

IT Act,2000 along with Amendments, Role of NCIIPC,CERT-IN, Govt. Notifications and Guidelines

VARUN KUMAR

Deputy Director

NPTI

Information Technology Act, 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 Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

Section 2 : Definitions

- "affixing digital 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 digital signature.
- 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.

- "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.
- "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.

Section – 3 : Electronic Records

- 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.
- "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.

Section - 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.

Section – 43 : Penalty for damage to computer, computer system, etc.

- Any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, access such system, shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Section - 48 : Appellate Tribunal

- Telecom Disputes Settlement and Appellate Tribunal (TDSAT).
- Established under section 14 of the Telecom Regulatory Authority of India Act, 1997.
- From the Commencement of Finance Act, 2017.

Section – 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.

Section – 66 : Hacking with computer system

- Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.
- Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.

Section – 67 : Publishing of information which is obscene in electronic form

- Punishment on first conviction with for a term which may extend to five years and with fine which may extend to one lakh rupees.
- And in the event of a second or subsequent conviction, imprisonment for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

Section – 70 : Protected System

- 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.
- "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.

- 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.
- The Central Government shall prescribe the information security practices and procedures for such protected system.

Section - 70 A : National Critical Information Infrastructure Protection Centre (NCIIPC)

- **National Nodal Agency** for all measures to protect nation's critical information infrastructure.
- Essentially protect and deliver advice that aims to reduce the vulnerabilities of critical information infrastructure, against cyber terrorism, cyber warfare and other threats.
- Identification of all critical information infrastructure elements for approval by the appropriate Government for notifying the same.

- Coordinating, sharing, monitoring, collecting, analysing and forecasting, national-level threats to critical information infrastructure for policy guidance, expertise-sharing and situational awareness for early warning or alerts.
- Assisting in the development of appropriate plans, adoption of standards, sharing of best practices and refinement of procurement processes in respect of protection of Critical Information Infrastructure.

- Evolving protection strategies, policies, vulnerability assessment and auditing methodologies and plans for their dissemination and implementation.
- Developing and executing national and international cooperation strategies.
- Undertaking research and development and allied activities.

- Issuing guidelines, advisories and vulnerability or audit notes etc. relating to protection of critical information infrastructure and practices, procedures, prevention and response in consultation with the stake holders, in close coordination with Indian Computer Emergency Response Team and other organisations working in the field or related fields.
- Call for information and give directions to the critical sectors or persons serving or having a critical impact on, in case of an event.

Section - 70B : Indian Computer Emergency Response Team (CERT-IN) to serve as national agency for incident response

- (a) collection, analysis and dissemination of information on cyber incidents;
- (b) forecast and alerts of cyber security incidents;
- (c) emergency measures for handling cyber security incidents;
- (d) coordination of cyber incidents response activities;
- (e) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
- (f) such other functions relating to cyber security as may be prescribed.

Section – 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.

Section - 79A : Central Government to notify Examiner of Electronic Evidence

- In exercise of the powers conferred by section 79A of the Information Technology Act 2000 (21 of 2000), the Central Government hereby notifies **Central Forensic Science Laboratory, Hyderabad under Directorate of Forensic Science Services, Ministry of Home Affairs as Examiner of Electronic Evidence within India with the following scope, namely:-**
 - (a) Computer (Media) Forensics excluding Floppy Disk Drive;
 - (b) Mobile Devices Forensics.

- In exercise of the powers conferred by section 79A of the Information Technology Act 2000 (21 of 2000), the Central Government hereby notifies **Directorate of Forensic Science, Gandhi Nagar (Gujarat), in the State of Gujarat as Examiner of Electronic Evidence within India with the following scope, namely:-**
 - (a) Computer (Media) Forensics;
 - (b) Mobile Devices Forensics.

- In exercise of the powers conferred by section 79A of the information Technology Act 2000 (21 of 2000) the Central Government hereby notifies **Cyber Forensic Laboratory, Air Force Cyber Group, New Delhi, as Examiner of Electronic Evidence within India, with the following scope, namely:-**
 - (a) Computer (Media) Forensics excluding Floppy Disk Drive;
 - (b) Mobile Devices Forensics.

- In exercise of the powers conferred by sub-section (1) of **section 69B** of the Information Technology Act, 2000 (21 of 2000), the Central Government, to enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country, hereby authorises the **Indian Computer Emergency Response Team**, an agency of the Central Government, appointed vide notification number S.O. 2689(E), dated the 27th October, 2009, **to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.**

References

- indiacode.nic.in
- meity.gov.in
- cert-in.org.in
- nciipc.gov.in
- https://cea.nic.in/wp-content/uploads/notification/2021/10/Guidelines_on_Cyber_Security_in_Power_Sector_2021-2.pdf