his return and secure his attendance according to such terms as it may deem fit.

(3) Should a person who has been granted bail under this section fails to return to Pakistan or abide by any of the terms thereof, the Court may cancel his bail and proclaim him an offender forthwith, ordering the investigating agency to take all measures through Interpol or mutual legal assistance treaties to secure the extradition and arrest of such person.

49. Appointment of amicus curiae and seeking expert opinion.- The Court may appoint amicus curiae or seek independent expert opinion on any matter connected with a case pending before it.

50. Appeal.- An appeal against an order of a Court shall lie within thirty days from the date of provision of its certified copy free of cost.

CHAPTER VI

PREVENTIVE MEASURES

51. Prevention of electronic crimes.- (1) The Federal Government or the Authority, as the case may be, may issue guidelines to be followed by the owners of the designated information systems or service providers in the interest of preventing any offence under this Act.

(2) Any owner of the information system or service provider who violates the guidelines issued under sub-section (1) may be liable to be charged a fine not exceeding one million rupees, which shall be determined by the Court with the object of seeking compliance with the guidelines keeping in view of the nature of the violation and the intent of the person liable for the violation.

52. Computer Emergency Response Teams.- (1) The Federal Government may formulate one or more Computer Emergency Response Teams to respond to any threat against or attack on any critical infrastructure information systems or critical infrastructure data, or widespread attack on information systems in Pakistan.

(2) A Computer Emergency Response Team constituted under sub-section (1) may comprise of technical experts from private or government sector, officers of any information agency or any sub-set thereof.

(3) A Computer Emergency Response Team shall respond to a threat or attack without causing any undue hindrance or inconvenience to the use and access of the information system or data as may be prescribed pursuant to the provisions of this Act.

CHAPTER VII

MISCELLANEOUS

53. Relation of the Act with other laws.- The provisions of this Act shall have effect notwithstanding anything to the contrary contained in any other law for the time being in force.

54. Power to make rules.- (1) The Federal Government may, by notification in the official Gazette, make rules for carrying out purposes of this Act.

(2) Without prejudice to the generality of the foregoing powers, such rules may *inter alia* specify:-

(a) qualifications and trainings of the officers and staff of the investigation agency and prosecutors;

(b) powers, functions and responsibilities of the investigation agency, its officers and prosecutors;

(c) standard operating procedures of the investigation and prosecution agency;

(d) mode and manner in which record of investigation under this Act may be maintained;

(e) working of joint investigation teams;

(f) qualifications and trainings of the officers, experts and staff of the forensic laboratory;

(g) powers, functions and responsibilities of the forensic laboratory, its officers, experts and staff;

(h) standard operating procedures of the forensic laboratory to interact with the investigation and prosecution agency;

(i) constitution of Computer Emergency Response Team and the standard operation procedure to be adopted by such team;

(k) appointment of designated agency having capability to collect real time information;

(l) manner of coordination between the investigation agency and other law enforcement and information agencies including designated agency;

(m) manner of soliciting and extending international cooperation, and

(n) matters connected or ancillary thereto.

55. Removal of difficulties.- If any difficulty arises in giving effect to the provisions of this Act, the Federal Government may, by order published in the official Gazette, make such guidelines not inconsistent with the guidelines of this Act as may appear to be necessary for removing the difficulty.

56. Prior publication of rules and bylaws.- (1) All rules, bylaws and guidelines proposed to be made by the Government or the Authority, as the case may be, under this Act shall be published in the official Gazette and in at least one English and one Urdu daily with nationwide circulation, in draft form at least thirty days before the intended date of their coming into operation.

(2) The Authority shall keep record of all comments received in the draft of the rules, bylaws and guidelines, and prepare a report, in consultation with the Government, addressing each comment.

(3) The notification of the rules, bylaws and guidelines in their final form shall be published in the official Gazette and shall be accompanied by the report of the Authority referred to in sub-section (2).

57. Amendment of Electronic Transactions Ordinance, 2002 (LI of 2002) and pending proceedings.-

(1) Sections 36 and 37 of the Electronic Transactions Ordinance, 2002 (LI of 2002) are omitted.

(2) Any action taken by or with the approval of the authority or proceedings pending under the provisions of the Electronic Transactions Ordinance, 2002 (LI of 2002) repealed by sub-section (1), shall continue and be so deemed to have been taken or initiated under this Act.

58. Savings of powers.- Nothing in this Act shall affect, limit or prejudice the duly authorized and lawful powers and functions of the State institutions performed in good faith.
