
Cyber Laws in India: The Information Technology Act 2008

Mohd. Akbar Khan

Assistant Professor, ICFAL, University, Jaipur

ABSTRACT:

The Information Technology Amendment Act, 2008 (IT Act 2008) is a substantial addition to India's Information Technology Act (ITA-2000). The IT Amendment Act was passed by the Indian Parliament in October 2008 and came into force a year later. The original Act was developed to promote the IT industry, regulate e-commerce, facilitate e-governance and prevent cybercrime. The Act also sought to foster security practices within India that would serve the country in a global context. The Amendment was created to cover further development of IT and related security concerns since the original law was passed. This article covers the salient features of present cyber laws in India i.e. Information Technology Amendment Act, 2008.

Key Words: Technology, e-commerce, cybercrime, e-governance, Cyber laws

INTRODUCTION

“Cyber” is a prefix used to describe a person, thing, or idea as part of the computer and information age. It was first used in cybernetics, a word coined by Norbert Wiener and his colleagues. The virtual world of internet is known as cyberspace and the laws governing this area are known as Cyber laws and all the natives of this space come under the ambit of these laws as it carries a kind of universal jurisdiction. Cyber law can also be described as that branch of law that deals with legal issues related to use of internetworked information technology. In short, cyber law is the law governing computers and the internet.

The growth of Electronic Commerce has propelled the need for vibrant and effective regulatory mechanisms which would further strengthen the legal infrastructure, so crucial to the success of Electronic Commerce. All these regulatory mechanisms and legal infrastructures come within the domain of Cyber law.

Cyber law is important because it touches almost all aspects of transactions and activities on and involving the internet, World Wide Web and cyberspace. Every action and reaction in cyberspace has some legal and cyber legal perspectives.

CYBER LAW IN INDIA

Cyber law encompasses laws relating to Cyber crimes, Electronic and digital signatures, Intellectual property & Data protection and privacy. In India, cyber laws are contained in the Information Technology Act, 2000 (“IT Act”) which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.ⁱ

With the passage of time, as technology developed further and new methods of committing crime using Internet & computers surfaced, the need was felt to amend the IT Act, 2000 to

insert new kinds of cyber offences and plug in other loopholes that posed hurdles in the effective enforcement of the IT Act, 2000. This led to the passage of the Information Technology (Amendment) Act, 2008 which was made effective from 27 October 2009. The IT (Amendment) Act, 2008 has brought marked changes in the IT Act, 2000 on several counts.

Information Technology Act, 2000 is India's nodal legislation regulating the use of computers, computer systems and computer networks as also data and information in the electronic format. This legislation has touched varied aspects pertaining to electronic authentication, digital (electronic) signatures, cyber crimes and liability of network service providers.

The Preamble to the Act states that it aims at providing 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 and aims at facilitating electronic filing of documents with the Government agencies.

The IT Act of 2000 was developed to promote the IT industry, regulate ecommerce, facilitate e-governance and prevent cybercrime. The Act also sought to foster security practices within India that would serve the country in a global context. The Amendment was created to address issues that the original bill failed to cover and to accommodate further development of IT and related security concerns since the original law was passed.

The IT Act, 2000 consists of 90 sections spread over 13 chapters [Sections 91, 92, 93 and 94 of the principal Act were omitted by the Information Technology (Amendment) Act 2008 and has 2 schedules.[Schedules III and IV were omitted by the Information Technology (Amendment) Act 2008]. Various Rules were notified under the Information Technology Act, 2000 for the enforcement of the Act.

The Information Technology Act was enacted with a view to give a fillip to the growth of electronic based transactions, to provide legal recognition for e-commerce and e-transactions, to facilitate e-governance, to prevent computer based crimes and ensure security practices and procedures in the context of widest possible use of information technology worldwide.

Applicability of the Act

The Act will apply to the whole of India unless otherwise mentioned. It applies also to any offence or contravention there under committed outside India by any person. The Act shall not apply to the following documents or transactions –

- A negotiable instrument as defined in Sec.13 of the Negotiable Instruments Act, 1881;
- A power of attorney as defined in Sec.1A of the Powers of Attorney Act, 1882;
- A trust as defined in Section 3 of the Indian Trusts Act, 1882;
- A Will as defined in Sec.2(h) of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called;
- Any contract for the sale or conveyance of immovable property or any interest in such property.

The Act contains twelve chapters and two schedules.

CYBER CRIME

Cyber terrorists usually use the computer as a tool, target, or both for their unlawful act either to gain information which can result in heavy loss/damage to the owner of that intangible sensitive information. Internet is one of the means by which the offenders can gain such price sensitive information of companies, firms, individuals, banks, intellectual property crimes (such as stealing new product plans, its description, market programme plans, list of customers etc.), selling illegal articles, pornography etc. this is done through many methods such as phishing, spoofing, pharming, internet phishing, wire transfer etc. and use it to their own advantage without the consent of the individual. Many banks, financial institutions, investment houses, brokering firms etc. are being victimised and threatened by the cyber terrorists to pay extortion money to keep their sensitive information intact to avoid huge damages. And it's been reported that many institutions in US, Britain and Europe have secretly paid them to prevent huge meltdown or collapse of confidence among their consumers.ⁱⁱ

ELECTRONIC COMMERCE

Electronic commerce, commonly known as e-commerce, is the buying and selling of products or services over electronic systems such as the Internet and other computer networks. Electronic commerce draws on such technologies as electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems. Modern electronic commerce typically uses the World Wide Web (www) at least at one point in the transaction's lifecycle, although it may encompass a wider range of technologies such as email, mobile devices and telephones as well.

Contemporary electronic commerce involves everything from ordering “digital” content for immediate online consumption, to ordering conventional goods and services, to “meta” services to facilitate other types of electronic commerce.

On the institutional level, big corporations and financial institutions use the internet to exchange financial data to facilitate domestic and international business. Data integrity and security are very hot and pressing issues for electronic commerce.

Ecommerce in India

India has an internet user base of over 100 million users. The penetration of ecommerce is low compared to markets like the United States and the United Kingdom but is growing at a much faster rate with a large number of new entrants. The industry consensus is that growth is at an inflection point with key drivers being:

- Increasing broadband Internet and 3G/ 4G penetration.
- Rising standards of living and a burgeoning, upwardly mobile middle class with high disposable incomes.
- Availability of much wider product range compared to what is available at brick and mortar retailers.
- Busy lifestyles, urban traffic congestion and lack of time for offline shopping.

- Lower prices compared to brick and mortar retail driven by disintermediation and reduced inventory and real estate costs.
- Increased usage of online classified sites, with more consumers buying and selling secondhand goods.
- Evolution of the online marketplace model with sites like ebay, Infibeam, and Tradus.

India had an internet user base of about 354 million as of June 2015ⁱⁱⁱ and is expected to cross 500 million in 2016.^{iv} Despite being the second-largest user base in world, only behind China (650 million, 48% of population), the penetration of e-commerce is low compared to markets like the United States (266 million, 84%), or France (54 M, 81%), but is growing at an unprecedented rate, adding around 6 million new entrants every month.^v The industry consensus is that growth is at an inflection point.^{vi}

In India, cash on delivery is the most preferred payment method, accumulating 75% of the e-retail activities.^{vii} Demand for international consumer products (including long-tail items) is growing much faster than in-country supply from authorised distributors and e-commerce offerings. Largest e-commerce companies in India are Flipkart, Snapdeal, Amazon India, Paytm.^{viii}

The Online Travel Industry is the biggest segment in e-commerce and is booming largely due to the Internet savvy urban population. Some of the aspects of Indian ecommerce that are unique to India (and potentially to other developing countries) are:

- Cash on Delivery as a preferred payment method. India has a vibrant cash economy as a result of which 80% of Indian ecommerce tends to be Cash on Delivery (COD).
- Direct Imports constitute a large component of online sales. Demand for international consumer products is growing much faster than in-country supply from authorized distributors and ecommerce offerings.

Ecommerce websites are Internet intermediaries within the meaning of IT Act, 2000. “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. The IT (Intermediaries Guidelines) Rules of 2011 regulate the functioning of ecommerce websites. Cyber law due diligence is the main aspect that all ecommerce site owners should comply with.

REGULATORY AUTHORITIES

Department of Electronics and Information Technology The Ministry of Communications and Information Technology comprises of the following Departments:

- Department of Information Technology (DEIT)
- Department of Posts
- Department of Telecommunications (DOT)

(1) Department of Electronics and Information Technology (DEIT)

under the Ministry of Communications and Information Technology, Government of India is responsible for all matters relating to Cyber Laws, administration of the Information

Technology Act. 2000 (21 of 2000) and other IT related laws. The functions of the Department of Electronics and Information Technology, Ministry of Communications & Information Technology, Government of India are as follows –

- Policy matters relating to Information Technology, Electronics and Internet.
- Initiatives for development of Hardware / Software industry including knowledge based enterprises, measures for promoting Information Technology exports and competitiveness of the industry.
- Promotion of Information Technology and Information Technology enabled services and Internet.
- Assistance to other departments in the promotion of E-Governance, E-Infrastructure, E-Medicine, E-Commerce, etc.
- Promotion of Information Technology education and Information Technology based Education.
- Matters relating to Cyber Laws, administration of the Information Technology Act. 2000 (21 of 2000) and other Information Technology related laws.
- Matters relating to promotion and manufacturing of Semiconductor Devices in the country.
- Interaction in Information Technology related matters with International agencies and bodies.
- Initiative on bridging the Digital Divide, Matters relating to Media Lab Asia.
- Promotion of Standardization, Testing and Quality in Information Technology and standardization of procedure for Information Technology application and Tasks.
- Electronics Export and Computer Software Promotion Council (ESC).
- National Informatics Centre (NIC)
- All matters relating to personnel under the control of the Department.

(2) Controller of Certifying Authorities (CCA):

The IT Act 2000 provides for the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities. The Certifying Authorities (CAs) issue digital signature certificates for electronic authentication of users. The CCA certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by a licensed CA. For this purpose it operates, the Root Certifying Authority of India (RCAI).

(3) Cyber Appellate Tribunal:

Cyber Appellate Tribunal has been established under the IT Act under the aegis of Controller of Certifying Authorities (CCA). A Cyber Appellate Tribunal consists of one Presiding Officer who is qualified to be a Judge of a High Court or is or has been a member of the Indian Legal Service and is holding or has held a post in Grade I of that service for at least three years supported by other official under him/her.

The Cyber Appellate Tribunal has, for the purposes of discharging its functions under the IT Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908. However, is not bound by the procedure laid down by the Code of Civil Procedure, 1908 but is guided by the principles of natural justice and, subject to the other provisions of this Act

and of any rules. The Cyber Appellate Tribunal has powers to regulate its own procedure including the place at which it has its sittings.

Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973. The composition of the Cyber Appellate Tribunal is provided for under section 49 of the Information Technology Act, 2000. Initially the Tribunal consisted of only one person who was referred to as the Presiding Officer who was to be appointed by way of notification by the Central Government. Thereafter the Act was amended in the year 2008 by which section 49 which provides for the composition of the Cyber Appellate Tribunal has been changed. As per the amended section the Tribunal shall consist of a Chairperson and such number of other Members as the Central Government may by notification in the Official Gazette appoint. The selection of the Chairperson and Members of the Tribunal is made by the Central Government in consultation with the Chief Justice of India. The Presiding Officer of the Tribunal is now known as the Chairperson.

(4) Indian Computer Emergency Response Team (ICERT):

The mission of ICERT is to enhance the security of India's Communications and Information Infrastructure through proactive action and effective collaboration. Its constituency is the Indian Cyber community. The purpose of the ICERT is, to become the nation's most trusted referral agency of the Indian Community for responding to computer security incidents as and when they occur; the ICERT will also assist members of the Indian Community in implementing proactive measures to reduce the risks of computer security incidents. It provides technical advice to system administrators and users to respond to computer security incidents. It also identifies trends in intruder activity, works with other similar institutions and organizations to resolve major security issues and disseminates information to the Indian cyber community. It functions under the Department of Information Technology, Ministry of Communications & Information Technology, and Government of India.

REFERENCE

- i. Rajkumar S. Adukia. (2014). Overview of Cyber Laws in India. Access from http://www.lawyersclubindia.com/articles/print_this_page.asp?article_id=6039 2/14
- ii. Gerald R Ferrera *et al.* (2012). Cyber Law: Text and Cases: 3rd Edition.
- iii. Sharma.P. (2014). Information Security & Cyber Laws.
- iv. <http://deity.gov.in/> Department of Electronics and Information Technology, Govt. of India
- v. <http://cybercellmumbai.gov.in/> Cybercrime investigation cell
- vi. <http://ncrb.gov.in/> National Crime Records Bureau
- vii. <http://catindia.gov.in/Default.aspx> Cyber Appellate Tribunal

-
- viii. <http://www.certin.org.in/> Indian Computer Emergency Response Team
ix. <http://cca.gov.in/rw/pages/index.en.do> Controller of Certifying Authorities

ENDNOTES:

-
- ⁱ Lawyersclubindia Article : Overview of Cyber Laws in India
http://www.lawyersclubindia.com/articles/print_this_page.asp?article_id=6039 2/14
- ⁱⁱ Access from- <http://www.legalserviceindia.com/cyber/cyber.htm>
- ⁱⁱⁱ “India’s internet user base 354 million, registers 17% growth in first 6 months of 2015: IAMAI report”. timesofindia-economic times. Retrieved 4 May 2016.
- ^{iv} “Internet users in India to cross 500 mn in 2016: Prasad”. Business Standard. 5 May 2016. Retrieved 23 May 2016.
- ^v “Online shoppers in India”. timesofindia.indiatimes/tech. 2014-11-20. Retrieved 2015-03-25.
- ^{vi} “Indian e-commerce at inflection point?”. Vccircle.com. 2010-08-19. Retrieved 2013-07-04.
- ^{vii} “In COD we trust”. translatemedia.com. 2015-02-06. Retrieved 2015-03-24.
- ^{viii} The Economic Times. Retrieved 4 May 2016.