Chapter 7

Cyber Law in India

7.1 Introduction

Mid 90’s saw an impetus in globalization and computerisation, with more and more nations computerizing their governance, and e-commerce seeing an enormous growth. With much of international trade being done through electronic communication and with email gaining momentum, an urgent and imminent need was felt for recognizing electronic records i.e. the data what is stored in a computer or an external storage attached thereto. The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on e-commerce in 1996. The General Assembly of United Nations (UN) passed a resolution on 30\textsuperscript{th} January 1997 inter alia, recommending all States in the UN to give favorable considerations to the said Model Law\textsuperscript{1}. It is against this background the Government of India enacted cyber law in form of Information Technology Act 2000, rules, regulations, guidelines etc to regulate cyberspace in India. The Act, rules, regulations, guidelines issued by government of India which constitute cyber law in India are enumerated as under\textsuperscript{2}:-

i) The Information Technology Act, 2000;

ii) The Information Technology (Certifying Authorities) Rules, 2000;

iii) The Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000;

iv) The Information Technology (Certifying Authority) Regulations, 2001;

\textsuperscript{1}J.Rattan, Cyber Laws & Information Technology, 63 (2011).

\textsuperscript{2}The Information Technology Act, 2000, Professional’s Bare Act with short notes, 1-206 (2013).

vi) The Information Technology (Other powers of Civil Courts vested in Cyber Appellate Tribunal) Rules 2003;

vii) The Information Technology (other standards) Rules 2003;

viii) The Information Technology (Qualification and Experience of Adjudicating Officers and manner of holding enquiry) Rules, 2003;

ix) The Cyber Regulations Appellate Tribunal (Salary Allowances and other terms and conditions of service of Presiding Officer) Rules, 2003;

x) Ministerial order on blocking of Websites

xi) The Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004;

xii) The Information Technology (Security Procedure) Rules, 2004;

xiii) The Information Technology Amendment Act, 2008;

xiv) Information Technology (Procedure and Safeguard for monitoring and Decryption of Information) Rules, 2009;

xv) Information Technology (Procedure and Safeguard for monitoring and collecting Traffic Data or Information) Rules, 2009;


xvii) Information Technology (Electronic Service Delivery) Rules, 2011.


 xx) Information Technology (Guidelines For Cyber Cafe) Rules, 2011.

xxi) Information Technology (Guidelines For Cyber Cafe) Rules, 2011.


7.2 The Genesis of Cyberspace legislation in India

The development of cyber regulation in India has an international perspective. General Assembly of the United Nations on 30th January 1997, adopted resolution A/RES/51/162 regarding the Model Law on Electronic Commerce which was earlier adopted by UNCITRAL in its twenty ninth session. It recommended that all states should give favorable consideration to the Model Law on Electronic Commerce when they enact or revise their laws. In view of the need for uniformity of the law applicable to paper based methods of communication and storage of information the Indian Parliament enacted in the Fifty First year of the Republic of India, an Act called the Information Technology Act, 2000. The Information Technology Act, 2000, was thus passed as the Act No.21 of 2000, got President Assent on 9 June and was made effective from 17 October 2000. The Act has captured the spirit of General Assembly’s recommendation and further amends the Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers’ Books Evidence Act 1891 and the Reserve Bank of India Act 1934.

Thereafter in exercise of powers conferred by various sections of the Information Technology Act, 2000 (21 of 2000), the Central Government or other authorities have made following rules and regulations:-

\[\text{\textsuperscript{1}}V. Sharma, \text{Information Technology: Law and Practice}, 3 (2012). \]
\[\text{\textsuperscript{2}}Y.Singh, \text{Cyber Laws}, 4 (2008). \]
• In exercise of powers conferred by section 87 of the Information Technology Act, 2000 (21 of 2000), the Central Government has made rules in form of “The Information Technology (Certifying Authorities) Rules, 2000” which contains 1-34 rules and Schedule I-V, regulating the application and other guidelines for certifying authorities. Schedule I provides for the form for Application for grant of License to be a certifying authority; Schedule II gives Information Technology security guidelines; Schedule III gives Security guidelines for certifying authorities; Schedule IV provides for Form A i.e. Application form for issue of Digital Certificates for subscriber of Government and banking sector and Form B provides for issue of Digital Signature Certificates for subscriber other than Government and banking sector and lastly Schedule V provides for Glossary.

• In exercise of powers conferred by section 87 of the Information Technology Act, 2000 (21 of 2000), the Central Government has made rules called as “The Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000” which contains rules 1-28 as well as two Forms.

• In exercise of powers conferred by clauses (c), (d), (e) and (g) of subsection (2) of section 89 of the Information Technology Act, 2000 (21 of 2000), the Controller after consultation with Cyber Regulations Advisory Committee and with previous approval of Central government has made regulations called as “The Information Technology (Certifying Authority) Regulations, 2001” containing rules 1-6 and a form.

• In exercise of powers conferred by clauses (s) of subsection (2) of section 87 read with sub-section (3) of section 54 of the Information Technology Act.

- As per powers conferred by clauses (v) of subsection (2) of section 87 read with clauses (g) of subsection (2) of section 58 of the Information Technology Act, 2000 (21 of 2000), the Central government has made rules namely “The Information Technology (Other powers of Civil Courts vested in Cyber Appellate Tribunal) Rules 2003” having rules 1-3.

- In exercise of powers conferred by clauses (g) of subsection (2) of section 87 read with subsection (2) of section 20 of the Information Technology Act, 2000 (21 of 2000), the Central government has made rules called as “The Information Technology (other standards) Rules 2003” containing 1-3 rules.

- Under clauses (p) and (q) of subsection (2) of section 87 of the Information Technology Act, 2000 (21 of 2000), the Central government has made rules known as “The Information Technology (Qualification and Experience of Adjudicating Officers and manner of holding enquiry) Rules, 2003” having 1-12 rules;

- In exercise of powers conferred by clauses (r) of subsection (2) of section 87 of the Information Technology Act, 2000 (21 of 2000), the Central government has made rules namely “The Cyber Regulations Appellate Tribunal (Salary Allowances and other terms and conditions of service of Presiding Officer) Rules, 2003” regulating terms and conditions of the service of the Presiding Officer.

---

10 The Information Technology Act, 2000, Professional’s Bare Act with short notes, 133 (2013).
12 The Information Technology Act, 2000, Professional’s Bare Act with short notes, 139-140 (2013).
Chapter 7  Cyber Law in India

- Vide Ministerial orders on blocking of Websites dt. 1 July 2003, Ministry of Communication and Information Technology has laid down the procedure for blocking of websites. As per orders the Indian Computer Emergency Response Team (CERT-IN) has to instruct the Department of Telecommunications to block the website after verifying the authenticity of the complaint. CERT-IN has been designated as the single authority for issuing instructions in the context of blocking websites for various reasons such as: Promoting hate content, slander or defamation of others, promoting gambling, racism, violence, terrorism and other such material, promoting pornography, including child pornography and violent sex or any other reason specified.

- As per powers conferred by clauses (b) and (c) of subsection (2) of section 87 read with subsection (1) and (2) of section 6 of the Information Technology Act, 2000 (21 of 2000), the Central government has made rules called as “The Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004” containing five rules.

- As per powers conferred by clauses (e) of subsection (2) of section 87 read with section 16 of the Information Technology Act, 2000 (21 of 2000), the Central government has made rules namely “The Information Technology (Security Procedure) Rules, 2004” containing four rules.

- The Information Technology Amendment Act, 2008;

The Implementation of Information Technology Act, 2000 brought into light multiple problems and led to growth of the perception that its enforcement was inadequate. An expert Committee chaired by Information Technology Department Secretary Brijesh Kumar was constituted in January 2005 to study

---

14 Ibid.
15 The Information Technology Act, 2000, Professional’s Bare Act with short notes, 141 (2013).
16 The Information Technology Act, 2000, Professional’s Bare Act with short notes, 142 (2013).
the proposed reforms of Information Technology Act, 2000. The committee was entrusted with responsibility of making necessary amendments to the Information Technology Act, 2000, to consider the feasibility of making the Act technology neutral and to recommend necessary amendments to that effect and to recommend suitable legislation for data protection under the Act. The Expert Committee recommended amendments to bring Information Technology Act, 2000 in line with global practices\(^\text{17}\).

As per the recommendation government agreed to create more provisions in the Act. On 15\(^\text{th}\) December 2006, Mr. Shakeel Ahmed, then Minister of State for communications introduced the Information Technology Amendment Bill, 2006 in Lok Sabha as an attempt to curb cyber crimes and provide for alternative technologies i.e. electronic signature. The bill was thus aimed at harmonizing Indian Law with the model law on electronic signatures adopted by the United Nations Commission on electronic signatures adopted by the United Nations Commission on International Trade Law in 2001. The 2006 bill was introduced in Rajya Sabha in December 2006. Thereafter the bill was referred to a joint parliamentary committee to discuss the same in detail and to make further suggestions, recommendations and comments to the bill. The standing committee heard the views of numerous individuals, experts associations, industrial representatives, CBI, Deptt. of Information Technology etc. However the 2006 bill was ultimately never passed by the parliament. The 2006 Bill was re-introduced in 2008 as the Information Technology (Amendment) Bill, 2008 (the 2008 bill). In the wake of tragic Nov. 26, 2008 terrorist attacks on Mumbai on December 22-23, 2008, both houses of Parliament passed the Information Technology (Amendment) Act, 2008 without any debate. The Bill received the ascent of President in early 2009. However, even after this, the Act did not come into force until October

26, 2009, when it was notified by the Central Government. The bill received the assent of the President on 5th February 2009 and was notified in Gazette of India on February 5, 2009.

- In exercise of powers conferred by clause (y) of subsection (2) of section 87 read with subsection (2) of section 69 of the Information Technology Act, 2000 (21 of 2000), the Central government has made rules called as “Information Technology (Procedure and Safeguard for monitoring and Decryption of Information) Rules, 2009” containing 1-25 rules;

- In exercise of powers conferred by clause (za) of subsection (2) of section 87 read with subsection (3) of section 69B of the Information Technology Act, 2000 (21 of 2000), the Central government has made rules called as “Information Technology (Procedure and Safeguard for monitoring and collecting Traffic Data or Information) Rules, 2009” having 11 rules;

- In exercise of powers conferred by clause (z) of subsection (2) of section 87 read with subsection (2) of section 69A of the Information Technology Act, 2000 (21 of 2000), the Central government has made rules called as “Information Technology (Procedure and Safeguard for Blocking Access of Information by Public) Rules, 2009” containing 16 rules;

- In exercise of powers conferred by clause (ca) of subsection (2) of section 87 read with subsection (2) of section 6A of the Information Technology Act, 2000 (21 of 2000), the Central government has made rules called as “Information Technology (Electronic Service Delivery) Rules, 2011” containing 9 rules.

---

19 The Information Technology Act, 2000, Professional’s Bare Act with short notes, 189-194 (2013).
20 The Information Technology Act, 2000, Professional’s Bare Act with short notes, (2013).
22 The Information Technology Act, 2000, Professional’s Bare Act with short notes, 183-188 (2013).
• In exercise of powers conferred by clause (ob) of subsection (2) of section 87 read with section 43A of the Information Technology Act, 2000 (21 of 2000), the Central government has made rules called as “Information Technology (Reasonable Security Practices and Procedures and sensitive personal data or Information) Rules, 2011” containing 8 rules.

• In exercise of powers conferred by clause (zg) of subsection (2) of section 87 read with subsection (2) of section 79 of the Information Technology Act, 2000 (21 of 2000), the Central government has made rules called as “Information Technology (Intermediaries guidelines) Rules, 2011” containing 3 rules.

• In exercise of powers conferred by clause (za) of subsection (2) of section 87 read with subsection (3) of section 69B of the Information Technology Act, 2000 (21 of 2000), the Central government has made rules called as Information Technology (Procedure And Safeguard For Monitoring And Collecting Traffic Data or Information) Rules, 2009 containing 11 rules.

• In exercise of the powers conferred by clause (ob) of sub-section (2) of section 87 read with section 43A of the Information Technology Act, 2000 (21 of 2000), the Central government has made rules called as Information Technology (Reasonable Security Practices And Procedures And Sensitive Personal Data Or Information) Rules, 2011 containing 8 rules.

• In exercise of the powers conferred by clause (zg) of sub-section (2) of section 87 read with sub-section (2) of section 79 of the Information

---

Technology Act, 2000 (21 of 2000), the Central Government has made rules called Information Technology (Guidelines For Cyber Cafe) Rules, 2011 containing 7 rules.

- In exercise of the powers conferred by clause (b) of sub-section (2) of Section 89 of the Information Technology Act, 2000 (21 of 2000), the Controller (after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government) has made rules called as Information Technology (Recognition Of Foreign Certifying Authorities Operating Under A Regulatory Authority) Regulations, 2013 containing 3 rules.

### 7.3 Reasons for enactment of Information Technology Act, 2000

There were both national as well as International reasons leading to the enactment of Information Technology Act, 2000.

- First reason was the increasing use of Information technology transactions in conducting business: Even International trade has switched from traditional paper based commerce to E-commerce. Therefore to boost up the business transactions there was need of law in form of the Act.

- Secondly, there was inadequacy of law while dealing with the Information technology itself: Changes brought about by the Information Technology has brought changes in the way we live. The courts through out the world were dealing with inadequacy of legal provisions in these areas and were coming up with inconsistent answers. So law was enacted to deal with these emerging problems.

---

29 J. Rattan, Cyber Laws & Information Technology, 63 (2011).
Cyber Law in India

7.4 Objectives of Information Technology Act, 2000

Preamble of the Act describes the objective of enactment as, “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.”

Thus the main objectives of Information Technology Act, 2000 were:-

- To provide for legal changes so as to facilitate e-commerce: The law of Evidence is traditionally based upon paper based records. Many legal provisions assume the existence of paper based records and documents which bear signatures. So existing laws were amended to switch paper based commerce to e-commerce.

- To bring legal provisions in India in tune with Model Law on Electronic Commerce adopted by UNCITRAL in 1996 so as to provide for equal legal

---

31 J. Rattan, Cyber Laws & Information Technology, 64 (2011).
Chapter 7 Cyber Law in India

treatment of users of electronic communication and paper based communication.

- To provide for legal recognition of electronic records and digital signatures.

- To enable conclusion of contacts and creation of rights and obligations through the electronic medium.

- To provide for a regulatory regime to supervise the certifying authorities issuing digital signature certificates.

- To prevent the possible misuse arising out of transactions and other dealings concluded over the electronic medium.

- To create civil and criminal liabilities for contravention of provisions of the proposed legislation.

- To facilitate electronic governance32.

7.5 Need of Information Technology Amendment Act, 2008

Being the first legislation in the nation on technology, computers and ecommerce and e-communication, the Information Technology Act, 2000 was the subject of extensive debates, elaborate reviews and detailed criticisms, with one arm of the industry criticizing some sections of the Act to be draconian and other stating it is too diluted and lenient. Due to various shortcomings in Information Technology Act, 2000 as enumerated below, a need was felt for its amendment33:-

32 Ibid.
Cyber Law in India

Chapter 7

Cyber crimes were increased manifold despite the Act. Need was felt for criminalisation of offences in cyberspace.

- There was lack of prosecution which was major factor for call of amendment.

- The rapid increasing in the publishing of sexually explicit materials in electronic form, video voyeurism etc.

- Much needed focus was not given to the issue of cyber terrorism. There was not a single provision in the whole act even when the country was battling against the heinous crime of terrorism during the Mumbai attacks of 26 November, 2008.

- A need was felt for technology neutral law.

After considerable administrative procedures, the consolidated amendment called the Information Technology Amendment Act 2008 was placed in the Parliament and passed without much debate.

7.6 Objectives of Information Technology Amendment Act, 2008 (ITAA)

The objectives of the Amendment Act, was multifold. It aimed to combat cyber terrorism, e-commerce fraud such as impersonation/ phishing and identity theft, the rapid increasing in the publishing of sexually explicit materials in electronic form, video voyeurism and leakage of data by the intermediaries. The amendments had far reaching consequences having as one of the main objectives to make the Information Technology Act as a self enabling piece of legislation which
will be capable of helping the law enforcement agencies to curb cyber crimes which has increased manifold. Some of the notable features of the ITAA are as follows:

- Focusing on data privacy
- Focusing on Information Security
- Defining cyber café
- Making digital signature technology neutral
- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries
- Recognising the role of Indian Computer Emergency Response Team
- Inclusion of some additional cyber crimes like child pornography and cyber terrorism authorizing an Inspector to investigate cyber offences (as against the DSP earlier).

### 7.7 Overview of amended Information Technology Act, 2000

The amended Act totally has 13 chapters and 90 sections and two schedules.

**Chapter I Preliminary (Section 1, 2)**

The Chapter provides for short title, extent, commencement and application; and definitions. Amendments have been made by The Information Technology (Amendment) Act, 2008 in sections 1, 2. New subsection (ha) has been inserted in section 2 by The Information Technology (Amendment) Act, 2008. The section

---

34Ibid, at 72.
Chapter 7 Cyber Law in India

1 of the Act provides for scope and extent of application of the Act. According to subsection (2) Section 1, the Act extends to the whole of India (including Jammu and Kashmir). In order to extend the provisions of the Act to the State of Jammu and Kashmir, Article 253 of the constitution has been used.

“Article 253 Legislation for giving effect to international agreements:- Notwithstanding anything in the forgoing provisions of this chapter, Parliament has power to make any law for the whole or any part of the territory of India for implementing any treaty, agreement, or convention with any other country or countries or any decision made at any international conference, association or body.”


In addition the Act also has extra territorial jurisdiction. As per section 75(1) of the Act, “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”. Thus it gives extraterritorial jurisdictional power to the Nation over the wrong doer, irrespective of his nationality, domicile, status, etc. The need for such provision is driven by the borderless nature of the internet.

41 Ibid, at 5.

The amended section 2 lays down statutory standards in form of definitions. These definitions bring in clarity and thereby help in understanding the underlying concepts and legislature intent. These articulate legal scope of certain important terms and concepts of Information technology and its applicants. The act provides definition of terms such as:-(a) “access”, (b) “addressee”, (c) “adjudicating officer”, (d) “affixing electronic signature”, (e) “appropriate Government”, (f) “asymmetric crypto system”, (g) “Certifying Authority”, (h) “certification practice statement”,

41 Ibid, at 5.
**Chapter II  Digital Signature and electronic signature (Section 3, 3A)**

The Chapter provides for authentication of electronic records and electronic signature. It provides for legal recognition to electronic records and electronic signatures to facilitate as well as safeguard electronic transactions in the electronic medium and their use in government offices and its agencies. The section 3 enumerates the whole process of digital signature creation and its verification. Amendments have been made by The Information Technology (Amendment) Act, 2008 in heading of Chapter II\(^{44}\). New subsection 3A has been added by The Information Technology (Amendment) Act, 2008\(^ {45}\). The section 3A advocates authentication of any electronic record by any such electronic signature or electronic authentication technique. With amendment “technology neutrality” has been introduced and a subscriber has a choice to adopt or use any electronic signatures.

**Chapter III  Electronic Governance (Section 4-10, 6A, 7A, 10A)**

---

\(^{42}\) The Information Technology Act, 2000, Section 2, Universal’s Bare Act with short notes, 4-8 (2013).

\(^{43}\) The Information Technology Act, 2000, Ibid, 8 (2013).

\(^{44}\) The Information Technology (Amendment) Act, 2008, Section 5, Ibid, III (2010).

\(^{45}\) The Information Technology (Amendment) Act, 2008, Section 6, Ibid, III (2010).

Chapter 7 Cyber Law in India

The chapter is meant to facilitate electronic filing of documents with the government agencies and to promote efficient delivery of government services by means of reliable electronic records. It deals with recognition of electronic records. The Chapter provides for legal recognition of electronic records, legal recognition of electronic signatures; use of electronic records and electronic signatures in government and its agencies; delivery of services for service provider; retention of electronic records; audit of documents etc. maintained in electronic form; publication of rule, regulation, etc., in electronic gazette; sections 6, 7 and 8 not to confer right to insist document should be accepted in electronic form; power to make rules by central government in respect of electronic signature; validity of contracts formed through electronic means. Amendments have been made by The Information Technology (Amendment) Act, 2008 in section 10. New sections has been inserted in form of new section 6A, 7A, 10A by The Information Technology (Amendment) Act, 2008. The sections in this chapter make electronic forms as a functional equivalent of writing or typewritten or printed form. Electronic signature as a functional equivalent of hand written signature; calls for decentralization of e-governance. It provides for private participation in delivery of e-government services, considers official gazette at par with electronic gazette. New section 10 A recognizes legal binding character of online contracts.

Chapter IV Attribution, Acknowledgement and dispatch of electronic records (Section 11-13)

The Chapter provides for attribution of electronic records, acknowledgement of receipts; time and place of dispatch and receipt of electronic record. The Act identifies three parties to electronic transmission:- the originator, the intermediary

---

Chapter 7 Cyber Law in India

and the addressee. It grants legal recognition to communication process involving computer, computer system and computer network by identifying attribution, acknowledgement and dispatch of electronic records as key statutory provisions. Amendments have been made by The Information Technology (Amendment) Act, 2008 in sections 12.

Chapter V Secure electronic records and secure electronic signatures (Section 14-16)

The Chapter provides for secure electronic record; secure electronic signatures; security procedures and practices. Amendments have been made by The Information Technology (Amendment) Act, 2008 in sections 15 and 16. Only a secure system leads to secure transactions. The section advocates application of any security procedure to make electronic record secure. It lays down security features for subscriber specific secure electronic signatures which includes digital signature as well. It gives liberty central government to adopt and assimilate any technology for providing a regime of secure electronic record and electronic signature.

Chapter VI Regulation of certifying authorities (Section 17-19, 21-34)

The Chapter provides for appointment of Controller and other officers; functions of Controller; recognition of foreign certifying authorities; license to issue Electronic Signature certificates; application for license; renewal of license; procedure for grant or rejection of licence; suspension of licence; notice of suspension or revocation of licence; power to delegate; power to investigate contraventions; access to computer and data; certifying authority to follow certain procedures; certifying authority to ensure compliance of the Act, etc.; display of

---

licence; surrender of licence; disclosure. Amendments have been made by the Information Technology (Amendment) Act, 2008 in sections 17-19, 21, 25, 30, 3455; 2956 New subsection has been inserted in form of (ca) and (cb) has been inserted in section 3057 by The Information Technology (Amendment) Act, 2008. The amendment act provides detailed provision for the Controller of certifying authorities to regulate certifying authorities. Furthermore, The Information Technology (Certifying Authorities) Rules, 2000; The Information Technology (Certifying Authority) Regulations, 2001 provided guidelines for certifying authorities. The office of Certifying Authority has three functional departments a) Technical; b) Finance and legal; c) Investigation. It is competent to resolve disputes between certifying authorities and subscribers. The act establishes the National Repository of digital signatures. Section 20 whereby Controller to act as repository has been repealed58.

Chapter VII Electronic Signature Certificates (Section 35-39)59

The Chapter provides for certifying authority to issue electronic signature certificate; representation upon issuance of digital signature certificate; suspension of digital signature certificate revocation of digital signature certificate; notice of suspension or revocation. Amendments have been made by The Information Technology (Amendment) Act, 2008 in section 3560. New subsection has been inserted in form of (ca) and (cb) has been inserted in section 36 by The Information

60 The Information Technology (Amendment) Act, 2008, Section 2 and Section 17, Ibid, I and V (2010).
Chapter 7

Cyber Law in India

Technology (Amendment) Act, 2008. The chapter is about the life cycle of digital signatures.

Chapter VIII Duties of Subscribers (Section 40-42, 40A)

The Chapter provides for generating key pair; duties of the subscriber of Electronic signature certificate; control of private key. The sections 40-42 provides for duties of subscriber under the Act. A new section 40 A has been inserted which provides for duties of subscriber of Electronic Signature certificate. By accepting a certificate a subscriber is bound by following obligations:

a) Generating the key pair on a secure medium as specified in certifying authority.

b) Providing correct information without any errors, omissions or misrepresentations as in the application.

c) Using the certificate only for the authorized purposes as specified in the certifying authority.

d) Demonstrate acceptance of digital signature certificate generated by the certifying authority when all information contained in the digital signature certificate as applied for and validated are true.

e) Protecting the private key in a pure medium.

f) Notifying immediately any change in the information included in the subscribers digital signature certificate that shall make the information in the certificate inaccurate or misleading.

g) Notifying immediately any suspected or actual compromise of the subscriber’s private key.

---

h) Terminating the use of certificate if the information in the certificate is found to be inaccurate and misleading.

**Chapter IX Penalties, Compensation and adjudication (Section 43-47, 43A)**

The Chapter provides for penalty and compensation for damage to computer, computer system, etc; compensation for failure to protect data; penalty for failure to furnish information, return, etc.; residuary penalty; power to adjudicate; factors to be taken into account by the adjudicating officer. The chapter is about cyber contraventions as it deals primarily with unauthorized access to computer, computer system or computer network. A new section has been inserted in form of 43A by The Information Technology (Amendment) Act, 2008. Two additional offences have been added in section 43 for which compensation is available. The defaulter has to make good of losses. Prior to amendment a person who commit any of offences was liable to pay damages by way of compensation to the person affected which was capped on amount of Rs 10 million (Rs 1Croc). The amendments have removed the 10 million cap on compensation.

**Chapter X The Cyber Appellate Tribunal (Section 48-64, 52 A-D)**

The Chapter provides for establishment of Cyber appellate tribunal; composition of Cyber appellate tribunal; qualifications for appointment as Chairperson and members of Cyber appellate tribunal; term of office, conditions; of service etc., of chairperson and members; salary, allowances and other terms and conditions of service of chairperson and members; powers of superintendence, direction, etc; distribution of business among benches; power of chairperson to transfer cases; decision by majority; filling up of vacancies; resignation and removal; orders constituting Appellate Tribunal to be final and not to invalidate its

---

Chapter 7 Cyber Law in India

proceedings; staff of the Cyber appellate tribunal; appeal to Cyber appellate tribunal; procedure and powers of the Cyber appellate tribunal; right to legal representation; limitation; civil court not to have jurisdiction; appeal to high court; compounding of contraventions; Recovery of penalty and compensation. Amendments have been made by The Information Technology (Amendment) Act, 2008 in the title of the chapter68, section 4869; sections 49-5270; 53-5671; 6472 of the old act.

Chapter XI Offences (Section 65-78; 66A-F; 67 A-C; 69 A, B; 70 A,B; 72A; 77A,B)73

The Chapter provides for tampering with computer source document; computer related offences; Punishment for sending offensive massage through communication, service, etc.; Punishment for dishonestly receiving stolen computer resource or communication device; Punishment for identity theft; Punishment for cheating by impersonation by using computer resource; Punishment for violation of privacy; Punishment for cyber terrorism; Punishment for publishing or transmitting obscene material in electronic form; Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form; Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form; preservation and retention of information by intermediaries; power of controller to give directions; power to issue directions for interception or monitoring or decryption of any information through any computer resource; Power to issue directions for blocking for public access of any information through any computer resource; Power to authorize to monitor and collect traffic data or

68 The Information Technology (Amendment) Act, 2008, Section 23 (c), Ibid, VI (2010).
70 The Information Technology (Amendment) Act, 2000, Section 26, Ibid, VIII (2010).
information through any computer resource for cyber security; protected system; National nodal agency; Indian Computer Emergency response team to serve as national agency for incident response; penalty for misrepresentation; penalty for breach of confidentiality and privacy; punishment for disclosure of information in breach of lawful contract; Penalty for misrepresentation; penalty for breach of confidentiality and privacy; punishment for disclosure of information in breach of lawful contract; penalty for publishing Electronic Signature Certificate false in certain particulars; publication for fraudulent purpose; act to apply for offence or contravention committed outside India; confiscation; compensation, penalties or confiscation not to interfere with other punishment; compounding of offences; offences with three imprisonment to be bailable; power to investigate offences. Amendments have been made by The Information Technology (Amendment) Act, 2008 in section 66-70; 71, 73, 74; 77 of old act. New sections has been inserted in form of 66A-F, 67 A-C; 69 A, B; 70 A,B; 72A; 77A,B. The amendment act introduced a series of new offences such as sending messages through communication services (section 66A); dishonestly receiving stolen computer resources (section 66B); identity theft (section 66C); Impersonation-phishing (section 66D); violation of privacy (section 66E). The notorious crime of phishing is dealt for the first time in the amended IT Act. The amendment has created a new offence of cyber terrorism which is punishable with life imprisonment (section 66F). Prior to amendment the Controller can intercept any information transmitted through any computer resource for specific reasons. Following amendments an officer specially authorized by the central government or

a state government may order any government agency not only to intercept but also monitor /decrypt any information transmitted. In addition to adding the powers for monitoring and decryption, the amendment also empowered government to issue directions for blocking public access to any information through any resource (section 69 A). Government can authorize monitoring and collection of traffic data or information through any computer resource for cyber security (section 69B). The amended act provides for designation of a national nodal agency for cyber security under section 70 A. Government can now declare any computer resource which directly or indirectly affects the facility of critical information infrastructure to be a protected system. Critical information infrastructure means any computer resource, the incapacitation or destruction of which shall have debilitating impact on national security, economy, public health or safety.

Chapter XII Intermediaries not to be liable in certain cases (Section 79)\(^8^2\)

The Chapter provides for exemption from liability of intermediary in certain cases. The chapter has been substituted by new chapter XII as provided in the section 40 of The Information Technology (Amendment) Act, 2008 for the older Act. The substituted section provides an exemption from liability to an Internet service provider (ISP) which functions as a passive service provider and not as a person who creates or modifies the content. However the exemption cannot be availed if ISP has conspired or abetted the unlawful act or, upon receiving actual knowledge, or on being notified by the appropriate government or its agency that any information in its system is being used to commit an unlawful act, doesn’t expediously remove or disable access to that material\(^8^3\).

Chapter XIIA Examiner of electronic evidence (Section 79A)

\(^8^2\) The Information Technology Act, 2000, Ibid, 44 (2013).
\(^8^3\) The Information Technology (Amendment) Act, 2008, Section 40, Ibid, XVI (2010).
Chapter 7 Cyber Law in India

The Chapter provides for Central government to notify Examiner of Electronic Evidence.\footnote{The Information Technology Act, 2000, Ibid, 45 (2013).}

Chapter XIII Miscellaneous (Section 80-90; 81A, 84 A-C)\footnote{The Information Technology Act, 2000, Ibid, 45-53 (2013).}

The Chapter provides for Power of police officer and other officer to enter, search etc.; Act to have overriding effect; Application of the Act to electronic cheque and truncated cheque; Chairperson, Members, Officers, and employees to be public servants; power to give directions; power to give directions; protection of action taken in good faith; modes or methods for encryption; punishment for abetment of offences; punishment for attempt to commit offences; offences by companies; removal of difficulties; power of central government to make rules; Constitution of Advisory Committee; Power of Controller to make regulations; power of state government to make rules. The amendment Act has amended sections 80\footnote{The Information Technology (Amendment) Act, 2008, Section 41, Ibid, XVII (2010).}, 81\footnote{The Information Technology (Amendment) Act, 2008, Section 42, Ibid, XVII (2010).}, 82\footnote{The Information Technology (Amendment) Act, 2008, Section 43, Ibid, XVII (2010).}, 84\footnote{The Information Technology (Amendment) Act, 2008, Section 44, Ibid, XVII (2010).}, 87, 90, 91; inserted new sections 84A-C\footnote{The Information Technology (Amendment) Act, 2008, Section 45, Ibid, XVII (2010).}; omitted sections 91-94.\footnote{The Information Technology (Amendment) Act, 2008, Section 46, Ibid, XVII (2010).} Now powers to investigate, enter public place, search and arrest under this Act can be exercised by any police officer not below the rank of inspector. The Part III of The Information Technology (Amendment) Act, 2008 provides for amendment (of sections 4, 40, 118, 119, 464) of Indian Penal Code\footnote{The Information Technology (Amendment) Act, 2008, Section 51, Ibid, XIX (2010).} and (of sections 3, 45A, 47A, 67A, 85A-C, 90A) of Indian Evidence Act, 1872.\footnote{The Information Technology (Amendment) Act, 2008, Section 52, Ibid, XX (2010).} Section 81 of the amended act now provides that nothing contained in Information Technology Act, 2000 shall
restrict any person from exercising any right conferred under the Copyright Act, 1957 or the patent act 1970.

**Schedules**

There has been substitution of new schedules for First Schedule and Second Schedule. The First Schedule contains Documents or transactions to which the Act shall not apply and The Second Schedule provides for Electronic Signature or Electronic Authentication Technique and Procedure. The Third Schedule and Fourth Schedule to the Principle Act have been omitted.

7.8 Importance/ Advantages of Information Technology, 2000

The Information Technology, 2000 recognized for the first time in Indian law the validity of electronic signature and paved the way for e-filings and electronic commerce to grow in India. The Information Technology, 2000 was intended to give a fillip to the growth and usage of computers, internet and software in the country as well as to provide a legal framework for the promotion of e-commerce. The legal recognition of electronic records and electronic signatures and the methods of authentication of legal records introduced by the Information Technology, 2000, ushered in the age of e-fillings and e-records in India. The various advantages of the amended enactments are:-

1. **Enactment provides legal recognition to for some level of data protection in India for the first time**

The Act provides for some level of data protection in India for the first time. Service providers are now subject to imprisonment and fine for disclosing personal

---

information in violation of contractual obligations. Moreover the disclosure of “sensitive personal data” makes the perpetrator liable to pay damages as compensation. A new civil provision prescribes damages for an entity that does not use “reasonable security practices and procedures” while handling “sensitive personal data or information” thereby resulting in wrongful loss or wrongful gain to any person. Criminal punishment is prescribed for a person if: (a) he discloses sensitive personal information; (b) does so without the consent of the person or in breach of the relevant contract; and (c) with an intention of, or knowing that the disclosure would cause wrongful loss or gain.

2. Enactment provides legal recognition to documents that are retained in electronic form for the first time

It accord legal recognition to record, files or documents that are retained in electronic form. It includes into its ambit legal recognition of electronic records and digital signatures, authentication and retention of electronic records. It enables public institutions and government departments to issue electronic licenses and thus pave way for electronic governance.

3. Enactment establishes the legal framework which will provide for setting up of a public key infrastructure.

The Act provides for appointment, power and functions of the Controller of Certifying authorities and also duties for the subscriber have been provided. It introduces some form of control over the use of encryption for communication in India. The Act takes into consideration the system of ‘key pair encryption’ for the

99 Ibid, at 189.
100 Ibid.
recording and authentication of digital signatures. The Act provides specifically, that the public key is to be deposited with a certifying authority.\(^\text{101}\)

4. **Enactment provides the legal framework for establishing special tribunal.**

   It provides for establishment of Cyber Appellate Tribunal. In leading cases Hon’ble Supreme Court has decided that legislature has the power to create Tribunals with reference to specific enactments including companies Act but such constitution must not be violative of the doctrine of separation of powers and independence of the Judiciary which are parts of the basic structure of the Constitution (Union of India vs. R.Gandhi, President, Madras Bar Association)\(^\text{102}\).

5. **Enactment conferred power on the police to prevent the commission of offences under the Act**

   The IT Act has conferred power on the police to prevent the commission of offences under the Act. A police officer can enter a cyber café on his/her regular rounds just to check if offences under the Act are being committed. Apart from this some state governments have also initiated moves to regulate the operation of cyber cafés including their registration and maintenance of records regarding accessing of computers at such places. Major change that the new amendments have done is that cyber crimes in India shall now be investigated not by a Deputy Superintendent of Police but shall now be done by a low level police inspector\(^\text{103}\).

6. **Enactment criminalises various kinds of offensive behaviour in the cyberspace**

   The Act criminalises various kinds of offensive behaviour in the cyberspace. With the introduction of new offences under the Amendment Act, there are a host of

---

\(^{101}\) Ibid.

\(^{102}\) Union of India vs. R.Gandhi, (2010), SC MANU 0378.

\(^{103}\) P. Duggal, The new Information Technology Act Amendments, 4 (2009).
differentiated offences that have criminal penalties attached to them. The new offences range from sending of offensive messages, hardware and password theft to voyeurism, pornography and cyber terrorism, which have been inserted through amendments to Section 66 and 67. In addition, the civil wrongs set out under S.43 of the IT Act have now been qualified as criminal offences under the ITAA 2008, if committed dishonestly or fraudulently. Newly introduced offences includes\textsuperscript{104}.

\textit{Sending of Offensive Messages (S.66A)}\textsuperscript{105}

The introduction of S.66A to the IT Act, 2000 unarguably expands the scope of the act to deal with instances of cyber stalking, threat mails, spam and phishing mails, with an attempt to strengthen the law and circumscribe aspects of unlawful cyber conduct that were left untouched under the old legislation.

\textit{Theft of Computer Resource (S.66B)}\textsuperscript{106}

The introduction of S.66B has lead to criminalisation of stolen information transmission and retention, which will have a crucial deterrent effect attached to illegitimate or illegal data exchanges which is the primary focus of the IT Act itself.

\textit{Identity Theft and Impersonation (S. 66C and S. 66D)}\textsuperscript{107}

While S.66C deals with deceitful use of passwords, electronic signatures and the like, S.66D involves use of a ‘communication device’ or ‘computer resource’ as a means of impersonation, which in effect, entails the use of computers, cellphones for fraudulent purposes.

\textit{Voyeurism (S. 66E)}\textsuperscript{108}

The Act prescribes imprisonment for a period of three years for the fine not

\textsuperscript{104}A.Viswanathan, Cyber Law: Indian & International Perspectives on key topics including Data Security, E-commerce, Cloud Computing and Cyber Crimes, 29 (2012).
\textsuperscript{105}The Information Technology (Amendment) Act, 2008 Universal’s Bare Act with short notes, IX (2010).
\textsuperscript{106}The Information Technology (Amendment) Act, 2008 Ibid, X (2010).
\textsuperscript{107}The Information Technology (Amendment) Act, 2008, Ibid, X (2010).
Chapter 7  

Cyber Law in India

exceeding rupees two lakh for the Intentional capturing, publishing or transmitting of an image of the private area of any person

**Sexually Explicit Content and Child Pornography (S.67A and S.67B)**\(^{109}\)

There are additional punishments for engaging in child pornography. The punishments are higher for second and subsequent acts.

**Cyber Terrorism (S.66F)**\(^{110}\)

The Act also makes cyber terrorism an offence. This covers accessing or denying access to computer resources or introducing computer contaminants with the intention of ‘threatening the unity, integrity, security or sovereignty of India or strike terror in the people’ or accessing any computer resource which is restricted owing to reasons of security of India. It is the first legislation which is preoccupied with preventing cyber terrorism and cyber crime.

7. **Enactment has introduced concept of technology neutrality.**

The recent amendments of the Information Technology Act, 2000 promise to take electronic commerce to the next level by introducing concept of technology neutrality. It moves away from digital signatures/asymmetric cryptography and instead adopts technology neutral “electronic signatures”. The result will certainly make electronic commerce a much more pervasive way of transacting in years to come\(^{111}\).

7.9 **Limitations / Disadvantages of Information Technology Act, 2000**

The Act has few advantages but many drawbacks. Thus, it cannot be considered as the right material to accomplish the task of giving a boost to electronic

---


\(^{110}\) The Information Technology (Amendment) Act, 2008, Universal’s Bare Act with short notes, X (2010).

deals and clearing institutional barriers that e-commerce currently faces. The Act suffers from “One Act Syndrome”\textsuperscript{112}. It cannot answer all the questions. The various pitfalls in IT Act are described as under:-

\textit{Enactment is Vague and Lack clarity}

The language in the enactment is ambiguous and lacks clarity. Some of the provisions are quite troubling. The language is very broad and is capable of misuse. Though the first legislation addressing the incidence of cyber terrorism, it falls drastically short in terms of comprehensiveness, clarity and particularity. Several of the words used in the section such as ‘inconvenience’, ‘annoyance’, ‘obstruction’ or ‘ill will’ are not defined either in the primary or Amendment Act, leading to uncertainty in interpretation and increasing the possibility of misuse of the provision, a possible reason for some statutes drafting defences to the charge, within the section itself\textsuperscript{113}.

\textit{Could not achieve objective of data protection}

By attempting to fit provisions for data protection into The IT Act, comprehensive data protection cannot be achieved. The IT Act concerning data protection makes it clear that while the industry and the legislators are familiar with terms like ‘personal data’, ‘sensitive personal data’, ‘personal privacy’, ‘data privacy’ and so on, there is a lot of ambiguity as to how these terms should be interpreted for effective data protection in India. Without an in-depth understanding of the industry’s all efforts will remain mere efforts and could not meet the current need for a comprehensive legal framework\textsuperscript{114}.

\textsuperscript{112}V. Sharma, Information Technology: Law and Practice, 355 (2012).
\textsuperscript{113}Ibid, at 352-355.
Limited jurisdiction of adjudicating officer or the Cyber Appellate Tribunal constituted under this Act.

The tribunal is one of limited jurisdiction. Nature of jurisdiction conferred upon the adjudicating authority under the IT Act is extremely restricted; he is not a special tribunal empowered to decide upon all causes as between parties, who have disputes including those under the Act. Necessarily, in such case, if there are claims or causes forming part of the same cause of action, or series of acts, Constituting causes of action, which are not covered by the Act, or are violation of other enactments, or infringe other legal obligations, the adjudicating officer would have no power to decide them. In majority of the cases it has been decided that even if some of the causes pleaded by the suit are seemingly barred, yet Court should not reject the plaint on the ground of the relief being barred in law; that can be gauged only at the final stage, having regard to the composite nature of the claims in the pleadings thus greatly limiting the jurisdiction of adjudicating officer or the Cyber Appellate Tribunal constituted under this Act (Roop Lal Sathi vs. Nachhatter Singh Gill115; Raptakos Brett & Co. Ltd. vs. Ganesh Property116).

Does not contain adequate provisions for benefit of victims

In certain offences such as Voyeurism the Amendment Act does not make mention of compensation to the victim despite explicit recommendation by the Expert Committee117.

Difficulty in enforcement

Although the act has articulated a series of new offences however it is unfortunate that the enforceability of these provisions have been undermined by

making offences subject to three years imprisonment a bailable offence. By amendment vast majority of offences under Act has been made bailable thus severely undermining the deterrent effect of the Act. The fertile liberal treatment meted out to cyber criminals, by the new IT Act amendments, facilitating the environment where they can tamper with, destroy and delete electronic evidence, is likely to make a mockery of the process of law and would put the law enforcement agencies under extreme pressure, apart from exposing corporates to undesirable headaches118.

**Does not define scope of offences**

Doctrine of Void for Vagueness, indigenous to the American legal system, having been derived from the due process clauses of the Fifth and Fourteenth Amendments to the U.S. Constitution. The basis of the doctrine is uncertainty and lack of specificity and the philosophy underlying the principle appears to be quite simple - no one may be required at peril of life, liberty, or property to speculate as to the meaning of a penal law. Thus, if it is found that a reasonably prudent man is unable to determine by himself the nature of the punishment, the prohibited conduct as envisaged under the statute, and what class of persons the law seeks to regulate, for lack of definiteness, the law may be regarded as void for vagueness. The application rests with the courts119.

The IT Act poses various problems in light of bad drafting and lack of understanding in this area. Apart from being just poorly drafted, it is also vague and criminalizes offences without defining the scope of the activity that could classify as criminal. The inadequacies of the enactment and the resultant realistically anticipated problems reinforce the notion that it cannot be left open to broad

---

118 Ibid, at 5.
119 V. Sharma, Information Technology: Law and Practice, 244 (2012).
interpretations. More amendments are necessary in other legislations also to provide adequate framework for the regulation of cyberspace\textsuperscript{120}.

\textbf{Lack of awareness}

There is no serious provision for creating awareness and putting such initiatives in place in the Act. The government or the investigating agencies like the Police department (whose job has been made comparatively easier and focused, thanks to the passing of the IT Act), have taken any serious step to create public awareness about the provisions in these legislations, which is absolutely essential considering the fact that this is a new area and technology has to be learnt by all the stake-holders like the judicial officers, legal professionals, litigant public and the public or users at large\textsuperscript{121}. Unless serious steps are taken on the issue, no matter how effective legal measures are taken the result will not be as good as it can be with wide and effective awareness of all the issues involved in cyberspace and cyber crime\textsuperscript{122}.

\textbf{Has potential to cause digital divide}

The act has potential to cause digital divide with low computer penetration, poor internet connectivity and infrastructure. It has tendency to divide Indian population into digital haves and have nots\textsuperscript{123}.

\textbf{Non coverage of major issues}

While there is much legislation to regulate cyberspace in not only Western countries but also some smaller nations in the East as discussed in previous chapter, India has one legislation only to regulate cyberspace -- the ITA and ITAA. Hence it

\textsuperscript{120} R. Singh, G.Singh, Cyberspace and the Law-Issues and Challenges, 84 (2004).
\textsuperscript{121} Available at www.iibf.org.in/.../Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf.
\textsuperscript{123} V. Sharma, Information Technology: Law and Practice, 245 (2012).
is quite natural that many issues on cyber crimes and many crimes per se are left uncovered.

Information Technology Act, 2000 is silent about the liability under Law of Tort, if arises in cyberspace, therefore wider interpretation should be given to the existing law of tort to answer such questions. Various taxation difficulties in E-Commerce still remain unanswered. The Act is also silent about the regulation of the payment gateways\(^\text{124}\).

### 7.10 Case Laws under Information Technology Act, 2000

Few of important case laws decided under the act are described below:-

- Certain content was made available on www.facebook.com., google etc., which was per-se inflammatory, unacceptable by any set of community standards; seeks to create enmity, hatred and communal violence against amongst any religious communities; in demeaning, degrading and obscene and will corrupt minds and will affect the religious sentiments of public at large. However it was held that intermediately shall not be liable for any third party information / or communication link made available or hosted by him Face Book India Online Services Pvt Ltd vs. Vinay Rai (11.01.2012 - DELHC)\(^\text{125}\), Google India Pvt. Ltd. vs. Vinay Rai and Anr. (11.01.2012 - DELHC)\(^\text{126}\)

- The accused indiscriminately sent e-mails and has published a large number of blogs on the website http://www.blogger.com/, which according to them was highly vulgar, disgusting and abusive references towards His Holiness Sri Sri. Ravi Shankar, owner of Art of Living Foundation, and towards various other

---


persons associated with the Art of Living. The Hon’ble court directed them to remove all defamatory contents (Vyakti Vikas Kendra, India Public Charitable Trust Thr Trustee Mahesh Gupta & Ors vs. Jitender Bagga & Anr (09.05.2012 - DELHC)\textsuperscript{127}).

- Accused generated and collected monies and revenues by sale of Data Doctor for FAT and NTFS as also the varied variants, altered, modified, reproduced version under different names supported by different domain name registrars, web hosting service providers and payment gateways. Accused was held liable for infringement of copyright, passing off, unfair competition, rendition of accounts etc., (Unistal System Pvt. Ltd. Vs Prodata Doctor Pvt. Ltd.)\textsuperscript{128}.

- Accused committed offence of defamation by publication of malicious imputation of print by electronic message/mail. It was held that the fact that such publication was also made at other places would not militate against cause of action for instituting complaint at that place. (Trade-Wings Limited, a public limited company incorporated under the Companies Act, 1956 and Ors. Vs. State of Maharashtra, through the office of the Government Pleader, The Ld. Addl. Chief Metropolitan Magistrate and Dwarkanath Boppanna, Director of Tulip Star Leisure and Health Resorts, a Company incorporated Under the Companies Act, 1956)\textsuperscript{129}.

- In another case accused persons published articles contained defamatory statements against the victim and they were made available in Cyber space for world wide audience. The intermediately failed to move its little finger to block the said material or to stop dissemination of the unlawful and objectionable material. Therefore it was held that intermediately cannot claim

\textsuperscript{129}Trade-Wings Limited and Ors. vs. State of Maharashtra, (2010) MH MANU 1438.
any exemption under Section 79 of the IT Act (Google India Pvt. Ltd. represented by its Managing Director and Mr. Sailesh Rao, S/o. Nagaraja S.Rao Vs. Visaka Industries Limited, rep. by its Authorized Signatory Sri R. Rajanikanth, S/o Shri R. Varadarajulu and State of A.P., rep. by the Public Prosecutor)\textsuperscript{130}.

- A company facilitates the sale of any property, for which it receives commission and also generates revenue from advertisements carried on its web pages. Company has not stopped payment through banking channels after learning of the illegal nature of the transaction held liable (Avnish Bajaj Vs. State (N.C.T.) of Delhi)\textsuperscript{131}.

7.11 Conclusion

Statute must be drafted with precision, leaving no room for ambiguity, particularly with reference to phrases that enumerate classes of persons, acts constituting an offence or a generic term that may be susceptible to multiple interpretations. Mere uncertainty in a single phrase of a hastily drafted statute could render the law unconstitutional and void, thereby necessitating precaution in the framing of penal statutes that are bound to affect a majority of citizens, as is certainly the case with a statute regulating activities in the cyberspace in a country as large as ours\textsuperscript{132}.

Lawyers are overwhelmingly technological ignoramuses, and yet technology is the single most important factor dominating the economy and creating new issues


and concerns calling for social management. Ironically, the law is one of the most powerful mechanisms for social management. The approach of lawyers and the legal system to issues all too often rejects new knowledge, and at the same time rejects any experimental approach. The consequence is that they consistently pass vague and ambiguous defective legislation, leaving it to the courts to hash out two, three, or five years down the road\textsuperscript{133}.

Advances in technology are testing the efficacy of the law in social ordering. Rapid changes in the socio-economic landscape are rendering certain laws that were created before the advent of cyberspace inadequate in many ways that cannot be overstated. Piecemeal and disparate, and oft-times inadequate and even non-existent, national laws are clearly not a satisfactory solution to such multi-party cross-border dealings. The Information Technology (Amendment) Act, 2008 was passed by the Lok Sabha with almost no discussion whatsoever. This fact that the Bill was not discussed prior to it being passed is clear in its drafting. Lack of prosecution was cited as one of the reasons for the amendments of the Information Technology Act, 2000. However, the situation is the same as that prior to amendments. The government continues to prefer filing criminal cases under the Indian Penal Code instead under Information Technology Act, 2000 despite the law enforcement authorities creating special cyber cells to train policeman. The efficacy of such an approach is hardly likely to withstand the test of time, given the current non-exposure and lack of training of Inspector level police officers to cyber crimes, their detection, investigation and prosecution. Implementation is viable only if there is mutual cooperation amongst enforcement authorities and governments\textsuperscript{134}.

\textsuperscript{134}P. Duggal, The new Information Technology Act Amendments, 5 (2009).