International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - TeLMISR 2015, ISSN : 2348-2273
Available Online at www.ijeecse.com

IT ACT 2000: Scope, Impacts and Amendments

Aastha Bhardwaj, Ms Priyanka Gupta
Assistant Professor, Vivekananda Institute of Professional Studies, New Delhi

Abstract: Rapid advancements in Information Technology sector have revolutionised work and personal lives of people globally. Technology has entered every sphere of life like banks, work place, social networking, stock markets, shopping etc. resulting in sharing of one's personal information with every bit of machine one comes across. With the availability of personal information on a single click, the data is vulnerable to cyber-crime. In mid-90s liberalisation of Indian economy resulted in manifold increase in e-transactions. Therefore, the need to bring technology under legislation was felt. With this objective in view, Parliament of India, passed the Information Technology Act in 2000. This first cyber law addressed various issues with a view to discourage misuse of digital medium and punishment for various offenses prescribed. Later on with more technological advancements, further amendments and notifications were issued to counter the menace of growing cyber - crime. This paper describes IT Act 2000, and discusses important dimensions of amendments in 2008.Further, various notifications issued till date have also been discussed. An attempt has also been made to touch areas, left unaddressed in the foregoing legislations.

Keywords: IT Act 2000, Cyber Crime, IT Act Amendment 2008.

I. INTRODUCTION

Digital information, communications, computers (in the form of pc, notebook, mobile phones etc.), software - the constituents of the information age - have entered in our life voluntarily or surreptitiously. Now, information technology has become an invaluable manager, touching every sphere of life i.e. social linkages via e-mail, Facebook, sms; Finances - spreadsheets online/internet banking, financial markets; Education - critical analysis, easy access to information via internet; Medical science and many more. This exponential growth of IT sector has seen rise of issues concerning security and privacy of electronically transmitted and stored information. Unscrupulous people have successfully siphoned off funds by misuse of data.

With extensive use of information available through computer resources, India was not adequately equipped to deal with cyber security concerns till the year 2000. With a view to maintain reasonable standard of security and privacy, a number of steps have been taken through various legislations. It was only in the year 2000 that an effort was made to address concerns regarding digital medium when IT Act saw light of the day in the country. In this first cyber law of its kind, various issues relating to e-documents were addressed so as to discourage misuse of digital medium and punishment for various offenses prescribed. It is of paramount importance that such grave concerns regarding potential misuse of sensitive information are addressed precisely so as to guarantee the integrity of systems and establish confidence for the reliability of the system. This guarantee of security and privacy of information has proven to be a milestone in restoring the credibility of the customers. Although an act such as IT Act is an evolving process but still a legal framework in the form of various laws/amendments/ is in place. The aim of this paper is to analyse the IT Act in a broader perspective by listing its amendments and notifications issued by the government.

The aim of this paper is to find out the limitations of the IT Act and to provide provisions for further amendments on the basis of International cyber laws. This paper is organised as follows. Section 2 explains the act by listing all its objectives followed by Section 3 which discusses the amendments to the Act made in year 2008.Information Technology is evolving quickly so as the methods of cyber fraud. Therefore, Section 4 lists all the notifications issued from 2009 to 2014 by the government of India for fighting against new kind of cyber frauds. Section 5 discusses the limitations of the IT Act as compared with International IT laws. Section 6 concludes the paper.

II. IT ACT 2000

Information technology is one of the important law relating to Indian cyber laws. In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000.This act is helpful to promote business with the help of internet. It contains set of rules and regulations which apply on any electronic business transaction. It is

"An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce" which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto".

IT Act, 2000 focuses on three main highlights:

a. Providing legal recognition to the transactions which are carried out through electronic means or use of Internet.

b. Empowering the government departments to accept filing, creating and retention of official documents in the digital format and

c. To amend outdated laws and provide ways to deal with cybercrimes.

1. Objectives of IT Act 2000: The following are the objectives of IT Act 2000 [1]

a. To give legal recognition to any transaction which is done by electronic way or use of internet?

b. To give legal recognition to digital signature for accepting any agreement via computer.

c. To provide facility of filling documents online relating to school admission or registration in employment exchange.

d. According to I.T. Act 2000, any company can store their data in electronic storage.

e. To stop computer crime and protect privacy of internet users.

f. To give more power to IPO, RBI and Indian Evidence act for restricting electronic crime.

g. To give legal recognition for keeping books of accounts by bankers and other companies in electronic form.

2. Scope of IT Act: The act shall apply to

a. Processing of personal data or partly by automatic means, and

b. Other processing of personal data which form part of or are intended to form part of personal data filing system.

This act shall not apply to the following:

a. Information technology Act 2000 is not applicable on the attestation for creating trust via electronic way. Physical attestation is must.

b. A contract of sale of any immovable property.

c. Attestation for giving power of attorney of property is not possible via electronic record.

3. Impact of IT Act: From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. [2]

a. Firstly, the implication of these provisions for the e-businesses is that email is now a valid and legal form of communication in our country that can be duly produced and approved in a court of law.

b. Companies are now able to carry out electronic commerce using the legal infrastructure provided by the Act.

c. Digital signatures have been given legal validity and sanction in the Act.

d. The Act opens the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signature Certificates.

e. The Act now allows Government to issue notification on the web thus heralding e-governance.

f. The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.

g. The IT Act also addresses the important issues of security, which are critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to be passed through a system of a security procedure, as stipulated by the Government at a later date.

Under the IT Act, 2000, it is possible for corporate to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.

III. IT ACT AMENDMENT 2008

Exponential growth of technology gave new ways and means to cybercrimes. To counter this growing cyber threats in 2008, the act was amended. Wide ranging crimes were incorporated in this amendment of the act with the provision of financial penalties as well as punishment varying from a three-year jail term to life sentence. This amendment came into force on 29th October, 2009. Broadly IT Act Amendment 2008 has covered following aspects:

1. Liability of Body Corporate towards sensitive personal data: Body corporate means any company and includes a firm, sole proprietorship or otherassociation of individuals engaged in commercial or professional activities. Any Body corporate dealing in sensitive personal data or information in a computer resource and lacking in providing sufficient security and control practices to safeguard the data has been made liable under Section 43A to pay damages to the affected party.

2. Identity Theft: Under section 63 C, Fraudulent/dishonest act by misuse of electronic

signature, password or any other unique identification feature of a person is punishable.

3. Spamming and Phishing: Explicitly no specific law exists against spamming and phishing but it appears that this aspect has been covered under section 66A. It says that sending messages of offensive nature or criminally intimidating through communication service has become punishable with imprisonment for a term which may extend upto three years or with fine.

4. *Introduction of virus, manipulating accounts, denial of services etc made punishable [3]:* Section 66 has been amended to include offences punishable as per section 43 which has also been amended to include offences as listed above; punishment may lead to imprisonment which may extend to three years or with fine which may extend to five lakh rupees or with both.

5. Cheating and Stealing of computer resource or communication device: Punishment for stealing or retaining of any stolen computer resource or communication device has been covered under section 66B.

Section 66D makes "cheat by personation" by means of any 'communication device' or 'computer resource' an offence.

6. Cyber Terrorism: An intent to threaten the unity, integrity, security or sovereignty of India contributes to cyber terrorism. Section 66D deals with punishment for acts like denial of services, unauthorized access etc related to cyber terrorism.

7. Child pornography: Section 67B lays Punishment for publishing, transmitting, browsing of material depicting children in sexually explicit act, etc. in electronic form.

8. Intermediary's liability: Intermediary means any person who on another person's behalf receives, stores or transmits the message or provides any service with respect to that message.

Sections 67C states that intermediaries should preserve and retain information in the format and for the period given by Central Government.

9. Surveillance, Interception and Monitoring: Section 69 empowers the government to issue directions for interception or monitoring or decryption of any information through any computer resource.

10. Cognizance of cases and investigation of offences: All cases which entail punishment of three years or more have been made cognizable.

In Act 2000, section 78 defines that investigation of offences is to be done only by Deputy Superintendent of police. In its amendment, Inspectors have been included as investigating officers which is more feasible.

11. Security procedures and Practices: Section 16empowersCentral Government to prescribe security procedure in respect of secure electronic records and secure digital signatures.

12. Indian Computer Emergency Response Team: On 27th October, 2009 CERT was appointed as national agency for performing functions in the area of cyber security.

IV. NOTIFICATIONS FOR AMENDMENT IN IT ACT 2000

After 2008 amendments, further notifications have been introduced to combat with the new kind of cyber frauds or crimes from 2009 to 2014 listed in Table 1.

Table 1: List of notifications issued by Government of India

S.N.	Date	Title	Objective
1.	11th April, 2011	Information Technology (Guidelines for Cyber Cafe) Rules, 2011	Rules and regulations for running and managing a cyber cafe's working. [4]
2.	11th April, 2011	Information Technology (Intermediaries guidelines) Rules, 2011	Prescribed due diligence to be observed by intermediary (any person who on behalf of another person receives, stores or transmits the message or provides any service with respect to that messages, e.g. network service provider)while discharging his duties. [5]
3.	11th April, 2011	Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011	Mishandling of any sensitive detail of a person was made punishable. It made corporate body liable for handling issues like obtaining consent before collection of sensitive data, disclosure of privacy policy , taking prior permission before disclosing such details to any third party ,ensuring same level of data protection in case it is transferred to any other body corporate or person etc. [6]

4.	11th April, 2011	Information Technology (Electronic Service Delivery) Rules, 2011.	Proposed a System of Electronic Service delivery, having a proper repository of electronically signed records. It empowered the respective government to direct service providers for providing guidelines for maintaining the accounts of records. [7]
5.	25th Oct, 2011	Information Technology (Certifying Authorities) Amendment Rules, 2011	Digital signature Certificate and Verification of Digital Signature Certificate was introduced to secure electronic record. [8]
6.	16th Mar, 2012	Information Technology (Guidelines for Cyber Cafe) Rules, 2011	Specifies the process of registration to be followed by each Registration Agency. [9]
7.	16th, Nov, 2012	Constitution of Cyber Regulations Advisory Committee	Regulations of internet. [10]
8.	18th Mar, 2013	Clarification on The Information Technology (Intermediary Guidelines) Rules,2013	Clarified that the intermediary shall respond or acknowledge to the complainant within thirty six hours of receiving the complaint/grievance.[11]
9.	16th Jan, 2014	Information Technology(National Critical Information Infrastructure Protection Centre and manner of performing functions and duties) Rules,2013	NCIIPC is being declared as the nodal agency for the protection of Critical Information Infrastructure of India. [12]
10.	16th Jan, 2014	Information technology(The Indian Computer Emergency Response team and manner of performing functions and duties)Rules,2013	It was made to enhance the security of India's communications and information infrastructure through proactive action and effective collaboration. [13]

V. LIMITATIONS OF IT ACT

Due to increasing crimes in cyber space, Government of India understood the problems of internet user and for safeguarding the interest of internet users, IT Act was made. A number of notifications for amending the law have been issued by the Government but still the following issues has not been taken care.

1. Spamming: Spam is an un-wanted e-mail message which is the electronic version of junk mail that is delivered by the postal service [14]. Emails' recipients don't have any existing business or personal relationship with the initiator. Such Unsolicited Bulk Email ("UBE") or Unsolicited Commercial Email ("UCE") is not sent at the request or with the consent of the recipient. There is no dedicated anti-spam law in India which imposes strict regulations for UCE/UBE. Spam Act 2003 of Australia bans all unsolicited commercial electronic messages and further states that all commercial emails must have the full information about the sender and contain a functional unsubscribe facility [15], whereas the USA:CAN-SPAM does not ban all UCE outright, but rather regulates it by prohibiting header information that is materially false or materially misleading. [16].

According to 2008 amendment, any email communication that causes annoyance or inconvenience or is sent to deceive or to mislead the recipient about the origin ofsuch a message, is punishable. Therefore the very act of sending such UCEs is not illegal, but if the content is objectionable, then it is an Internet crime under the Indian law [16].

2. Integrity of customer transactions: Integrity of data means unimpaired data while maintaining the accuracy and consistency of data. It is different from data confidentiality or denial of service. Modification of data by malicious programs or users can often cause more serious problems than confidentiality of data.

IT Act 2000, Section 43 provides law for unauthorized access but nothing has been said for any measure about the integrity of transaction by a bank. Guideline to maintain integrity of transaction exists but there is no specific law. Moreover, it is not considered as a criminal offence. On the other hand, many countries have a law in place for maintaining the integrity of transactions. Australia has Electronic Transactions (Queensland) Act 2001 and New Zealand has Electronic Transactions Act 2002 for maintaining the integrity of customer transactions.

3. Pornography: IT Act 2000 prohibits publishing of information which is obscene but there has not been any considerations or law on the viewing of such kind of information. Section 67 B of Amendment 2008, makes browsing of child pornography only punishable.

Nothing has been mentioned regarding browsing of adult pornography. But in UK possession of "extreme pornographic images" is an offence under Section 63 of the Criminal Justice and Immigration Act 2008 [17].

4. Phishing: Phishing is a criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication [18].In the Parliament while discussing the "Objects and Reasons of ITAA-2006" for the bill passed in 2008,phishing was part of the statement. But till date there is no provision specifically against phishing. US has anti-phishing Act in place to combat this fraudulent activity named "The Anti-Phishing Act of 2005", a bill to criminalize Internet scams involving fraudulently obtaining personal information, commonly known as phishing" . Thus it allows law enforcement officials to fight phishing scams, by creating an opportunity to prosecute before the actual fraud takes place [19].

VI. CONCLUSION

During the last two decades, Information Technology sector has witnessed exponential growth. Technology has become part and parcel of our daily life and has multiplier effect in every sector of industry .The major pitfall of this phenomenal growth has given rise to cybercrimes at an alarming rate. To combat this growing challenge, first legislation came in the year 2000. Since Cyber Criminals were found to be a step ahead of technology, regular amendments became need of the hour. Therefore, after introduction of Act 2000 many amendments/notifications are being issued as per requirement. In this paper we have discussed the legislations so far introduced and proposed the improvements that can be in corporated on issues like spamming, phishing, integrity of transactions and pornography in further amendments of IT Act.

VII. REFERENCES

[1] J. Vanathi, S. Jayaprasanna, "A Study on Cyber Crimes in Digital World", International Journal on Recent and Innovation Trends in Computing and Communication.

[2] Anil Kumar Gupta, Manoj Kumar Gupta, "E-Governance Initiative in Cyber Law Making", International Archive of Applied Sciences and Technology Volume 3 [2] June 2012: 97 – 101.

[3] Sanjay Pandey, " Curbing Cyber Crime: A Critique of Information technology Act 2000 and IT Act Amendment 2008", available at http://www.softcell.com/pdf/IT-Act-Paper.pdf.

[4] Aryan Chandrapal Singh, Kiran P. Somase and Keshav G. Tambre, "Phishing: A Computer Security Threat", International Journal of Advance Research in Computer Science and Management Studies, Volume 1, Issue 7, December 2013.

[5] Harris Drucker, Donghui Wu and Vladimir N. Vapnik, "Support Vector Machines for Spam Categorization", IEEE Transactions On Neural Networks, Vol. 10, No. 5, September 1999.

[6] "Spam act 2003", available at: http://www.acma.gov.au/webwr/consumer_info/spam/spam_act_pracguide_govt.pdf.

[7] Criminal Justice and Immigration Act 2008, http://www.legislation.gov.uk/ukpga/2008/4/part/5/crossheading/pornography-etc

[8] Junxiao Shi, Sara Saleem, "Phishing", available at"https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB8QFjAA&url=http%3A%2F%2Fwww.cs.arizona.edu%2F~collberg%2FTeaching%2F466-566%2F2012%2FResources%2Fpresentations%2F20"

[9] "Information Technology Act, 2000"available at http://www.dot.gov.in/act-rules/information-technology-act-2000.

[10] Priyanka Vora, Dr. KVK Santhy "Spam! Spam! Spam! The Need For An Anti-Spamming Law In India", Weblink: http://thegiga.in/LinkClick.aspx?fileticket=wMpHW5Ur8JA%3D&tabid=589.

[11] Weblinks:

http://deity.gov.in/sites/upload_files/dit/files/GSR315E_10511(1).pdf.

http://deity.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf.

http://deity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf.

http://deity.gov.in/sites/upload_files/dit/files/GSR316E_10511(1).pdf.

http://deity.gov.in/sites/upload_files/dit/files/GSR782_GSR783_08112011(1).pdf.

http://deity.gov.in/sites/upload_files/dit/files/GSR153E_242012.pdf.

http://deity.gov.in/sites/upload_files/dit/files/gazzate(1).pdf.

http://deity.gov.in/sites/upload_files/dit/files/Clarification%2079rules(1).pdf.

http://deity.gov.in/sites/upload_files/dit/files/GSR_19(E).pdf.

http://deity.gov.in/sites/upload_files/dit/files/G_S_R%2020%20(E)2.pdf.