Comparison between Information Technology Act, 2000 & 2008

1S. Praveen Raj and 2Aswathy Rajan
1Saveetha School of Law, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai.
praveenasking@gmail.com
2Saveetha School of Law, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai.
aswathyrajan.ssl@saveetha.com

Abstract

In the year 2000, India enacted its first law on Information Technology namely, the Information Technology Act, 2000. The IT Act, 2000 is based on the Model law of E-commerce adopted by UNCITRAL in 1996. The preamble to the IT Act, 2000 points out a threefold objective, firstly, to provide legal recognition for transactions carried out through electronic means, secondly, to facilitate the electronic filing of documents with government agencies, and thirdly to amend certain Act. The IT Act, 2000 gave legal validity and recognition to electronic documents and digital signatures and enabled conclusion of legally valid & enforceable e-contracts. It also provided a regulatory regime to supervise the Certifying Authorities issuing digital signature certificates and created civil and criminal liabilities for contravention of the provisions of the IT Act, 2000. 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. In this Paper the researcher intend to discuss the major changes brought about by the IT (Amendment) Act, 2008 & comment on its effectiveness in the context of Indian cyberlaw.

Key Words: Information technology, criminal liabilities, legal recognition, electronic documents, digital signature.
1. Introduction

The Information Technology Amendment Act, 2008 is a substantial addition to India's Information Technology Act, 2000. The IT Amendment Act was passed by the Indian Parliament in October 2008 and came into force a year later. The Act is administered by the Indian Computer Emergency Response Team (CERT-In). 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 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. Changes in the Amendment include: redefining terms such as "communication device" to reflect current use; validating electronic signatures and contracts; making the owner of a given IP address responsible for content accessed or distributed through it; and making corporations responsible for implementing effective data security practices and liable for breaches. The Amendment has been criticized for decreasing the penalties for some cybercrimes and for lacking sufficient safeguards to protect the civil rights of individuals. Section 69, for example, authorizes the Indian government to intercept, monitor, decrypt and block data at its discretion. According to Pavan Duggal, a cyber law consultant and advocate at the Supreme Court of India, "The Act has provided Indian government with the power of surveillance, monitoring and blocking data traffic. The new powers under the amendment act tend to give Indian government a texture and color of being a surveillance state."

2. Aim of the Study

- To know about the features of IT Act, 2000 & 2008
- To study about the various changes made in amendment Act, 2008
- To find out the pros and cons of IT Act 2000 & 2008
- To analyze the role of government to implement the IT Act, 2000 & 2008

Research Problem

Whether the IT Act 2000 is effectively address all the issues relating to cyber crime with comparison into the IT Act 2000 & 2008?

Hypothesis

IT Act, 2000 is effectively address all the issues relating to cyber crime.

3. Materials and Methods

The research is primarily doctrinal research. Here the data collection is necessarily secondary data which collected from books, journals, articles, law reports, newspapers, e-sources for the purpose of this study.
4. Chapterization

Chapter 1 deals with ‘Information Technology Act, 2000 - A General overview’

Chapter 2 deals with ‘changes made in IT Act, 2008’

Chapter 3 deals with ‘comparison between IT Act 2000 & 2008’

Chapter I

Information Technology Act, 2000 - A General Overview

The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce. It is based on the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model) recommended by the General Assembly of United Nations by a resolution dated 30 January 1997.

Background

The bill was passed in the budget session of 2000 and signed by President K. R. Narayanan on 9 May 2000. The bill was finalised by group of officials headed by then Minister of Information Technology Pramod Mahajan.

Summary

The original Act contained 94 sections, divided in 13 chapters and 4 schedules. The laws apply to the whole of India. Persons of other nationalities can also be indicted under the law, if the crime involves a computer or network located in India. The Act provides legal framework for electronic governance by giving recognition to electronic records and digital signatures. The formations of Controller of Certifying Authorities was directed by the Act, to regulate issuing of digital signatures. It also defines cyber crimes and prescribed penalties for them. It also established a Cyber Appellate Tribunal to resolve disputes rising from this new law. The Act also amended various sections of Indian Penal Code, 1860, Indian Evidence Act, 1872, Banker's Book Evidence Act, 1891, and Reserve Bank of India Act, 1934 to make them compliant with new technologies.

Salient Features of the Information Technology Act, 2000

The Information Technology Act, 2000, came into force with effect from 17th October, 2000. It has been amended in 2008 and the Amended Act is effective from February 5, 2009. The Rules under the Amended Act have also been framed, which became effective from October 27, 2009. The salient features of the Information Technology Act, 2000 may briefly be stated as follows:

1. The Act provides legal recognition to e-commerce, which facilitates commercial e-transactions.

2. It recognises records kept in electronic form like any other documentary record. In this way, it brings electronic transactions at par with paper transactions in documentary form.
3. The Act also provides legal recognition to digital signatures which need to be duly authenticated by the certifying authorities.

4. Cyber Law Appellate tribunal has been set up to hear appeal against adjudicating authorities.

5. The provisions of the I.T. Act have no application to negotiable instruments, power of attorney, trust, will and any contract for sale or conveyance of immovable property.

6. The Act applies to any cyber offence or contravention committed outside India by a person irrespective of his/her nationality.

7. As provided under Section 90 of the Act, the State Government may, by notification in ‘Official Gazette’ make rules to carry out the provisions of the Act.

8. Consequent to the passing of this Act, the SEBI had announced that trading of securities on the internet will be valid in India, but initially there was no specific provision for protection of confidentiality and net trading. This lacuna has been removed by the IT (Amendment) Act, 2008.

9. The Indian Penal Code, 1860 was found insufficient to cater to the needs of new crimes emerging from Internet expansion. Even some of the traditional crimes such as conspiracy, solicitation, securities, fraud, espionage etc. are now being committed through Internet which necessitates a new law to curb them. It was in this background that the Information Technology Act, 2000 was enacted in India for prevention and control of cyber crimes.

**IT Act and Cyber Space**

Prior to the enactment of this Act, the law applicable to cyber offences was the Indian Penal Code which was enacted long back in 1860 when no one even thought of computer technology or cyber criminality. With the coming into force of Information Technology Act, 2000, it became necessary to introduce certain consequential changes in certain provisions of the Penal Code as also in the Indian Evidence Act, 1872, in order to meet the new requirements of the cyberspace crimes.

With a view to widening the scope of applicability of the provisions of the IPC so as to include within its ambit, offences involving electronic records, a new Section 29-A has been inserted after Section 29 of the Indian Penal Code deals with issues relating to electronic record.

**Offences Punishable under IT Act, 2000**

The various offences and the punishment provided for them are contained in Chapters IX and XI of the Act. These offences are briefly stated as follows:

**Unauthorized Access (Section 43)**

The section lays down that any person who accesses or secures access to a computer, computer system or computer network without permission of the owner or any person in charge of such computer, computer system or computer
network, shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person who is so affected.

The term “access” as defined in Section 2(1)(a) of the I.T. Act, means “gaining entry into, instructing or communicating with the logical, arithmetic or monetary function resources of a computer, computer system or computer network. The following acts have been construed to fall within the purview of the term ‘access’ as contemplated by the Act:

(a) Unlawfully switching over a computer;
(b) Using a software program installed on a computer;
(c) Viewing the contents of a floppy disk illegally;
(d) Illegally switching off a computer;
(e) Taking a computer print-out illegally;
(f) Logging on the Internet; and
(g) Pinging a computer

Failure to Furnish Information, Return etc. (Section 44)

Where a person is required under this Act or any rules made there under to furnish any document, return or report to the Controller of Certifying Authority, fails to furnish the same, he shall be liable to pay penalty not exceeding 1.5 lakh rupees for each failure and in case of default, a penalty of 5,000/- rupees for everyday during which such failure or default continues.

Tampering with Computer Source Documents (Section 65)

Tampering with the computer source documents is made punishable under Section 65 of the I.T. Act. The offences in respect of computer source documents (codes) are to be kept or maintained by law include knowingly or intentionally (i) concealing; (ii) destroying; (iii) altering; (iv) causing another to conceal; (v) causing another to destroy; (vi) causing another to alter the computer source code. In simpler words, for the purpose of Section 65, tampering means to conceal (hide or keep secret), destroy (demolish or reduce to nothing) or alter (change in characteristic or position) the computer source document.

Hacking (Section 66)

The essential ingredients of the hacking are intention to cause wrongful loss or damage to any person by unlawful means or having knowledge that information residing in a computer resource document if concealed, destroyed or altered would cause damage to any person. This offence is punishable under this section with imprisonment which may extend to three years or with fine, which may extend to two lakh rupees or with both.

Publishing of Information which is Obscene in Electronic Form (Section 67)

Pornography on the internet is punishable under section 67 of the I.T. Act. The term ‘publishing’ for the purpose of this section means, “To make generally known, formally promulgate or issue copies for sale to public.”
disseminating of pornographic material on the website is an offence punishable with imprisonment upto three years or with fine which may extend to two lakh rupees, or with both.

**Failure to Comply with Directions of Controller (Section 68)**

Section 68 authorises the Controller or Certifying Authority to intercept any information transmitted through any computer resource whenever it is expedient to do so. Failure to comply with such order shall render a person liable to imprisonment for a term upto three years or fine upto two lakh rupees, or with both. However, the order passed by the Controller or Certifying Authority should be made if it is necessary to ensure compliance of any of the provisions of the I.T. Act or the rules made there under.

Power to issue directions of interceptions or monitoring or decryption of any information through any computer resource. (Section 69):

**Accessing Protected System (Section 70)**

The special provisions contained in Section 70 relate to protected systems. The section provides that the appropriate Government may, by notification in the Official Gazette, declare any computer, computer system or computer network to be a 'protected system'.

**Publishing Digital Signature Certificate False in Certain Particulars (Section 73)**

Publishing digital signature certificate false in certain particulars is a cyber offence punishable under section 73 of the Act. The punishment may extend to imprisonment upto two years, or with fine which may extend to one lakh rupees, or with both.

**Publishing Digital Signature Certificate for Fraudulent Purposes (Section 74)**

This section provides that whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose or knowingly publishes or makes it available for any such purpose, commits an offence under the I.T. Act and the offender may be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

**Compounding of Offences (Section 77-A)**

The new section inserted in the principal Act by the I.T. (Amendment) Act, 2008, provides for compounding of offences under the Act by the court of competent jurisdiction provided they are not punishable with imprisonment for life or imprisonment for a term exceeding three years.
Chapter II
Changes Made in IT (Amendment) Act, 2008

There are also challenges posed by the amended Act that can be foreseen and our country needs to be well equipped to overcome these challenges. Further, there are still some lacunae in the amended Act which I have briefly discussed at appropriate places. The role of Adjudicating Authority in the amended Act is very significant. The subject matter of its jurisdiction, adjudging matters alleging contravention and awarding compensation under chapter 9 is explained in clearer terms in the Amended IT Act. The amended Act also curtails the power & jurisdiction of the Adjudicating officers and excludes those matters where compensation claimed is more than 5 crores. This paper discusses the important, dimensions that emerge from the recent amendments and challenges that will be faced by the Adjudicating officers in complying with its prescribed duties under the IT Act, 2008.

The new amendments to the Information Technology Act, 2000 that got passed by the Lok Sabha last December deserve a careful reading. There are a number of positive developments, as well as many which dismay. Positively, they signal an attempt by the government to create a dynamic policy that is technology neutral. This is exemplified by its embracing the idea of electronic signatures as opposed to digital signatures. But more could have been done on this front (for instance, section 76 of the Act still talks of floppy disks). There have also been attempts to deal proactively with the many new challenges that the Internet poses.

Freedom of Expression

The first amongst these challenges is that of child pornography. It is heartening to see that the section on child pornography (s. 67B) has been drafted with some degree of care. It talks only of sexualized representations of actual children, and does not include fantasy play-acting by adults, etc. From a plain reading of the section, it is unclear whether drawings depicting children will also be deemed an offence under the section. Unfortunately, the section covers everyone who performs the conduct outlined in the section, including minors. A slight awkwardness is created by the age of “children” being defined in the explanation to section 67B as older than the age of sexual consent. So a person who is capable of having sex legally may not record such activity (even for private purposes) until he or she turns eighteen.

Another problem is that the word “transmit” has only been defined for section 66E. The phrase “causes to be transmitted” is used in section 67, 67A, and 67B. That phrase, on the face of it, would include the recipient who initiates a transmission along with the person from whose server the data is sent. While in India, traditionally the person charged with obscenity is the person who produces and distributes the obscene material, and not the consumer of such material. This new amendment might prove to be a change in that position.
Section 66A which punishes persons for sending offensive messages is overly broad, and is patently in violation of Art. 19(1) (a) of our Constitution.

The fact that some information is "grossly offensive" (s.66A(a)) or that it causes "annoyance" or "inconvenience" while being known to be false (s.66A(c)) cannot be a reasons for curbing the freedom of speech unless it is directly related to decency or morality, public order, or defamation (or any of the four other grounds listed in Art. 19(2)). It must be stated here that many argue that John Stuart Mill's harm principle provides a better framework for freedom of expression than Joel Feinberg's offence principle.

Section 69A grants powers to the Central Government to "issue directions for blocking of public access to any information through any computer resource". In English, that would mean that it allows the government to block any website. While necessity or expediency in terms of certain restricted interests are specified, no guidelines have been specified. Those guidelines, per s.69A (2), "shall be such as may be prescribed". It has to be ensured that they are prescribed first, before any powers of censorship are granted to anybody. In India, it is clear that any law that gives unguided discretion on an administrative authority to exercise censorship is unreasonable (In re Venugopal, AIR 1954 Mad 901).

**Intermediary Liability**

The amendment to the provision on intermediary liability (s.79) while a change in the positive direction, as is seeks to make only the actual violators of the law liable for the offences committed, still isn't wide enough. This exemption is required to be widely worded to encourage innovation and to allow for corporate and public initiatives for sharing of content, including via peer-to-peer technologies.

Firstly, the requirement of taking down content upon receiving "actual knowledge" is much too heavy a burden for intermediaries. Such a requirement forces the intermediary to make decisions rather than the appropriate authority (which often is the judiciary). The intermediary is no position to decide whether a Gauguin painting of Tahitian women is obscene or not, since that requires judicial application of mind. Secondly, that requirement is vitiates the principles of natural justice and freedom of expression because it allows a communication and news medium to be gagged without giving it, or the party communicating through it, any due hearing. It has been held by our courts that a restriction that does not provide the affected persons a right to be heard is procedurally unreasonable (Virendra v. State of Punjab)\(^1\)

**Privacy and Surveillance**

While the threat of cyber-terrorism might be very real, blanket monitoring of traffic is not the way forward to get results, and is sure to prove

---

\(^1\) AIR 1957 SC 896).
counterproductive. It is much easier to find a needle in a small bale of hay rather than in a haystack. Thus, it must be ensured that until the procedures and safeguards mentioned in subsections 69(2) and 69B (2) are drafted before the powers granted by those sections are exercised. Small-scale and targeted monitoring of metadata (called "traffic data" in the Bill) is a much more suitable solution, that will actually lead to results, instead of getting information overload through unchannelled monitoring of large quantities of data. If such safeguards aren't in place, then the powers might be of suspect constitutionality because of lack of guided exercise of those powers.

Very importantly, the government must also follow up on these powers by being transparent about the kinds of monitoring that it does to ensure that the civil and human rights guaranteed by our Constitution are upheld at all times.

Encryption

The amending bill does not really bring about much of a change with respect to encryption, except for expanding the scope of the government's power to order decryption. While earlier, under section 69, the Controller had powers to order decryption for certain purposes and order 'subscribers' to aid in doing so (with a sentence of up to seven years upon non-compliance), now the government may even call upon intermediaries to help it with decryption (s.69(3)). Additionally, Sec. 118 of the Indian Penal Code has been amended to recognize the use of encryption as a possible means of concealment of a 'design to commit [an] offence punishable with death or imprisonment for life'.

The government already controls the strength of permissible encryption by way of the Internet Service Provider licenses, and now has explicitly been granted the power to do so by s.84A of the Act. However, the government may only prescribe the modes or methods of encryption "for secure use of the electronic medium and for promotion of e-governance and e-commerce". Thus, it is possible to read that as effectively rendering nugatory the government's efforts to restrict the strength of encryption to 40-bit keys (for symmetric encryption).

Other Penal Provisions

Section 66F (1) (B), defining "cyber terrorism" is much too wide, and includes unauthorized access to information on a computer with a belief that that information may be used to cause injury to decency or morality or defamation, even. While there is no one globally accepted definition of cyber terrorism, it is tough to conceive of slander as a terrorist activity.

Another overly broad provision is s.43, which talks of "diminish its value or utility" while referring information residing on a computer, is overly broad and is not guided by the statute. Diminishing of the value of information residing on a computer could be done by a number of different acts, even copying of unpublished data by a conscientious whistleblower might, for instance, fall under this clause. While the statutory interpretation principle of noscitur a socii (that the word must be understood by the company it keeps) might be sought to
be applied, in this case that doesn't give much direction either.

While all offences carrying penalties above three years imprisonment have been made cognizable, they have also been made bailable and lesser offences have been made compoundable. This is a desirable amendment, especially given the very realistic possibility of incorrect imprisonments (Airtel case, for instance), and frivolous cases that are being registered (Orkut obscenity cases).

Cheating by personation is not defined, and it is not clear whether it refers to cheating as referred to under the Indian Penal Code as conducted by communication devices, or whether it is creating a new category of offence. In the latter case, it is not at all clear whether a restricted meaning will be given to those words by the court such that only cases of phishing are penalized, or whether other forms of anonymous communications or other kinds of disputes in virtual worlds (like Second Life) will be brought under the meaning of "personation" and "cheating".

While it must be remembered that more law is not always an answer to dealing with problems, whether online or otherwise, it is good to note that the government has sought to address the newer problems that have arisen due to newer technologies. But equally important is the requirement to train both the judiciary and the law enforcement personnel to minimize the possibility of innocent citizens being harassed.

Chapter III
Comparison between Information Technology Act, 2000 & 2008
Electronic Signatures Introduced

With the passage of the IT (Amendment) Act, 2008 India has become technologically neutral due to adoption of electronic signatures as a legally valid mode of executing signatures. This includes digital signatures as one of the modes of signatures and is far broader in ambit covering biometrics and other new forms of creating electronic signatures. This is a positive change as India has different segments people and all may not be technologically adept to understand and use the digital signatures. Therefore, allowing forms of authentication that are simpler to use such as retina scanning can be quite useful ineffective implementation of the Act. However, the challenge it poses is accessibility to authentication tools and imparting education to people to use the same. It is a challenging task for the Central government to prescribe conditions for considering reliability of electronic signatures or electronic authentication techniques under Section 3A (2), the procedure for ascertaining electronic signature or authentication under Section 3A(3), the manner in which information may be authenticated by electronic signatures in Section 5. It also involves expenditure as such authentication tools will require purchase, installation & training, particularly in all government departments where it is proposed to be used. Equally challenging will be the drafting of duties of subscriber of electronic signature certificate under Section 40 A of the Act which will need to incorporate security measures subscribers can adopt.
depending on electronic signature being used for signatures. Further, in a move to secure the flow of data and information on the internet, and promote e-commerce & e-governance, the amended Act in Section 84A has empowered the Central Government to prescribe modes or methods for encryption.

**Corporate Responsibility Introduced in S. 43A**

The corporate responsibility for data protection is incorporated in S 43A in the amended IT Act, 2000 whereby corporate bodies handling sensitive personal information or data in a computer resource are under an obligation to ensure adoption of "reasonable security practices" to maintain its secrecy, failing which they may be liable to pay damages. Also, there is no limit to the amount of compensation that may be awarded by virtue of this section. This section must be read with Section 85 of the IT Act, 2000 whereby all persons responsible to the company for conduct of its business shall be held guilty incase of offence was committed by a company unless no knowledge or due diligence to prevent the contravention is proved.

**Critique on Amended Section 43 of IT Act**

The amended Act provides the distinction between „contravention” and „offence” by introduction of the element of mens rea for an offence (s 43 for contraventions and s 66 of the Act for offences). It is pertinent to note that no ceiling limit for compensation is prescribed under s 43 of the Amendment Act, 2008 which was one crore rupees in the IT Act. The removal of the ceiling limit can be misused or abused particularly seen in instances where company files frivolous claims against its ex-employee who may have joined a competitor firm without breaching its employment contract.

The intention of the amended Act is to introduce the element of intention in this clause of the Section and this mens rea element also finds its roots in Section 66 where a person will be sentenced if he does the same act „dishonestly” or „fraudulently” within the meaning of IPC i.e with intention to defraud or cause wrongful loss. Intention to cause damage” in S.43(j) can be said to also include intention to cause wrongful loss. Per se „stealing” cannot be done without the mens rea in place and therefore this act should fall under s.66 and not 43 incase S.43 is to cover only acts done inadvertently or by negligence. This certainly cannot be the intention /objective of the amendment. Hence, a clarification on this point is necessary.

**Important Definitions Added**

Two very important definitions are added to the IT Act through IT Amendment Act,2008- Section 2(1) - “Communication device “ and Section 2 (w) – “intermediary”. Although cell phones and other devices used to communicate would fall under the definition of computer in the IT Act. This amendment removes any ambiguity and brings within the ambit of the Act all communication devices, cell phones, ipods or other devices used to communicate, send or transmit any text ,video ,audio or image. The insertion of definition of „intermediary” similarly clarifies the categories of service
providers that come within its definition that includes telecom service providers, network service providers, internet service provider, web hosting service providers, search engines, online payment sites, online auction sites, online marketplaces and cyber cafes.

**Legal Validity of Electronic Documents Re-emphasized**

Two new sections Section 7A and 10A in the amended Act reinforce the equivalence of paper based documents to electronic documents. Section 7A in the amended Act makes audit of electronic documents also necessary wherever paper based documents are required to be audited by law. Section 10A confers legal validity & enforceability on contracts formed through electronic means. These provisions are inserted to clarify and strengthen the legal principle in Section 4 of the IT Act, 2000 that electronic documents are attar with electronic documents and e-contracts are legally recognized and acceptable in law. This will facilitate growth of e-commerce activity on the internet and build netizen’s confidence.

**The Role of Adjudicating Officers under the Amended Act**

The Adjudicating officer’s power under the amended Act in Section 46 (1A) is limited to decide claims where claim for injury or damage does not exceed 5 crores. Beyond 5 crore the jurisdiction shall now vest with competent court. This has introduced another forum for adjudication of cyber contraventions. The words „competent court” also needs to be clearly defined. As per Section 46(2), the quantum of compensation that may be awarded is left to the discretion of Adjudicating officers.

In the IT Act, 2000 the office of adjudicating officer had the powers of civil court and all proceedings before it are deemed to be judicial proceedings. A new change is incorporated in Section 46(5) whereby the Adjudicating officers have been conferred with powers of execution of orders passed by it, including order of attachment and sale of property, arrest and detention of accused and appointment of receiver.

**Composition of CAT**

The amended Act has changed the composition of the Cyber Appellate Tribunal. The Presiding officer alone would earlier constitute the Cyber Regulations Appellate Tribunal which provision has now been amended. The tribunal would now consist of Chairperson and such number of members as Central Government may appoint. The qualifications for their appointment, term of office salary, power of superintendence, resignation and removal, filling of vacancies have been incorporated. The decision making process allows more objectivity with Section 52 D that provides that the decision shall be taken by majority.

**New Cyber Crimes as Offences under Amended Act**

Many cyber crimes for which no express provisions existed in the IT Act, 2000 now stand included by the IT (Amendment) Act, 2008. Sending of offensive or
false messages (s 66A), receiving stolen computer resource (s 66B), identity theft (s 66C), cheating by personation (s 66D), violation of privacy (s 66E). A new offence of Cyber terrorism is added in Section 66 F which prescribes punishment that may extend to imprisonment for life. Section 66 F covers any act committed with intent to threaten unity, integrity, security or sovereignty of India or cause terror by causing DoS attacks, introduction of computer contaminant, unauthorized access to a computer resource, stealing of sensitive information, any information likely to cause injury to interests of sovereignty or integrity of India, the security, friendly relations with other states, public order, decency, morality, or in relation to contempt of court, defamation or incitement to an offence, or to advantage of any foreign nation, group of individuals or otherwise. For other offences mentioned in Section 66, punishment prescribed is generally upto three years and fine of one/two lakhs has been prescribed and these offences are cognisable and bailable.

In certain offences, such as hacking (s 66) punishment is enhanced from 3 years of imprisonment and fine of 2 lakhs to fine of 5 lakhs. In S. 67, for publishing of obscene information imprisonment term has been reduced from five years to three years (and five years for subsequent offence instead of earlier ten years) and fine has been increased from one lakh to five lakhs (rupees ten lakhs on subsequent conviction).

Section 67A adds an offence of publishing material containing sexually explicit conduct punishable with imprisonment for a term that may extend to 5 years with fine upto ten lakhs. This provision was essential to curb MMS attacks and video voyeurism. Section 67B punishes offence of child pornography, child’s sexually explicit act or conduct with imprisonment on first conviction for a term upto 5 years and fine upto 10 lakhs. This is a positive change as it makes even browsing and collecting of child pornography a punishable offence. Punishment for disclosure of information in breach of lawful contract under sec 72 is increased from 2 yrs upto 5 yrs and from one lakh to 5 lakh or both.

Section 69B Added to Confer Power to Collect, Monitor Traffic Data

As a result of the amendments in 2008, Section 69 B confers on the Central government power to appoint any agency to monitor and collect traffic data or information generated, transmitted, received, or stored in any computer resource in order to enhance its cyber security and for identification, analysis, and prevention of intrusion or spread of computer contaminant in the country. The Information Technology (procedure and safeguard for monitoring and collecting traffic data or information) Rules, 2009 have been laid down to monitor and collect the traffic data or information for cyber security purposes under Section 69B.

5. Recommendation

In India well equipped with forensic knowledge and trained in cyber laws to effectively investigate cybercrime cases. The introduction of Examiner of
Electronic Evidence will also aid in effective analysis of digital evidence & cybercrime prosecution. Having discussed the new amendments and challenges before Indian cyber law regime, employing the strategies recommended below can facilitate the enforcement of cyber laws in our country. Which includes educating the common man and informing them about their rights and obligations in Cyberspace. The practical reality is that most people are ignorant of the laws of the cyberspace, different kinds of cybercrimes, and forums for redressal of their grievances. There is an imperative need to impart the required legal and technical training to our law enforcement officials, including the Judiciary and the Police officials to combat the Cybercrimes and to effectively enforce cyberlaws.

6. Conclusion

The IT(Amendment) Act, 2008 from an overall perspective has introduced remarkable provisions and amendments that will facilitate the effective enforcement of cyber law in India. India is now technologically neutral with electronic signatures replacing the requirement of digital signatures. IT (Amendment) Act, 2008 is a step in the right direction, however, there are still certain lacunae in the Act, (few of which were briefly pointed out in this paper) which will surface while the amendments are tested on the anvil of time and advancing technologies.

References

[1] Suresh.v, law relating to IT in India, published in international journal of current research, issn-0975
[2] https://pdfs.semanticscholar.org/4b3d.pdf.com visited on 13/05/2018