INTELLECTUAL PROPERTY RIGHTS .
PAPER – II

TOPIC : Salient features of The Information Technology Act, 2000 .

Name : Audi Shanoor Pandurang .
Class: Second Year L L.M .
Roll No. : 02 .
Year : 2013 -2014 .

Govind Ramnath Kare College Of Law.
Margao – Goa.

CONTENTS

CASES REFERRED

- **SAJEESH KRISHNAN V. STATE OF KERALA**
- **NIKHIL CHACKO SAM V. STATE OF KERALA**
- **J.R. GANGWANI AND ANOTHER V. STATE OF HARYANA AND OTHERS**
- **MOHAMMAD AMJAD V. SHARAD SAGAR SINGH AND ORS.**
- **SANDEEP VARGHESE VS. STATE OF KERALA.**
- **JAWAHARLAL NEHRU UNIVERSITY MMS SCANDAL**
- **NAGPUR CONGRESS LEADERS MMS SCANDAL**
- **JANHIT MANCH AND OTHERS VS. THE UNION OF INDIA**
- **STATE OF TAMIL NADU VS SUHAS KUTTI :**
- **SMC PNEUMATICS (INDIA) PVT. LTD. V. JOGESH KWATRA**
- **NASSCOM VS. AJAY SOOD & OTHERS**
- **GOOGLE INDIA PVT. LTD., VERSUS VISAKA INDUSTRIES LIMITED AND ANOTHER.**
- **MICROSOFT CORPORATION V. YOGESH PAPAT, DELHI HIGH COURT**

SALIENT FEATURES OF INFORMATION TECHNOLOGY ACT, 2000.

I) THE GENESIS OF INFORMATION TECHNOLOGY LEGISLATION IN INDIA:

Mid 90's saw an impetus in globalization and computerization, with more and more nations computerizing their governance, and e-commerce seeing an enormous growth. Until then, most of international trade and transactions were done through documents being transmitted through post and by telex only. Evidences and records, until then, were predominantly paper evidences and paper records or other forms of hard-copies only. With much of international trade being done through electronic communication and with email gaining momentum, an urgent and imminent need was felt for recognizing electronic records i.e. the data what is stored in a computer or an external storage attached thereto.

The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on e-commerce in 1996. The General Assembly of United Nations passed a resolution in January 1997 inter alia, recommending all States in the UN to give favorable considerations to the said Model Law, which provides for recognition to electronic records and according it the same treatment like a paper communication and record.

II) BRIEF HISTORY:

New communication systems and digital technology have made dramatic changes in the way we live and the means to transact our daily business. Businessmen are increasingly using computers to create, transmit and store information in electronic form instead of traditional paper documents. It is cheaper, easier to store and retrieve and speedier to communicate. Although people are aware of the advantages which the electronic form of

business provides, people are reluctant to conduct business or conclude and transaction in the electronic form due to lack of appropriate legal framework. Electronic commerce eliminates need for paper based transactions. The two principal hurdles which stand in the way of facilitating electronic commerce and electronic governance, are the requirements of writing and signature for legal recognition. At present many legal provisions assume the existence of paper based records and documents which should bear signatures. The Law of Evidence is traditionally based upon paper-based records and oral testimony. Hence, to facilitate e-commerce, the need for legal changes has become an urgent necessity.

The Government of India realized the need for introducing a new law and for making suitable amendments to the existing laws to facilitate e-commerce and give legal recognition to electronic records and digital signatures. The legal recognition to electronic records and digital signatures in turn will facilitate the conclusion of contracts and the creation of legal rights and obligations through the electronic communication like Internet. This gave birth to the Information Technology Bill, 1999.

In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the Information Technology Act, 2000.This Act aims to provide the legal infrastructure for e-commerce in India and would have a major impact for e-businesses and the new economy in India. Therefore, it is important to understand ‘what are the various perspectives of the Information Technology Act, 2000 and what it offers’.

The Information Technology Act, 2000 also aims to provide the legal framework under which legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability.

The Parliament of India passed its first Cyber law, the Information Technology Act, 2000. This not only provides the legal infrastructure for E-commerce in

India but it simultaneously awards draconian powers to the Police to enter and search, without any warrant, any public place for the purpose of nabbing cyber criminals and preventing cyber crime.

III) HOW THE ACT IS STRUCTURED:

The Act totally has 13 chapters and 90 sections (the last four sections namely sections 91 to 94 in the Information Technology Act , 2000 dealt with the amendments to the four Acts namely the Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and the Reserve Bank of India Act 1934). The Act begins with preliminary and definitions and from thereon the chapters that follow deal with authentication of electronic records, digital signatures, electronic signatures etc. Elaborate procedures for certifying authorities (for digital certificates as per Information Technology Act -2000 and since replaced by electronic signatures in the Information Technology Act Amendment -2008) have been spelt out. The civil offence of data theft and the process of adjudication and appellate procedures have been described. Then the Act goes on to define and describe some of the well-known cyber crimes and lays down the punishments therefore. Then the concept of due diligence, role of intermediaries and some miscellaneous provisions have been described. Rules and procedures mentioned in the Act have also been laid down in a phased manner, with the latest one on the definition of private and sensitive personal data and the role of intermediaries, due diligence etc., being defined as recently as April 2011.

IV) OBJECT OF THE INFORMATION TECHNOLOGY ACT, 2000 [1]:

The object of The Information Technology Act, 2000 as defined therein is as under :-

[1] New Delhi, the 9th June, 2000/Jyaistha19, 1922 (Saka)The following Act of Parliament received the assent of the President on the 9th June, 2000, and is hereby published for general information:—THE INFORMATION TECHNOLOGY ACT, 2000 (No. 21 OF 2000)

"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 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 Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

V) APPLICABILITY:

The Act extends to the whole of India and except as otherwise provided, it applies to also any offence or contravention there under committed outside India by any person. There are some specific exclusions to the Act (i.e. where it is not applicable) as detailed in the First Schedule, stated below:

- negotiable instrument (other than a cheque) as defined in Section 13 of the Negotiable Instruments Act, 1881;
- a power-of-attorney as defined in Section 1A of the Powers-of-Attorney Act, 1882;
- a trust as defined in Section 3 of the Indian Trusts Act, 1882
- a will as defined in clause (h) of Section 2 of the Indian Succession Act, 1925 including any other testamentary disposition
- any contract for the sale or conveyance of immovable property or any interest in such property;
- any such class of documents or transactions as may be notified by the Central Government.

VI) HIGHLIGHTS OF THE ACT :

Chapter-II of the Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by the use of a public key of the subscriber.

Chapter III of the Act details about the electronic governance and provides *inter alia* amongst others that where any law provides that information or any other matter shall be in writing or in typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is

(a) rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference

The said chapter also details the legal recognition of digital signatures.

Chapter IV of the said Act gives a scheme for the regulation of certifying authorities. The Act envisages a Controller who shall supervise the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities. The Controller will also specify the various forms and content of digital signature certificates. The Act accepts the need for recognizing foreign certifying authorities and it further details the various provisions for the issuance of license to issue digital signature certificates.

Chapter VII of the Act details the scheme of things relating to digital signature certificates. The duties of subscribers are also enshrined in the Act.

Chapter IX talks about penalties and adjudication for various offences. The penalties for damage to a computer system have been fixed as damages by way of compensation not exceeding Rs 1,00,00,000. The Act talks of appointment of an officer not below the rank of a Director to the Government of India or an equivalent officer of a state government as an Adjudicating Officer to judge whether any person has made a contravention of any of the provisions of the Act. The officer has been given the powers of a civil court.

The Act in **Chapter X** talks of the establishment of Cyber Regulations Appellate Tribunal, an appellate body where appeals against the orders passed by the Adjudicating Officers shall be preferred.

Chapter XI of the Act talks about various offences, which could be investigated only by a police officer not below the rank of Deputy Superintendent of Police. These offences include tampering with computer source documents, publishing of information that is obscene in electronic form and hacking.

Hacking has been properly defined in Section 66 as, "Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking." Further for the first time, punishment for hacking as a cyber crime prescribed in the form of imprisonment upto 3 years or with fine which may extend to Rs. 2,00,000/- or with both. This is a welcome measure as hacking has assumed tremendous importance in the present day scenario. On previous occasions, the web sites of the Government have been hacked into but no legal provision within the existing legislation could be invoked to cover "hacking" as a cyber crime. It shall now be possible to try and punish hackers under section 66 of the Information Technology Act , 2000,2000.

The said Act also provides for the constitution of the Cyber Regulations Advisory Committee which shall advice the government as regards any rules or for any other purpose connected with the said act. The said Act also has four Schedules which amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the Information Technology Act , 2000.

VII) SALIENT FEATURES OF THE INFORMATION TECHNOLOGY ACT, 2000:

(i) Extends to the whole of India (Section 1) ;

(ii) Authentication of electronic records (Section 3) ;

(iii) Legal Framework for affixing Digital signature by use of asymmetric crypto system and hash function (Section 3) ;

(iv) Legal recognition of electronic records (Section 4);

(v) Legal recognition of digital signatures (Section 5) ;

(vi) Retention of electronic record (Section 7);

(vii) Publication of Official Gazette in electronic form (Section 8);

(viii) Security procedure for electronic records and digital signature (Sections 14, 15, 16);

(ix) Licensing and Regulation of Certifying authorities for issuing digital signature certificates (Sections 17-42);

(x) Functions of Controller (Section 18);

(xi) Appointment of Certifying Authorities and Controller of Certifying Authorities, including recognition of foreign Certifying Authorities (Section 19);

(xii) Controller to act as repository of all digital signature certificates (Section 20);

(xiii) Data Protection (Sections 43 & 66);

(xiv) Various types of computer crimes defined and stringent penalties provided under the Act (Section 43 and Sections 66, 67, 72);

(xv) Appointment of adjudicating officer for holding inquiries under the Act (Sections 46 & 47);

(xvi) Establishment of Cyber Appellate Tribunal under the Act (Sections 48-56);

(xvii) Appeal from order of Adjudicating Officer to Cyber Appellate Tribunal and not to any Civil Court (Section 57);

(xviii) Appeal from order of Cyber Appellate Tribunal to High Court (Section 62);

(xix) Interception of information from computer to computer (Section 69);

(xx) Protection System (Section 70);

(xxi) Act to apply for offences or contraventions committed outside India (Section 75);

(xxii) Investigation of computer crimes to be investigated by officer at the DSP (Deputy Superintendent of Police) level;

(xxiii) Network service providers not to be liable in certain cases (Section 79);

(xxiv) Power of police officers and other officers to enter into any public place and search and arrest without warrant (Section 80);

(xxv) Offences by the Companies (Section 85);

(xxvi) Constitution of Cyber Regulations Advisory Committee who will advice the Central Government and Controller (Section 88).

VIII) THE AIMS AND OBJECTIVES OF THE ACT :

(a) a facilitating Act,

(b) an enabling Act, and

(c) a regulating Act

(a) A Facilitating Act:

The Information Technology Act, 2000 is a facilitating Act as it facilitates both e-commerce and e-governance. Interestingly, the UNCITRAL Model Law of E-commerce on which this Act is based has made no reference to e-governance. But it was the collective wisdom of the legislature, which saw the necessity of introducing concepts like e-governance in this Act. In fact, the entire Chapter III of the Act is devoted to e-governance and e-governance practices. There are 7 sections in the aforesaid Chapter III of the Act, from section 4 to section 10, which deal with e-governance issues. These sections form the basic law related to electronic governance rights, which have been conferred to the persons and the Government(s) both Central and State Governments. It is applicable to the whole of India, including the State of Jammu and Kashmir. It is important to understand that the Information Technology Act, 2000 is the first enactment of its kind in India, which grants e-governance rights to the citizens of India

(b) An Enabling Act :

The Information Technology Act, 2000 is an enabling Act as it enables a legal regime of electronic records and digital signatures. That is, in order to be called legally binding all electronic records, communications or transactions must meet the fundamental requirements, one authenticity of the sender to enable the recipient (or relying party) to determine who really sent the message, two messages integrity, the recipient must be able to determine whether or not the message received has been modified en route or is incomplete and third, non-repudiation, the ability to ensure that the sender cannot falsely deny sending the message, nor falsely deny the contents of the message. The Act provides for Digital signatures, which may be considered functional equivalent to physical world signatures capable of meeting all the fundamental requirements, like authenticity of the sender, message integrity and non-repudiation. Digital signature is a misnomer. It does not mean scanning the handwritten signatures electronically. In fact by applying digital signatures one may actually transform an electronic message into an alphanumeric code. It requires a key pair (private key for encryption and public key for decryption) and a hash function (algorithm).

(c) A Regulating Act :

The Information Technology Act, 2000 is a regulating Act as it regulates cyber crimes. As stated above, cyber crime is a collective term encompassing both cyber contraventions and cyber offences. The Act not only demarcates contraventions from offences, but also provides a separate redressal mechanism for both.

IX) ADVANTAGES OF INFORMATION TECHNOLOGY ACT , 2000 :

The Information Technology Act , 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.

From the perspective of e-commerce in India, the Information Technology Act 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.

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

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

The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.

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

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.

The Information Technology Act also addresses the important issues of security, which are so 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 have been passed through a system of a security procedure, as stipulated by the Government at a later date.

Under the Information Technology Act, 2000, it shall now be possible for corporates 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.

X) THE GREY AREAS OF THE INFORMATION TECHNOLOGY ACT, 2000[2]:

1. The Information Technology Act, 2000 is likely to cause a conflict of jurisdiction.

2. Electronic commerce is based on the system of domain names. The Information Technology Act, 2000 does not even touch the issues relating to domain names. Even domain names have not been defined and the rights and liabilities of domain name owners do not find any mention in the law.

3. The Information Technology Act, 2000 does not deal with any issues concerning the protection of Intellectual Property Rights in the context of the online environment. Contentious yet very important issues concerning online copyrights, trademarks and patents

[2] Mishra,RC , " Cyber crime: impact in the new millennium", 2002 ed., p.53

have been left untouched by the law, thereby leaving many loopholes.

4. As the cyber law is growing, so are the new forms and manifestations of cyber crimes. The offences defined in the Information Technology Act, 2000 are by no means exhaustive. However, the drafting of the relevant provisions of the Information Technology Act, 2000 makes it appear as if the offences detailed therein are the only cyber offences possible and existing. The Information Technology Act, 2000 does not cove various kinds of cyber crimes and Internet related crimes. These include:-

a) Theft of Internet hours

b) Cyber theft

c) Cyber stalking

d) Cyber harassment

e) Cyber defamation

f) Cyber fraud

g) Misuse of credit card numbers

h) Chat room abuse.

5. The Information Technology Act, 2000 has not tackled several vital issues pertaining to e-commerce sphere like privacy and content regulation to name a few. Privacy issues have not been touched at all.

6. Another grey area of the Information Technology Act is that the same does not touch upon any anti- trust issues.

7. The most serious concern about the Indian Cyber law relates to its implementation. The Information Technology Act, 2000 does not lay down parameters for its implementation. Also, when internet penetration in India is extremely low and government and police officials, in general are not very computer savvy, the new Indian cyber law raises more questions than it answers. It seems that the Parliament would be required to amend the Information Technology Act, 2000 to remove the grey areas mentioned above.

8. The Information Technology Act , 2000 does not touch at all the issues relating to Domain Names. Even Domain Names have not been defined and the rights and liabilities of Domain Name owners do not find any mention in the said law. It may be submitted that

Electronic Commerce is based on the system of Domain Names and excluding such important issues from the ambit of India's First Cyber law does not appeal to logic.

9. The Information Technology Act , 2000 does not also deal at all with the Intellectual Property Rights of Domain Name owners. Contentious yet very important issues concerning Copyright, Trademark and Patent have been left untouched in the said law thereby leaving many loopholes in the said law.

XI) CYBER CRIME AND INFORMATION TECHNOLOGY ACT 2000:

In Indian law, cyber crime has to be voluntary and willful, an act or omission that adversely affects a person or property. The Information Technology Act provides the backbone for e-commerce and India's approach has been to look at e-governance and e-commerce primarily from the promotional aspects looking at the vast opportunities and the need to sensitize the population to the possibilities of the information age. There is the need to take in to consideration the security aspects

XII) INFORMATION TECHNOLOGY ACT WITH AMENDMENTS[3]:

The IT Amendment Bill 2008 has been passed by the Lok Sabha and the Rajya Sabha in the last week of December, 2008. The said Bill aims to make sweeping changes in the existing Indian cyberlaw, namely the Information Technology Act, 2000[4].

The Information Technology Act, 2000 is India's mother legislation regulating the use of computers, computer systems and computer networks as also data and information in the electronic format. The said legislation has provided for the legality of the

[3] As passed by the Lok Sabha on 22.12.2008
[4] Bill No. 96-C of 2006

electronic format as well as electronic contracts. This legislation has touched varied aspects pertaining to electronic authentication, digital signatures, cyber crimes and liability of network service providers.

From 17th October, 2000 , when the Information Technology Act , 2000 came into implementation till date, the said legislation has seen some very interesting cases and challenges, being brought within its ambit. As time passed by, the inadequacies of the said legislation came to the forefront. There were various practical difficulties in the implementation of the said legislation. The inadequacy of the Information Technology Act , 2000 to address some of the emerging phenomena, challenges and cyber crimes, led to voices clamoring for change in the Indian cyber law.

Consequently, the Government of India tabled the Information Technology Amendment Bill, 2006 before both the houses of Parliament in December, 2006, which referred the said amendment bill to the Parliamentary Standing Committee on Information Technology. The Parliamentary Standing Committee examined the proposed amendments in a comprehensive manner and thereafter gave its report and recommendations thereon.

The Parliamentary Standing Committee on Information Technology headed by Shri Nikhil Kumar, MP did an excellent job in terms of producing its exhaustive recommendations. These recommendations were noteworthy for their fore vision and clarity of thought process. Way back in 2007, the Standing Committee had recommended that the entire menace of cyber terrorism needs to be addressed with a strong hand.

After examining the said recommendations, the Central Government brought the Information Technology Amendment Bill, 2008 in Parliament, which got passed by both the houses of Parliament.

Given the magnitude of the amendments, it is indeed strange and amazing that this Bill was passed in an unprecedented hurry, without any discussion in both the houses of the Parliament in the last week of December, 2008.

The IT Amendment Act 2008 brings about various sweeping changes in the existing Cyber law. While the lawmakers have to be complemented for their appreciable work removing

various deficiencies in the Indian Cyber law and making it technologically neutral, yet it appears that there has been a major mismatch between the expectation of the nation and the resultant effect of the amended legislation. The most bizarre and startling aspect of the new amendments is that these amendments seek to make the Indian cyber law a cyber crime friendly legislation; - a legislation that goes extremely soft on cyber criminals, with a soft heart; a legislation that chooses to encourage cyber criminals by lessening the quantum of punishment accorded to them under the existing law; a legislation that chooses to give far more freedom to cyber criminals than the existing legislation envisages; a legislation which actually paves the way for cyber criminals to wipe out the electronic trails and electronic evidence by granting them bail as a matter of right; a legislation which makes a majority of cyber crimes stipulated under the Information Technology Act , 2000 as bailable offences; a legislation that is likely to pave way for India to become the potential cyber crime capital of the world.

NEW PROVISIONS ADDED THROUGH AMENDMENTS [5]:

1. New Section to address technology neutrality from its present "technology specific" form (i.e. Digital Signature to Electronic Signature) Section 3A;

2. New Section to address promotion of e-Governance & other IT application (i) Delivery of Service; (ii) Outsourcing – Public Private Partnership Section 6A;

3. New Section to address electronic contract Section 10A;

4. New Section to address data protection and privacy Section 43;

5. Body corporate to implement best security practices Sections 43A & 72A;

6. Multimember Appellate Tribunal Sections 49-52.

7. New Section to address new forms of computer misuse

5 Information Technology act 2000 & amendments therein by E.K. Bharat Bhushan

Impersonation Section 419A

Identity theft and E-commerce frauds like phishing Section 417A

Video voyeurism Section 502A

Offensive messages and Spam Section 66A

Pornography Section 67A

8. Preservation and Retention of Data/Information Section 67C

9. Revision of existing Section 69 to empower Central Government to designate agencies and issue direction for interception and safeguards for monitoring and decryption Section 69

10. Blocking of Information for public access Section 69A

11. Monitoring of Traffic Data and Information for Cyber Security Section 69B

12. New section for designating agency for protection of Critical Information Infrastructure Section 70A

13. New Section for power to CERT-In to call and analyse information relating to breach in cyber space and cyber security Section 70B

14. Revision of existing Section 79 for prescribing liabilities Section 79of service providers in certain cases and to Empower Central Government to prescribe guidelines to be observed by the service providers for providing services. It also regulate cyber cafes. Section 79

15. New Section for Examiner of Digital Evidence Section 79A

16. New Section for power to prescribe modes of Encryption Section 84A

17. Punishment for most of offences were reduced from three years to two years.

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.[6]

Freedom of Expression

The first amongst these challenges is that of child pornography. It is heartening to see that the section on child pornography (Section 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 conducts 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 Article 19(1)(a) of our Constitution. The fact that some information is "grossly offensive" (Section 66A(a)) or that it causes "annoyance" or "inconvenience" while being known to be false (Section 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 Article 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. The latter part

---

6 Short note on IT Amendment Act, 2008 by Pranesh Prakash

of Section 66A(c), which talks of deception, is sufficient to combat spam and phishing, and hence the first half, talking of annoyance or inconvenience is not required. Additionally, it would be beneficial if an explanation could be added to Section 66A(c) to make clear what "origin" means in that section. Because depending on the construction of that word Section 66A(c) can, for instance, unintentionally prevent organisations from using proxy servers, and may prevent a person from using a sender envelope different form the "from" address in an e-mail (a feature that many e-mail providers like G-mail implement to allow people to send mails from their work account while being logged in to their personal account). Furthermore, it may also prevent remailers, tunneling, and other forms of ensuring anonymity online. This doesn't seem to be what is intended by the legislature, but the section might end up having that effect. This should hence be clarified.

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 Section 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 any body. In India, it is clear that any law that gives unguided discretion on an administrative authority to exercise censorship is unreasonable[7].

Intermediary Liability

The amendment to the provision on intermediary liability (Section 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

[7] re Venugopal, AIR 1954 Mad 901

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[8].

The intermediary loses protection of the act if (a) it initiates the transmission; (b) selects the receiver of the transmission; and (c) selects or modifies the information. While the first two are required to be classified as true "intermediaries", the third requirement is a bit too widely worded. For instance, an intermediary might automatically inject advertisements in all transmissions, but that modification does not go to the heart of the transmission, or make it responsible for the transmission in any way. Similarly, the intermediary may have a code of conduct, and may regulate transmissions with regard to explicit language (which is easy to judge), but would not have the capability to make judgments regarding fair use of copyrighted materials. So that kind of "selection" should not render the intermediary liable, since misuse of copyright might well be against the intermediary's terms and conditions of use.

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 counter-productive. It is much easy 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 sub-sections 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

8 Virendra v. State of Punjab, AIR 1957 SC 896

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 (Section 69(3)). Additionally, s.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 licences, 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 Section 43, which talks of "diminish[ing] 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 whistle blower 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 penalised, 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".

XIII) CYBER CRIMES AND POSITION IN INDIA:

Cases of cyber defamation do not fit neatly in the accepted categories of crimes. They represent harm of greater magnitude than the traditional crimes and of a nature different from them. Unlike the traditional crimes, they are not in the shape of positive aggressions or invasions[9]. They may not result in direct or immediate injury; nevertheless, they create a danger, which the law must seek to minimize. Hence, if legislation applicable to such offences, as a matter of policy, departs from legislation applicable to ordinary crimes, in respect of the traditional requirements as to mens rea and the other substantive matters, as well as on points of procedure, the departure would be justified[10]

An effort is still wanted to formulate an international law on the use of Internet to curb this imminent danger of cyber crimes and to achieve a crime free cyber space.

---

9 Chris Reed (Ed.), COMPUTER LAW, 5th ed., 2000, p.392.

10 Ibid.

Defamation laws should be sufficiently flexible to apply to all media.

The difficulty is that the defamation laws world over were principally framed at a time when most defamatory publications were either spoken or the product of unsophisticated printing.

We do need a stronger legal & enforcement regime in India to combat the increasing cyber crimes or in other words, efficacy in dispensation of justice will be instrumental in curtailing such activities.

The position in Indian law is not very clear and amendments should be brought to Section 67 of the Information Technology Act, 2000[11] and also to Section 499 of the Indian Penal Code[12] by expressly bring within their ambit offences such as defamation in cyber space, which is certainly a socio-economic offence.

---

[11] Publishing of information which is obscene in electronic form.
Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

[12] Defamation: - Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, of defame that person.

XIV) INDIAN CASE STUDIES:

SECTION 66 A : SENDING OFFENSIVE OR FALSE MESSAGES .

SAJEESH KRISHNAN V. STATE OF KERALA (KERALA HIGH COURT, DECIDED ON JUNE 5, 2012)

Petition before High Court for release of passport seized by investigating agency during arrest.

In the case of Sajeesh Krishnan v. State of Kerala (Decided on June 5, 2012), a petition was filed before the Kerala High Court for release of passport seized at the time of arrest from the custody of the investigating agency. The Court accordingly passed an order for release of the passport of the petitioner.

The Court, while deciding the case, briefly mentioned the facts of the case which were relevant to the petition. It stated that the "gist of the accusation is that the accused pursuant to a criminal conspiracy hatched by them made attempts to extort money by black mailing a Minister of the State and for that purpose they have forged some CD as if it contained statements purported to have been made by the Minister." The Court also noted the provisions under which the accused was charged. They are Sections 66-A(b) and 66D of the Information Technology Act, 2000 along with a host of sections under the Indian Penal Code, 1860 (120B – Criminal Conspiracy, 419 – Cheating by personation, 511- Punishment for attempting to commit offences punishable with imprisonment for life or other imprisonment, 420 – Cheating and dishonestly inducing delivery of property, 468 – Forgery for purpose of cheating, 469 – Forgery for purpose of harming and 201 – Causing disappearance of evidence of offence, or giving false information to screen offender read with 34 of Indian Penal Code, 1860)

NIKHIL CHACKO SAM V. STATE OF KERALA (KERALA HIGH COURT, DECIDED ON JULY 9, 2012)

Order of the Kerala High Court on issuing of the summons to the petitioner

In another case, the Kerala High Court while passing an order with respect to summons issued to the accused, also mentioned the charge sheet laid by the police against the accused in its order. The accused was charged under Section 66-A, ITA. The brief facts which can be extracted from the order of the Court read: "that the complainant and the accused (petitioner) were together at Chennai. It is stated that on 04.09.2009, the petitioner has transmitted photos of the de facto complainant and another person depicting them in bad light through internet and thus the petitioner has committed the offence as mentioned above."

J.R. GANGWANI AND ANOTHER V. STATE OF HARYANA AND OTHERS (PUNJAB AND HARYANA HIGH COURT, DECIDED ON OCTOBER 15, 2012)

Petition for quashing of criminal proceedings under section 482 of the Criminal Procedure Code, 1973

In the Punjab and Haryana High Court, an application for quashing of criminal proceeding draws attention to a complaint which was filed under Section 66-A(c). This complaint was filed under Section 66-A(c) on the ground of sending e-mails under assumed e-mail addresses to customers of the Company which contained material which maligned the name of the Company which was to be sold as per the orders of the Company Law Board. The Complainant in the case received the e-mails which were redirected from the customers. According to the accused and the petitioner in the current hearing, the e-mail was not directed to the complainant or the company as is required under Section 66-A (c).

The High Court held that, "the petitioners are sending these messages to the purchasers of cranes from the company and those purchasers cannot be considered to be the possible buyers of the company. Sending of such e-mails, therefore, is not promoting the sale of the company which is the purpose of the advertisement given in the Economic Times. Such advertisements are, therefore, for the purpose of causing annoyance or inconvenience to the company or to deceive or mislead the addressee about the origin of such messages. These facts, therefore, clearly bring the acts of the petitioners within the purview of section 66A(c) of the Act."

MOHAMMAD AMJAD V. SHARAD SAGAR SINGH AND ORS. (CRIMINAL REVISION NO. 72/2011 FILED BEFORE THE COURT OF SH. VINAY KUMAR KHANA ADDITIONAL SESSIONS JUDGE – 04 SOUTH EAST: SAKET COURTS DELHI)

Revision petition against the order of the metropolitan magistrate

In a revision petition came up before the Additional Sessions Judge on the grounds that the metropolitan magistrate has dismissed a criminal complaint under Section 156(3) of the Criminal Procedure Code without discussing the ingredients of section 295-A, IPC and 66-A, IT Act.

In this case, the judge observed that, "...Section 66A of Information Technology Act (IT Act) does not refer at all to any 'group' or 'class' of people. The only requirement of Section 66A IT Act is that the message which is communicated is grossly offensive in nature or has menacing character." He also observed that the previous order "not at all considered the allegations from this angle and the applicability of Section 66A Information Technology Act, 2000 to the factual matrix of the instant case."

SECTION 66 D PUNISHMENT FOR CHEATING BY IMPERSONATION BY USING COMPUTER RESOURCE

SANDEEP VARGHESE VS. STATE OF KERALA.

A Complaint filed by the representative of a Company which was engaged in the business of trading, and distribution of petrochemicals in India and overseas, a case was registered against nine persons, alleging offences under Sections 65, 66, 66 A , C and D of the Information Technology Act, 2000 along with Sections 419 and 420 of Indian Penal Code.

The company has a website in the name and style "wwww.jaypolychem.com" but, another web-site www.jayplychem.org was set up in the internet by first accused Sandeep Varghese @sam (who was dismissed from company) a conspiracy with other accused including Preeti and Charanjit Singh who are sister and brother-in-law of Sam.

Defamatory and malicious matters about the company and its directors were

made available in that website . The accused sister and brother-in-law were based in Cochin and they had been acting in collusion known and unknown persons, who have collectively cheated the company and committed acts of forgery, impersonation etc.

Two of the accused had visited Delhi and Cochin. The first accused and others sent e-mails from fake e-mail accounts of many of the customers , suppliers , Banks etc. to malign the name and image of the company and its directors. The defamation campaign run by all the said persons named above cause immense damage to the name and reputation of the company .

The Company suffered losses of several crores of rupees from producers , suppliers and customers and were unable to do business.

SECTION 66 E - PUNISHMENT FOR VIOLATION OF PRIVACY.

JAWAHARLAL NEHRU UNIVERSITY MMS SCANDAL

In severe shock to prestigious and renowned institute a pornographic MMS clip was apparently made into campus and transmitted outside the university.

Some media reports claimed that the two accused students initially tried to extort money from the girl in the video but when they failed the culprits put the video out on mobile phones and even sold C.D in the blue film market.

NAGPUR CONGRESS LEADERS MMS SCANDAL

On January 5, 2012 Nagpur Police arrested two engineering students one of them a son of Congress leader for harassing a 16 year old girl by circulating an MMS clip of their sexual acts. According to the Nagpur (rural) police the girl was in a relationship with Mithilesh Gajbhiye 19, son of Yashodha Dhanraj Gajbhiye, a zilla parishad member and an influential Congress leader of Saoner region in Nagpur district.

SECTION 66- F CYBER TERRORISM.

The Mumbai Police have registered a case of “cyber terrorism “ – the first in

the state since an amendment to the Information Technology Act – where a threat e-mail was sent to BSE and NSE on Monday. The MRA Marg Police and the Cyber crime Investigation Cell are totally probing the case. The suspect has been defamed in this case.

The police said an e-mail challenging the security agencies to prevent a terror attack was sent by one Shahab Mohammad with an ID sh.itayeb125@yahoo.in to BSE's administrative email id corp.relations@bseindia.com at around 10:44 a.m. on Monday.

The IP address of the sender has been traced to Patna in Bihar. The ISP is Sify. The email ID was created just four minutes before the email was sent. " The sender had while creating the new ID given two mobile numbers in the personal details column. Both the numbers belong to a photo frame maker in Patna." Said an officer .

STATUS: The MRA Marg Police have registered forgery for purpose of cheating , criminal intimidation cases under the IPC and a cyber terrorism case under the Information Technology Act .

SECTION 67 – PUNISHMENT FOR PUBLISHING OR TRANSMITTING OBSCENE MATERIAL IN ELECTRONIC FORM .

This case is about posting obscene defamatory and annoying message about a divorcee

Woman in Yahoo message group. Emails were forwarded to the victim for information by the accused through false email account opened by him in the name of the victim. These postings resulted in annoying phone calls to lady. Based on the complaint filed by the victim the police nabbed the accused . Investigation revealed that he was a known family friend of the victim and was interested in marrying her. She was married to another person but that marriage ended in divorce and the accused started harassing her through internet .

Verdict : The accused was found guilty of offences under Section 469 , 509, I.P.C and 67 of the Information Technology Act , 2000. he is convicted and sentenced for the offence as follows :

As per 469 of I.P.C imprisonment for 2 years and to pay fine of Rs. 500/-

As per 509 of I.P.C I year simple imprisonment and fine of Rs. 5000/-.

As per Section 67 of Information Technology Act , 2000 2 years imprisonment and pay fine

of Rs. 4000/-. All sentences to run concurrently. The accused paid fine amount and he was lodged at Central Prison, Chennai. This was considered the first case convicted under Section 67 of Information Technology Act, 2000 in India.

SECTION 67 – B PUNISHMENT FOR PUBLISHING OR TRANSMITTING OF MATERIAL DEPICTING CHILDREN IN SEXUALLY EXPLICIT ACT ETC. IN ELECTRONIC FORM.

JANHIT MANCH AND OTHERS VS. THE UNION OF INDIA 13

The petition sought a blanket ban on pornographic websites . The NGO had argued that websites displaying sexually explicit content had an adverse influence , leading youth on a delinquent path.

SECTION 69 – POWERS TO ISSUE DIRECTIONS FOR INTERCEPTION OR MONITORING OR DECRYPTION OF ANY INFORMATION THROUGH ANY COMPUTER RESOURCE .

In August 2007 , Lakshmana Kailash a techie from Bangalore was arrested on the suspicion of having posted insulting images of Chhatrapati Shivaji a major historical figure in the state of Maharashtra on the social networking site Orkut.

The police identified him based on IP address details obtained from Google and Airtel Lakshmana's ISP. He was brought to Pune and detained for 50 days before it was discovered that the IP address provided by Airtel was erroneous . The mistake was evident due to the fact that while requests information from Airtel the police had not properly specified whether the suspect had posted the content at 1:15 P.M.

Verdict :Taking cognizance of his plight from newspaper accounts, the state Human Rights Commission subsequently ordered the company to pay Rs. 2,00,000/- to Lakshmana as damages.

The incident highlights how minor privacy violations by ISPs and intermediaries could have impacts that gravely undermine other basic human rights .

---

13 10-03-2010, Public Interest Litigation.

PUNE CITIBANK MPHASIS CALL CENTER FRAUD:

US $ 3,50,000 from accounts of four US customers were dishonestly transferred to bogus accounts. This will give a lot of ammunition to those lobbying against outsourcing in US. Such cases happen all over the world but when it happens in India it is a serious matter and we can not ignore it. It is a case of sourcing engineering. Some employees gained the confidence of the customer and obtained their PIN numbers to commit fraud. They got these under the guise of helping the customers out of difficult situations. Highest security prevails in the call centers in India as they know that they will lose their business. There was not as much of breach of security but of sourcing engineering. The call center employees are checked when they go in and out so they can not copy down numbers and therefore they could not have noted these down. They must have remembered these numbers, gone out immediately to a cyber café and accessed the Citibank accounts of the customers. All accounts were opened in Pune and the customers complained that the money from their accounts was transferred to Pune accounts and that's how the criminals were traced. Police has been able to prove the honesty of the call center and has frozen the accounts where the money was transferred.

There is need for a strict background check of the call center executives. However, best of background checks can not eliminate the bad elements from coming in and breaching security. We must still ensure such checks when a person is hired. There is need for a national ID and a national data base where a name can be referred to. In this case preliminary investigations do not reveal that the criminals had any crime history. Customer education is very important so customers do not get taken for a ride. Most banks are guilt of not doing this.

Avnish Bajaj v State (N.C.T.) of Delhi [14](BAZEE.COM CASE):

CEO of Bazee.com was arrested in December 2004 because a CD with

[14] (2005) 3 Comp LJ 364 (Del).

objectionable material was being sold on the website. The CD was also being sold in the markets in Delhi. The Mumbai city police and the Delhi Police got into action. The CEO was later released on bail. This opened up the question as to what kind of distinction do we draw between Internet Service Provider and Content Provider. The burden rests on the accused that he was the Service Provider and not the Content Provider. It also raises a lot of issues regarding how the police should handle the cyber crime cases and a lot of education is required.

STATE OF TAMIL NADU VS SUHAS KUTTI : 2004

Assistant Commissioner of Police, Cyber Crime Cell, C.C.B.Egmore, Chennai.8 has filed Final Report against the accused, that on 7.2.04, evening at Cyber Café Hello World Centre, Sion, Mumbai having an I.P.61.11.10.99, the accused with intention of harming the reputation of the Complainant Ms. R, created user id in the name of her and composed an obscene message intending that such document shall be used for posting in different obscene Yahoo Group, with the intention to make others to believe that the document was made by her, so that the persons seeing the obscene message would send offending calls to her, in harming her reputation and by insulting her modesty by the words exhibited in the email and in the course of same transaction, on 7.2.04, evening at Cyber Café Hello World Centre, Sion, Mumbai, having an IP 61.11.10.99 the Accused posted obscene message which are lascivious and also have the effect to corrupt persons who are likely to read and see such obscene messages and caused to the published in different obscene Yahoo groups and in the course of same transaction, that on 9.2.04, morning, at Cyber Café Heighten Advertising, Mahim, Mumbai, having an IP 202.88.165.53 the accused with intention of harming the reputation of the complainant Ms. R entered user id. which was created by him in the name of the complainant and composed an obscene message intending that such document shall be used for posting in different obscene Yahoo groups, with the intention to make others to believe that the document was made by her, so that the persons seeing the obscene message would send offending calls to her, in harming her reputation and by insulting her modesty by the words exhibited in the email and that in the course of same transaction, that on 9.2.04, morning at cyber café Heighten Advertising, Mahim, Mumbai, having an IP 202.88.165.53, the accused posted obscene messages which are lascivious and also have the

effect to corrupt person who are likely to read and see such obscene messages and caused to be published in different obscene Yahoo groups and thereby the accused have committed offences u/s 469 IPC, 67 I.T Act. 469 & 509 IPC and 67 of I.T. Act.

P.W. 1 is the only daughter of P.W.2 and P.W.3. P.W.2 is the father, P.W.3 is the mother. Presently, P.W.1 is working as a senior Executive (H.R.) in a multinational Company at Chennai. She studied her MBA Course in Mumbai in the year 1997, the accused studied with P.W.1 and she was his classmate is Mumbai. Accused belongs to Mumbai. On 9.2.04, She opened her Rediff e-mail and noticed the receipt of two obscene messages which were posted on 7.2.04 and 9.2.04. She took computer output of the obscene message posted on 7.2.04, Ex P.1 is the obscene message. The obscene message carried her Office phone numbers and her e-mail I.D. The house Phone number was wrongly given. The said obscene messages have been sent through Yahoo website to 5 sex groups. The computer printout obscene message posted in @ Radha lovers group is EX.P.2. On seeing the said messages, several persons sent the responsive message and many persons tried to contact her over phone. Ex P3 series is the responsive messages. Several Phone calls came to her office. P.W.1 informed the said matter to her parents. The messages were likely to harm the reputation and morale of P.W.1.

P.W. 1 had married Jaichand Prajapathi of Uttar Pradesh in the year 2001. The family life was not happy and she obtained divorce through court in the year 2003. The Accused was citied as witness in the divorce petition. P.W.1 recollected one incident and suspected in the involvement of the Accused. During college days in the year 1997, the accused used to travel with P.W.1 in train at Mumbai. On one such occasion, Accused pointed out an obscene scribbling with phone number in the train and told P.W.1 that on seeing the phone number, many persons would try to contact the phone number and this is the best way to spoil the reputation of a woman. The Accused even expressed his desire to marry P.W.1, after the engagement of P.W.1 with Jaichand Prajapati was over. P.W.1 turned down his proposal. In the year 2003, the Accused stayed in the house of the P.W.1 for about 10 days stating that he has to attend an interview at Banglalore. At that time also, Accused offered to marry P.W.1 for which P.W.1 and her parents refused the alliance. Thereafter, P.W.1 after his return to Mumbai was in the habit of making Phone calls, sending S.M.S. Messages and sending E-mail to P.W.1

frequently. Hence P.W.1 blocked the e-mail I.D. of the Accused. Ex.P5 is the Computer output for blocking the e-mail I.D. of the Accused.

On seeing the obscene message, P.W.1 discussed the matter with P.W.2 and P.W.3 and sought the help of the Accused over phone. P.W.1 and her parents issued a warning message in the name of PW 2 and PW 3 by creating an email ID viz, parant2003@yahoo.co.in and transmitted same to the yahoo groups. She sent warning messages to the persons, who sent responsive message in ExP.6 series. A copy of warning message was also sent to the Accused.

P.W.1 lodged a complaint on 14/2/2004 along with Ex.P1 at Cyber Crime Police. The complaint is Ex. P.4 P.W.12 who received the complaint directed P.W.4 to obtain header details and other particulars to find out the origination of the messages. P.W.4 went to Cyber Café at Kennath Lane, Egmore along with P.W. 1 she down loaded the message took print out by using the e-mail I.D. Parant2003@Yahoo.Co.in Ex.P.9-Ex.P.12. She extracted and stored the messages in Mo.2 floppies. Thereafter P.W.12 gave a requisition to the Hathway Cable and Data Com. Pvt. Ltd; under Ex.P.13, for which it gave a reply in Ex. P.14. P.W.12 also gave a requisition to Dishnet D.S.L. in Ex.P.13 and the reply given by Dishnet D.S.L is Ex.P.15. P.W.5 speaks about Ex.P.13 and Ex.P.14. P.W.6 speaks about Ex.P.15.P.W.12 also examined P.W.11 and obtained particulars in Ex. P.29 series and confirmed that the messages were originated from Mumbai. P.W.12- Investigation Officer registered F.I.R. Ex.P.34 on 20.2.04.

Thereafter, P.W.12 proceeded to Mumbai on 24.2.04, and arrested the Accused at Mumbai on 25.2.04. He seized Mo.1 Cell Phone from the Accused under Mahazar Ex.P.8 P.W.8 and P.W.9 who are running browsing Centre at Mumbai, identified the Accused in the presence of P.W.12. He seized Ex.P.23, 24 registers from them. P.W.8 speaks about the Accused and the seizure of Ex.P.22 and the remarks made by P.W.12 in Ex.P.23, P.W. 9 speaks about the Accused that he came to the browsing centre and signed in the Register Ex.P24 as R. Ex.P.25 is the word written by the Accused.

P. W. 12, brought the Accused to Chennai on 28.2.04, after producing the Accused before a Mumbai Court. The Accused gave a confession statement in the presence of P.W. 10 and he gave the password “an rose”. The said word is Ex.P.27.

The particulars stored in the SIM Card were taken print out in Ex.P. 28 series through S.M.S. Reader. P.W.12 went to the office of P.W.7 and took computer print out by using the password “an rose”. He issued the certificate in Ex.P.21. The computer print outs are Ex. P 16-P.20. P.W.12 completed investigation and laid charge sheet against the Accused of offences u/s 67 of I T Act and u/s 469,509 of IPC.

Final Order

This court is not inclined to accept the theory projected by the Accused that the obscene messages would have been created by P.W.1, P.W.2 and P.W.3 or by Jaichand Prajapathi. It is clear that the Accused himself has composed and posted the obscene messages from the browsing centre of P.W.8 and P.W.9. This Court holds that the prosecution has proved its charges against the accused beyond all reasonable doubt and hence the Accused is liable to be punished.

The Accused was heard regarding the question of sentence u/s 248 (2) Cr.P.C. The Accused pleaded for admonition. The Accused is not a lay man. He is educated and studied upto M.B.A. P.W.1 is holding a responsible post in a multinational Company at Chennai. The Accused has chosen to post the obscene message for the simple reason that she refused to marry him. He did not behave like an educated man. Only a family woman can realise the mental sufferings and pain if unknown persons contacted her through phone and e-mail and invited her to bed. The mental sufferings and humiliation undergone by the P.W.1 cannot be compensated in terms of money or by solacial words. It cannot be stated that the Accused had acted in a heat of passion. Two days repeatedly he had sent the obscene message—Computer system and browsing centre are meant for learning things and updating knowledge in various fields. The Accused has misused the same to take revenge on a sophisticated lady. Therefore, the Accused does not deserve leniency and is liable to be punished.

In the result, the Accused is found guilty of offences u/s 469,509 IPC, and u/s 67 of I.T. Act. and the Accused is convicted and is sentenced to undergo Rigorous imprisonment for 2 years u/s 469 IPC, and to pay a fine Rs.500/- i/d, to undergo simple imprisonment for 1 month and for the offence u/s 509 IPC, sentenced to undergo 1 year simple Imprisonment and to pay a fine of Rs.500/- i/d to undergo simple imprisonment for 1 month and for the

offence u/s 67 of Information Technology Act 2000 to undergo Rigorous Imprisonment for 2 years and to pay a fine of Rs.4,000/- i/d to undergo S.I. for 6 months. All sentences to run concurrently. The period undergone by the Accused will be set off u/s 428 Cr.P.C.

THE BANK NSP CASE:

The Bank NSP case is the one where a management trainee of the bank was engaged to be married. The couple exchanged many emails using the company computers. After some time the two broke up and the girl created fraudulent email ids such as "Indian bar associations" and sent emails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a large number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

SMC PNEUMATICS (INDIA) PVT. LTD. V. JOGESH KWATRA[15]:

In India's first case of cyber defamation, a Court of Delhi assumed jurisdiction over a matter where a corporate's reputation was being defamed through emails and passed an important ex-parte injunction.

In this case, the defendant Jogesh Kwatra being an employ of the plaintiff company started sending derogatory, defamatory, obscene, vulgar, filthy and abusive emails to his employers as also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director Mr. R K Malhotra. The plaintiff filed a suit for permanent injunction restraining the defendant from doing his illegal acts of sending derogatory emails to the plaintiff.

On behalf of the plaintiffs it was contended that the emails sent by the defendant were distinctly obscene, vulgar, abusive, intimidating, humiliating and defamatory in nature. Counsel further argued that the aim of sending the said emails was to malign the high reputation of the plaintiffs all over India and the world. He further contended that the

[15] Suit No. 1279/2001 Delhi HC

acts of the defendant in sending the emails had resulted in invasion of legal rights of the plaintiffs. Further the defendant is under a duty not to send the aforesaid emails. It is pertinent to note that after the plaintiff company discovered the said employ could be indulging in the matter of sending abusive emails, the plaintiff terminated the services of the defendant. After hearing detailed arguments of Counsel for Plaintiff, Hon'ble Judge of the Delhi High Court passed an ex-parte ad interim injunction observing that a prima facie case had been made out by the plaintiff. Consequently, the Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails either to the plaintiffs or to its sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing departments. Further, Hon'ble Judge also restrained the defendant from publishing, transmitting or causing to be published any information in the actual world as also in cyberspace which is derogatory or defamatory or abusive of the plaintiffs.

This order of Delhi High Court assumes tremendous significance as this is for the first time that an Indian Court assumes jurisdiction in a matter concerning cyber defamation and grants an ex-parte injunction restraining the defendant from defaming the plaintiffs by sending derogatory, defamatory, abusive and obscene emails either to the plaintiffs or their subsidiaries.

PARLIAMENT ATTACK CASE:

Bureau of Police Research and Development at Hyderabad had handled some of the top cyber cases, including analysing and retrieving information from the laptop recovered from terrorist, who attacked Parliament. The laptop which was seized from the two terrorists, who were gunned down when Parliament was under siege on December 13 2001, was sent to Computer Forensics Division of BPRD after computer experts at Delhi failed to trace much out of its contents. The laptop contained several evidences that confirmed of the two terrorists' motives, namely the sticker of the Ministry of Home that they had made on the laptop and pasted on their ambassador car to gain entry into Parliament House and the the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal. The emblems (of the three lions) were carefully

scanned and the seal was also craftly made along with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop.

ANDHRA PRADESH TAX CASE:

Dubious tactics of a prominent businessman from Andhra Pradesh was exposed after officials of the department got hold of computers used by the accused person. The owner of a plastics firm was arrested and Rs 22 crore cash was recovered from his house by sleuths of the Vigilance Department. They sought an explanation from him regarding the unaccounted cash within 10 days. The accused person submitted 6,000 vouchers to prove the legitimacy of trade and thought his offence would go undetected but after careful scrutiny of vouchers and contents of his computers it revealed that all of them were made after the raids were conducted. It later revealed that the accused was running five businesses under the guise of one company and used fake and computerised vouchers to show sales records and save tax.

SONY.SAMBANDH.COM CASE:

India saw its first cyber crime conviction recently. It all began after a complaint was filed by Sony India Private Ltd, which runs a website called www.sony-sambandh.com, targeting Non Resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online. The company undertakes to deliver the products to the concerned recipients. In May 2002, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless head phone. She gave her credit card number for payment and requested that the products be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency and the transaction processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim. At the time of delivery, the company took digital photographs showing the delivery being accepted by Arif Azim.

The transaction closed at that, but after one and a half months the credit card

agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase. The company lodged a complaint for online cheating at the Central Bureau of Investigation which registered a case under Section 418, 419 and 420 of the Indian Penal Code. The matter was investigated into and Arif Azim was arrested. Investigations revealed that Arif Azim, while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company's site.

The CBI recovered the colour television and the cordless head phone. In this matter, the CBI had evidence to prove their case and so the accused admitted his guilt. The court convicted Arif Azim under Section 418, 419 and 420 of the Indian Penal Code — this being the first time that a cybercrime has been convicted. The court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. The court therefore released the accused on probation for one year.

The judgment is of immense significance for the entire nation. Besides being the first conviction in a cybercrime matter, it has shown that the the Indian Penal Code can be effectively applied to certain categories of cyber crimes which are not covered under the Information Technology Act 2000. Secondly, a judgment of this sort sends out a clear message to all that the law cannot be taken for a ride.

NASSCOM VS. AJAY SOOD & OTHERS[16]

In a landmark judgment in the case of National Association of Software and Service Companies vs Ajay Sood & Others, delivered in March, '05, the Delhi High Court declared `phishing' on the internet to be an illegal act, entailing an injunction and recovery of damages.

Elaborating on the concept of 'phishing', in order to lay down a precedent in India, the court stated that it is a form of internet fraud where a person pretends to be a legitimate association, such as a bank or an insurance company in order to extract personal data from a customer such as access codes, passwords, etc. Personal data so collected by misrepresenting the identity of the legitimate party is commonly used for the collecting party's advantage. court also stated, by way of an example, that typical phishing scams involve persons who

[16] 119 (2005) DLT 596, 2005 (30) PTC 437 Del

pretend to represent online banks and siphon cash from e-banking accounts after conning consumers into handing over confidential banking details.

The Delhi HC stated that even though there is no specific legislation in India to penalize phishing, it held phishing to be an illegal act by defining it under Indian law as "a misrepresentation made in the course of trade leading to confusion as to the source and origin of the e-mail causing immense harm not only to the consumer but even to the person whose name, identity or password is misused." The court held the act of phishing as passing off and tarnishing the plaintiff's image.

The plaintiff in this case was the National Association of Software and Service Companies (Nasscom), India's premier software association. The defendants were operating a placement agency involved in head-hunting and recruitment. In order to obtain personal data, which they could use for purposes of headhunting, the defendants composed and sent e-mails to third parties in the name of Nasscom.

The high court recognised the trademark rights of the plaintiff and passed an ex-parte ad interim injunction restraining the defendants from using the trade name or any other name deceptively similar to Nasscom. The court further restrained the defendants from holding themselves out as being associates or a part of Nasscom.

The court appointed a commission to conduct a search at the defendants' premises. Two hard disks of the computers from which the fraudulent e-mails were sent by the defendants to various parties were taken into custody by the local commissioner appointed by the court.

The offending e-mails were then downloaded from the hard disks and presented as evidence in court.

During the progress of the case, it became clear that the defendants in whose names the offending emails were sent were fictitious identities created by an employee on defendants' instructions, to avoid recognition and legal action. On discovery of this fraudulent act, the fictitious names were deleted from the array of parties as defendants in the case.

Subsequently, the defendants admitted their illegal acts and the parties settled the matter through the recording of a compromise in the suit proceedings. According to the terms of compromise, the defendants agreed to pay a sum of Rs1.6 million to the plaintiff as damages for violation of the plaintiff's trademark rights. The court also ordered the hard disks seized

from the defendants' premises to be handed over to the plaintiff who would be the owner of the hard disks.

This case achieves clear milestones: It brings the act of "phishing" into the ambit of Indian laws even in the absence of specific legislation; It clears the misconception that there is no "damages culture" in India for violation of IP rights; This case reaffirms IP owners' faith in the Indian judicial system's ability and willingness to protect intangible property rights and send a strong message to IP owners that they can do business in India without sacrificing their IP rights.

GOOGLE INDIA PVT. LTD., VERSUS VISAKA INDUSTRIES LIMITED AND ANOTHER[17]

ORDER:

1.) The petitioner/A-2 is accused of offences punishable under Sections 120-B, 500, 501/34 I.P.C in C.C. No.679 of 2009 on the file of XI Additional Chief Metropolitan Magistrate, Secunderabad along with another. The petitioner/A-2 is Google India Private Limited represented by its Managing Director (Sales and Operations). The 1st respondent/complainant is Visaka Industries Limited, Secunderabad represented by its authorised signatory who is its Deputy Manager- Legal. The complainant is engaged in business of manufacturing and selling of Asbestos cement sheets and allied products. It is alleged that A-1 viz., Gopala Krishna is a Co-ordinator "Ban Asbestos India" a group which is hosted by A-2 and publishes regular articles in the said group and that on 21.11.2008 an article was published in the said group and it was captioned as "poisoning the system; Hindustan Times" aiming at a single manufacturer of Asbestos cement products viz., the complainant and names of renowned politicians of the country G.Venkata Swamy and Sonia Gandhi who have nothing to do with the ownership or management of the complainant-company were named in that article. It is further alleged that on 31.07.2008 another article captioned as "Visaka Asbestos Industries making gains" and that both the above articles contained defamatory statements against the complainant and they are available in Cyber

[17] The Honourable Sri Justice Samudrala Govindarajulu, AP high court crl.p.no.7207 of 2009 19-04-2011

space in the form of articles for world wide audience. In the complaint, details of defamatory remarks made in several other articles published by A-1 in A-2 group are given in detail, which details may not be necessary for the purpose of disposal of this criminal petition.

2) It is contended by the senior counsel appearing for the petitioner/A-2 that actions of intermediaries such as Google Inc., which is a service provider providing platform for end users to upload content, does not amount to publication in law and consequently the question of holding such intermediaries liable for defamation does not arise. Senior Counsel appearing for the petitioner placed reliance on Section 79 of the Information Technology Act, 2000 (in short, the Act) in support of this contention.

3) Section 79 which occurs in Chapter XII of the Act originally as it stood enacted in the year 2000 reads as follows:

CHAPTER XII NETWORK SERVICE PROVIDERS NOT TO BE LIABLE IN CERTAIN CASES

Sec.79. Network service providers not to be liable in certain cases: For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made there under for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention. Explanation. For the purposes of this section,

(a) "network service provider" means an intermediary;

(b) "third party information" means any information dealt with by a network service provider in his capacity as an intermediary."

The said provision exempts network service providers from liability under the Act, rules or regulations made there under for any third party information or data made available by him. It did not exempt a network service provider from liability muchless criminal liability for the offences under other laws or more particularly under the Indian Penal Code. Further, the above provision exempts network service provider from liability, only on proof that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention. Proof in that regard can be let in by way of leading evidence by the accused. Therefore, the said question

is a question of fact which this Court may not go into in this petition filed under Section 482 Cr.P.C.

4) Chapter XII of the Act including Section 79 was amended by the Information Technology (Amendment) Act, 2008 (10 of 2009) dated 05.02.2009 with effect from 27.10.2009 by way of substituting the following in the place of original chapter:

CHAPTER XII - INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES

79. Exemption from liability of intermediary in certain cases:

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communciation link made available or hosted by him.

(2) The provisions of sub-section (1) shall apply if- (a) the functions of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or

(b) the intermediary does not-

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission;

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(3) The provisions of Sub-section(1) shall not apply if-

(a) The intermediary has conspired or abetted or aided or induces whether by threats or promise or otherwise in the commission of the unlawful act;

(b) upon receiving actual knowledge, or on being notified by information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation.- For the purposes of this section, the expression "third party information" means any information dealt with an intermediary in his capacity as an intermediary."

It is only under the said amendment, non-obstenti clause was incorporated in Section 79 keeping application of other laws outside the purview in a fact situation covered by the said provision. Now, after the amendment, an intermediary like a network service provider can claim exemption from application of any other law in respect of any third party information, data or communication link made available or hosted by him; provided he satisfied the requirements under Sub-section (2) of Section 79. Further, as per amended Sub- section (3) of Section 79, the exemption under Sub-section (1) cannot be applied by any Court and cannot be claimed by any intermediary in case the intermediary entered into any conspiracy in respect thereof. Also, the intermediary cannot claim exemption under Sub-section (1) in case he fails to expeditiously remove or disable access to the objectionable material or unlawful activity even after receiving actual knowledge thereof. In the case on hand, in spite of the 1st respondent issuing notice bringing the petitioner about dissemination of defamatory material and unlawful activity on the part of A-1 through the medium of A-2, the petitioner/A-2 did not move its little finger to block the said material or to stop dissemination of the unlawful and objectionable material. Therefore, the petitioner/A-2 cannot claim any exemption either under Section 79 of the Act as it stood originally or Section 79 of the Act after the amendment which took effect from 27.10.2009. The present case in the lower Court was instituted in January, 2009 relating to the offences which are being perpetrated from 31.07.2009 onwards i.e., since long prior to the amendment to the said provision.

5) There is no exemption of any criminal liability in respect of a company which is a juristic person and which has no body that can be damned or contemned. In case found guilty, the petitioner company can be awarded with appropriate punishment though not corporal punishment. In that view of the matter, I find no merit in this criminal petition.

6) Accordingly, the Criminal Petition is dismissed.

MICROSOFT CORPORATION V. YOGESH PAPAT, DELHI HIGH COURT[18].

Facts of the case:-

[18] http://www.cyberlawconsulting.com/cyber-cases.html

This case concerns the infringement of copyright in software and notably the interpretation of Sections 51 and 55 of the Copyright Act 1957. The Microsoft Corporation, the registered proprietor of the trademark MICROSOFT, requested a permanent injunction restraining the defendant, its directors and agents from copying, selling, offering for sale, distributing or issuing to the public counterfeit or unlicensed versions of Microsoft's software program in any manner that amounts to infringement of Microsoft's copyright in the computer programs, related manuals and Microsoft's registered trademarks. Microsoft also requested that the defendant be prevented from selling and distributing any product to which the trademark MICROSOFT or any variants of this trademark have been applied.

The defendant did not appear before the court, so the proceedings took place ex parte. The court eventually ruled against the defendant, who was downloading Microsoft software onto the hard drives of computers that it then sold, without a licence or permission to do so from Microsoft.

Decision

The court approached each piece of evidence in turn and, based on the assumption that 100 computers were sold each year and on the evidence of the software's popularity, held that Microsoft had suffered a total profit loss of Rs1.98 million, plus interest at 9% from the date of the decree until the date of payment.

The court, quoting an observation by Justice Laddie in the High Court of England and Wales in Microsoft Corporation v Electrowide Ltd, held that the defendant's actions "constituted a general threat to infringe the copyright in the class of software". Justice Predeep Nandrajog, who presided in this case, stated that:

"It stands established that the defendant has infringed the plaintiff's copyright by making illicit copies of the operating systems software by openly copying whatever operating system is currently saleable."

XVI) INTERNATIONAL REGIME IN CYBER LAWS IN PREVENTION OF CYBER CRIMES[19]:

International legislative responses and cooperation

G 8 : Group of Eight (G8) is made up of the heads of eight industrialized countries: the U.S., the United Kingdom, Russia, France, Italy, Japan, Germany, and Canada.

In 1997, G8 released a Ministers' Communiqué that includes an action plan and principles to combat cyber crime and protect data and systems from unauthorized impairment. G8 also mandates that all law enforcement personnel must be trained and equipped to address cyber crime, and designates all member countries to have a point of contact on a 24 hours a day/7 days a week basis.

United Nations

In 1990 the UN General Assembly adopted a resolution dealing with computer crime legislation. In 2000 the UN GA adopted a resolution on combating the criminal misuse of information technology. In 2002 the UN GA adopted a second resolution on the criminal misuse of information technology.

I.T.U.

The International Telecommunication Union (ITU), as a specialized agency within the United Nations, plays a leading role in the standardization and development of telecommunications and cyber security issues. The ITU was the lead agency of the World Summit on the Information Society (WSIS).

[19] http://en.wikipedia.org/wiki/International_cybercrime

In 2003, Geneva Declaration of Principles and the Geneva Plan of Action were released, which highlights the importance of measures in the fight against cyber crime.

In 2005, the Tunis Commitment and the Tunis Agenda were adopted for the Information Society.

Council of Europe

Council of Europe is an international organisation focusing on the development of human rights and democracy in its 47 European member states.

In 2001, the Convention on Cyber crime, the first international convention aimed at Internet criminal behaviors, was co-drafted by the Council of Europe with the addition of USA, Canada, and Japan and signed by its 46 member states. But only 25 countries ratified later. It aims at providing the basis of an effective legal framework for fighting cyber crime, through harmonization of cyber criminal offences qualification, provision for laws empowering law enforcement and enabling international cooperation.

Regional responses

APEC

Asia-Pacific Economic Cooperation (APEC) is an international forum that seeks to promote promoting open trade and practical economic cooperation in the Asia-Pacific Region. In 2002, APEC issued Cybersecurity Strategy which is included in the Shanghai Declaration.

The strategy outlined six areas for co-operation among member economies including legal developments, information sharing and co-operation, security and technical guidelines, public awareness, and training and education.

OECD

The Organisation for Economic Co-operation and Development (OECD) is an international economic organisation of 34 countries founded in 1961 to stimulate economic progress and world trade.

In 1990, the Information, Computer and Communications Policy (ICCP) Committee created an Expert Group to develop a set of guidelines for information security that was drafted until 1992 and then adopted by the OECD Council. In 2002, OECD announced the completion of "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security".

European Union

In 2001, the European Commission published a communication titled "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime".

In 2002, EU presented a proposal for a “Framework Decision on Attacks against Information Systems”. The Framework Decision takes note of Convention on Cybercrime, but concentrates on the harmonisation of substantive criminal law provisions that are designed to protect infrastructure elements.

Commonwealth

In 2002, the Commonwealth of Nations presented a model law on cyber crime that provides a legal framework to harmonise legislation within the Commonwealth and enable international cooperation. The model law was intentionally drafted in accordance with the Convention on Cyber crime.

ECOWAS

The Economic Community of West African States (ECOWAS) is a regional group of West African Countries founded in 1975 it has fifteen member states. In 2009, ECOWAS adopted the Directive on Fighting Cyber crime in ECOWAS that provides a legal framework for the member states, which includes substantive criminal law as well as procedural law.

G.C.C.

In 2007, the Arab League and Gulf Cooperation Council (GCC) recommended at a conference seeking a joint approach that takes into consideration international standards.

Voluntary industry response

During the past few years, public-private partnerships have emerged as a promising approach for tackling cybersecurity issues around the globe. Executive branch agencies (e.g., the Federal Trade Commission in US), regulatory agencies (e.g., Australian Communications and Media Authority), separate agencies (e.g., ENISA in the EU) and industry (e.g., MAAWG) are all involved in partnership.

In 2004, the London Action Plan was founded, which aims at promoting international spam enforcement cooperation and address spam related problems, such as online fraud and deception, phishing, and dissemination of viruses.

XVII) CONCLUSION:

The new legislation which can cover all the aspects of the Cyber Crimes should be passed so the grey areas of the law can be removed. The recent blasts in Ahmedabad, Bangalore and Delhi reflects the threat to the mankind by the cyber space activities against this I personally believe that only the technology and its wide expansion can give strong fight to the problems. The software's are easily available for download should be restricted by the Government by appropriate actions. New amendment should be included to the Information Technology Act, 2000 to make it efficient and active against the crimes. The training and public awareness programs should be organized in the Companies as well as in common sectors. The number of the cyber cops in India should be increased. The jurisdiction problem is there in the implementation part which should be removed because the cyber criminals does not have any jurisdiction limit then why do the laws have, after all the laws are there, to punish the criminal but present scenario gives them the chance to escape.

Information Technology Act , 2000 is a laudable effort by the Government to create the necessary legal infrastructure for promotion and growth of electronic commerce. The Information Technology Amendment Act , 2008 is a great achievement and a remarkable step ahead in the right direction. The Indian Information Technology Act also needs to evolve with the rapidly changing technology environment that breeds new forms of crime and criminals.

Despite the enactment of cyber laws and their existence for three years, a lot more needs to be done, both online and offline, as well as within the judiciary and law enforcement agencies. However, a number of right steps have also been taken to make the Information Technology Act more relevant in today's context.

REFERENCES :

- THE INFORMATION TECHNOLOGY ACT, 2000 (No. 21 OF 2000)
- Chris Reed (Ed.), COMPUTER LAW , 5th edition , Reprint 2000 .
- Mishra R.C , " Cyber crime: impact in the new millennium", 2002 Edition .
- E.K. Bharat Bhushan , Information Technology Act 2000 & Amendments
- Rodney D. Ryder , Introduction to Internet Law and Policy , 1st Edition 2007.

WEB REFRENCES :

- http: // www.westlaw.com
- http://www.cyberlawconsulting.com/cyber-cases.html
- http://en.wikipedia.org/wiki/International_cybercrime