Laws Governing Information Technology in India

By
A.P.Suresh
Advocate High Court of Telangana

INTRODUCTION

- The invention of the internet which dates back to the 1960s and the tremendous growth of internet usage in the 2000s around the globe, the cyber space became more and more sophisticated.
- Over time, the internet from being initially developed as a research and information sharing tool moved to became more transactional with e-business, e-commerce, e-governance and e-procurement, etc. Initially, the cyber space was unregulated which led to an increase in crime rates. Soon all legal issued related to crime were dealt with cyber laws.
- In India, the Information Technology Act, 2000 (in short "**IT Act**") came into force on October 17, 2000 with the main aim of providing legal recognition to electronic commerce and for the filing of electronic records with the Government.

OBJECT OF THE IT ACT

- The IT Act and rules were introduced in order to control and regulate the crimes that were being committed through the internet or the cyberspace or through the uses of computer resources.
- Some of the major legal issues related to the use of technology includes retaining and preserving evidence, bridging the gap between multi-jurisdictional boundaries, providing identity, decoding encryption, improving training at all levels of the organization, reporting of electronic crime, etc.
- The main object of the IT Act, 2000 was to **provide legal recognition to e-records and digital signatures, legal recognition to electronic governance**.
- Seeks to provide **punishment for cyber offences**.
- Seeks to establish the **Cyber Appellate Tribunal.**
- Seeks to **amend the provisions of the Indian Penal Code, Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934** for technological compliant.

Scheme of the Act

- The Act contains Sections 94 (of which several sections have been repealed) divided into 13 Chapters with 2 Schedules.
- Chapter – I: Section 1 & 2: **Object, applicability & Jurisdiction**
- Chapter –II: Section 3 & 3A: **Digital Signature & Electronic Signature**
- Chapter –III: Sections 4 to 10A: **Deals with legal recognition of electronic records.**
- Chapter –IV: Sections 11 to 13: **Attribution, acknowledgement, and Dispatch of electronic records. (Important case P.R. Transport Agency vs. Union of India & others, lays understanding of place of execution of electronic contract)**
- Chapter –V: Sections 14 to 16: **Deals with secure electronic records**
- Chapter – VI: Sections 17 to 34: **Regulation of Certifying Authorities (Section 24 deals with issuance of license to certifying authorities)**
- Chapter – VII: Section 35 to 39: **Provides the process for issue electronic signature certificate**.
- Chapter –VIII: Sections 40 to 42: **Duties of subscribers**
- Chapter – IX: Sections 43 to 47: **Adjudication of IT related issues, penalties, Compensation.**

Scheme of the Act Contd…

- Chapter – X: Sections 48 to 64: **Appellate Tribunal**
- Chapter –XI: Sections 65 to 78: **Offences , domain of the crime branch under section 78;**
- Chapter – XII: Sections 79: **Intermediaries are not to be liable in certain cases (Exception section 79 (3) (b)**
- Chapter – XIIA: Section 79A: **Examiner of Electronic evidence**
- Chapter – XIII: Section 80 to 94: **Miscellaneous (Rule making power of the Centre & other provisions governing the Information Technology business in India.**

JURISDICTION & APPLICABILITY

- When it comes to jurisdiction, the Act, as per **Section 1(2)** extends to the whole of India and also applies to any offence or contravention committed outside India by any person.
- **Section 75** of the Act talks about the applicability of the Act for any offence or contravention committed outside India.
- The Act applies 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.
- Without a duly signed extradition treaty or a multilateral cooperation arrangement, trial of such offences and conviction may be a difficult proposition.

Important Definitions

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

(d) —affixing [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 digital signature;

(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;

Important Definitions..contd

(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;

Important Definitions..contd

(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;

(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;

(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;]

Important Provisions ..contd

- **(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;] See Section 79 for exemption given to intermediaries:**

AMENDMENTS MADE IN THE INDIAN PENAL CODE, 1860

- The term ‘Electronic records’ was included in Section 91 of IPC.
- Section 167 was amended in order to enable the punishment for offence in the case of framing and translating electronic record by a public servant with the intention of damage or injury.
- Sections 172 and 173 have been amended for electronic records and deal with contempt of the lawful authority to enforce obedience.
- Section 463 was amended to make provision for forgery by electronic record.
- Section 464 was amended for making of false document and affixing digital signatures to it.
- Section 2(1) (d) of the IT Act has been amended with same effects in IPC for Sections 466, 470 and 474 for forgery and fraudulent of affixing digital signatures.

AMENDMENTS WERE MADE TO THE INDIAN EVIDENCE ACT, 1872

- Section 34 was amended to include preserving of electronic documents as evidence.
- Section 47A has been inserted with respect to issue of Digital Signature Certificate by relevant Certifying Authorities.
- Section 65A and 65B of the Evidence Act provides the bases for contents of electronic records.
- **Admissibility of Electronic records as evidence:** Section 65B of the Indian Evidence Act relates to admissibility of electronic records as evidence in a Court of law. The computer holding the original evidence does not need to be produced in court. A printout of the record, or a copy on a CD ROM, hard disk, floppy etc can be produced in court. However some conditions need to be met and a certificate needs to be provided. **(important case State vs. Mohd. Afzal and others)**
- Section 67A and 73A are related to verification of digital signatures.
- Section 90A allows keeping the electronic records to be five years old.

POWERS OF THE TRIBUNAL

- The Tribunals has the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely -
- summoning and enforcing the attendance of any person and examining him on oath;
- requiring the discovery and production of documents or other electronic records;
- receiving evidence on affidavits;
- issuing commissions for the examination of witnesses or documents;
- reviewing its decisions;
- dismissing an application for default or deciding it ex parte;
- any other matter which may be prescribed.

- The appeal lies to the High Court and any person aggrieved by any decision or order of the Tribunal may file and appeal within sixty days from the date of communication of the decision or order of the Tribunal.

Important Provisions

- Section 46 of the IT Act has enlisted the **powers, functions and appointment procedures for an adjudicating officer.**
- Further, Section 57 gives the **jurisdiction rights and controlling authorities to the Cyber Regulations Appellate Tribunal (in short "CRAT").**
- Section 58 provides a **special power to CRAT which states that it is not bound by any procedures under any Code of Civil Procedure, 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 **Civil Courts do not have the jurisdiction** as per Section 61 to entertain any suit in respect of any matter under this Act.
- Section 62 provides **CRAT the right to question the appeal of high court.**

OFFENCES

- Section 65 -Tampering with computer source documents (**punishable with imprisonment up to three years**, or with **fine which may extend up to two lakh rupees**, or with both)
- Section 66- Computer related offences (**imprisonment for a term which may extend to three years** or with **fine which may extend to five lakh rupees or with both)**
- Section 66A- Punishment for sending offensive messages through communication service, etc. **(punishable with imprisonment for a term which may extend to three years and with fine)**

  Important Judgment: Shreya Singhal Vs. Union of India (UOI)- Petition was filed which challenged the constitutional validity of Section 66A on the ground that it violates the right to freedom of expression guaranteed under Article 19 of the Constitution of India. It was held that-Section 66A was violative of right to freedom of speech and expression and is not under the grounds of reasonable restrictions given under Article 19(2).

Section 66A creates offence which was vague and overbroad, and, therefore, unconstitutional under Article 19(1)(a) and not saved by Article 19(2). Thus, Section 66A of Act, 2000 was struck down in its entirety being violative of Article 19(1)(a) and not saved under Article 19(2).

- Section 66B- Punishment for dishonestly receiving stolen computer resource or communication device. (**punishable with imprisonment for a term of up to three years, or/and with fine of up to rupees 1 lakh or with both).**
- Section 66C- Punishment for identity theft. **(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).**
- Section 66D- Punishment for cheating by personation by using computer resource (**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).**

- Section 66E- Punishment for violation of privacy (**imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both)**.
- Section 66F- Punishment for cyber terrorism. (**cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life**).
- Section 67-Punishment for publishing or transmitting obscene material in electronic form (**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).**

- Section 67A- Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form (**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).**
- Section 67B- Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form **(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**).

- Section 67C- Preservation and retention of information by intermediaries **(an imprisonment for a term which may extend to three years and also be liable to fine).**
- Section 68- Power of Controller to give directions (**imprisonment for a term not exceeding two years or a fine not exceeding one lakh rupees or with both).**
- Section 70- Protected system (**an imprisonment for a term of up to 10 years and also be liable to fine).**
- Section 71- Penalty for misrepresentation **(punished with an imprisonment up to three years, or/and with fine up to rupees one lakh).**

THE INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

- Some of the features of this Amendment Act included replacing the term **'digital signature'** with electronic signature'. The term '**Communication device**' has been inserted which 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.
- Section 10A has been inserted to the effect that contracts concluded electronically shall not be deemed to be unenforceable solely on the ground that electronic form or means was used.
- The damages of rupees One Crore prescribed under Section 43 of the earlier Act of 2000 for damage to computer, computer system etc. has been deleted and the relevant parts of the section have been substituted by the words, **'he shall be liable to pay damages by way of compensation to the person so affected**'.

- Section 69 which gave authorities the power of ‘inception or monitoring or decryption of any information through any computer resource’. It also introduced penalties for child porn, cyber terrorism and voyeurism. It also empowers Government of blocking of public access to information through computer resource.
- Section 70 states that any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure may be declared to be a protected system by the appropriate Government through a notification.
- The appropriate Government may authorize persons who are authorized to access the protected systems. Any person secures access or attempts to secure access to a protected system shall be punished with imprisonment of description for a term which may extend to ten years and shall also be liable to fine.
- Section 70A states that the Central Government may designate any organization as the national nodal agency in respect of Critical Information Infrastructure Protection and such a nodal agency shall be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.

INDIAN COMPUTER EMERGENCY RESPONSE TEAM (CERT)

- Section 70B provides that the Indian Computer Emergency Response Team (herein referred to as “CERT”) shall serve as the national agency for incident response. It is the nodal agency under the Ministry of Electronics and Information Technology with the objectives of preventing cyber-attacks against the country’s cyber space, responding to cyber-attacks and minimizing damage and recovery time reducing national vulnerability to cyber-attacks and enhancing awareness among common citizens.
- CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents.
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities.
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.

Intermediaries & Judicial Trends

- Section 2(w) of the IT Act as "*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, web-housing service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes.*"
- Section 79 of the IT Act is a 'safe harbour' provision and provides an exemption of liability for intermediaries under certain conditions.
- Section 79(1) of the IT Act grants intermediaries a conditional immunity in terms of any third party information or data which is made available or hosted by them.
- Section 79(2) states that Section 79(1) would be applicable if the function of the intermediary is limited to providing access to a communication system over which the information is made available by third parties is transmitted or temporarily stored or hosted and if the intermediary does not initiate the transmission and select or modify the information contained in the transmissions.

- Under Section 79(3)(b) an intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts relatable to Article 19(2) are going to be committed then fails to expeditiously remove or disable access to such material. Hence, the intermediary need not decide which content is to be removed or disabled unless it receives a court order or notification from an appropriate government or its agency.
- **Important Judgment: Google India Private Limited Vs.Visakha Industries and Ors:** The proceedings were initiated against Appellant for offences of defamation punishable under Sections 120B, 500 and 501 read with Section 34 of Code liable to be quashed. The Court rejected the Appellant's plea and directed that it undergo trial in the criminal defamation case. It was observed that proceeding on the basis of the assumption that the Appellant is the intermediary, and that it stood alerted by the complainant, the appellant has not removed the offensive posts although it could technically remove them. Therefore, it amounted to publication, and this attracts section 499 of the Indian Penal Code, 1860, which deals with defamation. The court further held that prior to its substitution, section 79 of the IT Act did not provide protection to intermediaries. Hence, the Appellant, as an intermediary, could not be exempted from the liability arising out of defamation.

The Information Technology (Intermediaries Guideline) Rules, 2011

The rules that are required to be followed by intermediaries in order to claim safe harbour protection are:

- Intermediaries to publish rules and regulations, privacy policy and user agreement;
- Rules and regulations, terms and conditions or user agreement shall specify all prohibited acts, i.e. belonging to other persons, grossly harmful, harassing or unlawful, harms minors, infringes any intellectual property rights, violates any law, is deceiving or misleading, impersonates any person, contains virus, threatens India etc. and the intermediary should inform users that violation of same shall lead to termination of access,
- Intermediaries to not knowingly host or publish information as specified in sub-rule (2),
- Intermediaries to disable such information within 36 hours and storage of same for 90 days for investigation purposes,
- Intermediaries to provide assistance to authorised government agencies,

- Intermediaries to take all reasonable measures to secure its computer resource,
- Intermediaries to report cyber security incidents to the Indian Computer Emergency Response Team and
- Intermediaries to appointment and publish the details of a Grievance Officer on its website.
- **Important Judgment: Myspace Inc. Vs. Super Cassettes Industries Ltd:** SCIL's suit claimed permanent injunction restraining My space from infringing and exploiting its intellectual property, primarily the copyright owned by it in cinematograph films, sound recordings, and literary and musical works and has also claimed damages for such exploitation.
- The issue which arose was whether MySpace could be said to have knowledge of infringement as to attract Section 51(a)(ii) of Act and consequent liability.
- It was held that both under Copyright Act and Information Technology Act, 2000/IT Act, "actual" knowledge and not just suspicion is essential to fasten liability. Merely apprehension of unlawful content on website and embargos placed through user agreements do imply its knowledge of infringement.

- MySpace clearly places an embargo on its users from uploading content in which they do not possess relevant rights and at same time gives content owners option of notifying them in event that they find content hosted on its website is without due license. It claims immunity from liability, as an intermediary following due diligence as well complying with provisions of Section 79 of IT Act. Further, **Section 79 of IT Act, is neither an enforcement provision nor does it list out any penal consequences for non- compliance**. It sets up a scheme where intermediaries have to follow certain minimum standards to avoid liability; it provides for an affirmative defence and not blanket immunity from liability .
- The Court also gave the concept of '**actual or specific knowledge**' and held that intermediaries can be held liable if they have actual or specific knowledge of the existence of infringing content on their website from content owners and despite such notice, they do not takedown the content. There is no necessity of a court order in such cases. The Division Bench further pronounced that "**in case of internet intermediaries, interim relief has to be specific and must point to actual content, which is being infringed**".

- **Important Judgment: RO Systems Ltd. and Ors. Vs. Amit Kotak and Ors:** Certain product listings such as that of water purifier systems, which were alleged by Kent RO Systems Ltd. ("**Kent RO Systems**") to infringe its registered designs under the Designs Act, 2000 ("**Designs Act**") were hosted on eBay.in, belonging to eBay India Private Limited ("**eBay**"). The issue which arose was whether **eBay** should be directed to remove all products infringing registered designs of Plaintiffs?
- The Delhi HC reaffirmed that under the IT Act, an intermediary is obligated to remove / disable the goods / information hosted on its portal only on receipt of an order from the relevant governmental agency or pursuant to a court order. The Delhi HC held that an intermediary should not "*on its own, screen all information being hosted on its portal for infringement of the rights of all those persons who have at any point of time complained to the intermediary*".
- The Delhi HC also held that, whether an intellectual property right has been infringed or not is a question to be determined by the courts, and an intermediary is neither equipped to determine this, nor is possessed with the required prowess for such an evaluation.

- The Court also accepted the fact that an obligation imposed on intermediaries to proactively remove infringing listings would bring the business of the intermediaries to a halt. **The Delhi HC also interpreted the IT Act and stated that the intent of the legislature to place a limit on such intermediary liability was clear as an intermediary is only obligated to perform its due diligence obligations such as informing its users not to host, display, upload, modify, publish, transmit, update or share any information that is obscene, defamatory , unlawful or is infringing the intellectual property of third parties, etc.**

THANK YOU

AP SURESH
& ASSOCIATES
LAW CHAMBERS