Government's Proposed And Modified Cybercrime Bill 2015

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

(2) It extends to the whole of Pakistan.

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

(4) It shall come into force at once.

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

a. "access to information system" means gaining control or right to use to the whole or any part of an information system whether or not through infringing any security measure;

b. "access to data" means gaining control or right to read, use, copy, modify or delete any data held in or generated by any device or information system;

c. "Authority" means Pakistan Telecommunication Authority established under Pakistan Telecommunication (Re-organization) Act, 1996 (Act No.XVII of 1996);

d. "authorization" includes authorization by law or the person empowered to make such authorization;

e. "authorized officer" means an officer of the special investigation agency authorized to perform any function on behalf of the special investigation agency under this Act;

f. "Code" means the Code of Criminal Procedure, 1898 (Act No.V of 1898);

g. "content data" means any representation of facts, information or concepts in a form suitable for processing in an information system, including source code or a program suitable to cause an information system to perform a function;

h. "Court" means the Court of competent jurisdiction designated to try offences specified under this Act;

i. "critical infrastructure" includes the infrastructures so designated by any Government in Pakistan and such other assets, systems and networks, whether physical or virtual, so vital to the State or its organs including judicature that their incapacitation or destruction may have a debilitating effect on national security, economy, public health,safety or matters related thereto;

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

k. “damage to an information system” includes any change in the ordinary working of an information system impairing its performance, access, output or change in location whether temporary or permanent and with or without causing any change in the information system itself;

l. “data” includes content data and traffic data;

m. “data damage” includes altering, deleting, deterioration, erasing, suppressing, changing location of data or making data temporarily or permanently unavailable;

n. “de*vi*ce” includes any physical device or virtual device capable of being connected with any information system;

o. “electronic” includes electrical, digital, magnetic, optical, biometric, electrochemical, wireless or electromagnetic technology;

p. “identity information” means any information which may authenticate or identify an individual or an information system and enable access to any data or information system;

q. “information” includes text, message, data, voice, sound, database, video, signals, software, computer programs, codes including object code and source code;

r. “information system” means an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing information;

s. “intelligence” means any speech, sound, data, signal, writing, image or video;“investigating officer” means an officer of the special investigation agency designated for investigation of offences under this Act;

t. "offence" means an offence punishable under this Act;

u. “references” (i) to an “act” includes a series of acts;
(ii) to an act by a “person” shall include acts done or to be done by such person either directly or through an automated information system or device and whether having temporary or permanent impact;
(iii) a reference to doing an act includes a reference to causing an act to be done;
(iv) a reference to impairing, damage, interference, preventing or hindering something includes a reference to doing so temporarily;

v. "rules" means rules made under this Act;

w. "seize" with respect to information system or data includes taking possession of such information system or data or making and retaining a copy of such information system or data;

x. "service provider" includes-

i. a person acting as a service provider in relation to sending, receiving, storing, processing or distribution of electronic communication or the provision of other services in relation to electronic communication through any information system;

ii. a person who owns, possesses, operates, manages or controls a public switched network or provides telecommunication services;

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

iv. any person who provides premises from where or facilities through which the public in general may access information systems and the internet such as cyber cafes;

y. "special investigation agency" means the law enforcement agency established or designated under this Act;

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

aa. "traffic data" means any data relating to a communication indicating its origin, destination, route, time, size, duration or type of service;

bb. "unauthorized access" means access to an information system or data without authorisation or in violation of the terms and conditions of the authorization;

cc. "unauthorised interception" shall mean in relation to an information system or data, any interception without authorization;

(3) Other expressions used in the Act or rules framed under it but not defined herein, unless their context provides otherwise, shall have meanings assigned to the expressions in the Pakistan Penal Code 1860, Code of Criminal Procedure 1898 and 'Qanoon-e-Shahadat Order 1984, as the case may be.

CHAPTER I
OFFENCES AND PUNISHMENTS

3. Unauthorized access to information system or data.- (1) Whoever with malicious intent gains unauthorized access to any information system or data shall be punished with imprisonment for a term which may extend to six months or with fine which may extend to one hundred thousand rupees or with both.

4. Unauthorized copying or transmission of data.- Whoever with malicious intent and without authorization copies or otherwise transmits or causes to be transmitted,

any data whether by gaining access to such data or otherwise, shall be punished with imprisonment for a term which may extend to six months, or with fine which may extend to one hundred thousand rupess or with both.

5. Unauthorized access to critical infrastructure information system or data.- Whoever with malicious intent gains unauthorized access to any critical infrastructure information system or data shall be punished with imprisonment upto three years or with fine which may extend to one million rupees or with both.

6. Criminal Interference with information system or data.- Whoever with malicious intent and without authorization interferes with or damages or causes to be interfered with or damaged any information system or any part thereof, or data or any part thereof, shall be punished with imprisonment which may extend to two years or with fine which may extend to five hundred thousand rupees or with both.

Explanation: Interference refers to doing of any unauthorized act in relation to an information system or data that may disturb normal working of such information system with or without causing any actual damage to such information system.

7. Criminal Interference with critical infrastructure information system or data.- Whoever with malicious intent and without authorization interferes with or damages, or causes to be inferred with or damaged, any critical information system or any part thereof, or critical infrastructure data or any part thereof, shall be punished with imprisonment which may extend to seven years or with fine which may extend to five million rupees or with both.

8. **Cyber terrorism**. –Whoever commits or threatens to commit any of the offences under sections 5 and 7 where-

(a) the 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 create a sense of fear or insecurity in society; or

(b) the use or threat is made for the purpose or motive of advancing a religious, ethnic or sectarian cause;

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. **Electronic forgery**.- (1) Whoever, for wrongful gain, interferes with any information system, device or data, with intent to cause damage or injury to the public or to any person, or to make any illegal claim or title or to cause any person to part with property or to enter into any express or implied contract, or with intent to commit fraud by any input, alteration, deletion, or suppression of data, resulting in unauthentic data with the intent that it be considered or acted upon for legal purposes

as if it were authentic, regardless of the fact that the data is directly readable and intelligible or not shall be punished with imprisonment of either description for a term which may extend to two years, or with fine which may extend to two hundred and fifty thousand rupees or with both.

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

10. **Electronic fraud**.- Whoever for wrongful gain interferes with or uses any information system, device or data or induces any person to enter into a relationship or with intent to deceive any person, which act or omission is likely to cause damage or harm to that person or any other person shall be punished with imprisonment for a term which may extent to two years or with fine which may extend to ten million rupess, or with both.

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

12. **Identity crime**.- (1) Whoever obtains, sells, possesses or transmits another person's identity information, without lawful justification shall be punished with imprisonment for a term which may extend to three months or with fine which may extend to fifty thousand rupees, or with both.

(2) Any person whose identity information is obtained, sold, possessed or retains may apply to the Court competent to try offence under sub-section (1) for passing of such others as the Court may deem fit in the circumstances for securing, destruction or preventing transmission of any such data.

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

14. Tempering etc. of communication equipment.- Whoever changes, alters, tampers with or re-programs unique device identifier or international mobile station equipment identity (IMEI) number of any stolen cellular or wireless handset and unlawfully or without authorization starts using or marketing it for transmitting and receiving intelligence through such mobile or wireless handsets shall be punished with imprisonment which may extend to three years or with fine which may extend to 1 million rupees or both.

15. **Unauthorized interception**.- Whoever intentionally commits unauthorized interception by technical means of-

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

(b) electromagnetic emissions from an information system that are carrying data,

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

16**. Offence against dignity of natural person**- (1) Whoever, with malicious intent, knowingly and publicly exhibits, displays, transmits any electronic communication that harms the reputation of a natural person, threatens any sexual acts against a natural person; superimposes a photograph of the face of a natural person over any sexually explicit images; distorts the face of a natural person; or includes a photograph or a video of a natural person in sexually explicit conduct, without the express or implied consent of the person in question, intending that such electronic communication cause that person injury or threatens injury to his or her reputation, his or her existing state of privacy or puts him or her in fear for him or her safety shall be punished with imprisonment for a term which may extend to one year or with fine which may extend to one million rupees or with both.

(2) Whoever commits an offence under sub-section (1) with respect to a minor, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to ten million rupees or with both.

(3) Any aggrieved person or his guardian where such person is a minor, may apply to the court for passing of such orders for removal, destruction or blocking access to such material referred in sub-section (1) and the Court on receipt of such application may pass such orders as deemed proper in the circumstances.

17. Malicious code.- Whoever wilfully writes, offers, makes available, distributes or transmits malicious code through an information system or device, with intent to cause harm to any information system or data resulting in the corruption, destruction, alteration, suppression, theft or loss of information system or data shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to one million rupees or both:

Provided that the provision of this section shall not apply to the authorized testing, research and development or protection of any code for any lawful purpose:

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

18. Cyber stalking.- (1) Whoever with intent to coerce, intimidate, or harass any person uses information system, information system network, internet, website, electronic mail or any other similar means of communication to,-

(a) communicate obscene, vulgar, contemptuous, or indecent intelligence;

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

(c) threaten any illegal or immoral act;

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

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

commits the offence of cyber stalking.

(2) Whoever commits the offence specified in sub-section (1) shall be punishable with imprisonment for a term which may extend to two years or with fine which may extend to one million rupees, or with both:

Provided that if the victim of the cyber stalking under sub-section (1) is a minor the punishment may extend to three years or with fine may extend to ten million rupees, or with both.

(3) Any person may apply to the court for issuance of a restraining order against an accused of cyber stalking and the court upon receipt of such application may pass such order as deemed appropriate in the circumstances of the case.

19. Spamming.- (1) Whoever transmits harmful, fraudulent, misleading, illegal or unsolicited intelligence to any person without the express permission of the recipient, or causes any information system to show any such intelligence commits the offence of spamming.

(2) Whoever commits the offence of spamming as described in sub-section (1) shall be punished with fine not exceeding fifty thousand rupees if he commits this offence of spamming for the first time and for every subsequent commission of offence of spamming he shall be punished with imprisonment for a term which may extend to three months or with fine which may extend to one million rupees or with both.

20. Spoofing.- (1) Whoever dishonestly, establishes a website or sends any intelligence with a counterfeit source intended to be believed by the recipient or visitor of the website, to be an authentic source commits spoofing.

(2) Whoever commits spoofing shall be punished with imprisonment for a tem which may extend to three years, or with fine which may extend to five hundred thousand rupees or with both.

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

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

(3) References in any law creating an offence to an act shall include actions taken or caused by use of an information system.

(4) References to an act by a person in this Act or any law establishing an offence shall include acts done or to be done by or through automated mechanisms and self-executing, adaptive or autonomous devices, programs or information systems.

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

CHAPTER II
ESTABLISHMENT OF INVESTIGATION AND PROSECUTION AGENCY AND PROCEDURAL POWERS FOR INVESTIGATION

23. **Establishment of investigation agencies and prosecution**.-(1) The Federal Government shall designate the Federal Investigation Agency or any other law enforcement agency as the 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 Code to the extent that it is not inconsistent with any provision of this Act.

(3) The Government shall organize specialized courses in digital forensics, information technology, computer science and other related matters for training of the officers and staff of the special investigation agency.

24. **No warrant, arrest, search, seizure or other power not provided for in the Act**.- (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 under this Act:

Provided that the Federal Government or the Provincial Government may, as the case may be, constitute joint investigation team comprising of the officers of special investigation agency and any other law enforcement agency including Police for

investigation of events involving commission of offences under this Act and any other law for the time being in force.

(2) No person other than a prosecutor designated as such by the special investigating agency shall prosecute any offence under this Act.

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

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

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

the 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 ninety days as specified in the notice.

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

26. Retention of traffic data.---(1) A service provider shall, within its existing or required technical capability, retain its traffic data for a minimum period of ninety days or such period as the Authority may notify from time to time and provide that data to the special investigating agency or the investigating officer whenever so required.

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

(3) Any person who contravenes the provisions of this section shall be punished with imprisonment for a term which may extend to six months or with fine which may extend to or with both.

27. **Warrant for search or seizure**.-(1) Upon an application 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, data, device or other articles that-

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

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

the Court may issue a warrant which shall authorise an investigating officer, with such assistance as may be necessary, to enter the specified place and to search the premises and any information system, data, device or storage medium relevant to the offence identified in the application and access, seize or similarly secure any information system, data or other articles relevant to the offence identified in the application.

28. **Warrant for disclosure of traffic data**.-(1) Upon an application 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 an offence made out under this Act, the Court may, after recording reasons, order that a person in control of the information system or data to provide such data or access to such data to the investigating officer.

(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.

29. **Powers of an investigating officer**.-(1) Subject to provisions of this Act, an investigating officer shall have the powers to -
(a) have access to and inspect the operation of any specified information system;

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

(c) obtain and copy any 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 any information system to provide him reasonable technical and other assistance as the investigating officer may require for investigation of an offence under this Act; 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:

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

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

(a) at all times act with proportionality;

(b) take all precautions to maintain integrity of the information system 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 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 information system or data, the investigating officer shall make all efforts to use technical measures while maintaining its integrity and chain of custody and shall only seize any information system, data, device or articles, 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.

30. **Dealing with seized data.-**(1) The Federal Government may prescribe rules for dealing with the information system, data or other articles seized under this Act.

31. Power to issue directions for removal or blocking of access of any intelligence through any information system: (1) The Authority or any officer authorized by it in this behalf may direct any service provider, to remove any intelligence or block access to such intelligence , if it considers it necessary in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, friendly relations with foreign states, public order, decency or morality, or in relation to contempt of court, commission of or incitement to an offence.

(2) The Federal Government may prescribe rules for adoption of standards and procedure by the Authority to monitor and block access and entertain complaints under this section. Until such procedures and standards are prescribed, the Authority shall monitor and block intelligence in accordance with the directions issued by the Federal Government.

32. **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 and determined:

Provided further that such allegation and its proof shall clearly identify with specificity the content, material or other aspect with respect to which civil or criminal liability is claimed including but not limited to unique identifiers such as the Account Identification (Account 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 25, 27, 28 and 29.

(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.

33. Information in cognizable cases.- (1) Information relating to the commission of a cognizable offence under this Act if given orally to an officer of the special investigation agency authorized in this behalf, shall be reduced to writing by him or

under his direction and then read over to the informant and every such information, whether given in writing or reduced to writing as aforesaid, shall be signed by the person giving it, and the substance thereof shall be entered in a book to be kept by such officer in such form as the Federal Government may prescribe in this behalf.

34. Information in non-cognizable cases: (1) When information is given to an officer of special investigation agency authorized in this behalf of the commission of a non cognizable offence, he shall enter in a book to be kept as aforesaid the substance of such information and refer the information to the Court.

35. Investigation into cognizable cases: Any authorized officer of the special investigation agency may, without the order of the Court, investigate any cognizable case.

36. **Investigation into non-cognizable cases.-** No officer of the special investigation agency shall investigate a non cognizable case without the order of the Court.
(2) Any officer of the special investigation agency receiving such order may exercise, the, same powers in respect of the investigation (except the power to arrest without warrant) as an officer incharge of a police-station may exercise in a cognizable case.

37. **Real-time collection and recording of data**.-(1) Notwithstanding anything contained in Investigation for Fair Trials Act 2013 (Act No.I of 2013) or any other law for the time in force, if a Court is satisfied on the basis of information furnished by an investigating officer that there are reasonable grounds to believe that the content of any intelligence or data is reasonably required for the purposes of a specific criminal investigation, the Court may order, with respect to intelligence or data held by or passing through a service provider, to the service provider to collect or record such data in real-time in coordination with the special investigation agency:

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

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

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

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

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

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

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

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

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

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

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

CHAPTER III
INTERNATIONAL COOPERATION

38. **International cooperation**.-(1) The Federal Government may cooperate with any foreign Government, 24 x 7 network, any foreign agency or any international agency for the purposes of investigations or proceedings concerning offences related to information systems, electronic communication or data or for the collection of evidence in electronic form of an offence or obtaining expeditious preservation and disclosure of data by means of an information system or real-time collection of data associated with specified communications or interception of data under this Act.
(2) The Federal Government may, without prior request, forward to such foreign Government, 24 x 7 network, any foreign agency or any international agency, any information obtained from its own investigations if it considers that the disclosure of such information might assist the other Government or agency in initiating or carrying out investigations or proceedings concerning any offence.

(3) The Federal Government may require the foreign Government, 24 x 7 network, any foreign agency or any international agency to keep the information provided confidential or use it subject to some conditions.

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

(5) The Federal Government may refuse to accede to any request made by such foreign Government, 24 x 7 network, any foreign agency or any international agency if the request concerns an offence which is likely to prejudice its sovereignty, security, public order or other national interests.

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

CHAPTER – IV
PROSECUTION AND TRIAL OF OFFENCES

39. **Offences to be compoundable and non-cognizable**.- (1) All offences under this Act and abetment thereof, except offence under section 8, shall be non-cognizable, bailable and compoundable.

(2) Offence under section 8 and abetment thereof shall be cognizable, non-bailable and non-compoundable

40. **Cognizance and trial of offences**.— (1) The Federal Government, in consultation with the Chief Justice of respective High Court, shall designate Magistrates and Session Judges at such districts or places as deemed necessary who shall be competent to try the offences under this Act.
(2) Notwithstanding the provisions of provincial public service commission laws, the designated judges under sub-section (1) shall have 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.

(3) All offences under this Act, except offence under section 8 and abetment thereof, shall be cognizable and tried by the Magistrate designated under sub-section (1).

(3) Offence under section 8 and abetment thereof shall be tried by the Sessions Judge designated under sub-section (1).

(4) In all matters with respect to which no procedure has been provided in this Act, the provisions of the Code and Qanun-e-Shahadat . 1984 (X of 1984) shall apply.

41. **Order for payment of compensation**.- (1) The Court may, on awarding punishment of imprisonment or fine or both for commission of any offence, make an order for payment of any compensation to the victim for any damage caused by commission of the offence and the compensation so awarded shall be recoverable as arrears of land revenue:

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

(2) Notwithstanding anything contained in the Code of Criminal Procedure, 1898 (Act V of 1898), it shall be lawful for the Court to award any compensation authorized by this Act even if such compensation exceeds its powers under the Code.
42. **Appeal**.- (1) An appeal from any judgment of a Session judge passed in trial of any offence under this Act, shall lie to the respective High Court within thirty days from the date of the pronouncement of order and an appeal from any order of a Magistrate passed in trial of any offence under this Act shall lie to the respective Court of Session within thirty days from the date of pronouncement of order.

CHAPTER V
MISCELLANEOUS

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

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

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