ZENITH International Journal of Business Economics & Management Research
Vol.2 Issue 5, May 2012, ISSN 2249 8826
Online available at http://zenithresearch.org.in/

THE INFORMATION TECHNOLOGY ACT OF INDIA: A CRITIQUE

DR. SHOBHALATA V. UDAPUDI*; BARNIK GHOSH**

*Associate Professor,
Gujarat National Law University,
Gandhinagar, Gujarat.
**Student,
Gujarat National Law University,
Gandhinagar, Gujarat.

ABSTRACT

From the last decade onwards, the march of India in the Information Technology Sectors has been phenomenal. The main reason for this is because of the large number of contracts grabbed by the Indian Companies from its foreign compatriots. These contracts have been mainly for performing data processing activities of the foreign offshore companies. The amount of revenue which came in from the procedure and the subsequent businesses have been remarkable and has boosted the otherwise stagnant and agriculturally dependant Indian economy. The initial phrases of these operational businesses have been simple transcription centers where the details of the voice recordings used to be converted to digitalized data. But of late, this practice has been transformed into centers of processing knowledge where there is a complete research being performed on different fields and several varied domains including that of medicine, technology, media, business, accounts and even that of law. Even within the country there has been increasing use of computers. Be it Airline or train reservation system or the initiative towards online collection of direct and indirect taxes, there is great amount of data about individuals and businesses which is available in digital format.

There have been concerns which have been raised from various quarters of scholars regarding the existent laws of information laws in India. Due to the increasing burden of technological transactions and entry of India into the unlimited and unbounded cyberspace made it compulsory for the Indian legislature to come up with the laws regarding control of technology in India. In the year 2000, the Information Technology Act, the first of its kind, was launched as an attempt to define the different aspects of cyber law in the country. It was also an instrument to address the misuse of e-information and subsequent securities which was proposed to be provided to the e-transactions which had tripled and increased its volume in multiple times in India.

In this paper, the author will attempt to analyze the provisions of the IT Act, 2000 and also delve into analyzing the different aspects of the recent amendments which has been instrumental in combating the various current trends which are existing in combating cyber crimes. Though this will remain the basic theme of the paper, the author will also analyze the current trends in cyber crimes which are coming up. A comparative aspect has been drawn with different countries and their respective legislations in cyber laws. Finally, the author looks to a possible way ahead.

INTRODUCTION

BACKGROUND OF THE ACT

The Model Law on Electronic Commerce was framed by the United Nations Commission on International Trade Law in the year 1996. By the Resolution A/RE S/51/162, dated January 30 1997, the United Nations General Assembly adopted this set of Model Law.

It was recommended by this resolution that all States need to give favourable considerations to the Model Law so made and in order to do this, the states should amend, enact or revise the existing laws in such a manner that there will be a uniformity with regards to the laws on Information Technology which will be applicable to the countries at large. By so doing, a common scheme of implementation can be affected in the countries on a single window format. There also needs to be a law in order to deal with the alternatives which are coming out with regard to the paper based storage and communication of information.

The Government of India through the Ministry of Commerce wing formed the first draft of the legislation following the Draft Laws of International nature on mind. This initial draft legislation was termed as the "E Commerce Act of 1998". But later, because of the projects and new ventures and transactions coming into the field, the government devised a separate ministry for the same kind of transactions which was called the Ministry of Information and Technology. They took up the task and revamping the draft and started drafting of a new legislation. This legislation piece was called the Information Technology Bill of 1999. This draft bill was placed for discussion in the Parliament in December 1999 and was finally passed in May 2000.

For the final notification of the Act to come in, the assent of the President was obtained on June 9, 2000 and finally on October 17, 2000, the Act was notified vide Notification Number G.S.R. 788 (E).

The reasons and jurisprudence behind the Act has been clearly indicated by the intention of legislature which is given in the beginning of the Act per se. This Act while being interpreted has been made very clear in its forms and procedures. Though some shady portions and incomplete enactments have been there due to the non continous nature of the Act, the act still covers the basic gist of the Government's intentions to make the Act a passing reality for the judges to stress more on the interpretative clauses.

The object of the Act has been clearly mentioned to be as follows:[1]

'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.'

[1] Shukla, Satishprakash S, Basic of Information Technology for teacher trainees, Varishen Publications, 2001

Most of the chapters and the subsequent sections of the Act have been formalized keeping in view the need to issue digital certificates and facilitate the growing trend of e commerce in India. Besides, the management of the digital certificates have also been tried to be addressed in the present Act by formation of the Root Authorities, controlling authorities and even a separating adjudicating and dispute solving authority to give the Act a boost due to its specific nature. It has also been tried that the Act should have special and overriding features of several of the Laws which are already existing in this country.[2]

But in this act, there has been only passing references to cyber crimes and as a subject, it has not been justified and has not been persuaded or perused in great depth.

Clearly, most sections addressed the need of issuance of digital certificates and management of these certificates. Cyber crime as a subject was not looked into at depth. There were only passing references to acts of cyber crime without mentioning the crime specifically. Since the implementation of the Act and since the time the legislature has brought the act into force, there has been a renewed vigor as to get all the cyber crimes adderessed through the means of this act. It has also to be understood that the cyber crimes which are taking place in India are not of a complete unique nature. It has always been emphasized that a uniform international model can be followed in order to deal with cyber crimes in general. It has also been contended by several scholars[3] that immediate redressal for the same is required in this field which has to be done with immediate effect.

THE FOUNDATIONS

From the time that the act has come into existence, there has been demands from all corners of society that there should be changes brought into the manner in which the Act is looking into the aspects of cyber crime in general and criminology in particular. It being a completely new form of law, we have seen how the aspects have developed and similarly come into being as regards the intention of the legislature so arises. Not only was cyber crimes restricted to that of siphoning of money from online bank accounts and credit cards, it included the practices of leakage of personal data and cyber pornography which played a big role in changing the very outlook of the society with regards to computers.

Computers penetrated across the length and breadth of India covering villages, towns and cities alike bringing the so long ungrided network in grided ones. Not long did it takefor the society to involve the concept of internet into regular parlance and social networking sites became a rage. Cyber crimes erupted to giant proportions taking into account even the perspectives of privacy issues.

The BPO industry in India fueled the debate for a more responsible system of the Information Technology Act and several consequent amendments were made in this regard to that of the Information Technology Act which has been of greater contentions not only with regard to that

[2] Ms Nidhi Kakkar v. Mr. Munish Kakkar, (2011)162PLR113

[3] T. SINHA and K. SUBHADRA, Sourcing the Outsourcing Arithmetic : A Journey from America to India, p. 8 available on http://papers.ssrn.com/sol3/papers.cfm?abstract_id=705801 as last accessed on the 18th of July, 2011.

of the Act in general but also with regard to that of the changing dimensions of the legal scenario which has evolved in this case. It has also been a contention that the Information Technology Act has been given a greater scope in India and an upper hand of the general criminal laws and civil laws since it is a specific act. But the point which is to be noted in this regard is how the whole development evolved through amendments.[4]

The first major amendment came about in February 2003 with the Negotiable Instruments Act being amended in this very regard. The whole scenario changed with the concepts of cheques in electronic form coming up which was somewhat of a hesitative existence from that of the time being. The act started recognizing not only the normal cheques but also electronic cheques and gave a legal validity to a concept which was in force in the market but not in the legal arguments. Several mythical science fictions were converted into legal reality and not just deeming fictions. The government slowly could relate to the growing importance of cyber laws in general and the added accelerations which were taking place with regard to that of developments in information technology and cyber laws in general.[5]

Several committees appointed by the IT Ministry looked into the changes which are taking place especially in the case of the information technology laws and consequently changed their stance about the same. The parliamentary committee, which was appointed to look into the IT Act and its applicability, suggested a list of amendments that can come in the domain of information technology laws. Several lacunas were pointed out by the committee and subsequently, the amendment bill of 2006 was brought in. Looking into the recent history of the Indian legislations, it is evident that the Information Technology Act has been amongst the most amended, criticized as well as discussed acts and the Government has played a major role in the same.

Personal data protection and privacy were the most important issues which were looked into in the 2006 amendment after the constant backlashes by fundamentalists as to the manner in which the country was running its legal system pertaining to cyber laws. It was often contended that the whole of the legislation was affected by means of the constant debates which were taking place in case of the IT Act. The Personal Data Protection Bill was introduced in the Rajya Sabha in the year 2006.[6] The most recent amendment which has shaken and stirred the general masses and companies at large was passed in 2008. The legal fraternity is waking up every day to new developments taking place during each and every passing day and hence, the author expects a lot of developments in the near future.

[4] Bhansali, S R., Information Technology and Cyber Laws, Vol. 1, Universal Book House Private Limited, 2009

[5] Lederman, Eli, Law, Information and Information technology, Kluwer law international, 2008

[6] Saxena, M K., Information technology law, Vol. 1, Mangal Deep Publications, 2007

IT ACT PROVISIONS AND AMENDMENTS

IT ACT 2000

The Indian Government took the bold step of bringing the Information Technology Act on the 17th of October, 2000 and brought it into force. The implementation of this act was thought to be a problem in the initial stages. The parliament passed the IT Act, 2000 in May 2010 while the assent was given by the President in June, 2000. The IT Act was made the lex loci or the law of the land by the Parliament in June 2000, but the very fact that Section 1(3) of the Act did not make it the law of land. It was to be made the law of land on the day the Government, may by notification appoint it to be.

The basic aim of the Information Technology Act, 2000, is to provide legal recognition to the transactions which are carried out by means of electronic data interchange and by other means of electronic communication. This is usually termed as that of e-commerce which deals with the alternatives to paper based methods of communication and the storage of information in a physical form. The Act has also been brought in to provide for and facilitate the electronic filing of documents with that of the government agencies. The filing of the documents electronically has been the latest trend in the modern times and this is how the system has changed over a period of time.[7]

The importance of the IT Act lies in the point that two distinct set of rules were provided by the Central Government. In addition, the Central Government also notified two distinct kinds of Rules. These rules are The Information Technology (Certifying Authorities) Rules, 2000 and the Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000. The Information Technology (Certifying Authorities) Rules, 2000 detail various aspects and issues concerning to Certification Authorities for digital signatures. These rules specify the manner in which information has to be authenticated by means of digital signatures, the creation and verification of digital signatures, licensing of certification authorities and the terms of the proposed licenses to issue digital signatures. The said rules also stipulate security guidelines for certification authorities and maintenance of mandatory databases by the said certification authorities and the generation, issue, term and revocation of digital signature certificates. The said rules further mandate the audit of the operations of the Certification Authority and classify various kinds of information. The said Rules also have in Schedule II the Information Technology Security Guidelines, which mandate various guidelines for the implementation and management of Information Technology Security. The said Security Guidelines are a virtual Bible for all Certification Authorities for the security aspects of their operations. The government has also specified the procedures relating to Cyber Regulations Appellate Tribunal in the notified Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000. These rules specify how an application to the Cyber Regulations Appellate Tribunal has to be preferred along with relevant documents and application fee. It further stipulates how proceedings have to be conducted by the Tribunal. It has also elaborated on the powers of the Registrar of the Cyber Regulations Appellate Tribunal. The government, by another notification of 17th October 2000, has also constituted the Cyber Regulation Advisory Committee. The committee shall advise the Central Government either generally as regards any

[7] Ryder, Rodney D., Guide to Cyberlaws: Information Technology Act, 2000, E Commerce, Data Protection and Internet, Wadhwa Publications, 2007

rules or for any other purpose connected with the IT Act, 2000. The said committee shall also advise the Controller for Certifying Authorities in framing the regulations under this Act. It comprises, amongst others, the Minister of IT, various Secretaries of different Ministries, representatives from different trade bodies and technical bodies, director of the Central Bureau of Investigation, police chiefs from the states and the Controller of Certifying Authorities. The overall net effect of all these notifications is that the IT Act, 2000 has come into operation.[8]

The information in the electronic format has been granted legal validity and sanction, digital signatures have been defined and made legal. It is now possible to retain information in an electronic format. Electronic contract has been recognized to be legal and binding. Some types of cyber crimes have been defined and made punishable offences like hacking, damage to computer source code, publishing of information which is obscene in the electronic form, breach of confidentiality and privacy and publishing digital signature certificate false in certain particulars and for fraudulent purpose. The appointment of the Controller for Certifying Authorities has kicked off the process of licensing of Certifying Authorities in India. It is expected that in a couple of months, Certifying Authorities, duly licensed by the Controller, would begin operations of issuing digital signature certificates in India. It has taken India nine Internet years to pass and notify the implementation of its first cyber law namely the Information Technology Act, 2000. The implementation of the IT Act is likely to throw up a gamut of complicated and complex legal issues as numerous areas have still not been covered under either the IT Act, 2000 or the various IT Rules. India has to face the challenges of cyberspace and its regulation in a very bold, prompt and decisive manner if it wants to become an IT superpower in the years to come.

As has been discussed earlier the IT Act 2000 was mainly to ensure legal recognition of e commerce within India. Due to this most provisions are mainly concerned with establishing digital certification processes within the country. Cyber crime as a term was not defined in the act. It only delved with few instances of computer related crime. These acts as defined in Chapter XI of the Act are:[9]

a. Illegal access, introduction of virus, denial of services, causing damage and manipulating computer accounts (Section 43)

b. Tampering, destroying and concealing computer code (Section 65)

c. Acts of hacking leading to wrongful loss or damage (Section 66)

d. Acts related to publishing, transmission or causing Publication of obscene/ lascivious in nature (section 67) Act of causing denial of service, introduction of virus etc as defined in section 43 only amounts to payment of damages which could be upto one crore. Punishment in section 65 and 66 is three years or fine up to two lakh rupees or both. For section 67 the first time offenders can be punished up to 5 years with fine up to one lakhs of rupees. Subsequent offence can lead to ten years of punishment and fine up to two lakhs of rupees.

[8] Rao, S V Jaga, Law of Cyber Crimes and Information Technology Laws, Wadhwa and Company, 2009
[9] Supra Note 4

IT ACT AMENDMENT 2008

IT Act Amendment which came into force after Presidential assent in Feb 2009 has following salient features

LIABILITY OF BODY CORPORATE TOWARDS SENSITIVE PERSONAL DATA

New amendment was brought in changes in section 43 of IT Act 2000 in which for the fist time any body corporate which deals with sensitive personal information does not have adequate controls resulting in wrongful loss or wrongful gain to any person is liable to pay damages to that person to the tune of five crores.

Introduction of virus, manipulating accounts, denial of services etc made punishable 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. This is a change from earlier position where introduction of virus, manipulating some ones account has been made punishable with imprisonment for the first time.

PHISHING AND SPAM

While this has not been mentioned specifically but this can be interpreted in the provisions mentioned here in section 66 A. Through this section sending of menacing, annoying messages and also misleading information about the origin of the message has become punishable with imprisonment up to three years and fine

STOLEN COMPUTER RESOURCE OR COMMUNICATION DEVICE

Newly added Section 66B has been introduced to tackle with acts of dishonestly receiving and retaining any stolen computer resource. This has also been made punishable with three years or fine of one lakh rupees or both.

MISUSE OF DIGITAL SIGNATURE

Section 66C. Dishonest use of somebody else's digital signature has been made punishable with imprisonment which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.

CHEATING

Cheating using computer resource has been made punished with 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 rupee (section 66D)

CYBER TERRORISM

The newly introduced section 66F talks about acts of cyber terror which threatens the unity, integrity or sovereignty of India or strike terror in the people or any section of the people include

a. Denial of service of resources in use by nation

b. Attempting to penetrate or access a computer resource without authorization or exceeding authorized access

c. Introducing or causing to introduce any computer contaminant likely to cause death or injuries to person or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or

d. knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restriced for reasons for the security of the State or foreign relations, or any restrictued information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

These acts have been made punishable with Imprisonment which may extend to imprisonment for life

CHILD PORNOGRAPHY

Newly introduced section 67 B attempts to address the issue of child pornography. Through this section it has made the publication or transmission of material in any electronic form which depicts children engaged in sexually explicit act or conduct, any one who creates, facilitates or records these acts and images punishable with imprisonment of five years and fine which may extend up to ten lakhs in first offence and seven years and fine of ten lakhs on subsequent offence.[10]

INTERMEDIARY'S LIABILITY

Intermediaries have been made liable to retain any information in the format that Central government prescribes. (Sections 67C) and are punishable for violation with a punishment of imprisonment of 3 years and fine In case of any act which affects national sovereignty intermediaries are liable to seven years (Section 69(4)).[11]

SURVEILLANCE, INTERCEPTION AND MONITORING

In order to compact cyber terrorism the government has further armed itself with drastic powers Sections 69 of IT Act 2000 amended enhances the scope from the 2000 version to include interception and monitoring. This has been a major change in the section which also empowers government not only to monitor any traffic but also block any site through any intermediary. Any

[10] Seth, Karnika, Cyber Laws in Information Technology Age, Lexis Nexis Butterworth and Wadhwa Publications, 2010
[11] Ibid

failure on part of the intermediary is punishable by seven years and also fine (Section 69(4)). Earlier the provision did not mention any fine.[12]

COGNIZANCE OF CASES

All cases, which entail punishment of three years or more, have been made cognizable. Offences with three years punishment have also been made bailable (Section 77B). This change though welcome will make sure most cases falling under IT Act will e bailable with sole exception of Cyber terrorism cases, cases related to child pornography and violations by intermediaries in some cases.[13]

INVESTIGATION OF OFFENCES

One major change has been inclusion of Inspectors as investigating officers for offences defined in this act (section 78). Earlier these investigations were being done only by an officer of the rank of Deputy Superintendent of Police which was a serious limitation mainly because number of officers in this rank is limited. With this change one can look forward to more cases being filed and investigated by police.[14]

SHORTCOMINGS

Till year 2000, India did not have any legislation governing cyber space or Information Technology Law.[15] To give consideration to the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) and to give legal recognition to electronic commerce the Information Technology Act, 2000 was enacted. Though this is comparatively a new legislation as far as others areas of law are concerned, still 8 years have passed since this act was enacted and in these 8 years Technology has changed at a much faster pace. Though law cannot possibly be expected to keep pace with changes in technology, still there are few areas in the current cyber laws which need some attention.[16]

SPAMMING

Spam may be defined as Unsolicited Bulk E-mail. Initially it was viewed as a mere nuisance but now it is posing major economic problems. I think almost all of us receive many unwanted mails daily. Though there are some technical methods to deal with spam, they are not very effective and adequate in dealing with this menace. In the absence of any adequate technical protection, stringent legislation is required to deal with the problem of spam. The Information Technology Act does not discuss the issue of spamming at all. USA and the European Union have enacted

[12] Rao, S V Jaga, Law of Cyber Crimes and Information Technology Laws, Wadhwa and Company, 2009
[13] Ibid
[14] Gupta, Apar, Commentary on Information Technology Act, Wadhwa Publications, 2010
[15] Ibid
[16] Jenkins, Glenn P., Information Technology and Innovation in Tax Administration, Kluwer law international, 2010

anti spam legislation. In fact Australia has very stringent spam laws under which the spammers may be fined up to 1.1 million dollars per day.[17]

PORNOGRAPHY

Though the Information Technology Act talks about publishing of information which is "obscene" in nature, it doesn't specifically define what is obscene and what may be classified as pornography. Even the punishment for pornography is not sufficient in India. In China the punishment for maintaining pornographic website is life imprisonment but by the proposed amendment in IT Act the imprisonment is being reduced to two years from the present five year imprisonment. Also the intermediaries are exempted from any liability. Though legislations worldwide contain severe provisions for child pornography there is no mention of child pornography in the Indian Act. It is interesting to note down that the Information Technology Act prohibits publishing of pornography but viewing of pornography is not an offence under the act.

PHISHING

According to scholars, phishing is the 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] Phishing is typically carried out by e-mail and often directs users to enter personal and financial details at a website. Phishing is an example of social engineering technique used to fool users. There is no law against phishing in the Information Technology Act though the Indian Penal Code talks about cheating, it is not sufficient to check the activity of phishing. Recently a phishing attack was noticed on the customers of State Bank of India in which a clone of the SBI website was used. What is worse is that even SBI has not alerted its customers. So the need of the hour is a legislation which prohibits the activity of phishing in India.

DATA PROTECTION IN INTERNET BANKING

Data protection laws primarily aim to safeguard the interest of the individual whose data is handled and processed by others. Internet Banking involves not just the banks and their customers, but numerous third parties too. Information held by banks about their customers, their transactions etc. changes hand several times. It is impossible for the banks to retain information within their own computer networks. High risks are involved in preventing leakage or tampering of data which ask for adequate legal and technical protection. India has no law on data protection leave alone a law governing an area as specific as protection of data in electronic banking.[19]

The Information Technology Act talks about unauthorized access but it does not talk about maintaining integrity of customer transactions. The act does not lay down any duty upon banks to protect the details of customers and clients. U.K has a data protection law which was enacted

[17] Lederman, Eli, Law, Information and Information technology, Kluwer law international, 2008
[18] Broderick, Terry R ., Regulation of Information Technology in the European Union, Kluwer law international, 2008
[19] Supra Note 12

10 years back that is in 1998 under which banks or any person holding sensitive information may be held liable for damages if it fails to maintain adequate security protection in respect of data. In India, a bank's liability would arise out of contract as there is no statute on the point.[20]

PRIVACY PROTECTION

Privacy and data protection are important issues that need to be addressed today as information technology assumes greater importance in personal, professional and commercial spheres. The European Union and the United States have strict policies relating to privacy and protection of personal data when such data or information is being transferred out of their domain.

It also pertinent to note here, that the absence of a specific privacy law in India has resulted in a loss of substantial foreign investment and other business opportunities. This deficiency has also served as an obstacle to the real growth of electronic commerce. Thus, a statute addressing various issues related to privacy is of utmost importance today, if not an entire act can be brought into force, then at least specific provisions relating to privacy and data protection be incorporated into the Act.

MAJOR DILUTIONS

SEXUALLY EXPLICIT CONTENT

Newly introduced section 66 E talks about acts of intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both. In fact the earlier section 67 of IT Act did mention 'any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave..' and was punishable for first offence with five years of imprisonment and fine of one lakh rupees. This change has made the provision lenient and open to misinterpretation.[21]

COMPLIANCE WITH ORDERS OF CONTROLLER

Section 68(2), which earlier made failure to comply with the direction of controller punishable with three years of imprisonment or fine of two lacks or both now, has been reduced to two years punishment or fine of one lakh of rupees or both

[20] Girot, Clarisse, User protection in IT contracts: comparative study of the protection of the user against defective performance in information technology, Kluwer Law Publications, 2010

[21] Seth, Karnika, Cyber Laws in Information Technology Age, Lexis Nexis Butterworth and Wadhwa Publications, 2010

INTERNATIONAL SCENARIO

ANTI SPAM LAWS

UNITED STATES

United States has a specific CAN-Spam Act 20037 which came into force in January 2004. Major provisions are

• False and misleading header information is banned

• Deceptive subject lines are prohibited

• Opt-out methods must be provided

• Commercial email must be identified as an advertisement and it must include the sender's valid physical postal address

• Receivers must be warned of sexually explicit material

Penalties include fine upto USD 11000 and also imprisonment in specific circumstances.

EUROPE

Europe union through directive on privacy and electronic communication, 2003 has been major driving force behind enactments of anti spam laws in Europe. UK imposes a fine of GBP 5000 on spammers if they fall within the ambit of its Anti Spam Act.[22]

CONCLUSION

Freedom of Expression is assured to all Indian citizens under the constitution. This lays the foundation for a free press which alone is responsible for making people aware of what is going on around them. But the information that is present in the newspapers and on television is not everything that the citizens would like to know. There is a lot that happens backstage!

There is a lot that never makes the headline. With all the corruption and the threatening in place, rarely can the journalists do their duty. With Journalism being the Fourth pillar of democracy, it becomes imperative for them to bring forward the truth. As if all the monetary censorship and paid news was not enough, the government is trying to tie a leash around the only avenue from where the public can acquire diverse information and engage in communication -Internet!

With the new IT Act 2011, the free exchange of information on Internet too would be restricted. The government has tried its level best to curb the freedom of the netizens in the past by demanding to access the emails of Blackberry users and now, by bringing up the IT law!

[22] Supra Note 7

The act has been drafted to keep in check the security breaches that happen due to free flow of information on the internet, or so the government says. In truth, such a law would give the power to the government and the corporates to get any content removed from the web. After looking at the role that the social networking websites played in getting out the story of involvement of Barkha Dutt and Vir Sanghvi in the 2G scam, I really think people would believe in the power of internet.

The draft talks about the removal of content that is 'Disparaging', 'Blasphemous'or 'Hateful'; what exactly do these terms refer to is not defined accurately. It gives a person a huge margin for ambiguous interpretations!

If this act gets passed as a law, it would become a deadly weapon in the hands of the rich and the powerful. The content on the web would be according to their whims and fancies. This would help them further their cause at the cost of ignorance for others. Apart from that the main reason given for drafting the act- security – might not even be taken care of.

Passing of the act would be a complete loss statement for the general public. They would be losing out on their last opportunity for expressing their thoughts freely as well as the last avenue offering them the scenes behind the curtain, that too without any benefit.

The UN has said that free internet should be a fundamental right of every citizen.

It would be a tragedy to have such a law in the country. India would not be much better off than China then. As our constitution says 'We the People', thus placing us at the topmost position in the hierarchy of power.