Legal Framework : Information Technology Act, 2000

Prafulla Kumar

pkumar@mit.gov.in

Information Technology Act, 2000

- Enacted in year 2000
- Promotion of e-governance & e-commerce
- Facilitator Act

Salient Features of the Act

- Legal recognition of electronic records and digital signature
- Various types of computer crimes defined and stringent penalties provided
- Appointment of Controller of Certifying Authorities and Adjudicating Officers
- Establishment of Cyber Appellate Tribunal

Provisions of the Act

(i) Extends to the whole of India (**Section 1**)

(ii) Authentication of electronic records (**Section 3**)

(iii) Legal Framework for affixing Digital signature by use of asymmetric crypto system and hash function (**Section 3**)

(iv) Legal recognition of electronic records (**Section 4**)

(v) Legal recognition of digital signatures (**Section 5**)

(vi) Retention of electronic record (**Section 7**)

(vii) Publication of Official Gazette in electronic form (**Section 8**)

(viii) Security procedure for electronic records and digital signature (**Sections 14, 15, 16**)

(ix) Licensing and Regulation of Certifying authorities for issuing digital signature certificates (**Sections 17-42**)

(x) Functions of Controller (**Section 18**)

Contd..

(xi) Appointment of Certifying Authorities and Controller of Certifying Authorities, including recognition of foreign Certifying Authorities (**Section 19**)

(xii) Controller to act as repository of all digital signature certificates (**Section 20**)

(xiii) Data Protection (**Sections 43 & 66**)

(xiv) Various types of computer crimes defined and stringent penalties provided under the Act (**Section 43 and Sections 66, 67, 72**)

(xv) Appointment of Adjudicating officer for holding inquiries under the Act (**Sections 46 & 47**)

(xvi) Establishment of Cyber Appellate Tribunal under the Act (**Sections 48-56**)

(xvii) Appeal from order of Adjudicating Officer to Cyber Appellate Tribunal and not to any Civil Court (**Section 57**)

(xviii) Appeal from order of Cyber Appellate Tribunal to High Court (**Section 62**)

(xix) Interception of information from computer to computer (Section 69)

(xx) Protected System (**Section 70**)

(xxi) Act to apply for offences or contraventions committed outside India (**Section 75**)

(xxii) Investigation of computer crimes to be investigated by officer at the DSP (Deputy Superintendent of Police) level

(xxiii) Network service providers not to be liable in certain cases (**Section 79**)

(xxiv) Power of police officers and other officers to enter into any public place and search and arrest without warrant (**Section 80**)

(xxv) Offences by the Companies (**Section 85**)

(xxvi) Constitution of Cyber Regulations Advisory Committee who will advice the Central Government and Controller (**Section 88**)

Information Technology (Amendment) Act, 2008

- Enacted on 5 Feb 2009
- Enforced on 27 Oct 2009

  - Data protection
  - Identity theft
  - Cheating by personation
  - Violation of privacy
  - Cyber terrorism
  - Child pornography
  - Spam
  - Technology neutrality
  - Multimember Appellate Tribunal

Computer Crime

- Computer crimes in the Act are classified into two categories :
    a) Civil offences
    b) Criminal offences

Civil offences

- Unauthorised copy or extract any data, database
- Unauthorised access & downloading files
- Introduction of virus
- Damage to computer system and computer network
- Disruption of computer, computer network
- Denial to authorised person to access computer
- Providing assistance to any person to facilitate unauthorised access to a computer
- Changing the service availed by a person to an account of another person by tampering and manipulation of other computer
- Failure to furnish information, return etc. to the Controller by certifying authorities
- Failure to protect data

Criminal offences

- Tampering with computer resource
- Electronic forgery
- Spam and offensive messages
- Stolen computer resource
- Identity theft
- Cheating by impersonation
- Violation of privacy, video voyerism
- Cyber terrorism
- Unauthorised access to protected system
- Confiscation of computer, network, etc.
- Publication of obscene information in electronic form
- Breach of confidentiality and privacy
- Publishing false electronic signature certificate

Security Provisions (1)

- Section 43A – Body corporate to implement reasonable security practices for data protection

- Rules notified
  - Body corporate to implement ISO27001 or other industry approved security practices to protect sensitive personal information
  - Sensitive personal information
    - Password
    - financial information such as Bank account, credit/debit card or other payment instrument details
    - physical, physiological and mental health condition
    - sexual orientation
    - medical records and history
    - Biometric information

Security Provisions (2) – Protected System

Section 70 – Protected System

- The appropriate Government may declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system
- Govt. to authorise persons to access these protected system
- 10 years imprisonment for unauthorised access

Security Provisions (3) – Critical Information Infrastructure

Section 70A : National nodal agency to protect critical information infrastructure

- Agency yet to be notified

Security Provisions (4) – CERT-IN

Section 70B : CERT-IN to serve as national nodal agency for incidence response

- Functions

  (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 whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;

- CERT-IN may call for information and give direction to the service providers, intermediaries, data centres, body corporate and any other person

Section 69

- **Power to issue directions for interception or monitoring or decryption of any information through any computer resource**
  - sovereignty or integrity of India
  - defence of India
  - security of the State
  - friendly relations with foreign States
  - public order
  - for preventing incitement to the commission of any cognizable offence relating to above
- **Rule - Procedure and Safeguards for Interception, Monitoring and Decryption of Information**
  - Union Home Secretary and Home Secretaries of States/UTs empowered to issue direction

Section 69A

- **Power to issue directions for blocking for public access of any information through any computer resource**
  - sovereignty or integrity of India
  - defence of India
  - security of the State
  - friendly relations with foreign States
  - public order
  - for preventing incitement to the commission of any cognizable offence relating to above

- **Rule - Procedure and Safeguards for Blocking for Access of Information by Public**
  - Group Coordinator, Cyberlaw, DIT empowered to issue direction as designated officer
  - Nodal officers nominated from Ministries/Depts and States to forward request for blocking

Section 69B

- Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security
  - to enhance cyber security
  - for identification, analysis and prevention of intrusion
  - spread of computer contaminant in the country

- Rule - Procedure and safeguard for Monitoring and Collecting Traffic Data or Information
  - Secretary, DIT empowered to issue direction

Rules notified on 27.10.2009

- Sec 52 - Cyber Appellate Tribunal (Salary, Allowances and Other Terms and Conditions of Service of Chairperson and Members)
- Sec 54 - Cyber Appellate Tribunal (Procedure for Investigation of Misbehaviour or Incapacity of Chairperson and Members)
- Sec 69 - Procedure and Safeguards for Interception, Monitoring and Decryption of Information
- Sec 69A - Procedure and Safeguards for Blocking for Access of Information by Public
- Sec 69B - Procedure and safeguard for Monitoring and Collecting Traffic Data or Information

Rules notified on 11.4.2011

- Sec 6A – Electronic service delivery
- Sec 43A – Sensitive personal information and Reasonable security practices and procedures
- Sec 79 – Intermediary Guidelines - Due diligence to be observed by intermediaries
- Sec 79 – Guidelines for cyber cafe

Thank You