AZAD GOVERNMENT OF THE STATE OF JAMMU AND KASHMIR
LAW, JUSTICE, PARLIAMENTARY AFFAIRS AND HUMAN RIGHTS
DEPARTMENT MUZAFFARABAD

Dated: 21st February, 2020
No. LD/Legis-Act/177-89/2020.The following Act, passed by the Azad Jammu and Kashmir Legislative Assembly on 31st January, 2020 and received the assent of the President on the 16th day of February, 2020, is hereby published for general information.
(ACT XIV OF 2020)

An

Act

further to amend the Azad Penal Code, 1860 and the Code of Criminal Procedure, 1898

WHEREAS, it is expedient further to amend the Azad Penal Code, 1860 (Act XLV of 1860) and the Code of Criminal Procedure, 1898 (Act V of 1898), for the purposes hereinafter appearing;

It is hereby enacted as follows:-

1. Short title and Commencement.- (1) This Act may be called the Criminal Law (2nd Amendment) Act, 2020.
(3) It shall come into force at once.

2. Addition of Chapter XXIV, Act XLV_of 1860.- In the Azad

Penal Code, 1860 (Act XLV of 1860), as adopted and enforced in Azad Jammu and Kashmir, after Chapter No. XVIII a new Chapter No. XVIII-A shall be added as under:-

“CHAPTER XVIII-A
OF OFFENCES REGARDING
ELECTRONIC TRANSACTION

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

(i) “act” includes-

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

(b) causing an act to be done by a person either directly or and through an automated information system or automated mechanism or self-executing, adaptive or autonomous device and

(ai)

(iii)

(iv)

(v)

(vi)

(vii)

(viii)

(ix)

(x)

whether having temporary or permanent impact;

“access to data” means gaining control or ability to use, copy, modify or delete any data held in or generated by any device or information system;

“access to information system” means gaining control or ability to use any part or whole of an information system whether or not through infringing any security measures;

“Authority” means an Authority established under the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996), as adapted and enforced in Azad Jammu and Kashmir;

“authorization” means authorization by law or by the person empowered to make such authorization under the law:

Provided that where an information system or data is available for open access by the general public, access to or transmission of such information system or data shall be deemed to be authorized for the purposes of this Act;

“authorized officer” means an officer of the investigation agency authorized to perform any function on behalf of the investigation agency by or under this Act;

“Code” means the Code of Criminal Procedure, 1898 (Act V of 1898), as adopted in AJ&K;

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

“Court” means the Court of competent jurisdiction designated under this Act;

“critical infrastructure” means critical elements of infrastructure namely assets, facilities, systems, networks or processes the loss or compromise of which could result in,-

(xi)

(xii)

(xiii)

(xiv)

(xv)

(a) major detrimental impact on the availability, integrity or delivery of essential services including those services, whose integrity, if compromised, could result in significant loss of life or casualties, taking into account significant economic or social impacts; or

(b) significant impact on security, defense, or the functioning of the state:

Provided that the Government may designate any private or Government infrastructure in accordance with the objectives of sub-paragraphs (a) and (b) above, as critical infrastructure as may be provided under this Act;

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

“damage to an information system” means any unauthorized change in the ordinary working of an information system that impairs its performance, access, output or change in location whether temporary or permanent and with or without causing any change in the system;

“data” includes content data and traffic data;

“data damage” means alteration, deletion, deterioration, erasure, relocation, suppression of data or making data temporarily or permanently unavailable;

“device’’ includes,-
(a) physical device or article;

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

(c) a password, access code or similar data

in electronic or other form, by which the whole or any part of an information system is capable of being accessed; or

(xvi)

(xvii)

(xviii)

(xix)

(xx)

(xxi)

(xxii)

(xxiii)

Volume XIV (2018-2020)

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

“dishonest intention’? means intention to cause injury, wrongful gain or wrongful loss or harm to any person or to create hatred or incitement to violence;

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

“Government” means the Azad Government of the State of Jammu and Kashmir;

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

“information” includes text, message, data, voice, sound, database, video, signals, software, computer programmes, any forms of intelligence as defined under the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996), as adopted and enforced in Azad Jammu and Kashmir and codes including object code and source code;

“information system” means an_ electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing any information;

“integrity” means, in relation to an electronic

document, electronic signature to advanced electronic signature, the electronic document, electronic signature or advanced electronic signature that has not been tampered with, altered or modified since a particular point in time;

“interference with information system or data” means and includes an unauthorized or in relation to an information system or data that may disturb its normal working or form with or

(xxiv)

(xxv)

(xxvi)

without causing any actual damage to such system or data;

“investigation agency” means,-
(a) the AJ&K police department;

(b) special law enforcement agency established under this Act;

“minor” means, notwithstanding anything contained in any other law, any person who has not completed the age of eighteen years;

“offence” means an offence punishable under this Act, except when committed by a person under ten years of age or by a person above ten years of age and under fourteen years of age, who has not attained sufficient maturity of understanding to judge the nature and consequences of his conduct on that occasion;

(xxvii) “rules” means rules made under this Act;

(xxviii) “seize” with respect to an information system or

(xxx)

(xxx1)

data includes taking possession of such system or data or making and retaining a copy of the data;

“service provider” includes a person who,-

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

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

(c) processes or stores data on behalf of such electronic communication service

or users of such service;

“subscriber information” means any information held in any form by a service provider relating to a subscriber other than traffic data;

489-H.

489-I.

489-J.

Volume XIV (2018-2020)

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

(xxxiil) “unauthorized access” means access to an information system or data which is or available for access by general public, without authorization or in violation of the terms and conditions of the authorization;

(xxxiv) “unauthorized interception” shall mean in relation to an information system or data, any interception without authorization; and

(xxxv) “unsolicited information’’ means an information which is sent for commercial and marketing purposes against explicit rejection of the recipient and does not include marketing authorized under the law.

(2) Unless the context provides otherwise, any other expression used in this Act but not defined in this Act, shall have the same meanings assigned to the expressions in the Azad Penal Code, 1860 (Act XLV of 1860), the Code of Criminal Procedure 1898 (Act V of 1898) and the Qanoon-e-Shahadat, 1984 (P.O-No. X of 1984), as adopted in AJ&K, as the case may be.

Unauthorized _ access to information system or data.- Whoever with dishonest intention gains unauthorized access to any information system or data 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.

Unauthorized copying or transmission of data.- Whoever with dishonest intention and without

authorization copies or otherwise transmits or causes to be transmitted any 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.

Interference with information system _or_data.- Whoever with dishonest intention interferes with or

damages or causes to be interfered with or damages any part or whole of an information system or data shall be punished with imprisonment which may extend to two

489-K.

489-L.

489-M.

489-N.

489-0.

years or with fine which may extend to five hundred thousand rupees or with both.

Unauthorized__access__to__critical__ infrastructure information system or data.- Whoever with dishonest intention gains unauthorized access to any critical infrastructure information system or data shall be punished with imprisonment which may extend to three years or with fine which may extend to one million rupees or with both.

Unauthorized copying or transmission of critical infrastructure data.- Whoever with dishonest intention and without authorization copies or otherwise transmits or causes to be transmitted any critical infrastructure 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.

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

Glorification of an offence and hate speech.- Whoever prepares or disseminates information, through any information system or device, with the intent to glorify an offence and the person accused or convicted of a crime relating to terrorism or activities of proscribed organizations shall be punished with imprisonment for a term which may extend to five years or with fine which may extend to ten million rupees or with both.

Explanation.-” glorification” includes depiction of any form of praise or celebration in a desirable manner.

Cyber_terrorism.—Whoever commits or threatens to commit any of the offences under Sections 6, 7, 8 or 9, where the commission or threat is with the intent to,-

(a) coerce, intimidate, create a sense of fear, panic

or insecurity in the Government or the public or a section of the public or community or sector create a sense of fear or insecurity in society; or

489-P.

489-Q.

489-R.

489-S.

Volume XIV (2018-2020)

(b) advance inter-faith, sectarian or ethnic hatred;

(c) advance the objectives of the organizations or individuals or groups proscribed under the laws, 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.

Hate Speech.- Whoever prepares or disseminate information, through any information system or device, that advances or is likely to advance inter faith, sectarian or racial hatred, shall be punished with imprisonment for a term which may extend to seven years or with fine or with both.

Recruitment, funding and planning of terrorism.- Whoever prepares or disseminate information, through

any information system or device, that invites or motivates to fund, or recruits people for terrorism or plan for terrorism shall be punished with imprisonment for a term which may extend to seven years or with fine or with both.

Electronic forgery.- (1) Whoever interferes with or uses any information system, device or data, with the 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 three 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 seven years or with fine which may extend to five million rupees or with both.

Electronic fraud.- Whoever with the intent for wrongful gain interferes with or uses any information system, device or data or induces any person to enter into a

489-T.

489-U.

489-V.

relationship or deceives any person, which act or omission is likely to cause damage or harm to that person or any other person shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to ten million rupees or with both.

Making, obtaining, or supplying device for_use_in offence.- Whoever produces, makes, generates, adapts,

exports, supplies, offers to supply or imports for use any information system, data or device, with the intent 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 six months or with fine which may extend to fifty thousand rupees or with both.

Unauthorized __use__of__ identity _ information.-

(1) Whoever obtains, sells, possesses, transmits or uses another person's identity information without authorization shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five million rupees, or with both.

(2) Any person whose identity information is obtained, sold, possessed, used or transmitted may apply to the Authority for securing, destroying, blocking access or preventing transmission of identity information referred to in sub-section (1) and the Authority on receipt of such application may take such measures as deemed appropriate for securing, destroying or preventing transmission of such identity information.

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

489-W. Tampering, etc. of communication equipment.-

489-X.

489-Y.

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

".

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

Unauthorized _interception.- Whoever with dishonest intention 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.

Offences against dignity of natural person.- (1) Whoever intentionally and publicly exhibits or displays

or transmits any information through any information system, which he knows to be false, and intimidates or harms the reputation or privacy of a natural person, shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both:

Provided that nothing under this sub-section shall apply to anything aired by a broadcast media or distribution service licensed under the Pakistan Electronic Media Regulatory Authority Ordinance, 2002 (XIII of 2002), as adopted and enforced in Azad Jammu & Kashmir.

(2) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such

information referred to in sub-section (1) and the Authority on receipt of such application, may pass such orders as deemed appropriate including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

Offences _against_modesty of a natural person and minor.- (1) Whoever intentionally and publicly exhibits or displays or transmits any information which, -

(a) superimposes a photograph of the face of a natural person over any sexually explicit image or video; or

(b) distorts the face of a natural person or includes a photograph or a video of a natural person in sexually explicit conduct; or

(c) intimidates a natural person with any sexual act or any sexually explicit image or video of a natural person; or

(d) cultivates, entices or induces a natural person to engage in a sexually explicit act, through an information system to harm a natural person or his reputation, or to take revenge, or to create hatred or to blackmail, shall be punished with imprisonment for a term which may extend to seven years or with fine which may extend to five 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 ten years and with fine which may extend to ten million rupees:

Provided that in case of a person who has been previously convicted of an offence under sub-section (1) with respect to a minor shall be punished with imprisonment for a term of fourteen years and with fine.

(3) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-sections (1) and (3) and the Authority, on receipt of such application, may pass such orders as deemed appropriate including an order for

removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

Child Pornography.- (1) Whoever _ intentionally produces, offers or makes available, distributes or transmits through an information system or procures for himself or for another person or without lawful jurisdiction possesses material in an information system, that visually depicts,-

(a) a minor engaged in sexually explicit conduct;

(b) a person appearing to be a minor engaged in sexually explicit conduct; or

(c) realistic images representing a minor engaged in sexually explicit conduct; or

(d) discloses the identity of the minor,

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

(2) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority, on receipt of such application shall forthwith pass such orders as deemed reasonable in the circumstances, including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

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

Explanation.-The expression “malicious code” includes, a computer program or a hidden function in a program that damages an information system or data or compromises the performance of such system or availability of data or uses it without proper authorization.

489-CC.Cyber_stalking.- (1) A person commits the offence of cyber stalking who, with the intent to coerce or intimidate or harass any person, uses information system, information system network, the Internet, website, electronic mail or any other similar means of communication to,-

(a) follow a person or contacts or attempts to contact such person to foster personal interaction repeatedly despite a clear indication of disinterest by such person;

(b) monitor the use by a person of the Internet, electronic mail, text message or any other form of electronic communication;

(c) watch or spy upon a person in a manner that results in fear of violence or serious alarm or distress, in the mind of such person; or

(d) take a photograph or make a video of any person and displays or distributes it without his consent in a manner that harms a person.

(2) Whoever commits the offence specified in sub-section (1) 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:

Provided that if victim of the cyber stalking under sub-section (1), is a minor the punishment may extend to five 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 Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority, on receipt of such application, may pass such orders as deemed appropriate including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority

489-DD.

489-EE.

489-FF.

Volume XIV (2018-2020)

may also direct any of its licensees to secure such information including traffic data.

Spamming.- (1) A person commits the offence of spamming, who with intent transmits harmful, fraudulent, misleading, illegal or unsolicited information to any person without permission of the recipient or who causes any information system to show any such information for wrongful gain.

(2) A person including an institution or an organization engaged in direct marketing shall provide the option to the recipient of direct marketing to unsubscribe from such marketing.

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

(4) Whoever commits the offence of spamming as described in sub-section (1) by transmitting unsolicited information, or engages in direct marketing in violation of sub-section (2), for the first time, shall be punished with fine not exceeding fifty thousand rupees, and for every subsequent violation shall be punished with fine not less than fifty thousand rupees that may extend up to one million rupees.

Spoofing.- (1) Whoever with dishonest intention establishes a website or sends any information 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 term which may extend to three years or with fine which may extend to five hundred thousand rupees or with both.

Legal recognition of offences committed in relation to information system.- (1) Notwithstanding anything

contained in any other law for the time being in force, an offence under this Act or any other law shall not be

denied legal recognition and enforcement for the sole reason of such offence being committed in relation to or through the use of an information system.

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

Addition of Chapter No. XLVII, Act V_ of 1898.- In the Code of Criminal Procedure, 1898 (Act V of 1898), as adopted and

enforced in Azad Jammu and Kashmir, after Chapter No. XLVI a new Chapter No. XLVII shall be added as under:-

176-A.

176-B.

“Chapter XIV-A
Procedure of Electronic Transaction
Crimes Investigation

Procedure for Investigation.- (1) Unless otherwise provided for under this Act, the Government shall

establish or designate an investigation agency for investigation of offences under this Chapter and the investigation agency and the authorized officer shall in all matters follow the procedure laid down in the Code to the extent that it is not inconsistent with any provision of this Act.

(2) The investigation agency may establish its own capacity for forensic analysis of the data or information system and the forensic analysis reports generated by the investigation agency shall not be inadmissible in evidence before any court for the sole reason that such reports were generated by the investigation agency.

(3) Notwithstanding provisions of any other law, the Government may make rules for specialized appointments and their promotion in the investigation agency including undertaking of specialized courses in digital forensics, information technology, computer science and other related matters for training of the officers and staff of the investigation agency.

Power to investigate.- Only an authorized officer of the investigation agency shall have the powers to investigate an offence under this Act:

Provided that the Government may, as the case may be, constitute one or more joint investigation teams comprising of an authorized officer of the investigation agency and any other law enforcement agency for

investigation of an offence under this Chapter and any other law for the time being in force.

176-C. Expedited preservation and acquisition of data.- (1) If

176-D.

an authorised 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 authorized officer may, by written notice given to the person in control of the information system, require that person to provide that data or 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:

Provided that the authorized officer shall immediately but not later than twenty-four hours bring to the notice of the Court, the fact of acquisition of such data and the Court on receipt of such information may pass such orders as deemed appropriate in the circumstances of the case including issuance of warrants for retention of such data or otherwise.

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

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 one year or such period as the Authority may notify from time to time and provide that data to the investigation agency or the authorized officer whenever so required.

(2) The service providers shall retain the traffic data under sub-section (1) by fulfilling all the requirement of data retention and its originality as provided under Sections 5 and 6 of the Electronic Transactions Ordinance, 2002 (LI of 2002) as adopted and enforced in Azad Jammu and Kashmir.

176-E.

(3) Any owner of the information system who is not licensee of the Authority and violates sub-section (1) shall guilty of an offence punishable, if committed for the first time, with fine which may extend to ten million rupees and upon any subsequent conviction shall be punishable with imprisonment which may extend to six months or with fine or with both:

Provided that where violation is committed by licensee of the authority, the same shall be deemed to be violation of the terms and conditions of the licensee and shall be treated as such under the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996) as adopted and enforced in AJ&K.

Warrant for search or _seizure.- (1) Upon an application by an authorized 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 authorize an officer of the investigation agency, 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, device or other articles relevant to the offence identified in the application.

(2) In circumstances involving an offence under Section 10, under which a warrant may be issued but cannot be obtained without the apprehension of destruction, alteration or loss of data, information system, data, device or other articles required for investigation, the authorized officer, who shall be a Gazetted Officer of the investigation agency, may enter the specified place and search the premises and any

information system, data, device or other articles relevant to the offence and access, seize or similarly secure any information system, data, device or other articles relevant to the offence:

Provided that the authorized officer shall immediately but not later than twenty-four hours bring to the notice of the Court, the fact of such search or seizure and the Court on receipt of such information may pass such orders as deemed appropriate in the circumstances of the case.

Warrant for disclosure of content data.-(1) Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that the content 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 the person in control of the data or information system, to provide such data or access to such data to the authorized 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.

Powers of an _authorized_officer.-(1) Subject to provisions of this Act, an authorized 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 system;

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

(d) have access to or demand any information in readable and comprehensible format or plain version;

(e) require any person by whom or on whose behalf, the authorized officer has reasonable cause to believe, any information system has been used to grant access to any data within an 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 authorized 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 data, device or information system in unencrypted or decrypted intelligible format 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 authorized officer at all times shall,-

(a) act with proportionality;

(b) take all precautions to maintain integrity and secrecy of the information system and data in respect of which a warrant for search or seizure 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 subjected to search or seizure under this Act; and

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

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

(4) Where an authorized officer seizes or secures any data or information system, the authorized officer shall ensure that data or information system while in the possession or in the access of the authorized officer is not released to any other person including competitors or public at large and details including log of any action performed on the information system or data is maintained in a manner prescribed under this Act.

Dealing with seized data or information system.- (1) If any data or information system has been seized or secured following a search or seizure under this Act, the authorized officer who undertook the search or seizure shall, at the time of the seizure,—

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

(b) give a copy of that list to-

(i) the occupier of the premises; or
(ii) the owner of the data or information system; or

(iii) the person from whose possession, the data or information system has been

seized, in a prescribed manner in the presence of two witnesses.

(2) The authorized officer, upon an application of the owner of the data or information system or an authorized agent of the owner and on payment of prescribed costs, shall provide forensic image of the data or information system to the owner or his authorized agent within a time prescribed under this Act.

(3) If the authorized officer has reasons to believe that providing forensic image of the data or information system to the owner under sub-section (2) may prejudice,-

(a) the investigation in connection with which the search was carried out; or

(b) another ongoing investigation; or

(c) any criminal proceedings that are pending or that

may be brought in relation to any of those investigations, the authorized officer shall, within seven days of receipt of the application under sub-section (2), approach the Court for seeking an order not to provide copy of the seized data or information system.

(4) The Court, upon receipt of an application from an authorized officer under sub-section (3), may after recording reasons in writing pass such order as deemed appropriate in the circumstances of the case.

(5) The costs associated with the exercise of rights under this Section shall be borne by the person exercising these rights.

Unlawful on-line content.-(1) The Authority shall have the power to remove or block or issue directions for removal or blocking of access to any information through any information system, if it considers it necessary in the interest of the glory of Islam or the integrity, security or defence of Azad Jammu and Kashmir or any part thereof, public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offence under this Act.

(2) The Authority may, with the approval of the Government, prescribe rules for adoption of standards and procedure for exercise of powers under sub-section

(1).

(3) Until such procedure and standards are prescribed under sub-section (2), the Authority shall exercise its powers under this Act or any other law for the time being in force in accordance with the directions issued by the Government not inconsistent with the provisions of this Act.

(4) Any person aggrieved from any order passed by the Authority under sub-section (1), may file an application with the Authority for review of the order within 30 days from the date of passing of the order.

(5) An appeal against the decision of the Authority in review shall lie before the High Court within thirty days of the order of the Authority in review.

Limitation of liability of service providers.- (1) No service provider shall be subject to any civil or criminal

liability, unless it is established that the service provider had specific actual knowledge and willful intent to proactively and positively participate, and not merely through omission or failure to act, and thereby facilitated, aided or abetted the use by any person of any information system, service, application, online platform or telecommunication system maintained, controlled or managed by the service provider in connection with a contravention of this Act or rules made thereunder or any other law for the time being in force:

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

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

(Account 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 service provider shall under any circumstance be liable under this Act, rules made thereunder or any other law for maintaining and making available the provision of their service in good faith.

(3) No service provider shall 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 service provider, for a period not exceeding fourteen days, shall keep confidential and not disclose the existence of any investigation or exercise of any power under this Act, when a notice to this effect is served upon it by an authorized officer, which period of confidentiality may be extended beyond fourteen days if, on an application by the authorized officer, the Court authorizes an extension for a further specified period upon being satisfied that reasonable cause for such extension exists.

(4) No 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 the provisions of this Act.

(5) No. 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.

Real-time collection and recording of information.-
(1) If a Court is satisfied on the basis of information

furnished by an authorized officer that there are reasonable grounds to believe that the content of any information is reasonably required for the purposes of a specific criminal investigation, the Court may order, with respect to information held by or passing through a service provider, to a designated agency as notified

under any law for the time being in force having capability to collect real time information, to collect or record such information in real-time in co-ordination with the investigation agency for provision in the prescribed manner:

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

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

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

(4) The Court may also require the designated agency to keep confidential the fact of the execution of any power provided for in this Section and any information relating to it.

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

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

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

(c) 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) specify what measures shall be taken to prepare and ensure that the real-time collection or

recording is carried out whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information of any person not part of the investigation;

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

(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.

Forensic laboratory.- The Government shall establish or designate a forensic laboratory, independent of the investigation agency, to provide expert opinion before the court or for the benefit of the investigation agency in relation to electronic evidence collected for purposes of investigation and prosecution of offences under this Act.

Confidentiality of information.- Notwithstanding immunity granted under any other law for the time being in force, any person including a service provider while providing services under the terms of a contract or otherwise in accordance with the law, or an authorized officer who has secured access to any material or data containing personal information about another person, discloses such material to any other person, except when required by law, without the consent of the person concerned or in breach of lawful contract with the intent to cause or knowing that he is likely to cause harm, wrongful loss or gain to any person or compromise confidentiality of such material or data, shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both:

Provided that the burden of proof of any defence taken by an accused service provider or an authorized officer that he was acting in good faith, shall be on such a service provider or the authorize officer, as the case may be.

176-N.

176-0.

176-P.

176-Q.

Volume XIV (2018-2020)

Offences to be compoundable and non-cognizable.-
(1) All offences under Chapter No. XVII-A of Azad

Penal Code, 1860 except the offences under Sections 489-O and 489-X and abetment thereof, shall be non-cognizable, bailable and compoundable:

Provided that offences under section 15 shall be cognizable by the investigation agency on a written complaint by the Authority.

(2) Offences under Sections 10 and 19 and abetment thereof shall be non-bailable, non-compoundable and cognizable by the investigation agency.

Cognizance_and_ trial of offences- (1) The Government, in consultation with the Chief Justice of

the High Court, shall designate presiding officers of the Courts to try offences under this Act at such places as deemed necessary.

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

(3) To the extent not inconsistent with this Act, the procedure laid down under the Code and the Qanoon-e-Shahadat Order, 1984 (P.O.No.X of 1984), as adopted and enforced in AJ&K shall be followed.

Order_for_payment_of compensation.- The Court may, in addition to award of any punishment including

fine under this Act, make an order for payment of compensation to the victim for any damage or loss caused and the compensation so awarded shall be recoverable as arrears of land revenue:

Provided that the compensation awarded by the Court shall not prejudice any right to a civil remedy for

the recovery of damages beyond the amount of compensation so awarded.

Appointment of amicus curiae and seeking expert opinion.- The Court may appoint amicus curiae or seek

176-R.

176-S.

independent expert opinion on any matter connected with a case pending before it.

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

(a) to the High Court against such judgment or order if passed by a court of sessions; or

(b) to the court of sessions concerned against such judgment or order if passed by a magistrate.

Criminal information exchange.- The Government may enter in to an agreement with Federal Investigating Agency (FIA), PTA or any other organization of Pakistan, for such technical support or for exchange of information as it may deem necessary for purposes of this chapter."

Amendment of Schedule II, Act V of 1898.- In the said Code, in the Schedule II,-

@

after Section 489-F, in column I, and the entries relating thereto in columns (2) to (8), the following shall be inserted, namely:-

eyep
yjog UIA JO soodns vor JO Wa}sks UOT}eULIOJUL
OUO 0} pud}xXo APU YSIYM sUTy oINjON.A|SBAUL
YIM JO srvoX 9014} 0} pud}xo yeonto 0}
ong | Aeuwr = yorym = uswuostidut ond ond ond oniq | sssooe = pezioyyneur) Y-68h
tog WM
Jo soodni puesnoyy pospuny
SAY. 0} pusyxo APU YOTyM ou eyep
YIM JO sieok OM) 0} pud}xo Jo wo\sks uonPULoyur
oniq | Aewr =yorym = uowuostidut ond onid ond ond | qm QOUdIOJIO}U] [-68P
YIOq YIM Jo soodni puesnoyy
pospuny suo 0} puoyxo Avur
yor OU, YIM JO syuOUL
xIS 0} puoyxo Aru YoryM Rep JO UOTssTUISURT] 10
ond | wWia) e Joy = yuowuostiduy ond ontd ond ontg | 3utkdoo pozioyyneur 1-684
YIOq YIM Jo soodni
puesnoyy Ay 0} puoyxo Avur yueliem
Yom Suyy YMA JO syyuoUr qnoyyIM vep 10
SUOISSOS | 991} 0} pUoyxo AevuT yoryM | o[qepunodutos ysoiie | woysXs uoTeULIOJUT 0}
jo ynop | ua, e Joy yuouTUOsTiduT JON | o]QeITeg | jUeLIE AA | JOU TTeYS | ssoooR — pozloyneUgQ H-68r
8 L 9 Sg v € (4 I,

(0Z0Z-810Z) AIX SuN]OA

£97

yuelem
YIOg YIM JO oULy YITA JO sIvOk ynoyyIAL
udAas 0} puayxa Ae YoIyM | s]qepunodwos ysoure
ond | wis, e Joy juoWwuOstdut JON | 9[QRIFeg | UREA, | JOU [[eYS yooods ae] d-68¢
y0q
YIM Jo soodns vol AY 0}
pus}xe ABUL YIM SUT YIM JO queue
s1eok ud9}INOJ 0} pus}xo AvUI jnoyyIM
YoIyM UIs} B Joy uoNdiosep grqeiieg qso.e
oniq | sya = Jo quowuostidut oniq -UON oniq Ae WISLIOLI9} 1aqhd) O-68r
Grog WM
Jo soodni UOT] U9} 0} pusyxo
ABU YOTYM OUTF YIM JO sIeVak yooods
SAY 0} pusyxo Aew yoy yey = puke = s0uaJo
ond | wie} eB Joy ywawuostdut ond ond ond onig | ue jo uoneoyL0[H N-68¢
YIOg TIM Jo soodns vor eyep
U9} 0} pusyxo AvuI YOM ou Jo waysXs uoneUlioyur
WIM JO s1eok UdAds 0} pud}xo oMjonseUL [OILIO
ong | Aeur yor = uowuostidut onid onid onid ond | yi QOUdIOJIOU] W-68r
YIog YA JO
soodni UOl|[MW SAY 0} pus}xo eyep
Aeur YOTYM UTF YIM JO ‘sIvok omMjonsesUT [eoIyLIO
OA 0} puoyxo Aer YoryM jo wuolssmusueyn Jo
oniq | wis, e Joy} jUoWUOSTIdwT oniqd onid oniq oniq | suikdoo poziioyjneug T-68r

(0Z0Z-810Z) AIX SuN]OA

v9T

Yj0q YBIM Jo soodni
puesnoyy Ay 0} puayxe Avur
YoryM oul YIM JO syjuoUT gouajjo ul osn
XIS 0} puo}xo APU YOIyM JoJ so1a0p surc<jddns
oig | wis, e sof JUoWUOSTIdUTT onid onid oniqd onig | Jo ‘Sururejgo ‘Suryeyy 1-687
tog WM
Jo soadni UoT][IW U9} 0} pus}xo
Ae YOIYM OUT} YIM JO suvak
OM} 0} puayxa Aeu YoIyM
oniqd | wo} e@ Joy = yuoWUOsTIduT ond ond ond onid pney oruono9]q S-68h
YOq YIM JO eyep
soodni uo] svt 0} pusyxo Jo wio\sks uoneUtIoyUr
ACU YOIYM UTE YIM JO sieVak OIMJONISVAFUT TBOTILIO B
UdADS 0} puo}xo AUT Yor 0} UONRIAI Ul DOUAJJO(IL
WLIO} & JO} yUOWUOSIIdUT = (I uosiod Aur 0} 10 o1jqnd
“YIOg YIM JO soodny oy} 0} Amnfur Jo o8eurep
puesnoy) Ayy pue pospuny omy OSNLd 0} JUOJUT OY) YIM
0} puoyxo APU OIA OUT YLAA “‘aep JO SolAop ‘Wio}sAs
Jo ‘sieoA 9074) 0} pusyxo AvUT uoneuoyur Aue sosn
YOM wo} B Jo} uoNdiosop JO YIM sosojioyur (I
opig | soya =jo jyuowuosudun (1 ond ond oniqd ond AJOB1O} OUONDI]|A W-68r
YO YIM JO OUTy YIM JO sIROA UISTIOLIO}
UdAdS 0} pudyxo Av YOIyM jo suruurjd = pue
omid | was} e Joy yuaWUOsTIduT ond onid ond ong | Suipuny = uowyiMnsd0y 0-687

(0Z0Z-810Z) AIX SuN]OA

S9T

t0q YIM JO
ssodni voli suo 0} pus}xs queLem
AW YSTYA UTZ YIM JO sIvoXk qnoyyA uossod
Soly} 0} pusjxo Aru YyoIyM | o[qepunodwos sore | enyeu jo = Ayrusip
wis} e Joy yuoWUOstIduT JON | 9]QRTIeqG | JURLIEA | JOU T]eYS | IsUTese sooudyyO K-68r
GI0q YHA JO
soodni puersnoy} pospuny sayy
0} puayxe ABU YOST OUT YIM queLEM
Jo sivak OM} 0} puajxa APU qnoyyLA
YOM Wa} e Joy uoNdrosap grqeyreg ysoure uondaosoqur
oid | ya = jo. uawuostidut ond -UON ond Ke poziioyneuy, X-68P
YIOg YIM Jo soodns oT]
OUO 0} pud}Xo ABU YIU oUTy yuoudinbo
YIM Jo sieok do1y} 0} pus}xo uoreorunuTU0S
omg | Aew = yorym = yuowuostidut ond ond ontqd oniq | Jo ‘99 «= ‘Buroduey, M-687
t0q YIM Jo saadni puesnoy}
pospuny oA 0} puayxo
ABUL YOTYM OUTF YIM JO sIvok
oor} 0} pusyxo Aeul yoryM "9}9 Spd ITS JO
ond | wi9) e Joy ywowuostiduT ond ond ond oniq | 99uensst poziioyyneuy) A-68P
tg IA JO
‘soodns UOT] SAT 0} pusyxo
ACU YOTYM OUT} YIM JO sIRok
soy} 0} pusyxo Aeur yoryM uoneusoyur AyUSpT
omid | was} e@ Joy yuaWUOsTIduT ond ond ond onid | JO 9sn poziioyyneuy) N-68r

(0Z0Z-810Z) AIX SuN]OA

997

ontd

GIOg IIA JO
soodni UOTT[IW SUO 0} pus}xo
AewW YOIYM OUI} YIM JO sueadk
OM} 0} puajyxa Aew YoTyM
wis} e JO} juoWwUOsTIduT

ond

ontd

onia

ontd

apoo snororeyy

ad-68h

ond

“YIOg YA JO
soodni uol[iur sat 0} pus}xo
ABUL YOIYM OUT, YIM Jo ‘svak
udAds 0} puayxa Aew YoIyM
uo} «8 JoJ uowUOstIdu

ond

ond

onia

ond

Aydeisoulog pry

VV-687

ond

“OUT YY
pue sivok usojmoy Jo Wo} &
Joy yuouUOsTIdw Jour YIM
souaYjo juonbesqns Joy (I

“soodni UOl]]I U9} 0} pusyxo
Aeut yor oul YM pue
sIevoX Ud} 0} puayxo Av YoTyM
Wo} e Joy jUowUOstdut
([) worses-qns Jopun soul
ST OOUDJJO JO WIA e JIC

“TIO YA JO
soodni uol[M dA 0} puoyxo
ACU YOTYM OUT} YIM JO sek
UdAVS 0} puo}xo AUT Yor
Wo} eB JO; yuoWUOSTIdUIT (1

ontd

onia

onl

oni

Jour pue uossod

yemjeu
ysulese

e@ jo A\sopour
soouayJO

Z-68v

(0Z0Z-810Z) AIX SuN]OA

L97

ond

puesnoyy Ayy surposoxo
jou oul YIM — poystund
9q [TeYs ‘our sy oy Joy (HH

Syj0q YIM JO soodns UOT]
ouo 0} puayxo Aew yYoryM
ouTy YIM JO syUOU aeI4} 0}
puojxo Aeur YOTYM Ws} & JOy
quowuosiidwi yim poystund
9q [[eYys uoNR[oIA yuonbasqns
AAD «JOY. puke ~— soon
puesnoy} Ayy sulposoxa
jou oul; YIM — poystund
oq [Teys ‘oun SIF OY} JO} (1)

ond onld

onid

ontld

*(Z) wordas-qns Jo
UONRIOIA Ul SurjoyreU

yop ul sosesuo
Jo ‘UOT}eULIOFUT
poworosun
Suyywusueyy

Aq (69) uoldes
-qns Ul = pequiosap

se Surmueds (U
({) worses-qns
Jopun Surumuedg (1

dd-68r

ond

“OQ
ya Jo soodni uolypmu us}
0} pus}xo APU YOIYM oUly ILM
Jo sievok dAlf 0} pus}xo AeuUl
yuourystund oy} Jou e& st
(1) woxsss-qns Japun Suryyeys
Jogho ayy JO WHOIA JT (11)

4i0q
YA Jo soodni uorypiu suo 0}
puoyxo AvUr YOM SULT JIM JO

Jeok ouo 0} pus}xo Aeur YOTyA
W9} B JOJ JUSWUOSIIdU (1)

ontd ontd

ond

onid

Suryers Jaqk—

00-687

(0Z0Z-810Z) AIX SuN]OA

(WOIJeISIBIT) I9d1JJO WoId9g
(aeyy poumpy zeginD)

“/PS

897

«Od

YI0g YIM Jo soodni puesnoyy
pompuny oA 0} pudyxo
ABUL YOIYM OUTE YIM JO svok
sory] 0} puayxo Aru yoryM
wo} eB Joy jyuatuUOstIdwt

ontd onld

onid

ontd

sulyoods

dd-687

soodni
UOT] oUO 0} dn puayxo AvuI
yey} soodns puesnoy} Ay uey}
sso] jou ouly WIM poystund
oq [[eys UoNeoIA Juonbosqns
AIOAD «OJ pues ‘saodni

(0Z0Z-810Z) AIX SuN]OA