THE INFORMATION TECHNOLOGY ACT, 2000

ARRANGEMENT OF SECTIONS

CHAPTER I

PRELIMINARY

SECTIONS

1. Short title, extent, commencement and application.
2. Definitions.

CHAPTER II

DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE

3. Authentication of electronic records.
3A. Electronic signature.

CHAPTER III

ELECTRONIC GOVERNANCE

4. Legal recognition of electronic records.
5. Legal recognition of electronic signatures.
6. Use of electronic records and electronic signatures in Government and its agencies.
6A. Delivery of services by service provider.
7. Retention of electronic records.
7A. Audit of documents, etc., maintained in electronic form.
8. Publication of rule, regulation, etc., in Electronic Gazette.
9. Sections 6, 7 and 8 not to confer right to insist document should be accepted in electronic form.
10. Power to make rules by Central Government in respect of electronic signature.
10A. Validity of contracts formed through electronic means.

CHAPTER IV

ATTRIBUTION, ACKNOWLEDGEMENT AND DESPATCH OF ELECTRONIC RECORDS

11. Attribution of electronic records.
12. Acknowledgment of receipt.
13. Time and place of despatch and receipt of electronic record.

CHAPTER V

SECURE ELECTRONIC RECORDS AND SECURE ELECTRONIC SIGNATURE

14. Secure electronic record.
15. Secure electronic signature.
16. Security procedure and practices.

CHAPTER VI

REGULATION OF CERTIFYING AUTHORITIES

17. Appointment of Controller and other officers.
18. Functions of Controller.
19. Recognition of foreign Certifying Authorities.
20. [*Omitted*.]
21. Licence to issue electronic signature Certificates.
22. Application for licence.
23. Renewal of licence.
24. Procedure for grant or rejection of licence.
25. Suspension of licence.
26. Notice of suspension or revocation of licence.

SECTIONS

27. Power to delegate.
28. Power to investigate contraventions.
29. Access to computers and data.
30. Certifying Authority to follow certain procedures.
31. Certifying Authority to ensure compliance of the Act, etc.
32. Display of licence.
33. Surrender of licence.
34. Disclosure.

CHAPTER VII

ELECTRONIC SIGNATURE CERTIFICATES

35. Certifying authority to issue electronic signature Certificate.
36. Representations upon issuance of Digital signature Certificate.
37. Suspension of Digital Signature Certificate.
38. Revocation of Digital Signature Certificate.
39. Notice of suspension or revocation.

CHAPTER VIII

DUTIES OF SUBSCRIBERS

40. Generating key pair.
40A. Duties of subscriber of Electronic Signature Certificate.
41. Acceptance of Digital Signature Certificate.
42. Control of private key.

CHAPTER IX

PENALTIES AND ADJUDICATION

43. Penalty and compensation for damage to computer, computer system, etc.
43A. Compensation for failure to protect data.
44. Penalty for failure to furnish information, return, etc.
45. Residuary penalty.
46. Power to adjudicate.
47. Factors to be taken into account by the adjudicating officer.

CHAPTER X

APPELLATE TRIBUNAL

48. Establishment of Appellate Tribunal.
49. [*Omitted*.]
50. [*Omitted*.]
51. [*Omitted*.]
52. [*Omitted*.]
52A. [*Omitted*.]
52B. [*Omitted*.]
52C. [*Omitted*.]
52D. Decision by majority.
53. [*Omitted*.]
54. [*Omitted*.]
55. Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings.
56. [*Omitted*.]
57. Appeal to Appellate Tribunal.
58. Procedure and powers of the Appellate Tribunal.
59. Right to legal representation.
60. Limitation.
61. Civil court not to have jurisdiction.
62. Appeal to High Court.
63. Compounding of contraventions.

SECTIONS

64. Recovery of penalty.

CHAPTER XI

OFFENCES

65. Tampering with computer source documents.
66. Computer related offences.
66A. [*Omitted*.].
66B. Punishment for dishonestly receiving stolen computer resource or communication device.
66C. Punishment for identity theft.
66D. Punishment for cheating by personation by using computer resource.
66E. Punishment for violation of privacy.
66F. Punishment for cyber terrorism.
67. Punishment for publishing or transmitting obscene material in electronic form.
67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.
67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.
67C. Preservation and retention of information by intermediaries.
68. Power of Controller to give directions.
69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource.
69A. Power to issue directions for blocking for public access of any information through any computer resource.
69B. Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security.
70. Protected system.
70A. National nodal agency.
70B. Indian Computer Emergency Response Team to serve as national agency for incident response.
71. Penalty for misrepresentation.
72. Penalty for Breach of confidentiality and privacy.
72A. Penalty for disclosure of information in breach of lawful contract.
73. Penalty for publishing electronic signature Certificate false in certain particulars.
74. Publication for fraudulent purpose.
75. Act to apply for offence or contravention committed outside India.
76. Confiscation.
77. Compensation, penalties or confiscation not to interfere with other punishment.
77A. Compounding of offences.
77B. Offences with three years imprisonment to be bailable.
78. Power to investigate offences.

CHAPTER XII

INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES

79. Exemption from liability of intermediary in certain cases.

CHAPTER XIIA

EXAMINER OF ELECTRONIC EVIDENCE

79A. Central Government to notify Examiner of Electronic Evidence.

CHAPTER XIII

MISCELLANEOUS

80. Power of police officer and other officers to enter, search, etc.
81. Act to have overriding effect.
81A. Application of the Act to electronic cheque and truncated cheque.
82. Chairperson, Members, officers and employees to be public servants.
83. Power to give directions.

SECTIONS

84. Protection of action taken in good faith.
84A. Modes or methods for encryption.
84B. Punishment for abetment of offences.
84C. Punishment for attempt to commit offences.
85. Offences by companies.
86. Removal of difficulties.
87. Power of Central Government to make rules.
88. Constitution of Advisory Committee.
89. Power of Controller to make regulations.
90. Power of State Government to make rules.
91. [*Omitted*].
92. [*Omitted*].
93. [*Omitted*].
94. [*Omitted*].

THE FIRST SCHEDULE.

THE SECOND SCHEDULE.

THE THIRD SCHEDULE. [*Omitted.*]

THE FOURTH SCHEDULE. [*Omitted.*]

THE INFORMATION TECHNOLOGY ACT, 2000

ACT NO. 21 OF 2000

[9*th June*, 2000.]

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto;

WHEREAS the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law;

AND WHEREAS the said resolution recommends *inter alia*, that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information;

AND WHEREAS it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records.

BE it enacted by Parliament in the Fifty-first Year of the Republic of India as follows:–

CHAPTER 1

PRELIMINARY

1. Short title, extent, commencement and application.–(*1*) This Act may be called the Information Technology Act, 2000.

(*2*) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.

(*3*) It shall come into force on such date[1] as the Central Government may, by notification, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision.

[2][(*4*) Nothing in this Act shall apply to documents or transactions specified in the First Schedule:

Provided that the Central Government may, by notification in the Official Gazette, amend the First Schedule by way of addition or deletion of entries thereto.

(*5*) Every notification issued under sub-section (*4*) shall be laid before each House of Parliament.]

2. Definitions.–(*1*) In this Act, unless the context otherwise requires,–

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

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

(*c*) "adjudicating officer" means an adjudicating officer appointed under sub-section (*1*) of section 46;

1. 17th October, 2000, *vide* notification No. G.S.R. 788 (E), dated 17th October, 2000, *see* Gazette of India, Extraordinary, Part II, sec. 3(*ii*).
2. Subs. by Act 10 of 2009, s. 3, for sub-section (*4*) (w.e.f. 27-10-2009).

(*d*) "affixing [1][electronic signature]" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of [1][electronic signature];

[2][(*da*) "Appellate Tribunal" means the Appellate Tribunal referred to in sub-section (*1*) of section 48;]

(*e*) "appropriate Government" means as respects any matter,–

(*i*) enumerated in List II of the Seventh Schedule to the Constitution;

(*ii*) relating to any State law enacted under List III of the Seventh Schedule to the Constitution,

the State Government and in any other case, the Central Government;

(*f*) "asymmetric crypto system" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

(*g*) "Certifying Authority" means a person who has been granted a licence to issue a [1][electronic signature] Certificate under section 24;

(*h*) "certification practice statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing [1][electronic signature] Certificates;

[3][(*ha*) "communication device" means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image;]

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

[4][(*j*) "computer network" means the inter-connection of one or more computers or computer systems or communication device through–

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

(*ii*) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the inter-connection is continuously maintained;]

(*k*) "computer resource" means computer, computer system, computer network, data, computer data base or software;

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

(*m*) "Controller" means the Controller of Certifying Authorities appointed under sub-section (*1*) of section 17;

[5]* * * * *

[3][(*na*) "cyber cafe" means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public;

1. Subs. by Act 10 of 2009, s. 2, for "digital signature" (w.e.f. 27-10-2009).
2. Ins. by 7 of 2017, s. 169 (w.e.f. 26-5-2017).
3. Ins. by 10 of 2009, s. 4 (w.e.f. 27-10-2009).
4. Subs. by s. 4, *ibid*., for clause (*j*) (w.e.f. 27-10-2009).
5. Clause (*n*) omitted by 7 of 2017, s.169 (w.e.f. 26-5-2017)

(*nb*) "cyber security means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction;]

(*o*) "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

(*p*) "digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

(*q*) "Digital Signature Certificate" means a Digital Signature Certificate issued under sub-section (*4*) of section 35;

(*r*) "electronic form" with reference to information, means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

(*s*) "Electronic Gazette" means the Official Gazette published in the electronic form;

(*t*) "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

[1][(*ta*) "electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature;

(*tb*) "Electronic Signature Certificate" means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate;]

(*u*) "function", in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

[1][(*ua*) Indian Computer Emergency Response Team" means an agency established under sub-section (*1*) of Section 70B;]

(*v*) "information" includes [2][data, message, text,] images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche;

[3][(*w*) "intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes;]

(*x*) "key pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

(*y*) "law" includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be, Regulations made by the President under article 240, Bills enacted as President's Act under sub-clause (*a*) of clause (*1*) of article 357 of the Constitution and includes rules, regulations, bye-laws and orders issued or made thereunder;

(*z*) "licence" means a licence granted to a Certifying Authority under section 24;

(*za*) "originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

(*zb*) "prescribed" means prescribed by rules made under this Act;

(*zc*) "private key" means the key of a key pair used to create a digital signature;

1. Ins. by Act 10 of 2009, s. 4 (w.e.f. 27-10-2009).
2. Subs. by s. 4, *ibid.*, for "data, text" (w.e.f. 27-10-2009).
3. Subs. by s. 4, *ibid.*, for clause (*w*) (w.e.f. 27-10-2009).

(*zd*) "public key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

(*ze*) "secure system" means computer hardware, software, and procedure that–

(*a*) are reasonably secure from unauthorised access and misuse;

(*b*) provide a reasonable level of reliability and correct operation;

(*c*) are reasonably suited to performing the intended functions; and

(*d*) adhere to generally accepted security procedures;

(*zf*) "security procedure" means the security procedure prescribed under section 16 by the Central Government;

(*zg*) "subscriber" means a person in whose name the [1][electronic signature] Certificate is issued;

(*zh*) "verify", in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions, means to determine whether–

(*a*) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;

(*b*) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

(*2*) Any reference in this Act to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

CHAPTER II

[2][DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE]

3. Authentication of electronic records.–(*1*) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.

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

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

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

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

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

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

[3]**[3A. Electronic signature.**–(*1*) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (*2*), a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which–

(*a*) is considered reliable; and

(*b*) may be specified in the Second Schedule.

(*2*) For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if–

1. Subs. by Act 10 of 2009, s. 2, for "digital signature" (w.e.f. 27-10-2009).
2. Subs. by s. 5, *ibid*., for the heading "DIGITAL SIGNATURE" (w.e.f. 27-10-2009).
3. Ins. by s. 6, *ibid*. (w.e.f. 27-10-2009).

(*a*) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and to no other person;

(*b*) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;

(*c*) any alteration to the electronic signature made after affixing such signature is detectable;

(*d*) any alteration to the information made after its authentication by electronic signature is detectable; and

(*e*) it fulfils such other conditions which may be prescribed.

(*3*) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated.

(*4*) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the Second Schedule:

Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable.

(*5*) Every notification issued under sub-section (*4*) shall be laid before each House of Parliament.]

CHAPTER III

ELECTRONIC GOVERNANCE

4. Legal recognition of electronic records.–Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is–

(*a*) rendered or made available in an electronic form; and

(*b*) accessible so as to be usable for a subsequent reference.

5. Legal recognition of [1][electronic signatures].–Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of [1][electronic signature] affixed in such manner as may be prescribed by the Central Government.

Explanation.–For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.

6. Use of electronic records and [1][electronic signatures] in Government and its agencies.–(*1*) Where any law provides for–

(*a*) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;

(*b*) the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner;

(*c*) the receipt or payment of money in a particular manner,

then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

(*2*) The appropriate Government may, for the purposes of sub-section (*1*), by rules, prescribe–

(*a*) the manner and format in which such electronic records shall be filed, created or issued;

1. Subs. by Act 10 of 2009, s. 2, for "digital signatures" (w.e.f. 27-10-2009).

(*b*) the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (*a*).

[1]**[6A. Delivery of services by service provider.**–(*1*) The appropriate Government may, for the purposes of this Chapter and for efficient delivery of services to the public through electronic means authorise, by order, any service provider to set up, maintain and upgrade the computerised facilities and perform such other services as it may specify, by notification in the Official Gazette.

Explanation.–For the purposes of this section, service provider so authorised includes any individual, private agency, private company, partnership firm, sole proprietor firm or any such other body or agency which has been granted permission by the appropriate Government to offer services through electronic means in accordance with the policy governing such service sector.

(*2*) The appropriate Government may also authorise any service provider authorised under sub-section (*1*) to collect, retain and appropriate such service charges, as may be prescribed by the appropriate Government for the purpose of providing such services, from the person availing such service.

(*3*) Subject to the provisions of sub-section (*2*), the appropriate Government may authorise the service providers to collect, retain and appropriate service charges under this section notwithstanding the fact that there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate e-service charges by the service providers.

(*4*) The appropriate Government shall, by notification in the Official Gazette, specify the scale of service charges which may be charged and collected by the service providers under this section:

Provided that the appropriate Government may specify different scale of service charges for different types of services.]

7. Retention of electronic records.–(*1*) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if–

(*a*) the information contained therein remains accessible so as to be usable for a subsequent reference;

(*b*) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(*c*) the details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record are available in the electronic record:

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

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

[2][**7A. Audit of documents, etc., maintained in electronic form.–**Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in the electronic form.]

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

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

9. Sections 6, 7 and 8 not to confer right to insist document should be accepted in electronic form.–Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any

1. Ins. by Act 10 of 2009, s. 7 (w.e.f. 27-10-2009).
2. Ins. by s. 8, *ibid.* (w.e.f. 27-10-2009).

Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

10. Power to make rules by Central Government in respect of [1][electronic signature].–The Central Government may, for the purposes of this Act, by rules, prescribe–

(*a*) the type of [1][electronic signature];

(*b*) the manner and format in which the [1][electronic signature] shall be affixed;

(*c*) the manner or procedure which facilitates identification of the person affixing the [1][electronic signature];

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

(*e*) any other matter which is necessary to give legal effect to [1][electronic signatures].

[2]**[10A. Validity of contracts formed through electronic means.**–Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic records, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.]

CHAPTER IV

ATTRIBUTION, ACKNOWLEDGMENT AND DESPATCH OF ELECTRONIC RECORDS

11. Attribution of electronic records.–An electronic record shall be attributed to the originator–

(*a*) if it was sent by the originator himself;

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

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

12. Acknowledgment of receipt.–(*1*) Where the originator has not [3][stipulated] that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by–

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

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

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

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

13. Time and place of despatch and receipt of electronic record.–(*1*) Save as otherwise agreed to between the originator and the addressee, the despatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

---

1. Subs. by Act 10 of 2009, s. 2, for "digital signature" (w.e.f. 27-10-2009).
2. Ins. by s. 9, *ibid*. (w.e.f. 27-10-2009).
3. Subs. by s. 10, *ibid*., for "agreed with the addressee" (w.e.f. 27-10-2009).

(*2*) Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely:–

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

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

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

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

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

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

(*5*) For the purposes of this section,–

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

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

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

CHAPTER V

SECURE ELECTRONIC RECORDS ANS SECURE [1][ELECTRONIC SIGNATURE]

14. Secure electronic record.–Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall he deemed to be a secure electronic record from such point of time to the time of verification.

[2]**[15. Secure electronic signature.**– An electronic signature shall be deemed to be a secure electronic signature if–

(*i*) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and

(*ii*) the signature creation data was stored and affixed in such exclusive manner as may be prescribed.

Explanation.–In case of digital signature, the "signature creation data" means the private key of the subscriber.

16. Security procedures and practices.–The Central Government may, for the purposes of sections 14 and 15, prescribe the security procedures and practices:

Provided that in prescribing such security procedures and practices, the Central Government shall have regard to the commercial circumstances, nature of transactions and such other related factors as it may consider appropriate.]

CHAPTER VI

REGULATION OF CERTIFYING AUTHORITIES

17. Appointment of Controller and other officers.–(*1*) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers [3][, Assistant Controllers, other officers and employees] as it deems fit.

---

1. Subs. by Act 10 of 2009, s. 2, for "digital signatures" (w.e.f. 27-10-2009).
2. Subs. by s 11, *ibid.*, for sections 15 and 16 (w.e.f. 27-10-2009).
3. Subs. by s.12, *ibid.*, for "and Assistant Controllers" (w.e.f. 27-10-2009).

(*2*) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.

(*3*) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

(*4*) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers [1][, Assistant Controllers, other officers and employees] shall be such as may be prescribed by the Central Government.

(*5*) The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

(*6*) There shall be a seal of the Office of the Controller.

18. Functions of Controller.–The Controller may perform all or any of the following functions, namely:–

(*a*) exercising supervision over the activities of the Certifying Authorities;

(*b*) certifying public keys of the Certifying Authorities;

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

(*d*) specifying the qualifications and experience which employees of the Certifying Authority should possess;

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

(*f*) specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a [2][electronic signature] Certificate and the public key;

(*g*) specifying the form and content of a [2][electronic signature] Certificate and the key;

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

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

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

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

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

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

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

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

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

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

1. Subs. by Act 10 of 2009, s. 12, for "Assistant Controllers" (w.e.f. 27-10-2009).
2. Subs. by s. 2, *ibid.*, for "digital signature" (w.e.f. 27-10-2009).

20. [*Controller to act as repository*.] *Omitted by the Information Technology* (*Amendment*) *Act*, 2008 (10 *of* 2009), *s*. 13 (*w.e.f*. 27-10-2009).

21. Licence to issue [1][electronic signature] Certificates.–(*1*) Subject to the provisions of sub-section (*2*), any person may make an application, to the Controller, for a licence to issue [1][electronic signature] Certificates.

(*2*) No licence shall be issued under sub-section (*1*), unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which arc necessary to issue [1][electronic signature] Certificates as may be prescribed by the Central Government.

(*3*) A licence granted under this section shall–

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

(*b*) not be transferable or heritable;

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

22. Application for licence.–(*1*) Every application for issue of a licence shall be in such form as may be prescribed by the Central Government.

(*2*) Every application for issue of a licence shall be accompanied by–

(*a*) a certification practice statement;

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

(*c*) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;

(*d*) such other documents, as may be prescribed by the Central Government.

23. Renewal of licence.–An application for renewal of a licence shall be–

(*a*) in such form;

(*b*) accompanied by such fees, not exceeding five thousand rupees, as may be prescribed by the Central Government and shall be made not less than forty-five days before the date of expiry of the period of validity of the licence.

24. Procedure for grant or rejection of licence.–The Controller may, on receipt of an application under sub-section (*1*) of section 21, after considering the documents accompanying the application and such other factors, as he deems fit, grant the licence or reject the application:

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

25. Suspension of licence.– (*1*) The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has–

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

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

[2][(*c*) failed to maintain the procedures and standards specified in section 30;]

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

revoke the licence:

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

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

1. Subs. by Act 10 of 2009, s. 2, for "digital signature" (w.e.f. 27-10-2009).
2. Subs. by notification No. S.O. 1015(E) (w.e.f. 19-9-2002).

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

(*3*) No Certifying Authority whose licence has been suspended shall issue any [1][electronic signature] Certificate during such suspension.

26. Notice of suspension or revocation of licence.–(*1*) Where the licence of the Certifying Authority is suspended or revoked, the Controller shall publish notice of such suspension or revocation, as the case may be, in the data base maintained by him.

(*2*) Where one or more repositories are specified, the Controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories:

Provided that the data base containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock:

Provided further that the Controller may, if he considers necessary, publicise the contents of data base in such electronic or other media, as he may consider appropriate.

27. Power to delegate.–The Controller may, in writing, authorise the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this Chapter.

28. Power to investigate contraventions.–(*1*) The Controller or any officer authorised by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder.

(*2*) The Controller or any officer authorised by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 (43 of 1961), and shall exercise such powers, subject to such limitations laid down under that Act.

29. Access to computers and data.–(*1*) Without prejudice to the provisions of sub-section (*1*) of section 69, the Controller or any person authorised by him shall, if he has reasonable cause to suspect that [2][any contravention of the provisions of this Chapter] has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

(*2*) For the purposes of sub-section (*1*), the Controller or any person authorised by him may, by order, direct any person in charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

30. Certifying Authority to follow certain procedures.–Every Certifying Authority shall,–

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

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

(*c*) adhere to security procedures to ensure that the secrecy and privacy of the [1][electronic signatures] are assured; [3]***

[4][(*ca*) be the repository of all electronic signature Certificates issued under this Act;

(*cb*) publish information regarding its practices, electronic signature Certificates and current status of such certificates; and]

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

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

---

1. Subs. by Act 10 of 2009, s. 2, for "digital signature" (w.e.f. 27-10-2009).
2. Subs. by s. 14, *ibid.*, for "any contravention of the provisions of this Act, rules and regulations made thereunder" (w.e.f. 27-10-2009).
3. The word "and" omitted by s. 15, *ibid.* (w.e.f. 27-10-2009).
4. Ins. by s. 15, *ibid.* (w.e.f. 27-10-2009).

32. Display of licence.–Every Certifying Authority shall display its licence at a conspicuous place of the premises in which it carries on its business.

33. Surrender of licence.–(*1*) Every Certifying Authority whose licence is suspended or revoked shall immediately after such suspension or revocation, surrender the licence to the Controller.

(*2*) Where any Certifying Authority fails to surrender a licence under sub-section (*1*), the person in whose favour a licence is issued, shall be guilty of an offence and shall be [1][liable to penalty which may extend to five lakh rupees].

34. Disclosure.–(*1*) Every Certifying Authority shall disclose in the manner specified by regulations–

(*a*) its [2][electronic signature] Certificate [3]***;

(*b*) any certification practice statement relevant thereto;

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

(*d*) any other fact that materially and adversely affects either the reliability of a [2][electronic signature] Certificate, which that Authority has issued, or the Authority's ability to perform its services.

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

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

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

CHAPTERVII

[2][ELECTRONIC SIGNATURE] CERTIFICATES

35. Certifying authority to issue [2][electronic signature] Certificate.–(*1*) Any person may make an application to the Certifying Authority for the issue of a [2][electronic signature] Certificate in such form as may be prescribed by the Central Government.

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

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

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

(*4*) On receipt of an application under sub-section (*1*), the Certifying Authority may, after consideration of the certification practice statement or the other statement under sub-section (*3*) and after making such enquiries as it may deem fit, grant the [2][electronic signature] Certificate or for reasons to be recorded in writing, reject the application:

[4]* * * * *

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

36. Representations upon issuance of Digital Signature Certificate.–A Certifying Authority while issuing a Digital Signature Certificate shall certify that–

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

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

1. Subs. by Act 18 of 2023, s. 2 and Schedule for certain words (w.e.f. 30-11-2023).
2. Subs. by Act 10 of 2009, s. 2, for "digital signature" (w.e.f. 27-10-2009).
3. Certain words omitted by s. 16, *ibid.* (w.e.f. 27-10-2009).
4. The first proviso omitted by s. 17, *ibid.* (w.e.f. 27-10-2009).
5. Subs. by s. 17, *ibid.*, for "Provided further" (w.e.f. 27-10-2009).

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

[1][(*ca*) the subscriber holds a private key which is capable of creating a digital signature;

(*cb*) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the subscriber;]

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

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

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

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

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

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

(*ii*) any person duly authorised to act on behalf of that subscriber;

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

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

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

38. Revocation of Digital Signature Certificate.–(*1*) A Certifying Authority may revoke a Digital Signature Certificate issued by it–

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

(*b*) upon the death of the subscriber; or

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

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

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

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

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

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

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

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

39. Notice of suspension or revocation.–(*1*) Where a Digital Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice.

1. Ins. by Act 10 of 2009, s. 18 (w.e.f. 27-10-2009).

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

CHAPTER VIII

DUTIES OF SUBSCRIBERS

40. Generating key pair.–Where any Digital Signature Certificate the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, [1]*** the subscriber shall generate [2][that key] pair by applying the security procedure.

[3]**[40A. Duties of subscriber of Electronic Signature Certificate.–**In respect of Electronic Signature Certificate the subscriber shall perform such duties as may be prescribed.]

41. Acceptance of Digital Signature Certificate.–(*1*) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorises the publication of a Digital Signature Certificate–

(*a*) to one or more persons;

(*b*) in a repository; or

otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

(*2*) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that–

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

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

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

42. Control of private key.–(*1*) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure [4]***.

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

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

CHAPTER IX

[5][PENALTIES, COMPENSATION AND ADJUDICATION]

43. [6]**[Penalty and compensation] for damage to computer, computer system, etc.**–If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network,–

(*a*) accesses or secures access to such computer, computer system or computer network [7][or computer resource];

1. The word "then" omitted by notification No. S.O. 1015(E) (w.e.f. 19-9-2002).
2. Subs. *ibid.*, for "the key" (w.e.f. 19-9-2002).
3. Ins. by Act 10 of 2009, s. 19 (w.e.f. 27-10-2009).
4. The words "to a person not authorised to affix the digital signature of the subscriber" omitted by notification No. S.O.1015(E) (w.e.f. 19-9-2002).
5. Subs. by Act 10 of 2009, s. 20, for "PENALTIES AND ADJUDICATION" (w.e.f. 27-10-2009).
6. Subs. by s. 21, *ibid.*, for "Penalty" (w.e.f. 27-10-2009).
7. Ins. by s. 21, *ibid.* (w.e.f. 27-10-2009).

(*b*) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(*c*) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(*d*) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(*e*) disrupts or causes disruption of any computer, computer system or computer network;

(*f*) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(*g*) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

(*h*) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;

[1][(*i*) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(*j*) steal, conceal, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;]

[2][he shall be liable to pay damages by way of compensation to the person so affected.]

Explanation.–For the purposes of this section,–

(*i*) "computer contaminant" means any set of computer instructions that are designed–

(*a*) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(*b*) by any means to usurp the normal operation of the computer, computer system, or computer network;

(*ii*) "computer data-base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(*iii*) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(*iv*) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

[1][(*v*) "computer source code" means the listing of programme, computer commands, design and layout and programme analysis of computer resource in any form.]

[3]**[43A. Compensation for failure to protect data.**–Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

1. Ins. by Act 10 of 2009, s. 21 (w.e.f. 27-10-2009).
2. Subs. by s. 21, *ibid*., for certain words (w.e.f. 27-10-2009).
3. Ins. by s. 22, *ibid.* (w.e.f. 27-10-2009).

Explanation.–For the purposes of this section,–

(*i*) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(*ii*) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

(*iii*) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.]

44. Penalty for failure to furnish information, return, etc.–If any person who is required under this Act or any rules or regulations made thereunder to–

(*a*) furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding [1][fifteen lakh] rupees for each such failure;

(*b*) file any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file return or furnish the same within the time specified therefor in the regulations, he shall be liable to a penalty not exceeding [2][fifty thousand] rupees for every day during which such failure continues;

(*c*) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding [3][one lakh] rupees for every day during which the failure continues.

45. Residuary penalty.–Whoever contravenes any [4][rules, regulations, directions or orders] made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a [5][penalty not exceeding one lakh rupees, in addition to compensation to the person affected by such contravention not exceeding—

(*a*) ten lakh rupees, by an intermediary, company or body corporate; or

(*b*) one lakh rupees, by any other person.]

46. Power to adjudicate.–(*1*) For the purpose of adjudging [6][under this Act] whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, [7][direction or order made thereunder which renders him liable to pay penalty or compensation,] the Central Government shall, subject to the provisions of sub-section (*3*), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government.

[8][(*1A*) The adjudicating officer appointed under sub-section (*1*) shall exercise jurisdiction to adjudicate matters in which the claim for [9]*** damage does not exceed rupees five crore:

Provided that the jurisdiction in respect of the claim for [9]*** damage exceeding rupees five crores shall vest with the competent court.]

(*2*) The adjudicating officer shall, after giving the person referred to in sub-section (*1*) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person

1. Subs. by Act 18 of 2023, s. 2 and Schedule, for "one lakh and fifty thousand" (w.e.f. 30-11-2023).
2. Subs. by *ibid*., s. 2 and Schedule, for "five thousand" (w.e.f. 30-11-2023).
3. Sub. by *ibid*., s. 2 and Schedule, for "ten thousand" (w.e.f. 30-11-2023).
4. Subs. by *ibid*., s. 2 and Schedule, for "rules or regulations" (w.e.f. 30-11-2023).
5. Subs. by *ibid*., s. 2 and Schedule, for certain words (w.e.f. 30-11-2023).
6. Subs. by ibid., s. 2 and Schedule, for "under this Chapter" (w.e.f. 30-11-2023).
7. Subs. by Act 10 of 2009, s. 23, for "direction or order made thereunder" (w.e.f. 27-10-2009).
8. Ins. by s. 23, *ibid*. (w.e.f. 27-10-2009).
9. Words omitted "injury or" omitted by Act 18 of 2023, s. 2 and Schedule (w.e.f. 30-11-2023).

has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

(*3*) No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government.

(*4*) Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

(*5*) Every adjudicating officer shall have the powers of a civil court which are conferred on the [1][Appellate Tribunal] under sub-section (*2*) of section 58, and–

(*a*) all proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code (45 of 1860);

(*b*) shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973 (2 of 1974);

[2][(*c*) shall be deemed to be a civil court for purposes of Order XXI of the Civil Procedure Code, 1908 (5 of 1908).]

47. Factors to be taken into account by the adjudicating officer.–While adjudging the quantum of compensation under this Chapter, the adjudicating officer shall have due regard to the following factors, namely:–

(*a*) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;

(*b*) the amount of loss caused to any person as a result of the default;

(*c*) the repetitive nature of the default.

CHAPTER X

[3][APPELLATE TRIBUNAL]

48. Establishment of [1][Appellate Tribunal].–[4][(*1*) The Telecom Disputes Settlement and Appellate Tribunal established under section 14 of the Telecom Regulatory Authority of India Act, 1997 shall, on and from the commencement of Part XIV of Chapter VI of the Finance Act, 2017, be the Appellate Tribunal for the purposes of this Act and the said Appellate Tribunal shall exercise the jurisdiction, powers and authority conferred on it by or under this Act.]

(*2*) The Central Government [5][shall specify, by notification] the matters and places in relation to which the [1][Appellate Tribunal] may exercise jurisdiction.

49. [Composition of Cyber Appellate Tribunal.]—*Omitted by the Finance Act*, 2017 (7 *of* 2017), *s.* 169 (*w.e.f.* 26-5-2017).

50. [Qualifications for appointment as Chairperson and Members of Cyber Appellate Tribunal.]—*Omitted by s.* 169, *ibid.* (*w.e.f.* 26-5-2017).

51. [Term of office, conditions of service, etc., of Chairperson and Members.]—*Omitted by s.* 169, *ibid.* (*w.e.f.* 26-5-2017).

52. [Salary, allowances and other terms and conditions of service of Chairperson and Members.]—*Omitted by s.* 169, *ibid.* (*w.e.f.* 26-5-2017).

52A. [Powers of superintendence, direction, etc.]—*Omitted by s.* 169, *ibid.* (*w.e.f.* 26-5-2017).

52B. [Distribution of business among Benches.]—*Omitted by s.* 169, *ibid.* (*w.e.f.* 26-5-2017).

52C. [Power of Chairperson to transfer cases.]—*Omitted by s.* 169, *ibid.* (*w.e.f.* 26-5-2017).

52D. Decision by majority.–If the Members of a Bench consisting of two Members differ in opinion on any point, they shall state the point or points on which they differ, and make a reference to the Chairperson of the [1][Appellate Tribunal] who shall hear the point or points himself and such point or

1. Subs. by Act 7 of 2017, s. 169, for "Cyber Appellate Tribunal" (w.e.f. 26-5-2017)
2. Ins. by Act 10 of 2009, s. 23 (w.e.f. 27-10-2009).
3. Subs. by Act 7 of 2017, s. 169, for Chapter heading (w.e.f. 26-5-2017).
4. Subs. by s. 169, *ibid*., for sub-section (*1*) (w.e.f. 26-5-2017).
5. Subs. by s, 169, *ibid*., for "shall also specify, in the notification referred to in sub-section (*1*)" (w.e.f. 26-5-2017).

points shall be decided according to the opinion of the majority of the Members who have heard the case, including those who first heard it.]

53. [Filling up of vacancies.]—*Omitted by the Finance Act*, 2017 (7 *of* 2017), *s*. 169 (*w.e.f*. 26-5-2017).

54. [Resignation and removal.]—*Omitted by s*. 169, *ibid*. (*w.e.f*. 26-5-2017).

55. Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings.–No order of the Central Government appointing any person as the [1][Chairperson or the Member] of a [2][Appellate Tribunal] shall be called in question in any manner and no act or proceeding before a [2][Appellate Tribunal] shall be called in question in any manner on the ground merely of any defect in the constitution of a [2][Appellate Tribunal].

56. [Staff of the Cyber Appellate Tribunal.]—*Omitted by the Finance Act*, 2017 (7 *of* 2017), *s*. 169 (*w.e.f*. 26-5-2017).

57. Appeal to [2][**Appellate Tribunal].**–(*1*) Save as provided in sub-section (*2*), any person aggrieved by an order made by controller or an adjudicating officer under this Act may prefer an appeal to a [2][Appellate Tribunal] having jurisdiction in the matter.

(*2*) No appeal shall lie to the [2][Appellate Tribunal] from an order made by an adjudicating officer with the consent of the parties.

(*3*) Every appeal under sub-section (*1*) shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed:

Provided that the [2][Appellate Tribunal] may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

(*4*) On receipt of an appeal under sub-section (*1*), the [2][Appellate Tribunal] may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

(*5*) The [2][Appellate Tribunal] shall send a copy of every order made by it to the parties to the appeal and to the concerned Controller or adjudicating officer.

(*6*) The appeal filed before the [2][Appellate Tribunal] under sub-section (*1*) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

58. Procedure and powers of the [2][Appellate Tribunal].–(*1*) The [2][Appellate Tribunal] shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908) but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the [2][Appellate Tribunal] shall have powers to regulate its own procedure including the place at which it shall have its sittings.

(*2*) The [2][Appellate Tribunal] shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely:–

(*a*) summoning and enforcing the attendance of any person and examining him on oath;

(*b*) requiring the discovery and production of documents or other electronic records;

(*c*) receiving evidence on affidavits;

(*d*) issuing commissions for the examination of witnesses or documents;

(*e*) reviewing its decisions;

(*f*) dismissing an application for default or deciding it *ex parte*;

(*g*) any other matter which may be prescribed.

1. Subs. by Act 10 of 2009, s. 29, *ibid.*, for "Presiding Officer" (w.e.f. 27-10-2009).
2. Subs. by 7 of 2017, s, 169, for "Cyber Appellate Tribunal" (w.e.f. 26-5-2017).

(*3*) Every proceeding before the [1][Appellate Tribunal] shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code (45 of 1860) and the [1][Appellate Tribunal] shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973 (2 of 1974).

59. Right to legal representation.–The appellant may either appear in person or authorise one or more legal practitioners or any of its officers to present his or its case before the [1][Appellate Tribunal].

60. Limitation.–The provisions of the Limitation Act, 1963 (36 of 1963), shall, as far as may be, apply to an appeal made to the [1][Appellate Tribunal].

61. Civil court not to have jurisdiction.–No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the [1][Appellate Tribunal] constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

62. Appeal to High Court.–Any person aggrieved by any decision or order of the [1][Appellate Tribunal] may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the [1][Appellate Tribunal] to him on any question of fact or law arising out of such order:

Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

63. Compounding of contraventions.–(*1*) Any contravention under this [2][Act] may, either before or after the institution of adjudication proceedings, be compounded by the Controller or such other officer as may be specially authorised by him in this behalf or by the adjudicating officer, as the case may be, subject to such conditions as the Controller or such other officer or the adjudicating officer may specify:

Provided that such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded.

(*2*) Nothing in sub-section (*1*) shall apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded.

Explanation.–For the purposes of this sub-section, any second or subsequent contravention committed after the expiry of a period of three years from the date on which the contravention was previously compounded shall be deemed to be a first contravention.

(*3*) Where any contravention has been compounded under sub-section (*1*), no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

64. Recovery of [3][penalty or compensation].–A [4][penalty imposed or compensation awarded] under this Act, if it is not paid, shall he recovered as an arrear of land revenue and the licence or the [5][electronic signature] Certificate, as the case may be, shall be suspended till the penalty is paid.

CHAPTER XI

OFFENCES

65. Tampering with computer source documents.–Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

---

1. Subs. by 7 of 2017, s. 169, for "Cyber Appellate Tribunal" (w.e.f. 26-5-2017).
2. Subs. by notification No. S.O. 1015(E) (w.e.f. 19-9-2002).
3. Subs. by Act 10 of 2009, s. 31, for marginal heading (w.e.f. 27-10-2009).
4. Subs. by s. 31, *ibid*., for "penalty imposed" (w.e.f. 27-10-2009).
5. Subs. by s. 2, *ibid*., for "digital signature" (w.e.f. 27-10-2009).

Explanation.–For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

[1]**[66. Computer related offences.**–If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

Explanation.–For the purposes of this section,–

(*a*) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code (45 of 1860);

(*b*) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code (45 of 1860).

[2]**66A. [Punishment for sending offensive messages through communication service, etc.]**– *Omitted by the Jan Vishwas (Amendment of Provisions) Act*, 2023 (18 *of* 2023), *s.* 2 and Schedule (*w.e.f.* 30-11-2023).

66B. Punishment for dishonestly receiving stolen computer resource or communication device.– Whoever dishonestly received or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

66C. Punishment for identity theft.–Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

66D. Punishment for cheating by personation by using computer resource.–Whoever, by means of any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

66E. Punishment for violation of privacy.–Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

Explanation.–For the purposes of this section–

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

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

(*c*) "private area" means the naked or undergarment clad genitals, public area, buttocks or female breast:

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

(*e*) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that–

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

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

1. Subs. by Act 10 of 2009, s. 32, for sections 66 and 67 (w.e.f. 27-10-2009).
2. Section 66A has been struck down by supreme Court's Order dated 24-3-2015 in the Shreya Singhal Vs. Union of India, AIR 2015 SC. 1523.

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 authorised to access computer resource; or

(*ii*) attempting to penetrate or access a computer resource without authorisation or exceeding authorised 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 authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base 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 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.–Whoever publishes or transmits or causes to be published or transmitted 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 three years and with fine which may extend to five lakh rupees and in the event of 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.

67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.–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.

67B. 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,

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:

Provided that 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 the interest of science, literature, art or learning or other objects of general concern; or

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

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

67C. 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 [1][liable to penalty which may extend to twenty-five lakh rupees].]

68. Power of Controller to give directions.–(*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 thereunder.

[2][(*2*) Any person who intentionally or knowingly fails to comply with any order under sub-section (*1*) shall be guilty of an offence and shall be liable [1][to penalty which may extend to twenty-five lakh rupees].]

[3]**[69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource.**–(*1*) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence 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 generated, transmitted, received or stored in 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 referred to in sub-section (*1*), extend all facilities and technical assistance to–

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

(*b*) intercept, 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 imprisonment for a term which may extend to seven years and shall also be liable to fine.

1. Subs. by Act 18 of 2023, s. 2 and Schedule for certain words (w.e.f. 30-11-2023).
2. Subs. by Act 10 of 2009, s. 33, for sub-section (*2*) (w.e.f. 27-10-2009).
3. Subs. by s. 34, *ibid*., for section 69 (w.e.f. 27-10-2009).

69A. 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 officers specially authorised 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, defence 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-section (*2*), for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the 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 authorise 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 intrusion or spread of computer contaminant in the country, by notification in the Official Gazette, authorise 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 or the computer resource shall, when called upon by the agency which has been authorised 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 any extend to [1][one year or shall be liable to fine which may extend to one crore rupees, or with both].

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, data, size, duration or type of underlying service and any other information.]

70. Protected system.–[2][(*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.

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.]

(*2*) The appropriate Government may, by order in writing, authorise the persons who are authorised 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.

[3][(*4*) The Central Government shall prescribe the information security practices and procedures for such protected system.]

[4]**[70A. National nodal agency.**–(*1*) The Central Government may, by notification published in the Official Gazette, designate any organisation of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.

1. Subs. by Act 18 of 2023, s. 2 and Schedule for "three years and shall also be liable to fine" (w.e.f. 30-11-2023).
2. Subs. by Act 10 of 2009, s. 35, for sub-section (*1*) (w.e.f. 27-10-2009).
3. Ins. by s. 35, *ibid.* (w.e.f. 27-10-2009).
4. Ins. by s. 36, *ibid.* (w.e.f. 27-10-2009).

(*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.

70B. 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, preventation, 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 centres, body corporate and any other person.

(*7*) Any service provider, intermediaries, data centres, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (*6*), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to [1][one crore] rupees or with both.

(*8*) No court shall take cognizance of any offence under this section, except on a complaint made by an officer authorised 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 licence or [2][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. Penalty for Breach of confidentiality and privacy.–Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, 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 [3][liable to penalty which may extend to five lakh rupees].

[4][**72A. [5][Penalty] for disclosure of information in breach of lawful contract.**–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

1. Subs. by Act 18 of 2023, s. 2 and Schedule, for "one lakh" (w.e.f. 30-11-2023).
2. Subs. by Act 10 of 2009, s. 2, for "digital signature" (w.e.f. 27-10-2009).
3. Subs. by Act 18 of 2023, s. 2 and Schedule, for certain world (w.e.f. 30-11-2023).
4. Ins. by Act 10 of 2009, s. 37, (w.e.f. 27-10-2009).
5. Subs. by Act 18 of 2023, s. 2 and Schedule, for "Punishment" (w.e.f. 30-11-2023).

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 [1][liable to penalty which may extend to twenty-five lakh rupees].]

73. Penalty for publishing [2][electronic signature] Certificate false in certain particulars.–(*1*) No person shall publish a [2][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 [2][electronic 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 [2][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 contravention 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.

(*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 thereunder 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 thereunder, 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 authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

[3]**[77. Compensation, penalties or confiscation not to interfere with other punishment.**–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.

77A. Compounding of offences.–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:

1. Subs. by Act 18 of 2023, s. 2 and Schedule, for certain word (w.e.f. 30-11-2023).
2. Subs. by Act 10 of 2009, s. 2, for "digital signature" (w.e.f. 27-10-2009).
3. Subs. by s. 38, *ibid*., for section 77 (w.e.f. 27-10-2009).

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 sections 265B and 265C of the Code of Criminal Procedure, 1973 (2 of 1974) shall apply.

77B. Offences with three years imprisonment to be bailable.–Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), 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.–Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of [1][Inspector] shall investigate any offence under this Act.

[2][CHAPTER XII

INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES

79. Exemption from liability of intermediary in certain cases.–(*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 made available or hosted by him.

(*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 hosted; 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.

(*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;

(*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 purposes of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

CHAPTER XIIA

EXAMINER OF ELECTRONIC EVIDENCE

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.

1. Subs. by Act 10 of 2009, s. 39, for "Deputy Superintendent of Police" (w.e.f. 27-10-2009).
2. Subs. by, s. 40, *ibid*., for Chapter XII (w.e.f. 27-10-2009).

Explanation.–For the purposes 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.]

CHAPTER 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 (2 of 1974), any police officer, not below the rank of a [1][Inspector], or any other officer of the Central Government or a State Government authorised 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.–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 (2 of 1974) 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.

[2][Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957 (14 of 1957) or the Patents Act, 1970 (39 of 1970).]

[3]**[81A. Application of the Act to electronic cheque and truncated cheque.–**(*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 sub-section (*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 that notification.

Explanation.–For the purposes of this Act, the expressions "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).]

[4][**82. Controller, Deputy Controller and Assistant Controller to be public servants**.–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 (45 of 1860).]

83. Power to give directions.–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 thereunder.

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

1. Subs. by Act 10 of 2009, s. 41, for "Deputy Superintendent of Police" (w.e.f. 27-10-2009).
2. Ins. by s. 42, *ibid.* (w.e.f. 27-10-2009).
3. Ins. by Act 55 of 2002, s. 13 (w.e.f. 26-2-2003).
4. Subs. by 7 of 2017, s. 169, for section 82 (w.e.f. 26-5-2017).

him, [1][and adjudicating officers] for anything which is in good faith done or intended to be done in pursuance of this Act or any rule, regulation or order made thereunder.

[2]**[84A. Modes or methods for encryption.**–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.

84B. Punishment for abetment of offences.–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.

84C. Punishment for attempt to commit offences.–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 thereunder 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 thereunder 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.

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

1. Subs. by Act 7 of 2017, s. 169, for "the Chairperson Members, adjudicating officers and the staff of the Cyber Appellate Tribunal" (w.e.f. 26-5-2017).
2. Ins. by 10 of 2009, s. 45 (w.e.f. 27-10-2009).

(*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:–

[1][(*a*) the conditions for considering reliability of electronic signature or electronic authentication technique under sub-section (*2*) of section 3A;

(*aa*) the procedure for ascertaining electronic signature or authentication under sub-section (*3*) of section 3A;

(*ab*) the manner in which any information or matter may be authenticated by means of electronic signature under section 5;]

(*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;

[2][(*ca*) the manner in which the authorised service provider may collect, retain and appropriate service charges under sub-section (*2*) of section 6A;]

(*d*) the matters relating to the type of [3][electronic signature], manner and format in which it may be affixed under section 10;

[4][(*e*) the manner of storing and affixing electronic signature creation data under section 15;

(*ea*) the security procedures and practices under section 16;]

(*f*) the qualifications, experience and terms and conditions of service of Controller, Deputy Controllers [5][, Assistant Controllers, other officers and employees] under section 17;

[6]* * * * *

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

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

(*j*) the form in which an application for licence may be made under sub-section (*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 licence under clause (*d*) of sub-section (*2*) of section 22;

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

[2][(*ma*) the form of application and fee for issue of Electronic Signature Certificate under section 35;]

(*n*) the form in which application for issue of a [3][electronic signature] Certificate may be made under sub-section (*1*) of section 35;

(*o*) the fee to be paid to the Certifying Authority for issue of a [3][electronic signature] Certificate under sub-section (*2*) of section 35;

[2][(*oa*) the duties of subscribers under section 40A;

(*ob*) the reasonable security practices and procedures and sensitive personal data or information under section 43A;]

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

(*q*) the qualification and experience which the adjudicating officer shall possess under sub-section (*3*) of section 46;

---

1. Subs. by Act 10 of 2009, s. 46, for clause (*a*) (w.e.f. 27-10-2009).
2. Ins. by s. 46, *ibid.* (w.e.f. 27-10-2009).
3. Subs. by s. 2, *ibid.*, for "digital signature" (w.e.f. 27-10-2009).
4. Subs. by s. 46, *ibid.*, for clause (*e*) (w.e.f. 27-10-2009).
5. Subs. by s. 46, *ibid.*, for "and Assistant Controllers" (w.e.f. 27-10-2009).
6. Clause (*g*) omitted by s. 46, *ibid.* (w.e.f. 27-10-2009).

[1]* * * *

(*u*) the form in which appeal may be filed and the fee thereof under sub-section (*3*) of section 57;

(*v*) any other power of a civil court required to be prescribed under clause (*g*) of sub-section (*2*) of section 58; and

[2][(*w*) the powers and functions of the Chairperson of the [3][Appellate Tribunal] under section 52A;

(*x*) the information, duration, manner and form of such information to be retained and preserved under section 67C;

(*y*) the procedures and safeguards for interception, monitoring or decryption under sub-section (*2*) of section 69A;

(*z*) the procedures and safeguards for blocking for access by the public under sub-section (*3*) of section 69 B;

(*za*) the procedure and safeguards for monitoring and collecting traffic data or information under sub-section (*3*) of section 69B;

(*zb*) the information security practices and procedures for protected system under section 70;

(*zc*) manner of performing functions and duties of the agency under sub-section (*3*) of section 70 A;

(*zd*) the officers and employees under sub-section (*2*) of section 70B;

(*ze*) salaries and allowances and terms and conditions of service of the Director General and other officers and employees under sub-section (*3*) of section 70B;

(*zf*) the manner in which the functions and duties of agency shall be performed under sub-section (*5*) of section 70B;

(*zg*) the guidelines to be observed by the intermediaries under sub-section (*2*) of section 79;

(*zh*) the modes or methods for encryption under section 84 A.]

(*3*) [4][Every notification made by the Central Government under sub-section (*1*) of section 70A 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 modification in [5]*** the rule or both Houses agree that [5]*** the rule should not be made, [5]*** the rule 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 notification or rule.

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.

1. Clauses (*r*), (*s*) and (*t*) omitted by Act 7 of 2017, s. 169 (w.e.f. 26-5-2017).
2. Subs. by Act 10 of 2009, s. 46, for clause (*w*) (w.e.f. 27-10-2009).
3. Subs. by Act 7 of 2017, s. 169, for "Cyber Appellate Tribunal"(w.e.f. 26-5-2017).
4. Subs. by Act 10 of 2009, s. 46, for certain words, brackets, letter and figures (w.e.f. 27-10-2009).
5. The words "the notification or" omitted by s. 46, *ibid.* (w.e.f. 27-10-2009).

(*4*) There shall be paid to the non-official members of such Committee such travelling 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 regulations consistent with this Act and the rules made thereunder to carry out the purposes of this Act.

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

(*a*) the particulars relating to maintenance of data base containing the disclosure record of every Certifying Authority under clause [1][(*n*)] of section 18;

(*b*) the conditions and restrictions subject to which the Controller may recognise any foreign Certifying Authority under sub-section (*1*) of section 19;

(*c*) the terms and conditions subject to which a licence may be granted under clause (*c*) of sub-section (*3*) of section 21;

(*d*) other standards to be observed by a Certifying Authority under clause (*d*) of section 30;

(*e*) the manner in which the Certifying Authority shall disclose the matters specified in sub-section (*1*) of section 34;

(*f*) the particulars of statement which shall accompany an application under sub-section (*3*) of section 35.

(*g*) the manner by which the subscriber shall communicate the compromise of private key to the Certifying Authority under sub-section (*2*) of section 42.

(*3*) Every regulation made under this Act 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 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.

90. Power of State Government to make rules.–(*1*) The State 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 electronic form in which filing, issue, grant, receipt or payment shall be effected under sub-section (*1*) of section 6;

(*b*) for matters specified in sub-section (*2*) of section 6;

[2]* * * * *

(*3*) Every rule made by the State Government under this section shall be laid, as soon as may be after it is made, before each House of the Stale Legislature where it consists of two Houses, or where such Legislature consists of one House, before that House.

91. [*Amendment of Act* 45 *of* 1860.]—*Omitted by the Information Technology* (*Amendment*) *Act*, 2008 (10 of 2009), *s.* 48 (*w.e.f.* 27-10-2009).

92. [*Amendment of Act* 1 *of* 1872.]—*Omitted by s.* 48, *ibid.* (*w.e.f.* 27-10-2009).

93. [*Amendment of Act* 18 *of* 1891.]—*Omitted by s.* 48, *ibid.* (*w.e.f.* 27-10-2009).

94. [*Amendment of Act* 2 *of* 1934.]—*Omitted by s.* 48, *ibid.* (*w.e.f.* 27-10-2009).

1. Subs. by notification No. S.O. 1015(E), for "(*m*)" (w.e.f. 19-9-2002).
2. Clause (*c*) omitted by Act 10 of 2009, s. 47 (w.e.f. 27-10-2009).

[1][THE FIRST SCHEDULE

[*See* sub-section (*4*) of section 1]

DOCUMENTS OR TRANSACTIONS TO WHICH THE ACT SHALL NOT APPLY

Sl. No.	Description of documents or transactions
[2][1.	A negotiable instrument (other than a cheque, a Demand Promissory Note or a Bill of Exchange issued in favour of or endorsed by an entity regulated by the Reserve Bank of India, National Housing Bank, Securities and Exchange Board of India, Insurance Regulatory and Development Authority of India and Pension Fund Regulatory and Development Authority) as defined in Section 13 of the Negotiable Instrument Act, 1881 (26 of 1881).]
2.	A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882 (7 of 1882) [3][but excluding those power-of-attorney that empower an entity regulated by the Reserve Bank of India, National Housing Bank, Securities and Exchange Board of India, Insurance Regulatory and Development Authority of India and Pension Fund Regulatory and Development Authority to act for, on behalf of, and in the name of the person executing them.].
3.	A trust as defined in section 3 of the Indian Trust Act, 1882 (2 of 1882).
4.	A will as defined in clause (*h*) of section 2 of the Indian Succession Act, 1925 (39 of 1925), including any other testamentary disposition by whatever name called.
5.	[4][***]

1. Subs. by Act 10 of 2009, s. 49, for the First Schedule and the Second Schedule (w.e.f. 27-10-2009).
2. Subs. by notification No S.O. 4720(E), for serial number 1 and the entries relating thereto, Dated 26-9-2022.
3. Ins. by S.O. 4720(E), Dated 26-9-2022.
4. Serial number 5 and the entries relating thereto Omitted by S.O. 4720(E), Dated 26-9-2022.

[1][THE SECOND SCHEDULE

[*See* sub-section (*1*) of section 3A]

ELECTRONIC SIGNATURE OR ELECTRONIC AUTHENTICATION TECHNIQUE AND PROCEDURE

Sl. No.	Description	Procedure
(1)	(2)	(3)
[2][1.	e-authentication technique using Aadhaar [3][or other] e-KYC services	Authentication of an electronic record by e-authentication Technique which shall be done by— (*a*) the applicable use of e-authentication, hash, and asymmetric crypto system techniques, leading to issuance of Digital Signature Certificate by Certifying Authority (*b*) a trusted third party service by subscriber's key pair-generation, storing of key pairs [4][* * *] and creation of digital signature provided that the trusted third party shall be offered by the certifying authority. The trusted third party shall send application form and certificate signing request to the Certifying Authority for issuing a Digital Signature Certificate to the subscriber. (*c*) Issuance of Digital Signature Certificate by Certifying Authority shall be based on e-authentication, particulars specified in Form C of Schedule IV of the Information Technology (Certifying Authorities) Rules, 2000, digitally signed verified information from Aadhaar [5][or other] e-KYC services and electronic consent of Digital Signature Certificate applicant. (*d*) The manner and requirements for e-authentication shall be as issued by the Controller from time to time. (*e*) The security procedure for creating the subscriber's key pair [6][and other e-KYC services] shall be in accordance with the e-authentication guidelines issued by the Controller. (*f*) The standards referred to in Rule 6 of the Information Technology (Certifying Authorities) Rules, 2000 shall be

1. Subs. by Act 10 of 2009, s. 49, (w.e.f. 27-10-2009).
2. Ins. by G.S.R. 61(E), dated 27-1-2015 (w.e.f. 28-1-2015).
3. Ins. by S.O. 1119(E), dated 1-3-2019.
4. The words "on hardware security module" omitted by G.S.R. 539(E), dt. 30-6-2015 (w.e.f. 6-7-2015).
5. Ins. by S.O. 1119(E), dated 1-3-2019.
6. Ins. by S.O. 1119(E), dated 1-3-2019.

		complied with, in so far as they relate to the certification function of public key of Digital Signature Certificate applicant. [1][(*g*) The manner in which the information is authenticated by means of digital signature shall comply with the manner and standards specified in Rules 3 to 12 of the Digital Signature (End entity) Rules, 2015 in so far as they relate to the creation, storage, and verification of Digital Signature]
[2][2.	e-authentication technique and procedure for creating and accessing subscriber's signature key facilitated by trusted third party	Authentication of an electronic record by e-authentication technique which shall be done by— (*a*) the applicable use of e-authentication, hash and asymmetric crypto system techniques leading to issuance of Digital Signature Certificate by Certifying Authority, provided that Certifying Authority shall ensure the subscriber identity verification, secure storage of the keys by trusted third party and subscriber's sole authentication control to the signature key. (*b*) Identity verification of Digital Signature Certificate applicant shall be in accordance with the Identity Verification Guidelines issued by Controller from time-to-time. (*c*) The requirement to operate as trusted third party shall be specified under e-authentication guidelines issued by the Controller. (*d*) a trusted third party shall (*i*) facilitate Identity verification of Digital Signature Certificate applicant; (*ii*) establish secure storage for subscriber to have sole control for creation and subsequent usage of subscriber's signature key by sole authentication of subscriber; (*iii*) facilitate key pair-generation, secure storage of subscriber's signature key and facilitate signature creation functions; (*vi*) facilitate the submission of DSC application form and certificate signing request to the Certifying Authority for issuing a Digital Signature Certificate to the DSC applicant, and

1. Subs. by G.S.R. 446(E), for "(g)" dated 27-4-2016 (w.e.f. 27-4-2016)."
2. Ins. by S.O. 3472(E), dated 29-9-2020.

	(*v*) facilitate revocation of Digital Signature Certificate and destruction of subscriber's signature key. (*e*) The manner and requirements for authentication and storage of keys shall be as issued by the Controller from time to time under e-authentication guidelines (*g*) The security procedure for creating the subscriber's key pair shall be in accordance with the e-authentication guidelines issued by the Controller. (*h*) The standards referred to in Rule 6 of the Information Technology (Certifying Authorities) Rules, 2000 shall be complied with, in so far as they relate to the certification function of public key of Digital Signature Certificate applicant. (*i*) The manner in which information is authenticated by means of digital signature shall comply with the manner and standards specified in Rule 3 to 12 of Digital Signature (End entity) Rules, 2015 in so far as they relate to the creation, storage and verification of Digital Signature.]

[*THE THIRD SCHEDULE.*] *Omitted by the Information Technology* (*Amendment*) *Act*, 2008 (10 of 2009), *s.* 50 (*w.e.f.* 27-10-2009).

[*THE FOURTH SCHEDULE*.] *Omitted by the Information Technology (Amendment) Act*, 2008 (10 of 2009), s. 50 (w.e.f. 27-10-2009).