

The Information Technology ACT, 2008

Section 66F - Punishment for cyber terrorism

(1) Whoever,-

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or

(iii) introducing or causing to introduce any Computer Contaminant.

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly

25

relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

67 Punishment for publishing or transmitting obscene material in electronic form
(Amended vide ITAA 2008)

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to two three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

67 A Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form (Inserted vide ITAA 2008)

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Exception: This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

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

(ii) which is kept or used bona fide for religious purposes.

67 B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.

Whoever,-

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or

(d) facilitates abusing children online or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

26

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or

figure is in the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bonafide heritage or religious purposes

Explanation: For the purposes of this section, "children" means a person who has not completed the age of 18 years.

67 C Preservation and Retention of information by intermediaries

(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

68 Power of Controller to give directions (Amended Vide ITAA 2008)

(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.

(2) Any person who intentionally or knowingly (Inserted vide ITAA 2008) fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or to both.

69 Powers to issue directions for interception or monitoring or decryption of any information through any computer resource (Substituted Vide ITAA 2008)

(1) Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.

(2) The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed

(3) The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub section (1), extend all facilities and technical assistance to -

(a) provide access to or secure access to the computer resource containing such information; generating, transmitting, receiving or storing such information; or

(b) intercept or monitor or decrypt the information, as the case may be; or

(c) provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

69 A Power to issue directions for blocking for public access of any information through any computer resource

(1) Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.

(3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

69B Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security

(1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating , transmitting, receiving or storing such traffic data or information.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Explanation: For the purposes of this section,

(i) "Computer Contaminant" shall have the meaning assigned to it in section 43

(ii) "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

70 Protected system (Amended Vide ITAA-2008)

(1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

28

Explanation: For the purposes of this section, "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety. (Substituted vide ITAA-2008)

(2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1)

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

(4) The Central Government shall prescribe the information security practices and procedures for such protected system. (Inserted vide ITAA 2008)

70 A National nodal agency. (Inserted vide ITAA 2008)

(1) The Central Government may, by notification published in the official Gazette, designate any organization of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.

(2) The national nodal agency designated under sub-section (1) shall be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.

(3) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

70 B Indian Computer Emergency Response Team to serve as national agency for incident response

(1) The Central Government shall, by notification in the Official Gazette, appoint an agency of the government to be called the Indian Computer Emergency Response Team.

(2) The Central Government shall provide the agency referred to in sub-section (1) with a Director General and such other officers and employees as may be prescribed.

(3) The salary and allowances and terms and conditions of the Director General and other officers and employees shall be such as may be prescribed.

(4) The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of Cyber Security,-

- (a) collection, analysis and dissemination of information on cyber incidents
- (b) forecast and alerts of cyber security incidents
- (c) emergency measures for handling cyber security incidents
- (d) Coordination of cyber incidents response activities

(e) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents

(f) such other functions relating to cyber security as may be prescribed

(5) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

(6) For carrying out the provisions of sub-section (4), the agency referred to in sub-section (1) may call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person

(7) Any service provider, intermediaries, data centers, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (6) , shall be

29
punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.

(8) No Court shall take cognizance of any offence under this section, except on a complaint made by an officer authorized in this behalf by the agency referred to in sub-section (1)

71 Penalty for misrepresentation

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

72 Breach of confidentiality and privacy

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

72 A Punishment for Disclosure of information in breach of lawful contract (Inserted vide ITAA-2008)

Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

73 Penalty for publishing electronic Signature Certificate false in certain particulars

(1) No person shall publish a Electronic Signature Certificate or otherwise make it available to any

other person with the knowledge that

- (a) the Certifying Authority listed in the certificate has not issued it; or
- (b) the subscriber listed in the certificate has not accepted it; or
- (c) the certificate has been revoked or suspended,

unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

74 Publication for fraudulent purpose

Whoever knowingly creates, publishes or otherwise makes available a Electronic Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both

75 Act to apply for offence or contraventions committed outside India

(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

30

(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

76 Confiscation

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation:

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit.

77 Compensation, penalties or confiscation not to interfere with other punishment. (Substituted Vide ITAA-2008)

No compensation awarded, penalty imposed or confiscation made under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force.

77 A Compounding of Offences

(1) A Court of competent jurisdiction may compound offences other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under this Act.

Provided that the Court shall not compound such offence where the accused is by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind.

Provided further that the Court shall not compound any offence where such offence affects the socio-economic conditions of the country or has been committed against a child below the age of 18 years or a woman.

(2) The person accused of an offence under this act may file an application for compounding in the court in which offence is pending for trial and the provisions of section 265 B and 265 C of Code of Criminal Procedures, 1973 shall apply.

77 B Offences with three years imprisonment to be cognizable

(1) Notwithstanding anything contained in Criminal Procedure Code 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

78 Power to investigate offences (Amended Vide ITAA 2008)

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector shall investigate any offence under this Act. (Amended Vide ITAA 2008)

XII. Intermediaries Not To Be Liable In Certain cases (Substituted Vide ITA-2006)

79 Exemption from liability of intermediary in certain cases

31

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link hosted by him. (corrected vide ITAA 2008)

(2) The provisions of sub-section (1) shall apply if-

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or

(b) the intermediary does not-

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf (Inserted Vide ITAA 2008)

(3) The provisions of sub-section (1) shall not apply if-

(a) the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act (ITAA 2008)

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation:- For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

XII A . Examiner of Electronic Evidence (Inserted Vide ITA-2006)

79A Central Government to notify Examiner of Electronic Evidence

The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the official Gazette, any department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

Explanation:- For the purpose of this section, "Electronic Form Evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines".

XIII. MISCELLANEOUS

80 Power of Police Officer and Other Officers to Enter, Search, etc

(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Inspector or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act

Explanation-

32

For the purposes of this sub-section, the expression "Public Place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

(2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

(3) The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section

81 Act to have Overriding effect

The provisions of this Act shall have effect notwithstanding anything inconsistent therewith

contained in any other law for the time being in force.

Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act 1957 or the Patents Act 1970 (Inserted Vide ITAA 2008)

81-A Application of the Act to Electronic cheque and Truncated cheque-* (Inserted vide Negotiable Instruments Amendment Act 2002, -Effective from 6th Day of February 2003.)

(1) The provisions of this Act, for the time being in force, shall apply to, or in relation to, electronic cheques and the truncated cheques subject to such modifications and amendments as may be necessary for carrying out the purposes of the Negotiable Instruments Act, 1881 (26 of 1881) by the Central Government, in consultation with the Reserve Bank of India, by notification in the Official Gazette.

(2) Every notification made by the Central Government under subsection (1) shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both houses agree in making any modification in the notification or both houses agree that the notification should not be made, the notification shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under the notification.

Explanation: For the purpose of this Act, the expression "electronic cheque" and "truncated cheque" shall have the same meaning as assigned to them in section 6 of the Negotiable Instruments Act 1881 (26 of 1881).

82 Chairperson, Members, Officers and Employees to be Public Servants (Amended Vide ITA-2008)

The Chairperson, Members and other officers and employees of a Cyber Appellate Tribunal, the Controller, the Deputy Controller and the Assistant Controllers shall be deemed to be Public Servants within the meaning of section 21 of the Indian Penal Code.

83 Power to Give Direction

The Central Government may give directions to any State Government as to the carrying into execution in the State of any of the provisions of this Act or of any rule, regulation or order made there under.

84 Protection of Action taken in Good Faith

No suit, prosecution or other legal proceeding shall lie against the Central Government, the State Government, the Controller or any person acting on behalf of him, the Chairperson, Members, Adjudicating Officers and the staff of the Cyber Appellate Tribunal for anything which is in good faith

33
done or intended to be done in pursuance of this Act or any rule, regulation or order made there under.

84 A Modes or methods for encryption (Inserted Vide ITA-2008)

The Central Government may, for secure use of the electronic medium and for promotion of e-

governance and e-commerce, prescribe the modes or methods for encryption

84 B Punishment for abetment of offences (Inserted Vide ITA-2008)

Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.

Explanation: An Act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.

84 C Punishment for attempt to commit offences (Inserted Vide ITA-2008)

Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both.

85 Offences by Companies.

(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a Company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Explanation-

For the purposes of this section

- (i) "Company" means any Body Corporate and includes a Firm or other Association of individuals; and
- (ii) "Director", in relation to a firm, means a partner in the firm

86 Removal of Difficulties

(1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as appear to it to be necessary or expedient for removing the difficulty:

Provided that no order shall be made under this section after the expiry of a period of two years from the commencement of this Act. (2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

34

87 Power of Central Government to make rules

(1) The Central Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely

(a) the conditions for considering reliability of electronic signature or electronic authentication technique under sub-section (2) of section 3A (Substituted vide ITA-2008)

(aa) the procedure for ascertaining electronic signature or authentication under sub-section (3) of section 3A (Inserted Vide ITA-2006) (Inserted vide ITAA-2008)

(ab) the manner in which any information or matter may be authenticated by means of electronic signature under section 5. (Inserted vide ITAA-2008)

(b) the electronic form in which filing, issue, grant or payment shall be effected under sub-section (1) of section 6;

(c) the manner and format in which electronic records shall be filed or issued and the method of payment under sub-section (2) of section 6;

(ca) the manner in which the authorized service provider may collect, retain and appropriate service charges under sub-section (2) of section 6A (Inserted vide ITAA-2008)

(d) the matters relating to the type of Electronic Signature, manner and format in which it may be affixed under section 10;

(e) the manner of storing and affixing electronic signature creation data under section 15 (substituted vide ITAA-2008)

(ea) the security procedures and practices under section 16 (Inserted vide ITAA-2008)

(f) the qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers, other officers and employees under section 17; (ITAA 2008)

(g) (omitted vide ITAA-2008)

(h) the requirements which an applicant must fulfill under sub-section (2) of section 21;

(i) the period of validity of license granted under clause (a) of sub-section (3) of section 21;

(j) the form in which an application for license may be made under subsection (1) of section 22;

(k) the amount of fees payable under clause (c) of sub-section (2) of section 22;

(l) such other documents which shall accompany an application for license under clause (d) of sub-section (2) of section 22;

(m) the form and the fee for renewal of a license and the fee payable thereof under section 23;

(ma) the form of application and fee for issue of Electronic Signature Certificate under section 35.(Inserted vide ITAA-2008)

(n) the amount of late fee payable under the proviso to section 23;

(o) the form in which application for issue of a Electronic Signature Certificate may be made under sub-section (1) of section 35;

(oa) the duties of subscribers under section 40A (Inserted vide ITAA-2008)

35

(ob) the reasonable security practices and procedures and sensitive personal data or information under section 43A (Inserted vide ITAA-2008)

(p) the fee to be paid to the Certifying Authority for issue of a Digital Signature Certificate under sub-section (2) of section 35;

(q) the manner in which the adjudicating officer shall hold inquiry under sub-section (1) of section 46;

(r) the qualification and experience which the adjudicating officer shall possess under sub-section (2) of section 46; (Ed: error in the act item number (vii). Bill mentions correction not in the original section-"Presiding Officer" to be replaced with "Chairman and Members")

(s) the salary, allowances and the other terms and conditions of service of the Chairman and Members under section 52; (amended vide ITAA-2008)

(t) the procedure for investigation of misbehaviour or incapacity of the Presiding Officer Chairman and Members under sub-section (3) of section 54; (Ed: Error: bill mentions corrections to (r) and (s) instead of (s) and (t)

(u) the salary and allowances and other conditions, of service of other officers and employees under sub-section (3) of section 56;

(v) the form in which appeal may be filed and the fee thereof under subsection (3) of section 57;

(w) the powers and functions of the Chairperson of the Cyber Appellate Tribunal under section 52 A (substituted vide ITAA-2008)

(wa) the information, duration, manner and form of such information to be retained and preserved under section 67 C (ITAA 2008)

(x) The Procedures and safeguards for interception, monitoring or decryption under sub-section (2) of section 69 (ITAA 2008)

(xa) the procedure and safeguards for blocking for access by the public under sub-section

(2) of section 69 A. (ITAA 2008)

(xb) the procedure and safeguards for monitoring and collecting traffic data or information under sub-section (3) of section 69 B (ITAA 2008)

(y) the information security practices and procedures for protected system under section 70 (Inserted vide ITAA-2008)

(ya) manner of performing functions and duties of the agency under sub-section (3) of section 70 A (ITAA 2008)

(yb) the officers and employees under sub-section (2) of section 70 (B) (ITAA 2008)

(yc) salaries and allowances and terms and conditions of service of the Director General and other officers and employees under sub-section (3) of section 70 B (ITAA 2008)

(yd) the manner in which the functions and duties of agency shall be performed under sub-section (5) of section 70 B (ITAA 2008)

(z) the guidelines to be observed by the intermediaries under sub section (4) (2) of section 79 (Inserted vide ITAA-2008)

(za) the modes or methods for encryption under section 84A (Inserted vide ITAA-2008)

(3) Every notification made by the Central Government under sub-section (1) of section 70 (A) and every rule made by it shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any

36

modification in the regulation or both Houses agree that the regulation should not be made, the regulation shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that regulation. (ITAA 2008)

88 Constitution of Advisory Committee

(1) The Central Government shall, as soon as may be after the commencement of this Act, constitute a Committee called the Cyber Regulations Advisory Committee.

(2) The Cyber Regulations Advisory Committee shall consist of a Chairperson and such number of other official and non-official members representing the interests principally affected or having special knowledge of the subject-matter as the Central Government may deem fit.

(3) The Cyber Regulations Advisory Committee shall advise -

(a) the Central Government either generally as regards any rules or for any other purpose connected with this Act;

(b) the Controller in framing the regulations under this Act

(4) There shall be paid to the non-official members of such Committee such traveling and other allowances as the Central Government may fix.

89 Power of Controller to make Regulations

(1) The Controller may, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government, by notification in the Official Gazette, make

SooperKanoon - India's Premier Online Legal Search - sooperkanoon.com