INTRODUCED ON 12-05-2014

[AS INTRODUCED IN THE SENATE]

A

BILL

to make provision for protection of cyber crimes

Whereas it is expedient to prevent unauthorized acts with respect to electronic crimes and for related offences as well as procedure for their investigation, trial, prosecution, punishment and international collaboration with respect thereof;

It is hereby enacted as follows:-

CHAPTER I
INTRODUCTION

1. Short title, extent, application and commencement.- (1) This Act may be called the Protection of Cyber Crimes Act, 2014.

(2) It extends to the whole of Pakistan.

(3) The provisions of this Act applies where-

(a) an offence under this Act was committed in Pakistan;

(b) any act of preparation towards an offence under this Act or any part of the offence was committed in Pakistan or where any result of the offence has had an effect in Grenada;

(c) an offence under this Act 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) an offence under this Act 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 an electronic system in Pakistan; or

(e) an offence under this Act was committed by any person, of any nationality or citizenship 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.

(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) "Access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

(b) “access to program or data” means access to any program or data held in any information systems if by causing an information system to perform any function whereby a person —

(i) alters, modifies or erases the program or data or any aspect or attribute related to the program or data; or

(ii) copies, transfers or moves it to any information system, device or storage medium other than that in which it is held; or to a different location in the same information system, device or storage medium in which it is held; or

(iii) uses it; or

(iv) has it output from the information system in which it is held, whether by having it displayed or in any other manner:

Provided that for the purposes of paragraph (b) (iii) above a person uses a program if the function he causes the information system to perform causes the program to be executed; or is itself a function of the program:

Provided further that for the purposes of paragraph (b) (iv) above a program is output if the instructions of which it consists are output; and the form in which any such instructions or any other data is output (and in particular whether or not it represents a form in which, in the case of instructions, they are capable of being executed or, in the case of data, it is capable of being processed by an information system) is immaterial;

(c) "addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

(d) “code” means the Code of Criminal Procedure (Act V of 1898)

(e) "Computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

(f) "Computer Network" means the interconnection of one or more Computers or Computer systems or Communication device through-

(i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

(ii) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained;

(g) "Computer Resource" means computer, communication device, computer system, computer network, data, computer database or software;

(h) "Computer System" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

(i) “Contaminant" means a set of electronic instructions that are designed–

(i) to modify, destroy, record, transmit data or program residing within an electronic system; or

(ii) by any means to usurp the normal operation of an electronic system or electronic network;

(j) “critical infrastructure” means the assets, systems and networks, whether physical or virtual, so vital to the State that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof;

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

(l) “Cyber incidents" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;

(m) “damage” includes modifying, altering, deleting, erasing, suppressing, changing location or making data temporarily unavailable, halting an electronic system or disrupting the networks;

(n) “data” includes representations of facts, information or concepts that are being prepared or have been prepared in a form suitable for use in an electronic system including electronic program, text, images, sound, video and information within a database or electronic system;

(o) “Decryption” means the process of transforming or unscrambling encrypted data from its unreadable and incomprehensible format to its plain version;

(p) “designated payment system” means designated payment system as defined under paragraph (q) of section 2 of the Payment Systems and Electronic Fund Transfers Act, 2007;

(q) “electronic” means relating to technology having electrical, digital, magnetic, optical, biometric, electrochemical, wireless, electromagnetic, or similar capabilities;

(r) "electronic database" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by an electronic system or electronic network and are intended for use in an electronic system or electronic network;

(s) “electronic device” is any hardware that accomplishes its functions using any form or combination of electrical energy;

(t) "electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature.

(u) “electronic system” means an electronic 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 an electronic storage medium;

(v) “encryption” means the process whereby data is 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;

(w) “function” includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within an electronic system;

(x) "information" includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche;

(y) “malicious code” means an electronic program or a hidden function in a program that infects data with or without attaching its copy to a file and is capable of spreading over an electronic system with or without human intervention including virus, worm or Trojan horse;

(z) “mobile phone tracking” means the tracking of the current position of a mobile phone and includes location based services that discloses the actual coordinates of a mobile phone;

(za) "Password" means a secret word or phrase or code or passphrase or secret key, or encryption or decryption keys that one uses to gain admittance or access to information;

(zb) "Personal information" means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person;

(zc) “plain version” means original data before it has been transformed or scrambled to an unreadable or incomprehensible format;

(zd) “Sensitive personal data or information” Sensitive personal data or information of a person means such personal information which consists of information relating to,—

(i) password;

(ii) financial information such as Bank account or credit card or debit card or other payment instrument details ;

(iii) physical, physiological and mental health condition;

(iv) sexual orientation;

(v) medical records and history;

(vi) Biometric information;

(vii) any detail relating to the above paragraphs as provided to body corporate for providing service; and

(viii) any of the information received under above paragraphs by body corporate for processing, stored or processed under lawful contract or otherwise:

Provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information under Article 19-A of the constitution of Pakistan or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

(ze) “service provider” means–

(i) a person who provides an information and communication service including the sending, receiving, storing or processing of the electronic communication or the provision of other services in relation to it through an electronic system;

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

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

(zf) “Special Court” means the Court of Sessions competent to try offences under this Act;

(zg) “subscriber” means a person listed as using the services of a service provider;

(zh) “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 thereto 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;

(zi) “source code” means the listing of programs, electronic commands, design and layout and program analysis of electronic system in any form;

(zj) “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

(zk) “unauthorized access” means access of any kind by a person to an electronic system or data held in an electronic system which is unauthorized or done without authority or is in excess of authority, if the person is not himself entitled to control access of the kind in question to the electronic system or data and the person does not have consent to such access from a person so entitled.

CHAPTER II

Authentication of Digital Signatures through regulatory authority

3. Subscriber can authenticate electronic records.- (1) Subject to the provisions of this section a subscriber is authorize to authenticate an electronic record by digital signature.

(2) The authentication of the electronic record by digital signatures shall be effected by the asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation.—For the purposes of this sub-section, "hash function" is an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as “hash result” such that an electronic yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible---

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any official by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

4. Legality of electronic records.- (1) Where any law provides that any information or any other matter shall be available in writing or typewritten or printed, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is rendered or made available in an electronic form and accessible so as to be usable for a subsequent reference.

(2) Where any law provides that information or any other matter shall be verified by affixing the signature or any document shall be authenticated or bear the signature of any person then notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Government.

(3) Use of electronic records and digital signatures in Government and its agencies.-

(a) Where any law provides for the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the Government in a particular manner, the issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner, the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been fulfilled if such filing, issue, grant, receipt or payment, as the case may be, is applied by means of such electronic form as may be prescribed by the Government or its agency; and

(b) The appropriate Government may for the purposes of sub-section (1) by rules and regulations, prescribe the manner and format in which such electronic records/ documents shall be filed, created, received or issued; the manner or procedure of payment of any fee or charges for filing, creation or issue any electronic record under paragraph *(a).*

5. Retention and maintenance of electronic records.- (1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been fulfilled if such documents, records or information are retained in the electronic form, if the information contained therein remains accessible so as to be usable for a subsequent reference; the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received; the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record:

Provided that this section does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

6. Publication of rule, regulation, etc., in Electronic Gazette.- Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been fulfilled if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:

Provided that where any rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

7. Sections 6, 7 and 8 not to confer right to insist document should be accepted in electronic form.- Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Federal Government or the Provincial Government or any authority or body established by or under any law or controlled or funded by the Federal or Provincial Government should accept, issue, create, retain, maintain and preserve any document in the form of electronic records or perform any monetary transaction in the electronic form.

8. Power to make rules. The Federal Government may, for the purposes of this Act, by rules, prescribe—

(a) the type of digital signature;

(b) the manner and format in which the digital signature shall be affixed;

(c) the manner or procedure which facilitates identification of the person affixing the digital signature;

(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) any other matter which is necessary to give legal effect to digital signatures.

9. Attribution of electronic records.- An electronic record shall be attributed to the author—

(a) if it was sent by the author himself;

(b) by a person who had the authority to act on behalf of the author in respect of that electronic record; or

(c) by an information system programmed by or on behalf of the author to operate automatically.

10. Acknowledgement.- (1) Where the author has not agreed with the addressee that the acknowledgment of receipt of electronic record be given in a particular format or by a particular mechanism, an acknowledgment may be given by,-

(a) any communication by the addressee, automated or otherwise; or

(b) any conduct of the addressee, sufficient to indicate to the author that the electronic record has been received.

(2) Where the author has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the author.

(3) Where the author has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the author within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the author may give notice to the addressee requiring that no acknowledgment has been received by him and mentioning a reasonable time by which the acknowledgment must be received and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

11. Time and place of dispatch and receipt of electronic record.- (1) Same as otherwise agreed to between the author and the addressee, the dispatch of an electronic record occurs when it enters a computer resource outside the control of the author.

(2) Same as otherwise agreed between the author and the addressee, the time of receipt of an electronic record shall be determined as follows, namely:—

(a) if the addressee has designated a computer resource for the purpose of receiving electronic records,—

(i) receipt occurs at the time when the electronic, record enters the designated computer resource; or

(ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

(b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

(3) Save as otherwise agreed between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the author has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(4) The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).

(5) For the purposes of this section, —

(a) if the author or the addressee has more than one place of business, the principal place of business, shall be the place of business;

(b) if the author or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

(c) "usual place of residence", in relation to a body corporate, means the place where it is registered.

12. Security of electronic record.- (1) Where any security mechanism has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

(2) Where if, by application of a security mechanism agreed to by the parties concerned, it can be authenticated that a digital signature, at the time it was affixed, was—

(a) unique to the subscriber affixing it;

(b) capable of identifying such subscriber;

(c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated.

Then such digital signature shall be deemed to be a secure digital signature.

13. Security mechanism.- (1) The Federal Government shall for the purposes of this Act prescribe the security mechanism having regard to commercial circumstances prevailing at the time when the procedure was used, including,-

(a) the nature of the transaction;

(b) the level of sophistication of the parties with reference to their technological skills;

(c) the volume of similar transactions engaged in by other parties;

(d) the availability of alternatives offered to but rejected by any party;

(e) the cost of alternative procedures; and

(f) the procedures in general use for similar types of transactions or communications.

(2) The Federal Government may, by notification in the Official Gazette, establish a Regulatory Authority for the purposes of this Act and may also by the same or subsequent notification appoint a Director General being the Chief Executive of the Authority.

(3) The Director General shall discharge his functions under this Act subject to the general control and directions of the Federal Government.

(4) The qualifications, experience and terms and conditions of service of the Director General shall be such as may be prescribed by the Federal Government.

(5) The Head Office and Branch Offices of the Director General of the Authority shall be at such places as the Federal Government may specify, and branch offices may be established at district level of all provinces of Pakistan.

(6) There shall be a seal of the Office of the Director General.

14. Functions of Director General.- The Director General may perform all or any of the following functions, namely:—

(a) Exercising supervision over the activities of the Certifying Authorities;

(b) Certifying public keys of the Certifying Authorities;

(c) Laying down the standards to be maintained by the Certifying Authorities;

(d) Specifying the qualifications and experience with employees of the certifying authorities should possess;

(e) Specifying the conditions subject to which the Certifying Authorities shall conduct their business;

(f) Specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key;

(g) Specifying the form and content of a Digital Signature Certificate and the key;

(h) Specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;

(i) Specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;

(j) Facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;

(k) Specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;

(l) Resolving any conflict of interests between the Certifying Authorities and the subscribers;

(m) laying down the duties of the Certifying Authorities; and

(n) Maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

15. Recognition of foreign Certifying Authorities. (1) Subject to such conditions and restrictions as may be specified by regulations, the Director General may with the previous approval of the Federal Government and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

(2) Where any Certifying Authority is recognised under sub-section (1), the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

(3) The Director General may if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under subsection (1) he may for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

16. Director General to act as repository.- (1) The Director General shall be the repository of all Digital Signature Certificates issued under this Act.

(2) The Director General shall—

(a) make use of hardware, software and procedures that are secure from intrusion and misuse; and

(b) observe such other standards as may be prescribed by the Federal Government, to ensure that the secrecy and security of the digital signatures are assured.

(3) The Director General shall maintain a computerized data base of all public keys in such a manner that such data base and the public keys are available to any member of the public.

17. License to issue Digital Signature Certificates.- (1) Subject to the provisions of sub-section (2), any person may make an application to the Director General for a license to issue Digital Signature Certificates.

(2) No license shall be issued under sub-section (1) unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities which are necessary to issue Digital Signature Certificates as may be prescribed by the Federal Government.

(3) A license granted under this section shall—

(a) be valid for such period as may be prescribed by the Federal Government;

(b) not be transferable or heritable; and

(c) be subject to such terms and conditions as may be specified by the regulations.

18. Application for license.- (1) Every application for issue of a license shall be in such form as may be prescribed by the Federal Government.

(2) Every application for issue of a license shall be accompanied by—

(a) A certification practice statement;

(b) A statement including the procedures with respect to identification of the applicant;

(c) Payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Federal Government; and

(d) Such other documents, as may be prescribed by the Federal Government.

19. Renewal of license.- An application for renewal of a license shall be, in such form and accompanied by such fees, as may be prescribed by the Federal Government and shall be made not less than thirty days before the date of expiry of the period of validity of the license.

20. Procedure for grant or rejection of license.- The Director General may on receipt of an application under sub-section (1) of section 18, after considering the documents accompanying the application and such other factors as he deems fit, grant the license or reject the application:

Provided that no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

21. Suspension and Revocation of license.- (1) The Director General may revoke the license, if he is satisfied after making such inquiry as he may think fit that a Certifying Authority has,—

(a) made a statement in, or in relation to, the application for the issue or renewal of the license, which is incorrect or false in material particulars;

(b) failed to comply with the terms and conditions subject to which the license was granted;

(c) failed to maintain the standards specified under paragraph *(d) of* sub-section (2) of section 26; and

(d) contravened any provisions of this Act, rule, regulation or order made thereunder:

Provided that no license shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

(2) The Director General may if he has reasonable cause to believe that there is any ground for revoking a license under sub-section (1), by order suspend such license pending the completion of any inquiry ordered by him:

Provided that no license shall be suspended for a period exceeding fifteen days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

(3) No Certifying Authority whose license has been suspended shall issue any Digital Signature certificate during such suspension.

22. Notice of suspension or revocation of license.- Where the license of the Certifying Authority is suspended or revoked, the Director General shall publish notice of such suspension or revocation, as the case may be, in the database maintained by him.

23. Power to delegate.- The Director General may in writing authorize the Additional Director General or any officer to exercise any of the powers of the Director General under this Chapter.

24. Power to investigate contraventions.- The Director General or any officer authorized by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder.

25. Access to computers and data.- The Director General or any person authorized by him shall if he has reasonable cause to suspect that any contravention of the provisions of this Act, rules or regulations made thereunder has been committed have access to any computer system any apparatus data or any other material connected with such system for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

26. Certifying Authority to follow certain procedures.- Every Certifying Authority shall —

(a) make use of hardware, software and procedures that are secure from intrusion and misuse;

(b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;

(c) adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and

(d) observe such other standards as may be specified by regulations.

27. Certifying Authority to ensure compliance of the Act, etc.- Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations and orders made thereunder.

28. Display of license.- Every Certifying Authority shall display its license at a conspicuous place of the premises in which it carries on its business.

29. Surrender of license.- (1). Every Certifying Authority whose license is suspended or revoked shall immediately after such suspension or revocation, surrender the license to the Director General.

(2) Where any Certifying Authority fails to surrender a license under sub-section (1), the person in whose favor a license is issued, shall be guilty of an offence and shall be punished with imprisonment which may extend up to six months or a fine which may extend up to fifty thousand rupees or with both.

30. Disclosure.- (1) Every Certifying Authority shall disclose in the manner specified by regulations,—

(a) its Digital Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate;

(b) any certification practice statement relevant thereto;

(c) notice of the revocation or suspension of its Certifying Authority certificate, if any; and

(d) any other fact that materially and adversely affects either the reliability of a Digital Signature Certificate, which that Authority has issued, or the Authority's ability to perform its services.

(2) Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Digital Signature Certificate was granted, then, the Certifying Authority shall—

(a) use reasonable efforts to notify any person who is likely to be affected by that occurrence; or

(b) act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

31. Certifying Authority to issue Digital Signature Certificate.- (1) Any person may make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Federal Government

(2) Every such application shall be accompanied by such fee not exceeding twenty-five thousand rupees as may be prescribed by the Federal Government to be paid to the Certifying Authority:

Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applicants'.

(3) Every such application shall be accompanied by a certification practice statement or where there is no such statement a statement containing such particulars, as may be specified by regulations.

(4) On receipt of an application under sub-section (1) the Certifying Authority may, after consideration of the certification practice statement or the other statement under sub-section (3) and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application:

Provided that no Digital Signature Certificate shall be granted unless the Certifying Authority is satisfied that—

(a) the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;

(b) the applicant holds a private key, which is capable of creating a digital signature; and

(c) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant:

Provided further that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

32. Representation upon issuance of Digital Signatures.- A Certifying Authority while issuing a Digital Signature Certificate shall certify that--

(a) it has complied with the provisions of this Act and the rules and regulations made thereunder;

(b) it has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;

(c) the subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;

(d) the subscriber's public key and private key constitute a functioning key pair;

(e) the information contained in the Digital Signature Certificate is accurate; and

(f) it has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations made in paragraphs (a) to (d).

33. Suspension of Digital Signature Certificate.- (1) Subject to the provisions of sub-section (2), the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate,—

(a) on receipt of a request to that effect *from*—

(i) the subscriber listed in toe Digital Signature Certificate; or

(ii) any person duly authorized to act on behalf of that subscriber; and

(b) if it is of opinion that the Digital Signature Certificate should be suspended in public interest.

(2) A Digital Signature Certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.

(3) On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

34. Revocation of Digital Signature Certificate.- (1) A Certifying Authority may revoke a Digital Signature Certificate issued by it—

(a) where the subscriber or any other person authorized by him makes a request to that effect; or

(b) upon the death of the subscriber; or

(c) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

(2) Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub-section (1), a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time, if it is of opinion that—

(a) a material fact represented in the Digital Signature Certificate is false or has been concealed;

(b) a requirement for issuance of the Digital Signature Certificate was not satisfied;

(c) the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability; and

(d) the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist.

(3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

35. Notice of suspension or revocation.- (1) Where a Digital Signature Certificate is suspended or revoked under section 33 or section 34, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be in the repository specified in the Digital Signature Certificate for publication of such notice.

(2) Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may he. in all such repositories.

36. Duties of Subscribers.- (1) Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, then, the subscriber shall generate the key pair by applying the security procedure.

(2) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate,—

(a) to one or more persons; and

(b) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

(3) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that,—

(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true; and

(c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

37. Control of private key.- (1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorized to affix the digital signature of the subscriber.

(2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by .the regulations.

Explanation.— For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

CHAPTER III
ESTABLISHMENT OF INVESTIGATION, PROSECUTION AGENCY AND SPECIAL COURT

38. Establishment of investigation agencies and prosecution.-(1) The Federal Government shall establish new law enforcement agency as special Investigation Agency for the purposes of investigation and prosecution of offences under this Act.

(2) Unless otherwise provided for under this Act the special investigation agency, the special investigating officer, prosecution and the court shall in all matters follow the procedure laid down in the Criminal Procedure Code (Act V of 1898) to the extent that it is not inconsistent with any provision of this Act:

(3) All investigating officers appointed under this Act or exercising any power, privilege, right or provision under this Act shall at a minimum, hold a specialized qualification in digital forensics, information technology or computer science, in such terms as may be prescribed.

39. Authority to investigate, warrant, arrest, search and seizer of material.- (1) No person whether a police officer investigation officer or otherwise other than an investigating officer of the special investigation agency shall investigate an offence with respect to, in connection with or under this Act.

(2) No person other than a prosecutor assigned by the special investigating agency shall prosecute any offence with respect to, in connection with or under this Act.

(3) No Court lower than the Special Court, in accordance with the provisions of this Act in particular section 45, shall conduct the trial, hearing of all proceedings in respect of, related to or in connection with an offence under this Act.

(4) No person, other than an investigating officer of the special investigation agency, shall exercise any power, including but not limited to arrest, access, search, seizure, preservation, production or real time collection or recording, under this Act, rules made thereunder or any other law, with respect to and in connection with any offence under this Act.

(5) No investigating officer shall exercise any power of arrest, access, search, seizure, preservation, production, or real time collection other than a power provided for under this Act.

(6) Notwithstanding any other law including sections 94 and 95 of CHAPTER VII Part B of the Code or any other provision of any law, and without prejudice to and subject at all times to sections 41, 42, 43 and 44 of this Act, no investigating officer shall conduct any inquiry or investigation or call for any information in connection with any offence under this Act without obtaining an order for the disclosure of such information from the Court and the Court shall only issue such order if the particulars of the investigation meet the qualification provided for under the relevant section of this Act to which the request for disclosure pertains.

(7) Any investigating officer, when mentioning any section of this Act in any application or any document, including but not limited to any application for any warrant or disclosure under this Act or any report under sections 154, 155 or 173 or any other provision of the Code of Criminal Procedure or any other law with respect to any investigation, inquiry, arrest, access, search, seizure, preservation, production, or real time collection under this Act, shall not merely mention the section but shall also specify the sub-section, paragraph and sub-paragraph to identify exactly which offence is being referred to.

40. Expedited Preservation of data.- (1) If an investigating officer is satisfied that-

(a) traffic data or content 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 traffic data or content data may be modified, lost, destroyed or rendered inaccessible, the investigating officer may, by written notice given to a person in control of the information system, require the person to ensure that the data specified in the notice be preserved and the integrity thereof is maintained for a period not exceeding seven days as specified in the notice.

(2) The period of preservation and maintenance of integrity may be extended beyond seven days if, on an application by the investigating officer, the Court authorizes an extension for a further specified period of time, upon being satisfied that reasonable cause for such extension exists.

(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 notice or for any extension thereof permitted by the Court;

(b) to the extent that such preservation and maintenance of integrity will not be administratively or financially burdensome; and

(c) where it is technically and practically reasonable to preserve and maintain the integrity such data.

41. Warrant for search and seizure.- (1) Upon an application on oath by an investigating 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, program, data, device or storage medium of a specified kind that-

(a) is reasonably 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 investigation officer, with such assistance as may be necessary, in the presence of a Magistrate, to enter only the specified place and to search only the specified information system, program, data, device or storage medium relevant to the offence identified in the application and access, seize or similarly secure only the specified data or specified program, device or storage medium relevant to the offence identified in the application, but without causing any of the results identified in any event without prejudicing the integrity and security of any data or program available in or through the specified information system, program or generally present or available at the specified place:

Provided that the Magistrate for the purposes of this Chapter shall not include any person who is employed or performs any function on behalf of the special investigating agency:

Provided further that the requirement of the presence of a Magistrate under paragraph (b) of sub-section (1) and paragraph (h) of sub-section (2) shall come into effect twelve months from the coming into force of this Act.

(2) The application under sub-section (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;

(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;

(c) identify and explain with specificity the type of evidence suspected will be found on the premises;

(d) identify and explain with specificity the relevant program or data that is sought and reasonably suspected to be available from each individual information system, device or storage medium;

(e) identify and explain with specificity the relevant individual information systems, devices or storage mediums expected to be searched or seized and reasonably suspected to contain the relevant program or data or any evidence;

(f) what measures shall be taken to prepare and ensure that the search and seizure is carried out through technical means such as mirroring or copying of relevant data and not through physical custody of information systems or devices;

Provided that this shall not prejudice the powers defined in sub-section (4) of section 39;

(g) describe and identify the persons to be authorised to accompany the officer executing the warrant and the reasons that necessitate their presence; and

(h) seek the Court to identify the Magistrate who will be accompanying the officer during execution of the warrant.

(3) No Court shall issue any warrant to enter and search any specific premises, any specific information system or any specific program or any specific data or any specific device or any specific storage medium 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 any specific premises occupied, any specific information system or any specific program or any specific data or any specific device or any specific storage medium controlled by the person identified in the application in order to find the material sought.

(4) Any person who obstructs the lawful exercise of the powers under sub-section (1) or sub-section (2) or misuses the powers granted under this section shall be liable to punishment with imprisonment of either description for a term which may extend to six month, or with fine not exceeding fifty thousand rupees, or with both.

42. Warrant for disclosure of traffic data.- (1) Upon an application on oath by an investigating 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 a specifically identified offence made out under this Act, the Court may, after recording reasons, order that a person in control of the information system disclose sufficient traffic data about a specified communication to identify-

(a) the service providers; and

(b) the path through which the communication was transmitted.

(2) The period of a warrant issued under sub-section (1) may be extended beyond seven days if, on an application, a Court authorizes 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,-

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

(b) identify and explain with specificity the type of traffic data suspected will be found on such information system;

(c) identify and explain with specificity the subscribers, users or unique identifier the subject of an investigation or prosecution suspected may be found on such information system;

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

(e) what measures shall be taken to prepare and ensure that the traffic data will be sought and carried out,-

(i) whilst maintaining the privacy of other users, customers and third parties; and

(ii) without the disclosure of data of any party not part of the investigation.

(4) Any person who obstructs the lawful exercise of the powers under sub-section (1) or sub-section (2) or misuses the powers granted under this section shall be liable to punishment with imprisonment of either description for a term which may extend to six month or with fine not exceeding fifty thousand rupees or with both:

Provided that it shall not be an offence for a person to refuse cooperation if that person is a suspect or accused or is by exercise of such power being compelled to incriminate himself, provide or procure information or evidence or be a witness against himself.

43. Powers of an investigating officer.- (1) Subject to obtaining a search warrant under section 39 an investigation officer shall be entitled to only the information system, program and data specified in the warrant to-

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

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

(c) obtain and copy that data, use equipment to make copies and obtain an intelligible output from an information system;

(d) have access to or demand any information, code or technology which has the capability of retransforming or unscrambling encrypted data contained or available to such information system into readable and comprehensible format or plain version;

(e) require any person by whom or on whose behalf, the investigating officer has reasonable cause to believe, any information system has been used to grant access to any data within any information system within the control of such person;

(f) require any person having charge of or otherwise concerned with the operation of such information system to provide him reasonable technical and other assistance as the investigating officer may require for the purposes of paragraphs (a), (b) and (c); and

(g) require any person who is in possession of decryption information of an information system, device or data under investigation to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence:

Provided that this power shall not empower an investigating 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 cipher text to its plain text.

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

(a) at all times act with proportionality;

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

(c) not disrupt or interfere with the integrity or running and operation of any information system, program 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 subject of the search or seizure; 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 similarly securing any data, the investigating officer shall make all efforts to use technical measures to copy or replicate the data, whilst maintaining its integrity and chain of custody and shall only seize any information system, device or storage medium physically, in whole or in part, 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:

Provided that where a physical seizure occurs, the investigating officer shall submit forthwith and in any event no later than twenty four hours a report detailing sufficient reasons for such seizure before the Court.

44. Cordons for investigation.- (1) An area is a cordoned area for the purposes of an investigation under this Act, if it is designated as such under this section.

(2) A designation may be made only by an investigating officer specially designated in this respect by the specialized investigation agency, if he considers it expedient for the purposes of the investigation.

(3) If a designation is made orally, the officer making it shall confirm it in writing, as soon as is reasonably practicable.

(4) The officer making a designation shall arrange for the demarcation of the cordoned area, so far as is reasonably practicable.

(5) An area may be designated a cordoned area for a period not exceeding fourteen days, which may be extended in writing from time to time, with each extension specifying the additional period:

(6) Any cordoning under this section shall adequately take into consideration and provide for the avoidance of any interruption, obstruction, hindrance or disruption to continued legitimate business operations and the premises or area so cordoned.

(7) Any person affected by such cordoning may seek the removal or modification or the cordoning before the Court and the Court shall consider, when passing any order in this respect no later than seven days, make such order that avoids any interruption, obstruction or hindrance or disruption to continued legitimate business operations without prejudice to the preservation and integrity of evidence in the case.

(8) Where a person knows or has reasonable cause to suspect that an investigation is being conducted or is proposed to be conducted, a person commits an offence if he interferes with material which is likely to be relevant to an investigation and shall be liable on conviction to imprisonment for a term not less than six months and not exceeding two years, and fine:

Provided that it is a defence for a person charged with an offence under sub-section (6) to prove that he did not know and had no reasonable cause to suspect that the disclosure or interference was likely to affect a terrorist investigation.

(9) For the purposes of this section a person interferes with any material if he falsifies it, conceals it, destroys it or disposes of it or if he causes or permits another to do any of these things.

45. Establishment of Special Courts etc.- (1) The Government may establish as many Special Courts under this Act however special court may be established at district level of all provinces of Pakistan.

(2) The Government, in consultation with the Chief Justice of the concerned High Court, may appoint any person as judge of the Special Court constituted under this Act who is or has been a Sessions Judge in any province of Pakistan or has been an Advocate of the High Court for a period of not less than ten years.

(3) Only a Court where the presiding judge has successfully completed training conducted by the Federal Judicial Academy with respect to all aspects of this Act including cyber forensics, electronic transactions and data protection shall be competent to hear any matter arising out of or in connection with this Act.

(4) A judge Special Court shall have all the powers of a Sessions Court as provided under the Code.

46. Appeal.- (1) An appeal against the final judgment of a Special Court shall lie to the High Court.

(2) Copies of the judgments of a Special Court shall be supplied to the accused and public prosecutor on the day the judgment is pronounced.

(3) Any aggrieved person or the Government may file an appeal against the final judgment of a Special Court within a period of thirty days from the pronouncement of judgment.

47. Offence committed in cyberspace.- An offence committed by an accused or offender with the use of or in connection with any information system, across a network or in cyberspace may be inquired into or tried by a Court through or into the local limits of whose jurisdiction data, communication or connectivity may have passed.

48. Offence committed on a journey.- An offence committed whilst the offender is in the course of performing a journey or voyage may be inquired into or tried by a Court through or within the local limits of whose Jurisdiction the accused or offender or the person against whom, or the data or communication in respect of which, the offence was committed, passed in the course of that journey or voyage.

49. 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 thirty days before the commencement of the trial:

Provided that the Court may direct that the cost of any storage devices required for supplying such copies may be paid by the accused in case the Court is satisfied that, for reasons to be recorded, the accused has access to such funds that would enable the accused to make such payment.

50. 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, paragraph and sub-paragraph to identify exactly which offence is being referred to.

51. 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 on oath by an investigating 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 investigation 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; the application is reasonably suspected of either having committed or participated in the commission of an offence under this Act,-

(a) identify and explain with specificity the source of the evidence or information so far available which leads the investigating officer to reasonably suspect that the person identified in the application committed or participated in the commission of an offence under this Act;

(b) what measures shall be taken to prepare and ensure that the arrest is carried out with the use of reasonable and proportionate force; and

(c) what measures shall be taken to safeguard the unnecessary publicity of the identity of the person identified in the application and safeguarding the privacy of the family of the person identified in the application.

(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) Any person who obstructs the lawful exercise of the powers under sub-section (1) or sub-section (2) shall be liable to punishment with imprisonment of either description for a term which may extend to one month or with fine not exceeding fifty thousand rupees or with both.

(6) Simultaneous to the arrest of the person identified in the application the investigating officer shall inform such person that-

(a) he has the right to remain silent;

(b) anything he says can and shall be used against him in the court of law;

(c) he has the right to communicate and consult with an advocate as well as have his advocate present at all times during and when any questioning or when making a statement or confession; and

(d) if he cannot afford an advocate he may elect to have the specialized investigation agency immediately appoint an advocate for him and subsequently also have the Court appoint a different advocate for him, if so elects, when he appears before the Court next morning.

(7) No person other than the investigating officer or a member of any joint investigation team shall have the right to question the person arrested under this Act.

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

(9) Any person arrested under this Act shall have the right to-

(a) not make any statement;

(b) not answer any questions;

(c) to remain silent; and

(d) have his advocate present.

(10) Any person arrested under this Act shall have the right without being compelled, to waive any of the rights mentioned above and such waiver and evidence of there being no compulsion shall be documented through video and audio recording.

(11) Notwithstanding anything contained in the Qanoon-e-Shahadat, 1984 (President's Order No. 10 of 1984) or any other law for the time being in force, where in any Court proceedings held under this Act the evidence, which includes circumstantial and other evidence, produced raises the presumption that there is a reasonable probability that the accused has committed the offence, any confession made by the accused during investigation without being compelled, before a Magistrate or an investigation officer specially designated by the specialized investigation agency in this respect, may be admissible in evidence against him, if such confession is documented through video and audio recording and demonstrates that the accused was under no compulsion in this regard:

Provided that the investigating officer before recoding any such confession, shall have explained to the person making the confession of his rights under this Act and that he is not under any compulsion whether direct or indirect to make a confession and that if he does so it may be used as evidence against him:

Provided further that no investigating officer shall record such confession unless, upon questioning the person making it the investigating officer had reason to believe that it was made voluntarily; and that when he recorded the confession, he made a memorandum at the foot of such record to the following effect, namely:-

"I have explained to (...name...) that:

(a) he has a right to remain silent;

(b) anything he says can and shall be used against him in the court of law;

(c) that he has the right to communicate and consult with an advocate as well as have his advocate present at all times during an when being questioned or making any statement or confession;

(d) if he cannot afford an advocate he may elect to have the specialized investigation agency immediately appoint an advocate for him and subsequently also have the Court appoint a different advocate for him, if he so elects, when he appears before the Court next morning;

(e) he is not under any compulsion whether direct or indirect to make any statement or any confession;

(f) if he does make a statement or confession can and shall be used as evidence against him which would open him to being convicted of an offence;

Before making the statement of confession I had seen to it that the person making it was left in isolation without the presence of any investigating officer or other person that may influence him being present. I have also checked his body to see if there exist any signs of torture and my findings are mentioned herein. I believe that this confession was voluntarily made without any direct or indirect compulsion. It was taken in my presence and was read over to the person making it and admitted by him to be correct and it contains a full and true account of the statement made by him. My explanation to the person making the confession and his entire statement of confession has been documented through video and audio recording without any break or interruption in the recording.

(Signed)
Investigating officer / Special Judge."

Explanation.- It shall not be necessary that the Magistrate or specially designated investigation officer receiving and recording a confession or statement should be a Magistrate having jurisdiction in the case or an investigation officer involved in the investigation of the case.

(12) Only evidence of statements or questioning conducted and documented through video and audio recording shall be admitted before any Court whether as evidence or otherwise.

52. Limitation of liability of intermediaries and service providers.- (1) No intermediary or service provider shall be subject to any civil or criminal liability, unless it is finally established that the intermediary or service provider had actual notice, specific actual knowledge, willful and malicious intent and motive 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 an intermediary or service provider in connection with a contravention of this Act, rules made thereunder or any other law:

Provided that the burden to prove that an intermediary or service provider had notice, specific actual knowledge, willful and malicious intent and motive to proactively and positively participate in any act that gave rise to any civil or criminal liability shall be upon the person alleging such facts and no interim or final orders, directions shall be issued with respect to any intermediary or service provider unless such facts have so been finally proved:

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 ID), Uniform Resource Locator (URL) Top Level Domain (TLD) Internet Protocol Addresses (IP Addresses) or other unique identifier and clearly state the statutory provision and basis of the claim.

(2) No intermediary or 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.

(3) No intermediary or service provider shall be 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 intermediary or service provider present and established in terms equivalent to the requirements of the Companies Ordinance 1984 within the territorial jurisdiction of Pakistan, 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 upon them by an investigating officer, which period of confidentiality may be extended beyond fourteen days if, on an application by the investigating officer, the Court authorizes an extension for a further specified period of time, upon being satisfied that reasonable cause for such extension exists.

(4) No intermediary or service provider shall be 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 and under sub-section (3) and sections 40, 41, 42 and 43.

(5) No intermediary or service provider shall be 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.

53. Information of offence.- On receiving any complaint or information with respect to any offence under this Act, the investigating officer shall immediately enter the information in a book to be kept by such officer in such form as the Provincial Government may prescribe in this behalf under section 155 of the Code.

CHAPTER IV
Offences, Penalties and Punishments

A person shall not knowingly or without lawful excuse or justification, or without permission of the owner or any other person who is in charge of a computer, computer system, electronic system or network–

54. Illegal Entree to Information System.- Whoever with intent to unauthorized entree or secures entree to such electronic system, computer or perform function unlawfully on an information system whole or any part of such electronic system, computer or an information system shall be punished with imprisonment of either for a term which may extend to nine months or with fine which may extend to two hundred thousand rupees or with both.

55. Illegal Entree to Program or Data.- Whoever unlawfully, whether temporarily or not with intent causes access to any program or data to be secured or to be enabled, download, copy or extract data, electronic database or information from such electronic system or network including information or data held or stored in a removable storage medium shall be punished with imprisonment of either for a term which may extend to one year or with fine which may extend to three hundred thousand rupees or with both.

56. Unlawful Intervention with Program or Data.- Whoever unlawfully damage or cause to be damaged an electronic system or network, data, electronic database or other program residing in such electronic system or network or disrupt or causes the disruption of an electronic system or network shall be punished with imprisonment of either for a term which may extend to one year or with fine which may extend to three hundred thousand rupees or with both.

57. Unauthorized Act with Information System.- Whoever unlawfully deny or cause the denial of access to a person authorized to obtain access to an electronic system or network by any means or charge the services availed of by a person to the account of another person by tampering with or manipulating an electronic system or network shall be punished with imprisonment of either for a term which may extend to three months or with fine which may extend to fifty thousand rupees or with both.

58. Illegal Destroy, Delete or Alter Data Information etc.- Whoever willfully destroy, delete or alter data information residing in an electronic system or diminishes its value or utility of affects it injuriously by any means or steal, conceal, destroy or alter or cause a person to steal, conceal, destroy or alter any source code used for an electronic system with an intention of causing damage shall be punished with imprisonment of either for a term which may extend to six months or with fine which may extend to one hundred thousand rupees or with both.

59. Cyber Extremism.- (1) Whoever commits or threatens to commit any of the offences,-

(a) does any unauthorised act in relation to an information system;

(b) at the time when he does the act he knows that it is unauthorised; and

(c) acts with intent—

(i) to destroy, damage, delete, erase, deteriorate, generate, modify or alter any program or data;

(ii) to render any program or data inaccessible, meaningless, useless or ineffective;

(iii) to obstruct, interrupt or interfere with any program or data or any aspect or attribute related to the program or data;

(iv) to obstruct, interrupt or interfere with any person in the use of any program or data or any aspect or attribute related to the program or data;

(v) to deny, prevent, suppress or hinder access to any program or data to any person entitled to it;

(vi) to deny, prevent, suppress or hinder access to any program or data or any aspect or attribute related to the program or data or make it inaccessible;

(vii) to impair the operation of any program or any aspect or attribute related to the program;

(viii) to impair the reliability of any data or any aspect or attribute related to the data;

(ix) to impair the security of any program or data or any aspect or attribute related to the program or data; or

(x) to enable any of the things mentioned in paragraphs (i) to (ix) to be done;

shall be punished with imprisonment of either description for a term which may extend to five years or with fine which may extend to seven hundred thousand rupees, or with both.

(2) Whoever commits any offence under sub-section (1) by circumventing or infringing security measures with respect to any information system, program or data shall be punished with imprisonment of either description for a term which may extend to five years or with fine which may extend to seven hundred thousand rupees or with both.

(3) Whoever commits any offence under sub-section (1) with respect to any Government controlled critical infrastructure information system, program or data that performs a critical public function shall be punished with imprisonment of either description for a term which may extend to ten years or with fine which may extend to ten million rupees or with both.

(4) Whoever intentionally, whether temporarily or not,—

(a) does any unauthorised act in relation to an information system;

(b) at the time when he does the act he knows that it is unauthorised; and

(c) acts with intent—

(i) to seriously interfere, hinder, damage, prevent, suppress, deteriorate, impair or obstruct the functioning of an information system;

(ii) to seriously interfere, hinder, damage, prevent, suppress, deteriorate, impair or obstruct communication between or with an information system;

(iii) to seriously interfere with or hinder access to any information system;

(iv) to seriously impair the operation of any information system;

(v) to seriously impair the reliability of any information system;

(vi) to seriously impair the security of any information system; or

(vii) to enable any of the things mentioned in paragraphs (i) to (vi) to be done;

shall be punished with imprisonment of either description for a term which may extend to five years or with fine which may extend to seven hundred thousand rupees or with both.

(5) Whoever commits any offence under sub-section (1) by circumventing or infringing security measures with respect to any information system, program or data shall be punished with imprisonment of either description for a term which may extend to five years or with fine which may extend to seven hundred thousand rupees or with both.

(6) Whoever commits any offence under sub-section (1) with respect to any Government controlled critical infrastructure information system, program or data that performs a critical public function shall be punished with imprisonment of either description for a term which may extend to ten years or with fine which may extend to ten million rupees or with both.

(7) Whoever commits any offence under sub-section (1),-

(a) with respect to any Government controlled or public information system, program or data that performs a public function; and

(b) that causes serious damage, injury or disruption to a widely and publicly utilized network of information systems;

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

(8) However any person use or threat is designed to 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 in society or the use or threat is made for the purpose or motive of advancing a cause whether political, religious, sectarian or ethnic, with the intention of.

(i) interfering with, disrupting or damaging a public utility service or a communications system used by the public at large; or

(ii) seriously interfering with, seriously disrupting or seriously damaging a designated payment system which interconnects with multiple financial institutions;

(iii) seriously interfering with, seriously disrupting or seriously damaging a mass transportation or mass traffic system;

(iv) seriously interfering with, seriously disrupting or seriously damaging a critical infrastructure that is used to serve a public function for the public at large;

(v) seriously interfering with, seriously disrupting or seriously damaging critical infrastructure in use by the armed forces, civil armed forces, security forces or law enforcement agencies;

(vi) causes injury through the acts mentioned in paragraphs (a), (c), (d) and (e);

(vii) enabling any of the things mentioned in sub-paragraphs (i) to (vi) to be done;

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

(9) Whoever commits any offence under sub-section (1) of this section by circumventing or infringing security measures with respect to any information system, program or data shall be punished with imprisonment of either description for a term which may extend to fourteen years or with fine which may extend to fifty million rupees or with both.

(10) However The intention referred to in sub-section (1) need not relate to,—

(a) any particular information system;

(b) any particular program or data; or

(c) a program or data of any particular kind.

(d) In this section,—

(i) a reference to doing an act includes a reference to causing an act to be done;

(ii) “act” includes a series of acts;

(iii) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily;

(e) a reference to an act by a person includes acts done or to be done,-

(i) by or through an automated mechanism and self-executing, adaptive or autonomous device, program or information system;

(ii) against Government controlled information systems or public information systems in exercise of a public function; or

(iii) against any information system.

60. Sending offensive messages through communication services, etc.- (1) A person shall not knowingly or without lawful excuse or justification send by means of an electronic system or an electronic device-information that is grossly offensive or has a menacing character;

(a) information which he or she knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such electronic system or an electronic device; or

(b) electronic mail or an electronic message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages.

(2) For the purpose of this section, the term “electronic mail” or “electronic message” means a message or information created or transmitted or received on an electronic system or electronic device including attachments in text, images, audio, video and any other electronic record which may be transmitted with the message.

(3) A person who contravenes sub-section (1) commits an offence shall be punished with imprisonment of either description for a term which may extend to two years or with fine which may extend to one hundred thousand rupees or with both.

(4) Identity theft,-

(a) a person shall not knowingly or without lawful excuse or justification make fraudulent or dishonest use of an electronic signature, password or other unique identifying feature of another person.

(b) a person who contravenes sub-section (1) commits an offence shall be punished with imprisonment of either description for a term which may extend to five years or with fine which may extend to three hundred thousand rupees or with both.

61. Electronic forgery.- (1) A person shall not knowingly or without lawful excuse or justification, interfere with data or an electronic system so that he, she, or another person uses the data or the electronic system to induce a person to accept it as genuine and by reason of so accepting it to do or not to do any act to his or her own or any other person's prejudice or injury.

(2) A person who contravenes sub-section (1) commits an offence shall be punished with imprisonment of either description for a term which may extend to five years or with fine which may extend to five hundred thousand rupees or with both.

62. Electronic fraud.- (1) A person shall not knowingly or without lawful excuse or justification gain, interfere with data or an electronic system,–

(a) to induce another person to enter into a relationship;

(b) with intent to deceive another person; or

(c) with intent to defraud a person, where such an act is likely to cause damage or harm to that person or any other person.

(2) A person who contravenes sub-section (1) commits an offence shall be punished with imprisonment of either description for a term which may extend to five years or with fine which may extend to five hundred thousand rupees or with both.

63. Violation of privacy.- (1) A person who, knowingly or without lawful excuse or justification, captures, publishes or transmits the image of a private area of a person without his or her consent, under circumstances violating the privacy of that person, commits an offence shall be punished with imprisonment of either description for a term which may extend to five years or with fine which may extend to five hundred thousand rupees or with both.

(2) For the purposes of this section,–

(a) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) “capture” with respect to an image, means to videotape, photograph, film or record by any means;

(c) “private area” means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

(d) “publishes” means reproduction in the printed or electronic form and making it available for public;

(e) “under circumstances violating privacy” means circumstances in which a person can have a reasonable expectation that,–

(i) he or she could disrobe in privacy, without being concerned that an image or his or her private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

64. Child pornography.- (1) For the purposes of this section a “child” means a person who is under the age of eighteen years.

(2) A person shall not knowingly and without lawful justification or excuse,–

(a) publish or transmit or cause to be published or transmitted material in an electronic form which depicts a child engaged in sexually explicit act or conduct;

(b) create text or digital images, collect, seek, browse, download, advertise, promote, exchange or distribute material in an electronic form depicting a child in obscene or indecent or sexually explicit manner;

(c) cultivate, entice or induce children to an online relationship with another child or an adult for a sexually explicit act or in a manner that may offend a reasonable adult on the electronic system;

(d) facilitate the abuse of a child online;

(e) record or own in an electronic form material which depicts the abuse of a child engaged in a sexually explicit act;

(f) procure and/or obtain child pornography through a computer system; or

(g) obtain access through information and communication technologies, to child pornography.

(3) It is a defence to a charge of an offence under paragraphs (f) and (g) of sub-section (2) if the person can establish that the child pornography was for a bona fide law enforcement purpose.

(4) A person who contravenes sub-section (2) commits an offence shall be punished with imprisonment of either description for a term which may extend to twelve years or with fine which may extend to five hundred thousand rupees or with both and in the event of second or subsequent shall be punished with imprisonment of either description for a term which may extend to twenty five years or with fine which may extend to ten million rupees or with both..

(5) Sub-section (2) does not apply to a book, pamphlet, paper, drawing, painting, representation or figure or writing in an electronic form,–

(a) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or

(b) which is kept or used for *bona fide* heritage or religious purposes.

65. Sensitive electronic system (1) A person shall not knowingly or without lawful excuse or justification disable or obtain access to a sensitive electronic system whether or not in the course of the commission of another offence under this Act.

(2) A person who contravenes subsection (1) commits an offence shall be punished with imprisonment of either description for a term which may extend to twelve years or with fine which may extend to five hundred thousand rupees or with both.

(3) For the purposes of this section a “sensitive electronic system” is an electronic system used directly in connection with or necessary for,–

(a) the security, defence or international relations of Pakistan;

(b) the existence or identity of a confidential source of information relating to the enforcement of criminal law;

(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, courts, public transportation or public key infrastructure;

(d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services; or

(e) the purpose declared as such by the Minister by Order published in the *Gazette*.

CHAPTER V
Miscellaneous

66. Application of Electronic Transactions Ordinance, 2002.- (1) Without prejudice to the application of the Electronic Transactions Ordinance, 2002 or any of its provisions, including sub-section (2) of section 16 or paragraph (f) of sub-section (1) of section 2 to the Electronic Transactions Ordinance, 2002 and any other law, the Federal Government may prescribe rules for communication, filing, submission or processing of any pleadings, evidence or documents by any person, including but not limited by or before the Court or by the investigating officer, the prosecutor, complainant or accused, with respect to any application or exercise of any power or provision under this law through electronic means or in electronic form.

(2) When prescribing rules for the application under sub-section (1), the Federal Government shall have due regard to the availability, accessibility, security, authenticity and integrity of the electronic form or electronic means by which the enabling powers under sub-section (1) may be exercised by the Court, prosecutor, investigation agency or any other person.

Explanation:- The Federal Government may, where it is appropriate in terms of the availability, accessibility and security, prescribe rules for the communicating, filing, submissions and processing of applications, pleadings and evidence and other documents in electronic form before the Court or by the prosecution, the investigation agency, complainant, accused or any other person. The use of these means would include instances such as electronic applications for any warrants; the supply of statements and documents to the accused; supply of evidence recorded; applying for a copy of seized data and other provisions under this law. However, the Federal Government shall ensure that such rules shall provide for the security, integrity and authenticity at all times of such means of communication, filing, submission and processing and only enable these means at locations where appropriate under the circumstances.

67. Exclusion of telecommunication law related offences.- (1) Nothing in this Act shall apply to any offence with respect to telecommunication or matters related to laws, or any subsequent amendment thereof, specified under the Schedule and vice versa.

(2) No offence in any law specified in the Schedule shall be included in or form the basis of any investigation, prosecution or trial before any Court related to any offence under this Act.

(3) Offences under laws specified under the Schedule shall be excluded from any investigation, prosecution, trial or exercise of powers conferred by, or operation of, any provision of this Act.

(4) Any investigating officer who exercises any power or attempts to exercise any power conferred by this Act or include offences specified under the First Schedule in any investigation, prosecution, trial or exercise of powers conferred by, or operation of, any provision of this Act, shall be subject to disciplinary action and shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to two million rupees or with both.

(5) No offence under this Act shall be included in or form the basis of any investigation, prosecution or trial before any Court related to any offence under this Act or any other law mentioned in the Schedule.

68. Savings of Intelligence Services powers.- (1) Offences, powers and procedures provided under this Act are not related to and have no application upon the activities, powers or functions of intelligence agencies or services and are without prejudice to the operation of or powers exercised under-

(a) section 54 of the Pakistan Telecommunication (Re-organization) Act, 1996;

(b) the Army Act, 1952;

(c) the Air Force Act, 1953;

(d) the Navy Ordinance, 1961;

(e) the purview of the Intelligence Bureau;

(f) the investigation agency or intelligence service notified by the Federal Government under section 38 of this Act; and

(g) any other intelligence agency or service that does not itself undertake the investigation or prosecution of any criminal offence.

69. Act to override other laws.- The provisions of this Act shall have effect notwithstanding anything to the contrary contained in any other law and shall survive any amendment of any other law unless specifically amended or repealed.

70. Power to amend Schedule.- The Federal Government may, by notification in the official Gazette, amend the Schedule so as add any entry thereto but not omit any entry therein.

STATEMENT OF OBJECTS AND REASONS

Currently Pakistan has no complete laws to deal with the increasing threat of cybercrime. All prevailing laws of the land remained fail to address the refined online threats of the existing era. Telecommunication laws have no such provision to deal with traditional offline crime. Effectively addressing these unique and unprecedented crimes with similarly unique and necessary procedural powers requires a completely new and comprehensive legal framework that focuses on online conduct in the virtual world. It is requirement of the day to address new offences including illegal access of data, as well as interference with data and information systems, specialized cyber related electronic forgery and electronic fraud, cyber terrorism, unauthorized interception conducted by civilians, use of malicious code viruses, identity theft etc.

The legislation provides new investigative powers hitherto unavailable such as search and seizure of digital forensic evidence using technological means, production orders for electronic evidence, electronic evidence preservation orders, partial disclosure of traffic data, real time collection of data under certain circumstances and other enabling powers which are necessary to effectively investigate cyber crime cases.

This can only be achieved through strengthening existing protections and establishing new safeguards especially against abuse of these new and invasive powers. The Bill also includes specific safeguards to balance against these intrusive and extensive procedural powers in order to protect the privacy of citizens and avoid abuse of the exercise of these powers.

MR. KARIM AHMED KHAWAJA
Member-in-charge