A Review on Information Technology and Cyber Laws

Shailesh P. Thakare, Nitin M, Shivratriwar, Shrikant N. Sarda

***Abstract*— now a day's most of the activities and financial transactions uses internet, since internet is accessible from anywhere, perpetrator takes advantage of this and commit a crime. Cybercrime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity. Cyber criminals take full advantage of the anonymity, secrecy, and interconnections provided by the Internet. In this paper we have tried to provide information about Cyber crime, its nature, Perpetrators, Classification of cyber crime, Reasons for its emergence, In next section of this paper we have given an information about cyber law, IT legislation in India. Further in next section we have discuses about Cyber crime scenario in India. Finally Last two sections of this paper discuss about some cyber crime cases in India and some cyber crimes and punishments related with those crime.**

***Index Terms*— Cybercrime, Cyber laws, Indian Cyber Crime Cases, I.T. legislation in India**

I. INTRODUCTION

The combination of computer network and telecommunications developed by the digital technologies has given birth to a common space called 'cyberspace'. This cyberspace has become a platform for human activities which converge on the internet. Internet is increasingly being used for communication, commerce, advertising, banking, education, research and entertainment. It has become a place to do all of activities which are prohibited by law. it is increasingly being used for pornography, gambling, trafficking in human organs and prohibited drugs, hacking, infringing copyright, terrorism, violating individual privacy, money laundering, fraud, software piracy and corporate espionage, etc. Cyber crime is easy to commit, hard to detect and often hard to locate in jurisdictional terms [1]. The heavy reliance of individuals/organizations on internet has resulted in to a corresponding increase in the cybercrimes. Lack of proper training and education, the low level of awareness of the Indian population about the cybercrime has resulted into a cybercrimes. The objectives of this research work are to touch all the important facets of the cyber crimes in a comprehensive way and to achieve new insights into it [1] [2].

Mr. Shailesh P. Thakare, Department of Information Technology, S.G.B. Amravati University/ Prof. Ram Meghe Institute of Technology & Research, Badnera, Amravati, India, 9049528079

Mr. Nitin M. Shivratriwar, Department of Information Technology, S.G.B. Amravati University/ Prof. Ram Meghe Institute of Technology & Research, Badnera, Amravati, India, 9175440929

Mr. Shrikant N. Sarda, Department of Information Technology, S.G.B. Amravati University/ Prof. Ram Meghe Institute of Technology & Research, Badnera, Amravati, India, 9403310320

The law enforcement officers do not have proper training and other requisite expertise for tackling cybercrime.

The main objectives of this paper is to present basic concepts of the cyber world, trace the origin and development of the cyber crimes, examine critically the position of intellectual property rights in cyber space, analyse the principles of jurisdiction in cyber offences, discuss comprehensively the concept of electronic evidence, decipher as to how the issue of cyber crimes has been dealt with in the Indian scenario, find out the international initiatives to curb cyber menace, point out the possible defects and loopholes in the existing laws relating to cyber crimes, suggest the reforms and remedial measures for the prevention and control of cyber crimes.

II. CYBER CRIME

A. Nature of Cyber Crime:

The hackers, cyber criminals are always in search of any weakness or security holes in system. As they find it, they try to get into the system by applying some tricks known to them. Ignoring such activities may cause danger for individual as well as society. Cyber criminals can do anything with their destructive mind. They may destroy web sites and portals by hacking and planting viruses, play transaction related frauds, they may gain access to highly confidential and sensitive information. Moreover they may harass someone by e-mail or obscene material, play tax related frauds, it also indulges cyber pornography involving children, and commits many other crimes on the internet. Increasing use of the internet in day to day life, cyber crime would affect all of us all, either directly or indirectly [2].

B. Who commit cyber crime [3]?

Type of perpetrator	Motives
Hacker	Test limits of system and/or gain publicity
Cracker	Cause problems, steal data, and corrupt systems
Malicious insider	Gain financially and/or disrupt company's information systems and business operations
Industrial spy	Capture trade secrets and gain competitive advantage
Cybercriminal	Gain financially
Hacktivist	Promote political ideology
Cyberterrorist	Destroy infrastructure components of financial institutions, utilities, and emergency response units

C. Classifications of cyber crimes

There are certain offences which affect the personality of individuals can be defined as:

• **Harassment via e-mails:** it is very common type of harassment through sending letters, attachments of files & folders i.e. Via e-mails. At present harassment is common as usage of social sites i.e. Facebook, twitter etc. Increasing day by day.

• **Cyber-stalking:** it means expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.
• **Dissemination of obscene material:** it includes indecent exposure/ pornography (basically child pornography), hosting of web site containing these prohibited materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.
• **Hacking:** it means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programmes. Hackers usually hacks telecommunication and mobile network.
• **E-mail spoofing:** a spoofed e-mail may be said to be one, which misrepresents its origin. It shows its origin to be different from which actually it originates.
• **Child pornography:** it involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children.
• **Internet phishing:** phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.
• **Cyber squatting:** it means where two persons claim for the same domain name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. For example two similar names i.e. Www.google.com and www.gogle.com.
• **Cyber vandalism:** vandalism means deliberately destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.
• **Virus:** viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computerize system of the individuals.
• **Cyber terrorism:** cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.
• **Distribution of pirated software:** it means distributing pirated software from one computer to another intending to destroy the data and official records of the government. • possession of unauthorized information: it is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, Religious, social, ideological objectives [3].

D. Reason for emergence of cyber crime

- **Increasing complexity increases vulnerability:**

The computing environment has become enormously complex. Networks, computers, operating systems, applications, web sites, switches, routers, and gateways are interconnected and driven by hundreds of millions of lines of code. This environment continues to increase in complexity every day. The number of possible entry points to a network expands continually as more devices are added, increasing the possibility of security breaches.

- **Higher computer user expectations:**

Today, time means money, and the faster computer users can solve a problem, the sooner they can be productive. As a result, computer help desks are under intense pressure to respond very quickly to users' questions. Under duress, help desk personnel sometimes forget to verify users' identities or to check whether they are authorized to perform a requested action. In addition, even though they have been warned against doing so, some computer users share their login id and password with other co-workers who have forgotten their own passwords. This can enable workers to gain access to information systems and data for which they are not authorized.

- **Expanding and changing systems introduce new risks**

Business has moved from an era of stand-alone computers, in which critical data was stored on an isolated mainframe computer in a locked room, to an era in which personal computers connect to networks with millions of other computers, all capable of sharing information. Businesses have moved quickly into e-commerce, mobile computing, collaborative work groups, global business, and interorganizational information systems. Information technology has become ubiquitous and is a necessary tool for organizations to achieve their goals. However, it is increasingly difficult to keep up with the pace of technological change, successfully perform an ongoing assessment of new security risks, and implement approaches for dealing with them.

- **Increased reliance on commercial software with known vulnerabilities**

In computing, an exploit is an attack on an information system that takes advantage of particular system vulnerability. Often this attack is due to poor system design or implementation. Once the vulnerability is discovered, software developers quickly create and issue a "fix," or patch, to eliminate the problem. Users of the system or application are responsible for obtaining and installing the patch, which they can usually download from the web. Any delay in installing a patch exposes the user to a security breach. It can be difficult to keep up with all the required patches. A zero-day attack takes place before the security community or software developer knows about the vulnerability or has been able to repair it. Companies increasingly rely on commercial software with known vulnerabilities. Even when vulnerabilities are exposed, many corporate IT organizations prefer to use already installed software "as is" rather than implement security fixes that will either make the software harder to use or eliminate "nice-to-have" features suggested by current users or potential customers that will help sell the software [3].

III. What Is Cyber Law?

Cyber law is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less of a distinct field of

law in the way that property or contract are, as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to apply laws designed for the physical world, to human activity on the Internet. In India, The IT Act, 2000 as amended by The IT (Amendment) Act, 2008 is known as the Cyber law. It has a separate chapter XI entitled "Offences" in which various cyber crimes have been declared as penal offences punishable with imprisonment and fine.

Cyber Legislation in India

In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") enacted after the United Nation General Assembly Resolution A/RES/51/162, dated the 30th January, 1997 by adopting the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law and which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government. The following Act, Rules and Regulations are covered under cyber laws:

1. Information Technology Act, 2000
2. Information Technology (Certifying Authorities) Rules, 2000
3. Information Technology (Security Procedure) Rules, 2004
4. Information Technology (Certifying Authority) Regulations, 2001

The Act essentially deals with the following issues:

- Legal Recognition of Electronic Documents
- Legal Recognition of Digital Signatures
- Offenses and Contraventions
- Justice Dispensation Systems for cyber-crimes.

National Policy on Information Technology 2012

The Union Cabinet has recently in September 2012, approved the National Policy on Information Technology 2012. The Policy aims to leverage Information & Communication Technology (ICT) to address the country's economic and developmental challenges [2].

The vision of the Policy is
"To strengthen and enhance India's position as the Global IT hub and to use IT and cyber space as an engine for rapid, inclusive and substantial growth in the national economy".

IV. Cyber Crime Scenario In India

The crime is defined as an act, which subjects the doer to legal punishment or any offence against morality, social order or any unjust or shameful act. The "offence" is defined in the Code of Criminal Procedure to mean as an act or omission made punishable by any law for the time being in force. Cyber crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity [4].

Cyber Crime variants

There are many cyber crime variants. A few varieties are:

- **Cyber stalking**
- **Hacking**
- **Phishing**
- **Cross Site Scripting**
- **Vishing**
- **Cyber Squatting**
- **Bot Networks**

A Primer on Cyber Laws in India:

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

Cyber law encompasses laws relating to
i. Cyber crimes
ii. Electronic and digital signatures
iii. Intellectual property
iv. Data protection and privacy

In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government [5].

Objectives of I.T. legislation in India: It is against this background the Government of India enacted its Information Technology Act 2000 with the objectives as follows, stated in the preface to the Act itself. "to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."
The Information Technology Act, 2000, was thus passed as the Act No.21 of 2000, got President assent on 9 June and was made effective from 17 October 2000. The Act essentially deals with the following issues:

- Legal Recognition of Electronic Documents
- Legal Recognition of Digital Signatures
- Offenses and Contraventions
- Justice Dispensation Systems for cyber crimes.

Amendment Act 2008: Being the first legislation in the nation on technology, computers and ecommerce and e-communication, the Act was the subject of extensive debates, elaborate reviews and detailed criticisms, with one arm of the industry criticizing some sections of the Act to be draconian and other stating it is too diluted and lenient. There

were some conspicuous omissions too resulting in the investigators relying more and more on the time-tested (one and half century-old) Indian Penal Code even in technology based cases with the I.T. Act also being referred in the process and the reliance more on IPC rather on the ITA. Thus the need for an amendment – a detailed one – was felt for the I.T. Act almost from the year 2003-04 itself. Major industry bodies were consulted and advisory groups were formed to go into the perceived lacunae in the I.T. Act and comparing it with similar legislations in other nations and to suggest recommendations. Such recommendations were analysed and subsequently taken up as a comprehensive Amendment Act and after considerable administrative procedures, the consolidated amendment called the Information Technology Amendment Act 2008 was placed in the Parliament and passed without much debate, towards the end of 2008 (by which time the Mumbai terrorist attack of 26 November 2008 had taken place). This Amendment Act got the President assent on 5 Feb 2009 and was made effective from 27 October 2009. Some of the notable features of the ITAA are as follows:

- Focusing on data privacy
- Focusing on Information Security
- Defining cyber café
- Making digital signature technology neutral
- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries
- Recognizing the role of Indian Computer Emergency Response Team
- Inclusion of some additional cyber crimes like child pornography and cyber terrorism
- authorizing an Inspector to investigate cyber offences (as against the DSP earlier) [6].

V. Cyber Crime – Indian Cases

1. Pune Citibank Mphasis Call Center Fraud

It is a case of sourcing engineering. US $ 3,50,000 from City bank accounts of four US customers were dishonestly transferred to bogus accounts in Pune, through internet. Some employees of a call centre gained the confidence of the US customers and obtained their PIN numbers under the guise of helping the customers out of difficult situations.. Later they used these numbers to commit fraud. Highest security prevails in the call centres in India as they know that they will lose their business. The call centre employees are checked when they go in and out so they cannot 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 centre and has frozen the accounts where the money was transferred.

2. State of Tamil Nadu Vs Suhas Katti

The case related to posting of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting. Based on a complaint made by the victim in February 2004, the Police traced the accused to Mumbai and arrested him within the next few days. The accused was a known family friend of the victim and was reportedly interested in marrying her. She however married another person. This marriage later ended in divorce and the accused started contacting her once again. On her reluctance to marry him, the accused took up the harassment through the Internet. On the prosecution side 12 witnesses were examined and entire documents were marked as Exhibits. The court relied upon the expert witnesses and other evidence produced before it, including witnesses of the Cyber Cafe owners and came to the conclusion that the crime was conclusively proved and convicted the accused. This is considered as the first case in Tamil Nadu, in which the offender was convicted under section 67 of Information Technology Act 2000 in India.

3. 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.

4. SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra

In this case, the defendant Jogesh Kwatra being an employee 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 sending derogatory emails to the plaintiff. The plaintiff contended that the emails sent by the defendant were distinctly obscene, vulgar, abusive, intimidating, humiliating and defamatory in nature and the aim of sending the said emails was to malign the high reputation of the plaintiffs all over India and the world. 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 injunction restraining the defendant from defaming the plaintiffs by sending defamatory emails.

5. Parliament Attack Case

Bureau of Police Research and Development at Hyderabad had handled some of the top cyber
cases, including analyzing 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. 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 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.

6. Andhra Pradesh Tax Case

The owner of a plastics firm in Andhra Pradesh was arrested and Rs. 22 crore cash was recovered from his house by the Vigilance Department. They sought an explanation from him regarding the unaccounted cash. The accused person submitted 6,000 vouchers to prove the legitimacy of trade, 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 was revealed that the accused was running five businesses under the guise of one company and used fake and computerized vouchers to show sales records and save tax. Thus the dubious tactics of the prominent businessman from Andhra Pradesh was exposed after officials of the department got hold of computers used by the accused person.

7. Sony.Sambandh.Com Case

A complaint was filed by Sony India Private Ltd, which runs a website called www.sonysambandh. 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. 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. The court convicted Arif Azim for cheating under Section 418, 419 and 420 of the Indian Penal Code — this being the first time that a cyber crime 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 cyber crime matter, it has shown that 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.

8. Nasscom v. Ajay Sood & Others –

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 head-hunting, 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 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. It became clear that the defendants in whose names the offending e-mails 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. 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 misused." The court held that, to the consumer but even to the person whose name, identity or password is act of phishing as passing off and tarnishing the plaintiff's image. This case achieves clear milestones: It brings the act of "phishing" into the ambit of India 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.

9. Bazee.com case

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

10. SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra

In India's first case of cyber defamation, a Court of Delhi assumed jurisdiction over a matter where a corporate 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 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.

11. Infinity e-Search BPO Case

The Gurgaon BPO fraud has created an embarrassing situation for Infinity e-Search, the company in which Mr Karan Bahree was employed. A British newspaper had reported that one of its undercover reporters had purchased personal information of 1,000 British customers from an Indian call-center employee. However, the employee of Infinity eSearch, a New Delhi-based web designing company, who was reportedly involved in the case has denied any wrongdoing. The company has also said that it had nothing to do with the incident. In the instant case the journalist used an intermediary, offered a job, requested for a presentation on a CD and later claimed that the CD contained some confidential data. The fact that the CD contained such data is itself not substantiated by the journalist. In this sort of a situation we can only say that the journalist has used "Bribery" to induce a "Out of normal behavior" of an employee. This is not observation of a fact but creating a factual incident by intervention. Investigation is still on in this matter. [7] [8]

VI. Some Laws And Punishments

1. Hacking

Hacking is not defined in The amended IT Act, 2000. According to wiktionary, Hacking means unauthorized attempts to bypass the security mechanisms of an information system or network. Also, in simple words Hacking is the unauthorized access to a computer system, programs, data and network resources. (The term “hacker” originally meant a very gifted programmer. In recent years though, with easier access to multiple systems, it now has negative implications.)

Law & Punishment: Under Information Technology (Amendment) Act, 2008, Section 43(a) read with section 66 is applicable and Section 379 & 406 of Indian Penal Code, 1860 also are applicable. If crime is proved under IT Act, accused shall be punished for imprisonment, which may extend to three years or with fine, which may extend to five lakh rupees or both. Hacking offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

2. Data Theft

According to Wikipedia, Data Theft is a growing problem, primarily perpetrated by office workers with access to technology such as desktop computers and handheld devices, capable of storing digital information such as flash drives, iPods and even digital cameras. The damage caused by data theft can be considerable with today’s ability to transmit very large files via e-mail, web pages, USB devices, DVD storage and other hand-held devices. According to Information Technology (Amendment) Act, 2008, crime of data theft under Section 43 (b) is stated as - If any person without permission of the owner or any other person, who is in charge of a computer, computer system of computer network - downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium, then it is data theft.

Law & Punishment: Under Information Technology (Amendment) Act, 2008, Section 43(b) read with Section 66 is applicable and under Section 379, 405 & 420 of Indian Penal Code, 1860 also applicable. Data Theft offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

3. Spreading Virus or Worms

In most cases, viruses can do any amount of damage, the creator intends them to do. They can send your data to a third party and then delete your data from your computer. They can also ruin/mess up your system and render it unusable without a re-installation of the operating system. Most have not done this much damage in the past, but could easily do this in the future. Usually the virus will install files on your system and then will change your system so that virus program is run every time you start your system. It will then attempt to replicate itself by sending itself to other potential victims.

Law & Punishment: Under Information Technology (Amendment) Act, 2008, Section 43(c) & 43(e) read with Section 66 is applicable and under Section 268 of Indian Penal Code, 1860 also applicable. Spreading of Virus offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

4. Identity Theft

According to wikipedia Identity theft is a form of fraud or cheating of another person's identity in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name. Information Technology (Amendment) Act, 2008, crime of identity theft under Section 66-C, whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person known as identity theft. Identity theft is a term used to refer to fraud that involves stealing money or getting other benefits by pretending to be someone else. The term is relatively new and is actually a misnomer, since it is not inherently possible to steal an identity, only to use it. The person whose identity is used can suffer various consequences when they are held responsible for the perpetrator's actions. At one time the only way for someone to steal somebody else's identity was by killing that person and taking his place. It was typically a violent crime. However, since then, the crime has evolved and today's white collared criminals are a lot less brutal. But the ramifications of an identity theft are still scary.

Law & Punishment: Under Information Technology (Amendment) Act, 2008, Section 66-C and Section 419 of Indian Penal Code, 1860 also applicable. Identity Theft offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

5. E-Mail Spoofing

According to wikipedia, e-mail spoofing is e-mail activity in which the sender addresses and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. E-mail spoofing is sending an e-mail to another person in such a way that it appears that the e-mail was sent by someone else. A spoof email
is one that appears to originate from one source but actually has been sent from another source. Spoofing is the act of electronically disguising one computer as another for gaining as the password system. It is becoming so common that you can no longer take for granted that the e-mail you are receiving is truly from the person identified as the sender. Email spoofing is a technique used by hackers to fraudulently send email messages in which the sender address and other parts of the email header are altered to appear as though the email originated from a source other than its actual source. Hackers use this method to disguise the
actual email address from which phishing and spam messages are sent and often use email spoofing in conjunction with Web page spoofing to trick users into providing personal and confidential information.

Law & Punishment: Under Information Technology (Amendment) Act, 2008, Section 66-D and Section417, 419 & 465of Indian Penal Code, 1860 also applicable. Email spoofing offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate. [9]

VII. CONCLUSION

A In this paper we have tried to focus on basic concepts of cybercrime, cyber laws and some legal issues related to it. While preparing this paper we came to know that, Cyber crimes are easy to commit and hard to detect, due to increase in use of computers and internet it is very easy for criminals to commit a crime by using IT resources. Since most of Indian population is not aware about legal issues related with IT, it is very easy for perpetrators to get into their systems and steal their personal information. We also include some of the cybercrime cases in India for better understanding. Finally we conclude that is necessary to gear up the efforts to prevent the cybercrimes as technology and its related issues are increasing India.

ACKNOWLEDGMENT

We express our sincere and deep gratitude to all the senior faculty members of our department and those who are directly and indirectly helped us. We express our special and sincere thanks to our head of department who motivated and guide us time to time, which enabled us to complete this paper.

REFERENCES

[1] Saroj Mehta & Vikram Singh, "A study of awareness about cyberlaws in the Indian society " , International journal of computing and business research (IJCBR), ISSN (online) : 2229-6166, Volume 4 issue 1 January 2013

[2] Prabhash Dalei and Tannya Brahme, "Cyber Crime and Cyber Law in India: An Analysis", International Journal of Humanities and Applied Sciences (IJHAS) Vol. 2, No. 4, 2013 ISSN 2277 – 4386, PP-106-109

[3] George W. Reynolds, "Ethics in Information Technology", Third Edition, © 2010 Course Technology, Cengage Learning, ISBN-13: 978-0-538-74622-9

[4] Dr. B. muthukumaran," cyber crime scenario in India", Criminal investigation department review- january2008

[5] Rajnish kumar, "A primer on cyber laws in India "Professor (IT), national academy of Indian railways

[6] Cyber Laws in India, "Source: Book on "IT" Security of IIBF Published by M/s Taxmann Publishers"

[7] Talwant Singh, "Cyber law & Information Technology" Addl. district & sessions judge, delhi,talwant@yahoo.com.

[8] "Cyber Crimes: Law and Practice", source: http://delhicourts.nic.in/ejournals/cyber%20law.pdf

[9] Adv. Prashant Mali, "Types of Cyber Crimes & Cyber Law in India", Security Corner, IT Act 2000.