CYBER CRIME
LAW AND PRACTICE

THE INSTITUTE OF
Company Secretaries of India
IN PURSUIT OF PROFESSIONAL EXCELLENCE
Statutory body under an Act of Parliament

November 2016

Price : Rs. 200/- (*Excluding postage*)

Published by :

THE INSTITUTE OF COMPANY SECRETARIES OF INDIA
ICSI House, 22, Institutional Area, Lodi Road
New Delhi - 110 003

Phones : 45341005, 41504444; *Fax* : 24626727
E-mail : info@icsi.edu ; *Website* : www.icsi.edu

ISBN : 978-93-82207795

Printed at Samrat Offset Works/500/November 2016

PREFACE

"As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace." *- Newton Lee*

The prologue of Information and Communication Technology (ICT) has paved the way for an advanced and swift communication for the civilization. At petite, this avant-garde dawn of the ICT has replaced the traditional communication channels leading to an ease, swiftness, convenience and expediency in our regular transactions. Along the way, it has enhanced the modus operandi of carrying out trade and commerce and has indeed escorted the trade and commerce to reach the higher indices of growth and development. However, there is a flip side, with an ease in communication and elevated trade and commerce, the crimes committed through the means and the end of ICT commonly known as Cyber Crimes have also risen exponentially leading to proportionately expanding the dimensions of Cyber Law.

The increasing number of incidents, different methods and modes employed in committing such speckled crimes through the use of computers has raised alarm bells to provide for a colossal legal protection including the provision for punishments for the use of ICT for illegal purposes. Indeed, this specialized field of law has been identified to regulate the use of ICT with two main objectives viz., promoting transactions with the use of ICT and preventing the unauthorized and illegal use of ICT.

This Book titled "Cyber Crime: Laws and Practices" is an effort made to explain the nuances of cyber crimes, including types of Cyber Crimes along with some real time cases that recently happened in the Indian Jurisdiction. The book also analyses the present position of Indian law on the subject and recommends some amendments needed in the present legal set-up for an enhanced legal protection at par with those in other jurisdictions.

I commend the dedicated efforts put in by Dr. Gargi Rajvanshi, Assistant Director, ICSI in preparing the manuscript of this publication under the guidance of Ms. Sonia Baijal, Director, Professional Development, Perspective Planning & Studies, ICSI. I convey my thanks to Mr. Nitin Satija, LexisNexis India for vetting the publication.

I sincerely believe that this book will be of utmost utility and interest to the professionals and would act as a valuable academic aid for the scholars on the subject.

Place : New Delhi **(CS Mamta Binani)**

Date : November 04, 2016 *President*

The Institute of Company Secretaries of India

CONTENTS

Chapter 1

Introduction

1.1 Introduction

The dawn of Information and Communication Technology ('ICT' in short) has witnessed an emergence of a revolutionised transformation in the form of advancement and development of the civilized society. ICT has gradually replaced the conventional systems of communication, authentication and submission. Alongside, it has created pace, ease, swiftness and convenience in concluding transactions. Thus, it may not be wrong to say that with such an increasing pace of use of ICT, the World is getting shrunk like a palm. This is also contributing towards a constant growth of our society in almost all imperative sectors. Among others things, the businesses too are going global with the prospect of ease and swiftness rendered by the ICT.

The advancements made by the modern technology have facilitated the community to develop and expand their communication networks thus enabling faster and easier networking along with information exchange. In short, the ICT has shaped a commendable platform for the society enabling it to grow by leaps and bounds.

In the world today, technology has become an essential part of our day to day life and has virtually got imbedded into it. With the expansion of use of technology in almost every sphere of human life, there is virtually no room left for us to think of a life without the blessings of technology. Fortuitously, India is also advancing in the matter of use of ICT and at a pace which is helping to stave off stagnation.

UN International Telecommunications Union's flagship

annual measuring the Information Society Report states that globally 3.2 billion people are now online, representing 43.4 per cent of the world's population, while mobile-cellular subscriptions have reached almost 7.1 billion worldwide, with over 95 per cent of the global population now covered by a mobile-cellular signal[1].

As per the report published in The Indian Express[2], India has been ranked 131 out of 167 nations on a global index that measures the level of Information and Communication Technology access, even as the number of households with a computer and internet connection has increased to a good extent in the country over the last five years.

Everyone is getting increasingly dependent on consistent access and accuracy of these communication channels. The internet users have increased significantly especially in the last 15 years. Data[3] shows that presently around 40% of the World Population has an internet connection. In 1995 however, it was less than one percent of the present users of internet and today there are more than 3 billion internet users all over the World.

As per the reports of Internet World Stat[4], after China, India has the 2nd largest number of internet users in the World with more than 1 billion users as on June 2016. The Internet penetration in India is 36.5% of the overall population and the growth that it has registered has seen a remarkable growth in the last one decade.

This clearly indicates that the impact of Information Technology is very profound. Both Society and the Technology are operating in a way so as to harmonize with the pace of each other's growth. As the World is developing, more technology is emerging with each passing day and thus there is more development taking place in the society. All the facets of human life including education, health, entertainment and communication are being influenced by and have been impacted by the advent of the Information and Communication Technology.

This way it is serving with several advantages like greater

efficiency, increased communication channels through email, discussion groups and chat rooms, beneficial motivational influence on learning and knowledge, e-governance and citizens contribution, expanding global business and alike.

With boon comes the bane and thus the World of ICT is no exception to this rule. Along with abundant opportunities that it has brought about, there are also some challenges too. Broadly speaking, it has posed certain major concerns like privacy threat, over riding cultural impact, more reliance on technology, boycott of societal engagements, computer virus, malware, spam phishing and many more. One of the major challenges in this era of ICT is of an increasing number of cyber crimes taking place in the World today.

The tremendous growth in the field of ICT coupled with an increased frequency of use of internet for different activities has also given rise to several mischievous activities taking place in the form of Cyber Crimes. To put in a layman's language, Cyber Crime is a technology based crime committed by the technocrats.

In a recent data[5] published, it is stated that "with increasing mobile and internet penetration in the country, cyber crimes have also increased proportionately. Between 2011 and 2015, more than 32000 cyber crimes were reported across the country. More than 24000 of these cases are registered under the IT Act and the remaining under the various sections of IPC and other State Level Legislations (SLL)."

As per the Data given by the report of National Crime Report Bureau[6], a total of 7,201 cases were registered under the IT Act during the year 2014 as compared to 4,356 cases during the previous year (2013), showing an increase of 65.3% in 2014 over 2013. 77% (5,548 cases) of the total 7,201 cases under the IT Act were computer related offences (under section 66A, 66B, 66C, 66D and 66E of IT Act) followed by 10.5% (758 cases out of 7,201 cases) related to publication/ transmission of obscene/sexually explicit content (under section 67A, 67B and 67C of IT Act).

Along with it, the global spam rate, malware rate and

phishing rate is increasing rapidly and there is a potential impact of cyber crimes on the economy, consumer trust and production time. The counter measures in the form of GPRS Security architecture, Intrusion Detection and prevention System and Agent Based Distributed Intrusion, Detection Systems have thus been employed for security purposes.

Considering the significant increase in number of Cyber Crimes reported these days, it becomes important and imperative to enquire as to meaning of the term Cyber Crime, the kinds of Cyber Crimes, their impacts and effects on the Society at large, the law/statute dealing with cyber crimes in India and the deterrent effect of law on Cyber Crimes in India.

Therefore, this manuscript deals with (a) the meaning and variants of cyber crimes like Salami Attack, Packet Sniffing, Tempest Attacks, and Bot Networks; (b) the real world cyber crime cases, their scenario as well as the modus operandi employed for commission of such crimes.

It also focuses on the legal regime on the subject of Cyber Crimes in India and its strong analysis leading to the viable recommendations towards the effective legal protection against the cyber crimes in India.

1.2 Cyber Crime: Meaning and Definition

Crime is not per se a legal term. It derives its meaning and has a connotation in the background of a society than the State as such. Thus, it defies an attempt to lay down a straight jacket definition with clearly defined boundaries. However, usually it is put synonymous to something which is "a wrong", "an offence", "a misdemeanour" or "a felony". Crime is both a social and an economic phenomenon. It is as old and historical as the human society itself. Many ancient books, right from the pre-historic days, and mythological stories have spoken about crimes being committed by individuals; be it committed against an individual like ordinary theft and burglary or against the nation at large like the crimes of spying, treason, etc.

Kautilya's Arthashastra, a document written around in the

350 BC is considered to be one of the most authentic administrative treatises in India which discusses the various crimes committed in the society, security initiatives to be taken by the rulers to curb them, possible crimes in a State, etc. It also advocates awarding different punishments for different offences listed therein. Further, the concept of restoration of loss to the victims has also been discussed in it.

In his theory of probable crime, he has discussed as to how with the changes in society, different crimes emerge. To illustrate the weak position of women in the society it lays down that the crimes against women will increase in the society; with the strong position of a specific sector, the abuse of power will result in commission of crimes associated with the power-play.

Certainly, the advent of Information and Communication Technology has lead to the emergence of a new kind of crime called the Cyber Crime.

To clearly understand the meaning of Cyber Crime, one should first understand the meaning of the term Crime and then the meaning of Cyber Crime.

1.2.1 Meaning of Crime

Crime in any form does adversely affects the members of the society. According to **Merriam Webster Dictionary**, Crime is an act or the commission of an act that is forbidden or the omission of a duty that is commanded by a public law and that makes the offender liable to punishment by that law, especially - a gross violation of law.

According to **Oxford English Dictionary**, Crime is an action or activity or omission considered to be evil, shameful, or wrong; which constitutes an offence and is punishable by law.

Blackstone defines Crime as an act committed or omitted in violation of a public law either forbidding or commanding it.

Stephen observed, "a crime is a violation of a right

considered in reference to the evil tendency of such violation as regards the community at large" .

Oxford Dictionary defines Crime as an act punishable by law as forbidden by statute or injurious to the public welfare.

In a layman's language, a crime can be defined as an unlawful act punishable by a State or other authority. The term "crime" does not, under the modern criminal law, has a simple and universally accepted definition, though statutory definitions have been provided for certain purposes.

The most popular view is that Crime is a category created by law; in other words, something is a Crime if it is declared as such by the relevant and applicable law. One proposed definition is that a Crime or an Offence (or criminal offence) is an act harmful not only to an individual or individuals but also to the community, society or the State at large ("a public wrong"). Such acts are thus forbidden and punishable by law.

Therefore, an inclusive definition of the term Crime can be that it is an act or an omission which is prohibited by law.

Deducing from the definitions of the term 'Crime' above, Cyber Crime can be defined as an act or omission prohibited by law which is carried out either with the means of or where the target is a computer, computer source or computer network.

1.2.2 Meaning of Cyber Crime

It is rightly said that everything has a cost associated with it and so is the case with growing popularity and convenience of digital networks. The ease, convenience and swift communication provided by the Information and Communication technology does also come at a cost. As the businesses and societies are increasingly relying on computers and internet-based networking, the cyber crimes and digital attack incidents have increased many fold.

These attacks are generally classified as crimes that involve the use of a computer or computer source or computer

networks. The instances of different cyber crimes being committed include the financial scams carried out through the mode of computer, computer hacking, downloading pornographic images from the internet, virus attacks, e-mail stalking and creating websites that promote racial hatred.

The first major instance of a cyber crime being committed was reported in the late 90's, when a computer virus mailed to the masses affected nearly 45 million computer users worldwide.

As in the developed world, in developing economies too, the cyber crimes have increased manifold, owing to the rapid diffusion of Internet and the digitisation of economic activities. Thanks to the huge penetration of technology in almost all areas of operation of society, from corporate governance and state administration to the level of petty shop keepers computerizing their billing system, we find computers and other electronic devices pervading the human life. The penetration is so deep that we cannot think of operating without being associated with computers.

The term 'Crime' has neither been defined in the Information Technology Act, 2000 nor in the Information Technology (Amendment) Act, 2008 nor in any other legislation in India. In fact, it is quite difficult, if not impossible, to define the word Crime. The word 'Offence' has been defined under the Indian Penal Code, 1860 and also in quite a few other legislations too. In order to define Cyber Crime, we can say, it is a crime associated with or committed with the help of computers. To put it in simple words 'an offence or a crime in which a computer is used can be said to be a cyber crime'. Interestingly, even a petty offence like stealing or pick-pocket can be brought within the broader purview of cyber crime if the basic data or aid to such an offence is given through a computer or the information stored in a computer used (or misused) by the offender. The I.T. Act, 2000 does define words like computer, computer network, data, information and all other associated terms that form a part of the term cyber crime, about which we will now be discussing in detail.

In a cyber crime, the computer or the data itself is either a target or the object of an offence or a tool employed in committing some offence, and thus providing the necessary inputs for that offence. All such acts of crime come under the broad definition of the term Cyber Crime.

Cyber crimes are technology based crimes wherein the computer or internet itself is used as a weapon or means to commit such crimes. They are organized and white collar crimes like cyber frauds, hacking, data theft, phishing, identity theft, etc. Cyber crimes are committed with the help of technology and cyber criminals have a deep understanding of technology. In fact, cyber criminals are technocrats who understand the intricacies of Information Technology. Cyber crimes do not know or recognise any territorial boundary or barrier.

In general, a Cyber Crime can be classified into the following three categories:

1. *Target Cyber Crime* : It is a crime wherein a computer is the target of the offence.
2. *Tool Cyber Crime* : It is a crime wherein a computer is used as a tool in committing the offence.
3. *Computer incidental* : It is a crime wherein the computer plays only a minor role in the commission of the offence.

Accordance to the Information Technology Act, 2000 a Cyber Crime can be defined as "an act or omission that is punishable under the Information Technology Act, 2000". This however is not an exhaustive definition as the Indian Penal Code also covers certain cyber crimes, such as email spoofing and cyber defamation, sending threatening emails, etc.

***

Chapter 2

Classification of Cyber Crimes

2.1 Taxonomy of Cyber Crime

With an enormous growth witnessed in the field of communication technology and with the ease of transactions under it, there is swift growth as well as development in the world. The World Wide Web (www) sounds like a vast phenomenon but surprisingly one of its qualities is that it has brought the world closer which has also made it a closely linked place to live in for its users.

However, it has also resulted in creation of a major challenge in the form of Cyber Crimes.

Cyber crime is an intricate concept to be defined in a simple and in layman's language. However, it can be said that when any crime is committed over the Internet it can be referred to as a Cyber Crime.

There are different cyber crimes which are taking place in the present world which is dominated by the Information and Communication Technology. It could be hackers vandalizing your website, viewing confidential information, stealing trade secrets or intellectual property with the use of internet. It can also include 'denial of services' and virus attacks preventing regular traffic from reaching your website. Cyber crimes are not limited to outsiders except in case of viruses and with respect to security related cyber crimes that are usually committed by the employees of particular company/organisation who can easily access the password and the data storage of the company for their illegal purposes. Cyber crimes also include criminal activities carried out with the use of computers which further perpetuates different crimes, e.g. financial crimes, sale of

illegal articles, pornography, online gambling, intellectual property crime, e-mail, spoofing, forgery, cyber defamation, cyber stalking, unauthorized access to Computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system, etc.

Although the law enforcement agencies are working to deal with this problem and trying their best to deal with this menace; yet it is growing steadily and thus people are increasingly becoming victims of cyber crimes like hacking, theft, identity theft, etc.

Though there is a protection provided by law against such cyber crimes, there is also a need to protect your sensitive information by using impenetrable security that uses a unified system of software and hardware to authenticate an information that is sent or accessed over the Internet.

However, before one can understand the legal regime surrounding cyber crimes, one need to understand different cyber crimes taking place in this contemporary world.

2.2 Classifications of Cyber Crimes

The number of Cyber Crimes committed is increasing with each passing day, and it is very difficult to find out as to what is actually a cyber crime and what is the conventional crime. However, to deal with this challenge, the most common cyber crimes can be categorised and discussed under the following heads:

1. Cyber Crime Against Person;
2. Cyber Crime Against Property;
3. Cyber Crime Against Government;
4. Cyber Crime Against Society.

2.2.1. Cyber Crimes against Persons

There are certain offences which affect the personality of an individual and can be defined as:

(i) *Harassment via E-Mails* : It is a very common type of

harassment done through letters, attachments of files & folders, i.e., via e-mails. At present, harassment is common with the increase in the usage of social networking sites, like Facebook.com, Twitter.com, etc.

(ii) *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.

(iii) *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.

(iv) *Malware* : Malware is software that takes control of any individual's computer to spread a bug to other people's devices or social networking profiles. Such software can also be used to create a 'botnet'— a network of computers controlled remotely by hackers, known as 'herders,' — to spread spam or viruses.

(v) *Defamation* : It is an act of imputing any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with vulgar language to unknown persons mail account.

(vi) *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 hack telecommunication and mobile network.

(vii) *Cracking* : It is amongst the gravest cyber crimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.

(viii) *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.

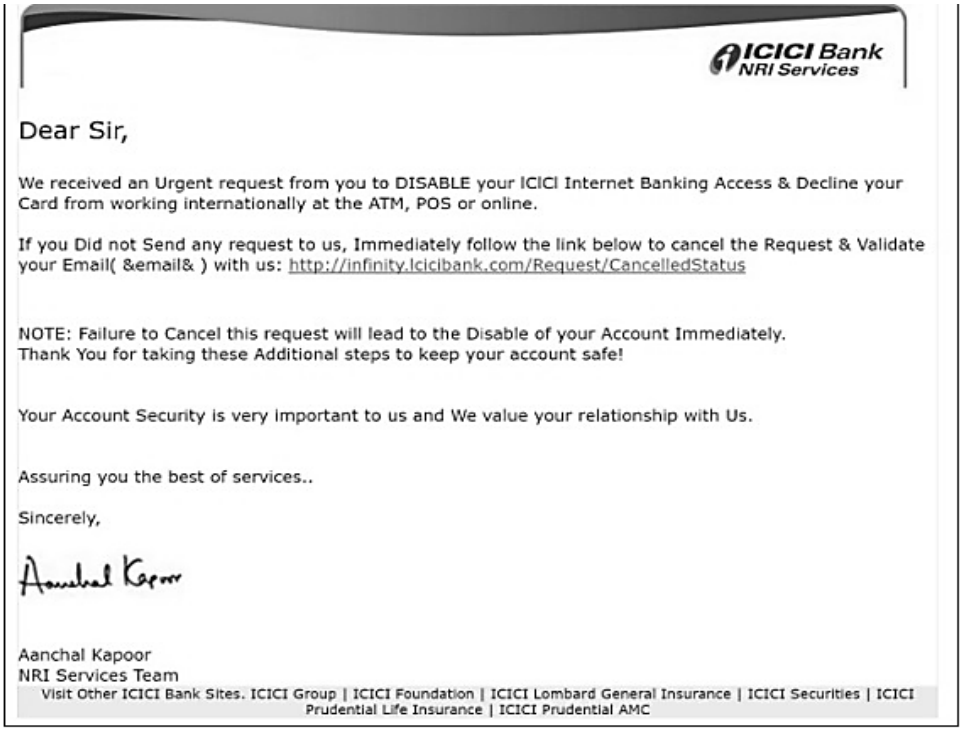
(ix) *SMS Spoofing* : Spoofing is a blocking through spam which means the unwanted uninvited messages. Here a offender steals identity of another in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is very serious cyber crime against any individual.

(x) *Carding* : It means false ATM cards, i.e., Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account mala-fidely. There is always unauthorized use of ATM cards in this type of cyber crimes.

(xi) *Cheating & Fraud* : It means the person who is doing the act of cyber crime i.e. stealing password and data storage has done it with wrongful intention which leads to fraud and cheating.

(xii) *Child Pornography* : It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children.

(xiii) *Phishing* : Phishing is just one of the many frauds on the Internet, Phishing trying to fool people into parting with their money. Phishing refers to the receipt of unsolicited emails by customers of financial institutions, requesting them to enter their username, password or other personal information to access their account for some reason. Customers are directed to a fraudulent replica of the original institution's website when they click on the links on the email to enter their information, and so they remain unaware that the fraud has occurred. The fraudster then has access to the customer's online bank account and to the funds contained in that account.



ICICI Bank NRI Services

Dear Sir,

We received an Urgent request from you to DISABLE your ICICI Internet Banking Access & Decline your Card from working internationally at the ATM, POS or online.

If you Did not Send any request to us, Immediately follow the link below to cancel the Request & Validate your Email(&email&) with us: http://infinity.icicibank.com/Request/CancelledStatus

NOTE: Failure to Cancel this request will lead to the Disable of your Account Immediately.
Thank You for taking these Additional steps to keep your account safe!

Your Account Security is very important to us and We value your relationship with Us.

Assuring you the best of services..

Sincerely,

Aanchal Kapoor
NRI Services Team

Visit Other ICICI Bank Sites. ICICI Group | ICICI Foundation | ICICI Lombard General Insurance | ICICI Securities | ICICI Prudential Life Insurance | ICICI Prudential AMC

The above fraud message is a classic example of a phishing scam. This is how fraudsters operate. The full site address is same except "s" missing in "https" and small letter "L" used instead of "i" as in ICICI. It looks similar to ICICI banks Web address. You may receive similar messages from fraudsters. Please DO NOT click on such links.

(xiv) *Vishing* : Vishing is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private personal and financial Information from the public for the purpose of financial reward. The term is a combination of "voice" and phishing.

(xv) *Bot networks* : A cyber crime called 'Bot Networks', wherein spamsters and other perpetrators of cyber crimes remotely take control of computers without the users realizing it, is increasing at an alarming rate. Computers get linked to Bot Networks when users

unknowingly download malicious codes such as Trojan horse sent as e-mail attachments. Such affected computers, known as zombies, can work together whenever the malicious code within them get activated, and those who are behind the Bot Networks attacks get the computing powers of thousands of systems at their disposal. Attackers often coordinate large groups of Bot-controlled systems, or Boot networks, to scan for vulnerable systems and use them to increase the speed and breadth of their attacks. Boot networks create unique problems for organizations because they can be remotely upgraded with new exploits very quickly and this could help attackers pre-empt security efforts.

(xvi) *Assault by Threat* : It refers to threatening a person with fear for their lives or lives of their families through the use of a computer network, i.e., E-mail, videos or phones.

(xvii) *Buffer overflow* : This is the most common way of breaking into a computer. Buffers are created to hold a finite amount of data. When it overflows, it goes into adjacent buffers which can cause data to be overwritten. In buffer overflow attacks, the extra data can contain instructions that trigger specific actions. These actions can cause damage to files and/or change data.

2.2.2. Crimes against Persons' Property

As there is rapid growth in the international trade where businesses and consumers are increasingly using computers to create, transmit and to store information in the electronic form instead of traditional paper documents. There are certain offences which affect person's properties which are as follows:

(i) *Intellectual Property Crimes* : Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.

(ii) *Software piracy* : Many people do not consider software piracy to be theft. They would never steal a rupee from someone but would not think twice before using pirated software. There is a common perception amongst normal computer users to not consider software as "property". This has led the software piracy to become a flourishing business.

The software pirate sells the pirated software in physical media (usually CD ROMs) through a close network of dealers.

The suspect uses high speed CD duplication equipment to create multiple copies of the pirated software. This software is sold through a network of computer hardware and software vendors

(iii) *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.yahoo.com and www.yaahoo.com.

(iv) *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.

(v) *Hacking Computer System* : Hacktivism attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity there will be loss of data as well as computer. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company.

A hacker is an unauthorized user who attempts to or

gains access to an information system. Hacking is a crime even if there is no visible damage to the system, since it is an invasion in to the privacy of data. There are different classes of Hackers.

(a) *White Hat Hackers* - They believe that information sharing is good, and that it is their duty to share their expertise by facilitating access to information. However there are some white hat hackers who are just "joy riding" on computer systems.

(b) *Black Hat Hackers* -They cause damage after intrusion. They may steal or modify data or insert viruses or worms which damage the system. They are also called 'crackers'.

(c) *Grey Hat Hackers* - Typically ethical but occasionally violates hacker ethics Hackers will hack into networks, stand-alone computers and software. Network hackers try to gain unauthorized access to private computer networks just for challenge, curiosity, and distribution of information. Crackers perform unauthorized intrusion with damage like stealing or changing of information or inserting malware (viruses or worms)

(vi) *Transmitting 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.

(vii) *Packet Sniffing* : This is used by hackers and forensic experts. Data travels in the form of packets and vary in size depending on the network bandwidth and amount of data. The hacker intercepts the transmission between computer A and B. All the hacker needs is the IP address from one of the computers and any data can be stolen. The data is not stolen because sniffers don't do that. Instead they copy the hex and translate it into original

data. This is why it is hard for firewalls to detect this because they only provide application level security.

(viii) *Cyber Trespass* : It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.

(ix) *Salami Attack* : Those attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. e.g., a bank employee inserts a program into bank's servers, that deducts a small amount from the account of every customer.

(x) *Internet Time Thefts* : Basically, Internet time theft comes under hacking. It is the use by an unauthorised person, of the Internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. You can identify time theft if your Internet time has to be recharged often, despite infrequent usage.

(xi) *Trojan and Rats* : Trojan horses are programs that appear to be doing what the user wants while they are actually doing something else such as deleting files or formatting disks. All the user sees is the interface of the program that he wants to run. RATs are remote access Trojans that provide a backdoor into the system through which a hacker can snoop into your system and run malicious code.

(xii) *Data Diddling* : Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. The culprit can be anyone involved in the process of creating,

recording, encoding, examining, checking, converting, or transmitting data. This is one of the simplest methods of committing a computer-related crime, because it requires almost no computer skills whatsoever. Despite the ease of committing the crime, the cost can be considerable.

(xiii) *Email account hacking* : Emails are increasingly being used for social interaction, business communication and online transactions. Most email account holders do not take basic precautions to protect their email account passwords. Cases of theft of email passwords and subsequent misuse of email accounts are becoming very common.

The victim's email account password is stolen and the account is then misused for sending out malicious code (virus, worm, Trojan etc) to people in the victim's address book. The recipients of these viruses believe that the email is coming from a known person and run the attachments. This infects their computers with the malicious code.

The suspect would install key loggers in public computers (such as cyber cafes, airport lounges etc.) or the computers of the victim.

2.2.3. Cybercrimes Against Government

There are certain offences done by group of persons intending to threaten the international governments by using internet facilities. It includes:

(i) *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.

(ii) *Web defacement* : Website defacement is usually the substitution of the original home page of a website

with another page (usually pornographic or defamatory in nature) by a hacker.

Religious and government sites are regularly targeted by hackers in order to display political or religious beliefs. Under the scenario, the homepage of a website is replaced with a pornographic or defamatory page. In case of Government websites, this is most commonly done on symbolic days (e.g., the Independence Day of the country).

The defacer may exploit the vulnerabilities of the operating system or applications used to host the website. This will allow him to hack into the web server and change the home page and other pages. Alternatively he may launch a brute force or dictionary attack to obtain the administrator passwords for the website. He can then connect to the web server and change the WebPages.

(iii) *Cyber Warfare* : It refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation.

(iv) *Use of Internet and Computers by terrorists* : Many terrorists are using virtual as well as physical storage media for hiding information and records of their illicit business. They also use emails and chat rooms to communicate with their counterparts around the globe. The suspects carry laptops wherein information relating to their activities is stored in encrypted and password protected form. They also create email accounts using fictitious details. In many cases, one email account is shared by many people. E.g., one terrorist composes an email and saves it in the draft folder. Another terrorist logs into the same account from another city / country and reads the saved email. He then composes his reply and saves it in the draft folder. The emails are not actually sent. This makes

email tracking and tracing almost impossible. For committing this crime the terrorists purchase small storage devices with large data storage capacities. They also purchase and use encryption software. The terrorists may also use free or paid accounts with online storage providers.

(v) *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.

(vi) *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.

2.2.4. Cybercrimes Against Society at large

An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. These offences include:

(i) *Child Pornography* : It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity.

(ii) *Cyber Trafficking* : It may be trafficking in drugs, human beings, arms weapons etc. which affects large number of persons. Trafficking in the cyberspace is also a gravest crime.

(iii) *Online Gambling* : Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.

(iv) *Financial Crimes* : This type of offence is common as there is rapid growth in the users of networking sites and phone networking where culprit will try to attack by sending bogus mails or messages through internet. Ex: Using credit cards by obtaining password illegally.

v. *Forgery* : It means to deceive large number of persons by sending threatening mails as online business transactions are becoming the habitual need of today's life style.

2.3 Causes of Cyber Crime

(i) *Economically Motivated Cyber Crime*

As is the case with many crimes committed outside the Internet, money is a major motivator for many cyber criminals. Especially because the dangers of criminality are less apparent when you're hiding behind a network, the perception of low risk and very high financial reward prompts many cyber criminals to engage in malware, phishing, identity theft and fraudulent money request attacks. Business week estimates that cyber crimes targeting online banking accounts alone, for example, pull in nearly 700 million dollars per year globally.

(ii) *Ideologically Motivated Cyber Crime*

After financial companies like Visa, MasterCard and PayPal refused to let account and card holders make contributions to the controversial non-profit WikiLeaks, the "hacktivist" group Anonymous coordinated a series of bot attacks on the companies' servers, rendering them unreachable to Internet users. These kinds of attacks are conducted for perceived ethical, ideological or moral reasons, damaging or disabling computer equipment and networks to express grievances against individuals, corporations, organizations or even national governments.

(iii) *Structural Causes*

Beyond the causes that motivate criminals, the environment in which cyber crime is committed also serves to explain the prevalence of the phenomenon. While more and more personal and sensitive information is stored online -- increasing the potential rewards for cyber criminals -- neither computer security nor applications like email filters have improved dramatically

in terms of coverage. According to the anti-virus manufacturer Norton, for example, as many as 41 percent of computers did not have up-to-date security protection in 2012.

(iv) *Personally Motivated Cyber Crime*

Cyber criminals are still human beings and what they do including their crimes is often the cause of personal emotions and vendettas. From the disgruntled employee installing a virus on office computers to a jealous boyfriend hacking into a girlfriend's social media accounts or a teenager taking down a school website just to prove that he could do it, many cyber crimes are essentially crimes of passion committed over the Internet. Many of these crimes, however, can still have very serious impacts and cause considerable property damage.

2.4 Impact and Effects of Cyber Crimes

The effects of a single, successful cyber attack can have far-reaching implications including financial losses, theft of intellectual property, and loss of consumer confidence and trust. The overall monetary impact of cyber crime on society and government is estimated to be billions of dollars a year. Cyber Crimes always affects the companies of any size because almost all the companies gain an online presence and take advantage of the rapid gains in the technology but greater attention to be given to its security risks. In the modern cyber world cyber crimes is the major issue which is affecting individual as well as society at large too.

(i) *Loss of Revenue*

One of the main effects of cyber crime on a company is a loss of revenue. This loss can be caused by an outside party who obtains sensitive financial information, using it to withdraw funds from an organization. It can also occur when a business e-commerce site becomes compromised while inoperable, valuable income is lost when consumers are unable to use the site.

(ii) *Potential Economic Impact*

As today's consumer has become increasingly dependent

on computers, networks, and the information these are used to store and preserve, the risk of being subjected to cyber-crime is high. Some of the surveys conducted in the past have indicated as many as 80% of the companies' surveyed acknowledged financial losses due to computer breaches. As the economy increases its reliance on the internet, it is exposed to all the threats posed by cyber-criminals. Stocks are traded via internet, bank transactions are performed via internet, purchases are made using credit card via internet. All instances of fraud in such transactions impact the financial state of the affected company and hence the economy.

(iii) *Wasted Time*

Another major effect or consequence of cyber crime is the time that is wasted when IT personnel must devote great portions of their day handling such incidences. Rather than working on productive measures for an organization, many IT staff members spend a large percentage of their time handling security breaches and other problems associated with cyber crime.

(iv) *Damaged Reputations*

In cases where customer records are compromised by a security breach associated with cyber crime, a company's reputation can take a major hit. Customers whose credit cards or other financial data become intercepted by hackers or other infiltrators lose confidence in an organization and often begin taking their business elsewhere. The impact of the damaged reputation can be clearly understood by the example of the hacking of Walmart server making a huge loss of reputation to the one of the biggest retailer of the US and Europe.

Walmart Case Study

In year 2006, WALMART became the victim of a serious security breach in which hackers targeted the development team in charge of the chain's point-of-sale system and siphoned source code and other sensitive data to the company's server in Europe[7].

KIM ZETTER SECURITY 10.13.09 7:00 AM

BIG-BOX BREACH: THE INSIDE STORY OF WAL-MART'S HACKER ATTACK

Reproduced from Big Box Breach

Wal-Mart had a number of security vulnerabilities at the time of the attack, according to internal security assessments seen and acknowledged as genuine by Wal-Mart. For example, at least four years' worth of customer purchasing data, including names, card numbers and expiration dates, were housed on company networks in unencrypted form. Wal-Mart says it was in the process of dramatically improving the security of its transaction data, and in 2006 began encrypting the credit card numbers and other customerinformation, and making other important security changes.

Wal-Mart really made every effort to segregate the data, to make separate networks, to encrypt it fully from start to finish through the transmission, and not just in one area but across the different uses of credit card systems.

Investigators found that the tool had been installed remotely by someone using a generic network administrator account.

The intruder had reached the machine through a VPN account assigned to a former Wal-Mart worker in Canada, which administrators had failed to close after the worker left the company. The day the server crashed, the intruder had been connected to Wal-Mart's network for about seven hours, originating from an IP address in Minsk, the documents show.

The intruders' interest in Wal-Mart's point-of-sale system is consistent with large data breaches that occurred at other companies around the same time.

This has shaken the trust of consumers in doing transactions at Walmart and it has subsequently reduced the business of Walmart too.

(v) *Reduced Productivity*

Due to the measures that many companies must implement to counteract cyber crime, there is often a negative effect on employees' productivity. This is because, due to security measures, employees must enter more passwords and perform other time-consuming acts in order to do their jobs. Every second wasted performing this task is a second not spent working in a productive manner.

(vi) *Impact on consumer trust*

Since cyber-attackers intrude into others' space and try and break the logic of the page, the end customer visiting the concerned page will be frustrated and discouraged to use the said site on a long term basis. The site in question is termed as the fraudulent, while the criminal masterminding the hidden attack is not recognized as the root cause. This makes the customer lose confidence in the said site and in the internet and its strengths.

2.5 Cyber Crime: Some Landmark Occurrence

1. *Official Website of Maharashtra Government Hacked*

On September, 2007 in Mumbai the official website of the government of Maharashtra was hacked.

Cyber Crime Branch police got active in investigating the matters and tracking down the hackers. For a day the

website, http://www.maharashtragovernment.in, remained blocked.

The state government website contains detailed information about government departments, circulars, reports, and several other topics. IT experts who worked on restoring the website told that they fear that the hackers may have destroyed all of the website's contents.

According to sources, the hackers may be from Washington. IT experts said that the hackers had identified themselves as "Hackers Cool Al-Jazeera" and claimed they were based in Saudi Arabia. They added that this might be a red herring to throw investigators off their trail.

The official website has been affected by viruses on several occasions in the past, but was never hacked. The official added that the website had no firewall.

2. *Official Website of IRCTC Hacked*

Another incidence of cyber crime was reported when the official website of IRCTC was hacked and around 1 crore customer's details were put at risk[8].

Reproduced from Daily Bhaskar

3. *CBI Website Hacked*

In an incidence, it was reported in year 2013 that the official website of CBI was hacked for few hours[9].


Central Bureau of Investigation
Industry • Impartiality • Integrity

Oooopssss! WTF? CBI? Cyber Crime? Hacked? hahaha funny a

This attempt is in response to the pakistani websites hacked by **'Indian Cyber Army'**. We told you before too ..we are sleeping but
cyber army)'..back off kids or we will smoke your d00rs off like we did before..lets see what you investigating agency so called CBI
more attempt from your side..we got your every website lying around here like its our local server! hahahaha..so we would like to s
31337 NIC team..go and read some more books ..you guys are seriously bunch of script_kiddies! ..you know nothing rite now..got
defacements..how about something like this..a planned attack! haha..btw we got r00t to your NIC too :P ..your filtering sucks..have
better things to do.. :D ..stop complaining about pakistani websites security..secure your own ass first..thats what intelligent people

A message by Pakistan Cyber Army

Pakistan Zindabad!

Reproduced from Rediff News

4. *ICICI - Pune Bank Fraud case*

Three people held guilty in on line credit card scam. Customer's credit card details were misused through online means for booking air-tickets. These culprits were caught by the city Cyber Crime Investigation Cell in Pune. It was found that details misused were belonging to 100 people. Mr. Parvesh Chauhan, ICICI Prudential Life Insurance officer had complained on behalf of one of his customer. In this regard Mr. Sanjeet Mahavir Singh Lukkad, Dharmendra Bhika Kale and Ahmead Sikandar Shaikh were arrested. Lukkad being employed at a private institution, Kale was his friend. Sheikh was employed in one of the branches of State Bank of India.

According to the information provided by the authorities, one of the customers received a SMS based alert for purchasing of the ticket even when the credit card was being held by him. Customer was alert and came to know something was fishy; he enquired and came to know about the misuse. He contacted the Bank in this regard. Police observed involvement of many Bank's in this reference.

The tickets were book through online means. Police requested for the log details and got the information of the Private Institution. Investigation revealed that the details were obtained from State Bank of India. Sheikh was working in the credit card department; due to this he had access to credit card details of some customers.

He gave that information to Kale. Kale in return passed this information to his friend Lukkad. Using the information obtained from Kale, Lukkad booked tickets. He used to sell these tickets to customers and get money for the same. He had given few tickets to various other institutions.

Cyber Cell was involved in eight days of investigation and finally caught the culprits.

In this regard various Banks have been contacted; also four airline industries were contacted and alerted.

5. *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.

6. *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 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 crafty made along with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop.

7. *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.

8. *Insulting Images of Warrior Shivaji on Google - Orkut*

   An Indian posts 'insulting images' of respected warrior-saint Shivaji on Google's Orkut. Indian police come knocking at Google's gilded door demanding the IP address (IP uniquely identifies every computer in the world) which is the source of this negative image. Google, India hands over the IP address.

   No such incident in India would be complete without a few administrative slip-ups. The computer with that IP

address is using Airtel, India as the ISP to connect to the internet and Orkut. Airtel gives police the name of an innocent person using a different IP address. How two IP addresses could be mixed-up in a sensitive police case is anyone's guess.

An innocent Indian, Lakshmana Kailash K, is arrested in Bangalore and thrown in jail for 3 weeks. Eventually, his innocence is proved and he is released in Oct, 2007.

A number of news media report this incident. American citizen and India lover Christopher Soghoian (home page http://www.dubfire.net/chris/) studies Informatics at Indiana University and researches/writes about security, privacy and computer crime. Christopher does an excellent article on this topic for the blogs at respected tech media group CNET.

Like all good writers, Christopher Soghoian, gives Google, India a list of questions so that he can give a balanced perspective to the millions of CNET readers.

9. *India's First ATM Card Fraud*

The Chennai City Police busted an international gang involved in cyber crime, with the arrest of Deepak Prem Manwani (22), who was caught red-handed while breaking into an ATM in the city in June last, it is reliably learnt. The dimensions of the city cops' achievement can be gauged from the fact that they have netted a man who is on the wanted list of the formidable FBI of the United States.

At the time of his detention, he had with him Rs 7.5 lakh knocked off from two ATMs in T Nagar and Abiramipuram in the city. Prior to that, he had walked away with Rs 50,000 from an ATM in Mumbai. While investigating Manwani's case, the police stumbled upon a cyber crime involving scores of persons across the globe.

Manwani is an MBA drop-out from a Pune college and served as a marketing executive in a Chennai-based firm for some time. Interestingly, his audacious crime career

started in an Internet cafe. While browsing the internet one day, he got attracted to a site which offered him assistance in breaking into the ATMs. His contacts, sitting somewhere in Europe, were ready to give him credit card numbers of a few American banks for $5 per card. The site also offered the magnetic codes of those cards, but charged $200 per code.

The operators of the site had devised a fascinating idea to get the personal identification number (PIN) of the card users. They floated a new site which resembled that of a reputed telecom company's website. That company has millions of subscribers. The fake site offered the visitors to return $11.75 per head which, the site promoters said, had been collected in excess by mistake from them. Believing that it was a genuine offer from the telecom company in question, several lakh subscribers logged on to the site to get back that little money, but in the process parted with their PINs.

Armed with all requisite data to hack the bank ATMs, the gang started its systematic looting. Apparently, Manwani and many others of his ilk entered into a deal with the gang behind the site and could purchase any amount of data, of course on certain terms, or simply enter into a deal on a booty-sharing basis. Meanwhile, Manwani also managed to generate 30 plastic cards that contained necessary data to enable him to break into ATMS.

He was so enterprising that he was able to sell away a few such cards to his contacts in Mumbai. The police are on the lookout for those persons too.

On receipt of large-scale complaints from the billed credit card users and banks in the United States, the FBI started an investigation into the affair and also alerted the CBI in New Delhi that the international gang had developed some links in India too.

Manwani has since been enlarged on bail after interrogation by the CBI. But the city police believe that this is the beginning of the end of a major cyber crime.

10. *Chennai's Violation of Software Terms*

Two managers of Chennai based Radiant Software a Computer Education Company was arrested for an alleged violation of the licensing terms of Software. The top management team had to obtain anticipatory bail to avoid arrests until a compromise was worked out.

11. *Napster Case*

Napster, a very successful E-Venture was hauled to the Court and beaten to death for having caused violation of Copyright of music companies. Despite willing customers and working technology, the business of the Company had to be shelved under an enormous loss to the promoters. There are many websites in India which could be held to be infringing the Patent rights of somebody abroad and asked to shut down or pay compensation putting an end to their entrepreneurial dreams.

***

Chapter 3

Information Technology Law : A Bird's Eye View

3.1 Cyber World *vis-a-vis* need of Legal Protection

Information technology has spread throughout the world. The computer is used in each and every sector wherein cyberspace provides equal opportunities to all for economic growth and human development. Along with this, the users of cyberspace are growing increasingly in the diverse and the range of online interaction. This has also led to the opening out of the cyber crimes like breach of online contracts, perpetration of online torts and crimes etc. too.

Therefore with a view to enhance the proactive use of Information and Communication Technology while encountering the occurrences of cyber crime, there was a need of balanced law for the purposes of ensuring the promotion of secured cyber transactions.

While focussing on the prevention of the cyber crime, it was realized that the government should adopt a strict law to regulate criminal activities relating to cyberspace and to provide better administration of justice to the victim of cyber crime.

It has been established time and again, that the frequent occurrence of cyber crime and a low level of legal protection against cyber crime leads to decrease in online transactions. This might lead to lack of technological development and its utilization at par with global fora. For instance of infringement of the privacy and violation of data is prohibited under Information Technology Act, 2000 under section 43 and 43A; if this protection would not have been provided against data theft and privacy violation in electronic mode, then no one would have been interested

in doing electronic transactions for the want of privacy protection.

In addition to this, in the modern cyber technology world it is very much necessary to regulate cyber crimes and most importantly cyber law should be made stricter in the case of cyber terrorism and hackers.

3.2 Information Technology Act, 2000: A Beginning

Mid 90's saw an impetus in globalization and computerisation, 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 United Nations to give favourable 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.

Therefore, with a view to promote electronic transactions and to give favourable consideration to the Model Law on e-commerce, the Government of India has led to the enactment of Information Technology Act, 2000.

The Information Technology Act, 2000, was thus passed as the Act No.21 of 2000, got Presidential Assent on 9 June and was made effective from 17 October, 2000.

3.2.1 Objectives of Information Technology Act, 2000

The Information Technology Act 2000 has been enacted with the following objectives:

1. To give legal recognition to any transaction this is done by electronic way or use of internet
2. To give legal recognition to digital signature for accepting any agreement via computer.
3. To provide facility of filling document online relating to school admission or registration in employment exchange.
4. To facilitate that any company can store their data in electronic storage.
5. To stop computer crime and protect privacy of internet users.
6. To give legal recognition for keeping books of accounts by bankers and other companies in electronic form.
7. To make more power to IPO, RBI and Indian Evidence act for restricting electronic crime.

The major focus of the Act is 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 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.

3.3 Scope of Information Technology Act, 2000

Every electronic information is under the scope of I.T. Act, 2000 but following electronic transaction are not under I.T. Act 2000:

1. Information Technology Act, 2000 is not applicable on the attestation for creating trust via electronic way. Physical attestation is must.
2. I.T. Act, 2000 is not applicable on the attestation for making will of any body. Physical attestation by two witnesses is must.
3. A contract of sale of any immovable property.
4. Attestation for giving power of attorney of property is not possible via electronic record.

3.4 Applicability of Information Technology Act, 2000

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 exclusion to the Act (i.e., where it is not applicable) as detailed in the First Schedule, stated below:

(a) Negotiable Instrument (Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;

(b) A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;

(c) A trust as defined in section 3 of the Indian Trusts Act, 1882;

(d) A will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition;

(e) Any contract for the sale or conveyance of immovable property or any interest in such property;

(f) Any such class of documents or transactions as may be notified by the Central Government.

3.5 Information Technology Act, 2000: A Snapshot

The Act totally has 13 chapters and 94 sections (the last four sections namely sections 91 to 94 in the ITA 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 there on 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 IT Act, 2000 and since replaced by electronic signatures in the ITAA, 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.

There are 13 chapters in law and all provision is included in this chapters.

Chapter I : Preliminary

This chapter deals with the introduction applicability and scope of the Act.

Chapter II : Digital Signature and Electronic Signature

This chapter states that any contract which is done by subscriber can be executed through online medium too; if he signs the electronic agreement by digital signature. Then it will be valid and will be called e-contract. In this case the

verification of digital signature can be on the basis of key pair.

Chapter III : Electronic Governance

This chapter explains the detail that all electronic records of government are acceptable unless any other law has any rules regarding written or printed record.

Chapter IV : Attribution, Acknowledgement and Dispatch of Electronic Records

This chapter deals with receipts or acknowledgement of any electronic record. Every electronic record has any proof that is called receipt and it should be in the hand who records electronic way.

Chapter V : Secure Electronic Records and Secure Electronic Signatures

This chapter discusses the powers to organization for securing the electronic records and secure digital signature. They can secure by applying any new verification system.

Chapter VI : Regulation of Certifying Authorities

This chapter states that government of India will appoint controller of certifying authorities and he will control all activities of certifying authorities. "Certifying authority is that authority who issues digital signature certificate."

Chapter VII : Electronic Signature Certificates

In this chapter powers and duties of certifying authority is given. Certifying Authority (C.A.) will issue digital signature certification after getting Rs. 25000. If it is against public interest, then C.A. can suspend the digital signature certificate.

Chapter VIII : Duties of Subscribers

This chapter tells about the duties of subscribers regarding digital signature certificate. It is the duty of subscriber to accept that all information in digital signature certificate that is within his knowledge is true.

Chapter IX : Penalties, Compensation and Adjudication

If anybody or group of body damages the computers, computer systems and computer networks by electronic hacking, then they are responsible to pay penalty upto Rs. 1 crore .

Chapter X : The Cyber Appellate Tribunal

Under this chapter, provisions are given to establish cyber regulation appellate tribunal. It will solve the cases relating to orders of adjudicating officers.

Chapter XI : Offences

For controlling Cyber Crime, government can appoint cyber regulation advisory committee who will check all cyber crime relating to publishing others information. If any fault is done by anybody, he will be liable for paying Rs. 2 lakh or punishment of 3 years imprisonment or both.

Chapter XII : Intermediaries not to be liable in certain cases

The Chapter states that in certain cases intermediaries' cannot to be held liable. This chapter owes its genesis from the Bazee.com case.[10]

Chapter XII-A : Examination of Electronic Evidences

Police officers have also power to investigate dangerous cyber crime under Indian Penal Code, 1860; Indian Evidence Act, 1872; and Reserve Bank of India Act, 1934.

Chapter XIII : Miscellaneous

3.6 Information Technology (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 Information Technology Act, 2000.

Thus in the light of ongoing changes, the need was felt for making a detailed amendment in the Information Technology Act, 2000. 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 Presidential assent on 5 Feb 2009 and was made effective from 27 October 2009.

Some of the notable features of the ITAA are as follows:

- Focussing on data privacy
- Focussing 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
- Recognising 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)

3.7 Recompense of Information Technology Law

Following are the major advantages of having a law to regulate Information and Communication Technology:

1. *Promotion of E-commerce*

   Above all things validity in eye of Indian law is very

necessary. After the enactment of IT Act, 2000, all above things are valid and these things are very helpful to promote e-commerce in India.

- Helpful to promote e-commerce
- Email communication is valid and source of legal evidence and authentication
- Digital signature is validated
- Payment via credit card is valid and under the contour of law
- Online contracts are valid and enforceable

2. *Enhance the corporate business*

   After issuing digital signature, certificate by Certifying authority, now Indian corporate business can enhance.

3. *Filling online forms*

   After providing facility, filling online forms for different purposes has become so easy.

4. *High penalty for cyber crime*

   Law has power to penalize for doing any cyber crime. After enacting this law, the number of cyber crimes has reduced.

3.8 Limitation of Information Technology Law

The law is suffering from following weaknesses:

1. Infringement of copyright has not been included in this law.
2. No protection for domain names.
3. The act is not applicable on the power of attorney, trusts and will.
4. Act is silent on taxation.
5. No, provision of payment of stamp duty on electronic documents.

***

Chapter 4

Legal Protection against Cyber Crimes

Cybercrimes are a new class of crimes which are increasing day by day due to extensive use of internet these days. To combat the crimes related to internet the Information Technology Act, 2000 was enacted with prime objective to create an enabling environment for commercial use of I.T. The IT Act specifies the acts which have been made punishable. The Indian Penal Code, 1860 has also been amended to take into its purview cybercrimes. The various offenses related to internet which have been made punishable under the IT Act and the IPC are enumerated below:

4.1 Criminal Liabilities under Information Technology Act, 2000

- Sec.65: Tampering with Computer source documents
- Sec.66: Hacking with Computer systems, Data alteration and other computer related Offences
- Sec. 66A: Punishment for sending offensive messages through communication service etc.
- Sec. 66B: Punishment for dishonestly receiving stolen computer resource or communication device
- Sec. 66C: Punishment for identity theft
- Sec. 66D: Punishment for Cheating by personating by using computer resource
- Sec. 66E: Punishment for Violation of Privacy
- Sec. 66F: Punishment for Cyber Terrorism
- Sec.67: Publishing obscene information
- Sec. 67A: Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form

- Sec. 67B: Punishment for Child Pornography
- Sec. 67C: Preservation and Retention of Information by Intermediaries
- Sec.70: Un-authorized access to protected system
- Sec. 70A: National Nodal Agency
- Sec. 70B: CERT-in
- Sec. 71: Penalty for Misrepresentation
- Sec.72: Breach of Confidentiality and Privacy
- Sec.73: Publishing false digital signature certificates
- Sec. 74: Publication for fraudulent purposes

The criminal provisions of the IT Act and those dealing with cognizable offences and criminal acts follow from Chapter IX titled "Offences"

Section 65 : *Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.*

Explanation—For the purposes of this section, "computer source code" means the listing of programmes, computer Commands, design and layout and programme analysis of computer resource in any form.

This section deals with Tampering with computer source code and related documents. Concealing, destroying, and altering any computer source code when the same is required to be kept or maintained by law is an offence punishable with three years imprisonment or two lakh rupees or with both. Fabrication of an electronic record or committing forgery by way of interpolations in CD produced as evidence in a court (*Bhim Sen Garg* vs *State of Rajasthan and others*[11])

attract punishment under this Section. Computer source code under this Section refers to the listing of programmes, computer commands, design and layout etc. in any form.

Case Laws

(i) *Frios* vs *State of Kerala*[12]

Facts : In this case it was declared that the FRIENDS application software as protected system. The author of the application challenged the notification and the constitutional validity of software under Section 70. The court upheld the validity of both. It included tampering with source code. Computer source code the electronic form, it can be printed on paper.

Held : The court held that tampering with Source code are punishable with three years jail and or two lakh rupees fine of rupees two lakh rupees for altering, concealing and destroying the source code.

(ii) *Syed Asifuddin And Ors. vs The State of Andhra Pradesh*[13]

Facts : In this case the Tata Indicom employees were arrested for manipulation of the electronic 32- bit number (ESN) programmed into cell phones, theft were exclusively franchised to Reliance Infocom.

Held : Court held that Tampering with source code invokes Section 65 of the Information Technology Act.

(iii) *State vs Mohd. Afzal And Others*[14] *(Parliament Attack Case)*

Facts : In this case several terrorist attacked on 13 December, 2001 Parliament House. In this the Digital evidence played an important role during their prosecution. The accused argued that computers and evidence can easily be tampered and hence should not be relied.

In Parliament case several smart device storage disks and devices, a Laptop were recovered from the truck intercepted at Srinagar pursuant to information given by two suspects. The laptop included the evidence of

fake identity cards, video files containing clips of the political leaders with the background of Parliament in the background shot from T.V. news channels. In this case design of Ministry of Home Affairs car sticker, there was game "wolf pack" with user name of "Ashiq". There was the name in one of the fake identity cards used by the terrorist. No backup was taken therefore it was challenged in the Court.

Held : Challenges to the accuracy of computer evidence should be established by the challenger. Mere theoretical and generic doubts cannot be cast on the evidence.

Section 66 : *If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.*

Explanation.—For the purpose of this section,—

(a) The word "dishonesty" shall have the meaning assigned to it in section 24 of the Indian Penal Code (45 of 1860).

(b) The word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code (45 of 1860).

Computer related offences are dealt with under this Section. Data theft stated in Section 43[15] is referred to in this Section. Whereas it was a plain and simple civil offence with the remedy of compensation and damages only, in that Section, here it is the same act but with a criminal intention thus making it a criminal offence. The act of data theft or the offence stated in Section 43 if done dishonestly or fraudulently becomes a punishable offence under this Section and attracts imprisonment upto three years or a fine of five lakh rupees or both. Earlier hacking was defined in Sec 66 and it was an offence.

Now after the amendment, data theft of Section 43 is

being referred to in Section 66 by making this section more purposeful and the word 'hacking' is not used. The word 'hacking' was earlier called a crime in this Section and at the same time, courses on 'ethical hacking' were also taught academically. This led to an anomalous situation of people asking how an illegal activity be taught academically with a word 'ethical' prefixed to it. Then can there be training programmes, for instance, on "Ethical burglary", "Ethical Assault" etc. say for courses on physical defence? This tricky situation was put an end to, by the ITAA when it re-phrased the Section 66 by mapping it with the civil liability of Section 43 and removing the word 'Hacking'. However the act of hacking is still certainly an offence as per this Section, though some experts interpret 'hacking' as generally for good purposes (obviously to facilitate naming of the courses as ethical hacking) and 'cracking' for illegal purposes. It would be relevant to note that the technology involved in both is the same and the act is the same, whereas in 'hacking' the owner's consent is obtained or assumed and the latter act 'cracking' is perceived to be an offence.

Case Laws

1. *R vs. Gold & Schifreen*[16]

   In this case it is observed that the accused gained access to the British telecom Prestly Gold computers networks file amount to dishonest trick and not criminal offence.

2. *R vs. Whiteley*[17]

   In this case the accused gained unauthorized access to the Joint Academic Network (JANET) and deleted, added files and changed the passwords to deny access to the authorized users.Investigations had revealed that Kumar was logging on to the BSNL broadband Internet connection as if he was the authorized genuine user and 'made alteration in the computer database pertaining to broadband Internet user accounts' of the subscribers. The CBI had registered a cyber crime case against Kumar

and carried out investigations on the basis of a complaint by the Press Information Bureau, Chennai, which detected the unauthorised use of broadband Internet. The complaint also stated that the subscribers had incurred a loss of Rs 38,248 due to Kumar's wrongful act. He used to 'hack' sites from Bangalore, Chennai and other cities too, they said.

Verdict: The Additional Chief Metropolitan Magistrate, Egmore, Chennai, sentenced N G Arun Kumar, the techie from Bangalore to undergo a rigorous imprisonment for one year with a fine of Rs 5,000 under section 420 IPC (cheating) and Section 66 of IT Act (Computer related Offense).

Thanks to ITAA, Section 66 is now a widened one with a list of offences as follows:

***66A** : Punishment for sending offensive messages through communication service, etc.—Any person who sends, by means of a computer resource or a communication device,— (a) any information that is grossly offensive or has meaning character, or (b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such message, shall be punishable with imprisonment for a term which may extend to three years and with fine.*

Explanation.—For the purposes of this section, terms "electronic mail" and "electronic mail message" means a message or information created to transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

The section covers the offences like sending offensive messages through communication service, causing annoyance etc. through an electronic communication or sending an email to mislead or deceive the recipient about the origin of such messages (commonly known as IP or email spoofing).

Punishment for these acts is imprisonment up to three years or fine.

Case Laws

Fake profile of President posted by imposter

On September 9, 2010, the imposter made a fake profile in the name of the Hon'ble President Smt. Pratibha Devi Singh Patil. A complaint was made from Additional Controller, President Household, President Secretariat regarding the four fake profiles created in the name of Hon'ble President on social networking website, Facebook. The said complaint stated that president house has nothing to do with the facebook and the fake profile is misleading the general public. The First Information Report under Sections 469 IPC and 66A Information Technology Act, 2000 was registered based on the said complaint at the police station, Economic Offences Wing, the elite wing of Delhi Police which specializes in investigating economic crimes including cyber offences.

Bomb Hoax mail

In 2009, a 15-year-old Bangalore teenager was arrested by the cyber crime investigation cell (CCIC) of the city crime branch for allegedly sending a hoax e-mail to a private news channel. In the e-mail, he claimed to have planted five bombs in Mumbai, challenging the police to find them before it was too late. At around 1 p.m. on May 25, the news channel received an e-mail that read: "I have planted five bombs in Mumbai; you have two hours to find it." The police, who were alerted immediately, traced the Internet Protocol (IP) address to Vijay Nagar in Bangalore. The Internet service provider for the account was BSNL, said officials.

66B *Punishment for dishonestly receiving stolen computer resource or communication device.—*

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

The section clearly states that dishonestly receiving stolen computer resource or communication device will be leading to the punishment upto three years or one lakh rupees as fine or both.

66C *Punishment for identity theft -*

Whoever, fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Electronic signature or other identity theft like using others' password or electronic signature etc.

Punishment is three years imprisonment or fine of one lakh rupees or both.

66D : *Punishment for cheating by personation by using computer resource*

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

In accordance with this section, Cheating by personating using computer resource or a communication device shall be punished with imprisonment of either description for a term which extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Case Laws

Sandeep Vaghese vs. State of Kerala[18]

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 crime was registered against nine persons, alleging offenses under Sections 65, 66, 66A, C and D of the Information Technology Act along with Sections 419 and 420 of the Indian Penal Code.

The company has a web-site in the name and style `www.jaypolychem.com' but, another web site `www. jayplychem.org' was set up in the internet by first accused Samdeep Varghese @ Sam, (who was dismissed from the company) in conspiracy with other accused, including Preeti and Charanjeet Singh, who are the 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 with known and unknown persons, who have collectively cheated the company and committed acts of forgery, impersonation etc.

Two of the accused, Amardeep Singh and Rahul had visited Delhi and Cochin. The first accused and others sent e-mails from fake e-mail accounts of many of the customers, suppliers, Bank etc. to malign the name and image of the Company and its Directors. The defamation campaign run by all the said persons named above has caused 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.

66E *Punishment for violation of privacy*

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which

may extend to three years or with fine not exceeding two lakh rupees, or with both

Explanation.- For the purposes of this section--

(a) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) "capture", with respect to an image, means to videotape, photograph, film or record by any means;

(c) "private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

(d) "publishes" means reproduction in the printed or electronic form and making it available for public;

(e) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that--

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

Data Protection and Privacy

This section deals with the punishment for Privacy violation– Publishing or transmitting private area of any person without his or her consent etc. Punishment is three years imprisonment or two lakh rupees fine or both. This section needs to be read along with section 43 and Section 43A which creates civil remedies for data theft wherein section 66 E provides criminal liability for the gross violation of one's privacy.

Cases

(i) *Jawaharlal Nehru University MMS scandal*

In a severe shock to the prestigious and renowned institute – Jawaharlal Nehru University, a pornographic

MMS clip was apparently made in the 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, on the internet and even sold it as a CD in the blue film market.

(ii) *Nagpur Congress leader's son MMS scandal*

On January 05, 2012 Nagpur Police arrested two engineering students, one of them a son of a 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 zila parishad member and an influential Congress leader of Saoner region in Nagpur district.

66F *Punishment For Cyber Terrorism*

(1) Whoever -

(A) With intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

- *denying or cause the denial of access to any person authorized to access computer resource; or*
- *attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or*
- *introducing or causing to introduce any Computer Contaminant and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or*

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

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.

Critique : We find the terminology in multiple sections too vague to ensure consistent and fair enforcement. The concepts of 'annoyance' and 'insult' are subjective. Clause (d) makes it clear that phishing requests are not permitted, but it is not clear that one cannot ask for information on a class of individuals.

Cyber terrorism – Intent to threaten the unity, integrity, security or sovereignty of the nation and denying access to any person authorized to access the computer resource or attempting to penetrate or access a computer resource without authorization. Acts of causing a computer contaminant (like virus or Trojan Horse or other spyware or malware) likely to cause death or injuries to persons or damage to or destruction of property etc. come under this Section. Punishment is life imprisonment.

It may be observed that all acts under Section 66 are cognizable and non-bailable offences. Intention or the

knowledge to cause wrongful loss to others i.e. the existence of criminal intention and the evil mind, i.e., concept of mens rea, destruction, deletion, alteration or diminishing in value or utility of data are all the major ingredients to bring any act under this Section.

To summarise, what was civil liability with entitlement for compensations and damages in Section 43, has been referred to here, if committed with criminal intent, making it a criminal liability attracting imprisonment and fine or both.

Cases

Threat Mail to BSE and NSE[19]

In May 5, 2009, the Mumbai police have registered a case of 'cyber terrorism'—the first in the state since an amendment to the Information Technology Act—where threats email was sent to the BSE and NSE on May 4, 2009. The MRA Marg police and the Cyber Crime Investigation Cell are jointly probing the case. The suspect has been detained in this case. The police said an email challenging the security agencies to prevent a terror attack was sent by one Shahab Md with an ID sh.itaiyeb125@yahoo.in to BSE's administrative email ID corp.relations@bseindia.com at around 10.44 am 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 IT Act, 2000.

Section 67 *: 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 two three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

This section deals with publishing or transmitting obscene material in electronic form. The earlier Section in ITA, 2000 was later widened as per ITAA, 2008 in which child pornography and retention of records by intermediaries were all included.

Publishing or transmitting obscene material in electronic form is dealt with here. Whoever publishes or transmits 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 to read the matter contained in it, shall be punished with first conviction for a term upto three years and fine of five lakh rupees and in second conviction for a term of five years and fine of ten lakh rupees or both.

This Section is of historical importance since the landmark judgement in what is considered to be the first ever conviction under I.T. Act, 2000 in India, was obtained in this Section in the famous case *State of Tamil Nadu* vs.*Suhas Katti*[20] on 5 November, 2004. The strength of the Section and the reliability of electronic evidences were proved by the prosecution and conviction was brought about in this case, involving sending obscene message in the name of a married women amounting to cyber stalking, email spoofing and the criminal activity stated in this Section.

Case Laws

1. *The State of Tamil Nadu vs. Suhas Katti*[21]

   Facts : This case is about posting obscene, defamatory and annoying message about a divorcee woman in the Yahoo message group. E-mails were forwarded to the

victim for information by the accused through a false e-mail account opened by him in the name of the victim. These postings resulted in annoying phone calls to the lady. Based on the complaint police nabbed the accused. He was a known family friend of the victim and was interested in marrying her. She married to another person, but that marriage ended in divorce and the accused started contacting her once again. And her reluctance to marry him he started harassing her through internet.

Held : The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act, 2000 and the accused is convicted and is sentenced for the offence to undergo Rigorous Imprisonment for 2 years under section 469 IPC and to pay fine of Rs.500/-and for the offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo Rigorous Imprisonment for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently.'

The accused paid fine amount and he was lodged at Central Prison, Chennai. This is considered the first case convicted under section 67 of Information Technology Act 2000 in India.

In a recent case, a groom's family received numerous emails containing defamatory information about the prospective bride. Fortunately, they did not believe the emails and chose to take the matter to the police. The sender of the emails turned out to be the girl's step-father, who did not want the girl to get married, as he would have lost control over her property, of which he was the legal guardian.

2. *Avnish Bajaj vs. State*[22]

This is famously known as Avnish Bajaj (CEO of bazzee.com – now a part of the eBay group of companies) case.

Facts : There were three accused first is the Delhi school

boy and IIT Kharagpur Ravi Raj and the service provider Avnish Bajaj.

The law on the subject is very clear. The sections slapped on the three accused were Section 292 (sale, distribution, public exhibition, etc., of an obscene object) and Section 294 (obscene acts, songs, etc., in a public place) of the Indian Penal Code (IPC), and Section 67 (publishing information which is obscene in electronic form) of the Information Technology Act, 2000. In addition, the schoolboy faced a charge under Section 201 of the IPC (destruction of evidence), for there is apprehension that he had destroyed the mobile phone that he used in the episode. These offences invite a stiff penalty, namely, imprisonment ranging from two to five years, in the case of a first time conviction, and/or fines.

Held : In this case the Service provider Avnish Bajaj was later acquitted and the Delhi school boy was granted bail by Juvenile Justice Board and was taken into police charge and detained into Observation Home for two days.

3. *Daskhina Kannada police solved the first case of cyber crime in the district*

Dakshina Kannada Police solved a case where a Father at a Christian institution in the city had approached the Superintendent of Police with a complaint that he was getting offensive and obscene e-mails.

Police said that all the three admitted that they had done this to tarnish the image of the Father. As the three tendered an unconditional apology to the Father and gave a written undertaking that they would not repeat such act in future, the complainant withdrew his complaint. Following this, the police dropped the charges against the culprit.

The release said that sending of offensive and obscene e-mails is an offence under the Indian Information Technology Act 2000.

Section 67-A *Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form:*

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct 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 ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Exception: This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

- *the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art, or learning or other objects of general concern; or*
- *which is kept or used bona fide for religious purposes.*

It deals with publishing or transmitting of material containing sexually explicit act in electronic form. Contents of Section 67 when combined with the material containing sexually explicit material attract penalty under this Section.

Section 67B *: Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form:*

Whoever,-

(a) Publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or

(b) Creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or

distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or

(c) Cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or

(d) Facilitates abusing children online or

(e) Records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bonafide heritage or religious purposes

Explanation: For the purposes of this section, "children" means a person who has not completed the age of 18 years.

Child Pornography has been exclusively dealt with under Section 67B. Depicting children engaged in sexually explicit act, creating text or digital images or advertising or promoting such material depicting children in obscene or indecent manner etc or facilitating abusing children online

or inducing children to online relationship with one or more children etc come under this Section.

'Children' means persons who have not completed 18 years of age, for the purpose of this Section. Punishment for the first conviction is imprisonment for a maximum of five years and fine of ten lakh rupees and in the event of subsequent conviction with imprisonment of seven years and fine of ten lakh rupees.

Bonafide heritage material being printed or distributed for the purpose of education or literature etc. are specifically excluded from the coverage of this Section, to ensure that printing and distribution of ancient epics or heritage material or pure academic books on education and medicine are not unduly affected.

Screening video graphs and photographs of illegal activities through Internet all come under this category, making pornographic video or MMS clippings or distributing such clippings through mobile or other forms of communication through the Internet fall under this category.

Section 67C fixes the responsibility to intermediaries that they shall preserve and retain such information as may be specified for such duration and in such manner as the Central Government may prescribe. Non-compliance is an offence with imprisonment up to three years or fine.

` **Case Laws**

Janhit Manch & Ors. vs. The Union of India[23]

In this case it was Public Interest Litigation to ban child pornography. 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.

Transmission of electronic message and communication:

Section 69: Powers to issue directions for interception or

monitoring or decryption of any information through any computer resource:

(1) Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.

(2) The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub section (1), extend all facilities and technical assistance to –

(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

(b) intercept or monitor or decrypt the information, as the case may be; or

(c) provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

[Section 69B] Power to authorize to monitor and collect

traffic data or information through any computer resource for Cyber Security:

(1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of subsection

(2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Explanation: For the purposes of this section,

(i) "Computer Contaminant" shall have the meaning assigned to it in section 43

(ii) "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

Critique: Though we recognize how important it is for a government to protect its citizens against cyber-terrorism, we are concerned at the friction between these provisions

and the guarantees of free dialog, debate, and free speech that are Fundamental Rights under the Constitution of India.

Specifically:

(a) There is no clear provision of a link between an intermediary and the information or resource that is to be monitored.

(b) The penalties laid out in the clause are believed to be too harsh, and when read in conjunction with provision 66, there is no distinction between minor offenses and serious offenses.

(c) The ITA is too broad in its categorization of acts of cyber terrorism by including information that is likely to cause: injury to decency, injury to morality, injury in relation to contempt of court, and injury in relation to defamation.

This is an interesting section in the sense that it empowers the Government or agencies as stipulated in the Section, to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource, subject to compliance of procedure as laid down here.

This power can be exercised if the Central Government or the State Government, as the case may be, is satisfied that it is necessary or expedient in the interest of sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence. In any such case too, the necessary procedure as may be prescribed, is to be followed and the reasons for taking such action are to be recorded in writing, by order, directing any agency of the appropriate Government. The subscriber or intermediary shall extend all facilities and technical assistance when called upon to do so.

Cases

Posting Insulting Images of Chhatrapati Shivaji:

In August 2007, Lakshmana Kailash K., 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 evidently due to the fact that while requesting 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 lakh 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.

Section 69A *: Power to issue directions for blocking for public access of any information through any computer resource*

(1) Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.

(3) The intermediary who fails to comply with the direction

issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

The section as inserted in the ITAA, vests with the Central Government or any of its officers with the powers to issue directions for blocking for public access of any information through any computer resource, under the same circumstances as mentioned above.

Section 69B discusses the power to authorise to monitor and collect traffic data or information through any computer resource.

Commentary on the powers to intercept, monitor and block websites

In short, under the conditions laid down in the Section, power to intercept, monitor or decrypt does exist. It would be interesting to trace the history of telephone tapping in India and the legislative provisions (or the lack of it) in our nation and compare it with the powers mentioned here. Until the passage of this Section in the ITAA, phone tapping was governed by Clause 5(2) of the Indian Telegraph Act of 1885, which said that "On the occurrence of any public emergency, or in the interest of the public safety, the Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order". Other sections of the act mention that the government should formulate "precautions to be taken for preventing the improper interception or disclosure of messages". There have been many attempts, rather many requests, to formulate rules to

govern the operation of Clause 5(2). But ever since 1885, no government has formulated any such precautions, maybe for obvious reasons to retain the spying powers for almost a century.

A writ petition was filed in the Supreme Court in 1991 by the People's Union for Civil Liberties, challenging the constitutional validity of this Clause 5(2). The petition argued that it infringed the constitutional right to freedom of speech and expression and to life and personal liberty.

In December 1996, the Supreme Court delivered its judgment, pointing out that "unless a public emergency has occurred or the interest of public safety demands, the authorities have no jurisdiction to exercise the powers" given to them under Clause 5(2). They went on to define them thus: a public emergency was the "prevailing of a sudden condition or state of affairs affecting the people at large calling for immediate action", and public safety "means the state or condition of freedom from danger or risk for the people at large". Without those two, however "necessary or expedient", it could not do so. Procedures for keeping such records and the layer of authorities etc were also stipulated.

Now, this **Section 69 of ITAA is far more intrusive** and more powerful than the above-cited provision of Indian Telegraph Act 1885. Under this ITAA Section, the nominated Government official will be able to listen in to all phone calls, read the SMSs and emails, and monitor the websites that one visited, subject to adherence to the prescribed procedures and without a warrant from a magistrate's order. In view of the foregoing, this Section was criticised to be draconian vesting the government with much more powers than required.

Having said this, we should not be oblivious to the fact that this power (of intercepting, monitoring and blocking) is something which the Government represented by the **Indian Computer Emergency Response Team**, (the National Nodal Agency, as nominated in Section 70B of ITAA) has very rarely exercised. Perhaps believing in the freedom

of expression and having confidence in the self-regulative nature of the industry, the CERT-In has stated that these powers are very sparingly (and almost never) used by it.

Critical Information Infrastructure and Protected System have been discussed in Section 70.

The Indian Computer Emergency Response Team (CERT-In) coming under the Ministry of

Information and Technology, Government of India, has been designated as the National Nodal Agency for incident response. By virtue of this, CERT-In will perform activities like collection, analysis and dissemination of information on cyber incidents, forecasts and alerts of cyber security incidents, emergency measures for handling cyber security incidents etc.

The role of CERT-In in e-publishing security vulnerabilities and security alerts is remarkable.

The then Minister of State for Communications and IT Mr.Sachin Pilot said in a written reply to the Rajya Sabha said that (as reported in the Press), CERT-In has handled over 13,000 such incidents in 2011 compared to 8,266 incidents in 2009. CERT-In has observed that there is significant increase in the number of cyber security incidents in the country. A total of 8,266, 10,315 and 13,301 security incidents were reported to and handled by CERT-In during 2009, 2010 and 2011, respectively, "

These security incidents include website intrusions, phishing, network probing, spread of malicious code like virus, worms and spam, he added. Hence the role of CERT-In is very crucial and there are much expectations from CERT In not just in giving out the alerts but in combating cyber crime, use the weapon of monitoring the web-traffic, intercepting and blocking the site, whenever so required and with due process of law.

Penalty for breach of confidentiality and privacy is discussed in Section 72 with the punishment being imprisonment for a term upto two years or a fine of one lakh rupees or both.

***Section 71**: Penalty for misrepresentation*

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or which fine which may extend to one lakh rupees, or with both.

Penalties:

Punishment : imprisonment which may extend to two years

Fine : may extend to one lakh rupees or with both.

***Section 72** : Penalty for breach of confidentiality and privacy*

Save as otherwise provide in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulation made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Explanation: This section relates to any to any person who in pursuance of any of the powers conferred by the Act or it allied rules and regulations has secured access to any: Electronic record, books, register, correspondence, information, document, or other material.

If such person discloses such information, he will be punished with punished. It would not apply to disclosure of personal information of a person by a website, by his email service provider.

Penalties :

Punishment : term which may extend to two years.

Fine: one lakh rupees or with both.

Section 72A *: Punishment for Disclosure of information in breach of lawful contract*

Any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

Section 73 *: Penalty for publishing electronic Signature Certificate false in certain particulars:*

No person shall publish an Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that

- *the Certifying Authority listed in the certificate has not issued it; or*
- *the subscriber listed in the certificate has not accepted it; or*
- *the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation*

Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Explanation : The Certifying Authority listed in the certificate has not issued it or,

The subscriber listed in the certificate has not accepted it or the certificate has been revoked or suspended.

The Certifying authority may also suspend the Digital Signature Certificate if it is of the opinion that the digital signature certificate should be suspended in public interest.

A digital signature may not be revoked unless the subscriber has been given opportunity of being heard in the matter. On revocation the Certifying Authority need to communicate the same with the subscriber. Such publication is not an offence it is the purpose of verifying a digital signature created prior to such suspension or revocation.

Penalties:

Punishment: imprisonment of a term of which may extend to two years.

Fine: fine may extend to 1 lakh rupees or with both

Case Laws

Bennett Coleman & Co. v/s Union of India[24]

In this case the publication has been stated that ?publication means dissemination and circulation. In the context of digital medium, the term publication includes and transmission of information or data in electronic form.

Section 74 – *Publication for fraudulent purpose:*

Whoever knowingly creates, publishes or otherwise makes available a Electronic Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 75 *– Act to apply for offence or contraventions committed outside India*

Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

4.2 Common Cyber Crimes and Applicable Legal Provisions : A Snapshot

S.No.	*Cyber Crime*	*Applicable Provisions*
1.	*Harassment via fake public profile on social networking site* :A fake profile of a person is created on a social networking site with the correct address, residential information or contact details but he/she is labeled as 'prostitute' or a person of 'loose character'. This leads to harassment of the victim	*Sections 66A, 67 of IT* Act and Section 509 of the Indian Penal Code.
2.	*Online Hate Community* : Online hate community is created inciting a religious group to act orpass objectionable remarks against a country, national figures etc.	Section 66A of IT Act and 153A & 153B of the Indian Penal Code.
3.	*Email Account Hacking :* If victim's email account is hacked and obscene emails are sent to people in victim's address book	Sections 43, 66, 66A, 66C, 67, 67A and 67B of Information Technology Act.
4.	*Credit Card Fraud* : Unsuspecting victims would use infected computers to make online transactions.	Sections 43, 66, 66C, 66D of IT Act and section 420 of the Indian Penal Code.
5.	*Web Defacement* : The homepage of a website is replaced with a pornographic or defamatory page. Government sites generally face the wrath of hackers on symbolic days	Sections 43 and 66 of IT Act and Sections 66F, 67 and 70 of IT Act also apply in some cases.
6.	*Introducing Viruses, Worms, Backdoors, Rootkits, Trojans, Bugs* : All of the above are some sort of	Sections 43, 66, 66A of IT Act and Section 426 of Indian Penal Code.

S.No.	Cyber Crime	Applicable Provisions
	malicious programs which are used to destroy or gain access to some electronic information	
7.	*Cyber Terrorism* : Many terrorists are use virtual (G-Drive, FTP sites) and physical stoarage media (USB's) hard drives) for hiding information and records of their illicit business.	Conventional terrorism laws may apply along with Section 69 of IT Act.
8.	*Online sale of illegal Articles :* Where sale of narcotics, drugs weapons and wildlife is facilitated by the Internet	Generally conventional laws apply in these cases.
9.	*Cyber P ornography :* Among the largest businesses on Internet. Pornography may not be illegal in many countries, but child pornography is prohibited at large.	Sections 67, 67A and 67B of the IT Act.
10.	*Phishing and Email Scams :* Phishing involves fraudulently acquiring sensitive information through masquerading a site as a trusted entity. (E.g. Passwords, credit card information)	Section 66, 66A and 66D of IT Act and Section 420 of IPC
11.	*Theft of Confidential Information* : Many business organizations store their confidential information in computer systems. This information is targeted by rivals, criminals and disgruntled employees.	Sections 43, 66, 66B of IT Act and Section 426 of Indian Penal Code.
12.	*Source Code Theft* : A Source code generally is the most coveted and important "crown jewel" asset of a company.	Sections 43, 66, 66B of IT Act and Section 63 of Copyright Act.

S.No.	*Cyber Crime*	*Applicable Provisions*
13.	*Tax Evasion and Money Laundering :* Money launderers and people doing illegal business activities hide their information in virtual as well as physical activities.	Income Tax Act and Prevention of Money Laundering Act. IT Act may apply case-wise.
14.	*Online Share Trading Fraud :* It has become mandatory for investors to have their demat accounts linked with their online banking accounts which are generally accessed unauthorized, thereby leading to share trading frauds.	Sections 43, 66, 66C, 66D of IT Act and Section 420 of Indian Penal Code.

4.3 Civil Liabilities under Information Technology Act, 2000

The concept of accrued liability applies only to substantive laws and not to procedural laws as no one can claim a vested right in the procedure. In India we have both substantive and procedural laws. The Indian Penal Code and Information Technology Act are substantive laws whereas the Indian Evidence Act, Criminal Procedure Code and Civil procedure Code are procedural laws. Thus, by a retrospective law the procedure can be amended, changed or even repealed. Similarly, the protection of Article 20(1) is available for and can be seeked against criminal matters only and it does not extend to civil matters'. Thus, a civil liability can be enhanced with retrospective effect.

Data Protection

According to the Section: 43-whoever destroys, deletes, alters and disrupts or causes disruption of any computer with the intention of damaging of the whole data of the computer system without the permission of the owner of the computer, shall be liable to pay fine up to 1crore to the person so affected by way of remedy.

Section 43A *which is inserted by 'Information Technology (Amendment) Act, 2008 states that where a body corporate*

is maintaining and protecting the data of the persons as provided by the central government, if there is any negligent act or failure in protecting the data/ information then a body corporate shall be liable to pay compensation to person so affected. And Section 66 deals with 'hacking with computer system' and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both.

Section 43A of IT Act deals with the aspect of compensation for failure to protect data. The Central Government has not prescribed the term 'sensitive personal data,' nor has it prescribed a standard and reasonable security practice. Until these prescriptions are made, data is afforded security and protection only as may be specified in an agreement between the parties or as may be specified in any law. However, Explanation (ii) to Section 43A is worded in such a way that there is lack of clarity whether it would be possible for banks, (or anybody corporate) to enter into agreement which stipulate standards lesser than those prescribed by Central Government and in the event of the contradiction (between the standards prescribed by the Central Government and those in the agreement) which would prevail. Whether a negligence or mala fide on the part of the customer would make the financial institution liable for no fault of it or whether by affording too much protection to banks, a customer is made to suffer are the two extremes of the situation. The need is for striking a balance between consumer protection and protection of the banks from liability due to no fault of theirs. Apart from affording protection to personal data (sensitive personal data- 43A), the IT Act, 2000 also prescribes civil and criminal liabilities (Section 43 and Section 66 respectively) to any person who without the permission of the owner or any other person who is in charge of a computer, computer system etc., inter alia, downloads, copies or extracts any data or damages or causes to be damaged any computer data base etc. In this context Section 72 and 72A of the amended IT Act, 2000 are also of relevance. Section 72 of the Act prescribes the punishment if any person who, in pursuance of the powers conferred under the IT Act, 2000, has secured access to any

electronic record, information etc. and without the consent of the person concerned discloses such information to any other person then he shall be punished with imprisonment up to two years or with fine up to one lakh or with both. Section 72A on the other hand provides the punishment for disclosure by any person, including an intermediary, in breach of lawful contract. The purview of Section 72A is wider than section 72 and extends to disclosure of personal information of a person (without consent) while providing services under a lawful contract and not merely disclosure of information obtained by virtue of powers granted under IT Act, 2000.

Critical Analysis: Comparative Jurisdiction

However, the attempt is such a limited one, and so replete with shortcomings that the need for a proper data protection law still stands. Given the proposed initiation of the UID scheme, in particular, there is a compelling need for a robust and intelligent law in this regard. Most other countries regimes clearly do at least the following:

- Define and classify types of data (for example, in most European countries, personal data is any data that identifies an individual, sensitive personal data is data that reveals details of ethnicity, religion, health, sexuality, political opinion, etc.),
- Fine-tune the nature of protection to the categories of data (i.e., greater standards of care around sensitive personal data),
- Apply equally to data stored offline and manually as to data stored on computer systems,
- Distinguish between a data controller (i.e., one who takes decisions as to data) and a data processor (i.e., one who processes data on the instructions of the data controller),
- Impose clear restrictions on the manner of data collection (for example, must be obtained fairly and lawfully),
- Give clear guidelines on the purposes for which that data can be put to and by whom (often involving a consent requirement that gives the individual a great degree of control over their data),

- Require certain standards and technical measures around the collection, storage, access to, protection, retention and destruction of data,
- Ensure that the use of data is adequate, relevant and not excessive given the purpose for which it was gathered,
- Cater for opt-in and opt-out type regimes, again to provide individuals with a measure of control over the use of their data even after the stage of initial collection (which has a huge impact on invasive telemarketing or unsolicited written communication),
- Impose a knowledge requirement and procedures for allowing individuals to seek information on what data is held on them, and
- Create safeguards and penalties that are well tailored to breaches of any of the above.

Unfortunately, and perhaps understandably, the ITA barely begins to scratch the surface of what a good data protection regime entails. The provisions that it does introduce (sections 43-A and 72-A) have glaring inadequacies which are as follows:

- The term sensitive personal data or information is used indiscriminately without any definition,
- The provisions only cover electronic data and records, not data stored in non-electronic systems or media,
- They offer no guidance on most of the principles set out above such as in relation to accuracy, adequacy, consent, purpose, etc.,
- In the absence of the controller-processor distinction, liability is imposed on persons, who are not necessarily in a position to control data, even if it is in their possession,
- Civil liability for data breaches only arises where negligence is involved (i.e., failure to have security procedures or failure to implement them correctly will not automatically result in damages unless negligence is proven),

- Similarly, criminal liability only applies to cases of information obtained in the context of a service contract, and requires an element of willfulness, or a disclosure without consent or in breach of a lawful contract – this is a very limited remit aimed largely at preventing disgruntled or unscrupulous employees from dealing in company/customer data.

In addition to the criticisms levelled at the data protection provisions, the other large subset of concerns has been in relation to the civil liberties implications of the ITA. There has been some horror expressed in various forums and media about the ITA contributing to the growth of a police state, to severe curtailment of the freedom of speech and expression, to the invasion of privacy, and to the disproportionate severity of penalization for offences that are placed on crimes committed in cyberspace compared to crimes committed in the here and now. Sadly, this is true to a large extent given the clunky treatment of cyber terrorism, the intolerable pre-censorship that is enabled by the blocking of websites, the broad approach to the monitoring and collection of data, and the demanding obligations of intermediaries to cooperate with interception, monitoring and decryption of data for poorly defined reasons.

While our Constitution's fundamental rights chapter, which enshrines certain basic, democratic, and profound rights, might not have the same vocabulary of due process as we see in the US, it nevertheless requires restrictions to be reasonable. Precedents and the wider jurisprudence in the field have further developed the concepts of checks and balances, procedural safeguards and legitimacy of restraints that a functioning democracy like India must accord to its people. It can be argued that several provisions of the ITA cause significant tension with the right to freedom of speech and expression, the right against self-incrimination, the right to equality before the law, and the right to practice a trade or profession.

Privacy and surveillance

This topic pulls together concerns around the blanket

monitoring and collecting of traffic data or information, the interception and decryption (under duress) by intermediaries (now a large superset of ISPs, search engines, cyber cafes, online auction sites, online market places, etc.) and the wide definition of cyber terrorism (which ludicrously even casts defamation as a terrorist activity).

Some of the broad concerns in relation to interception, monitoring and decryption in (section 69) are that:

- There is no provision for a clear nexus between an intermediary and the information or resource sought to be monitored or intercepted,
- The usual internationally recognised exception to liability where an intermediary operates purely as a conduit and has no control over data flowing through its network is not clearly spelt out,
- The penalties for non-cooperation are extremely harsh, especially given the absence of a) and b) above,
- These onerous penalties can be said to be in violation of Article 14 as they seem entirely disproportionate. Similar offences and remedies in the Code of Criminal Procedure or the Indian Penal Code prescribe less severe penalties, by an order of magnitude in fact. When the only difference between the offences is the medium in which information is contained, it seems arbitrary to impose a much harsher punishment on an online intermediary than on a member of the public who, for example, furnishes false information to the police in connection with a trial or enquiry,
- The rules made in relation to monitoring, interception and decryption, offer some procedural safeguards, in that they impose a time limit on how long a directive for interception or monitoring can remain in force, a ceiling on how long data can be kept before it is required to be destroyed, etc. However, the effect of these is greatly diluted by exceptions for functional requirements, etc. The astonishing irony is that rule 20 requires the intermediary to maintain 'extreme secrecy', 'utmost care

and precaution' in the matter of interception, monitoring or decryption of information as it affects the privacy of citizens.

In a similar vein, there are concerns around the monitoring and collection of traffic data (Section 69B) as the section contains an unreasonably long list of grounds for monitoring. These include such extreme excesses as forecasting of imminent cyber incidents, monitoring network application with traffic data or information on computer resource, identification and determination of viruses/ computer contaminant, and the catch-all any other matter relating to cyber security.

Finally, the main criticism of the ITA approach to cyber terrorism is the very wide net that it seeks to cast, looking for a game that has little or nothing to do with the named offence. Amongst the cast of creatures unwittingly caught during this fishing expedition, we find some unlikely victims. In addition to the usual grounds of offence against sovereignty, national security, defence of India, etc., which we have seen in relation to other sections, the ITA considers the following as acts of cyber terrorism broadly speaking, unauthorized access to information that is likely to cause:

- Injury to decency,
- Injury to morality,
- Injury in relation to contempt of court, and
- Injury in relation to defamation.

This would almost be laughable if these grounds were not enacted into law, posing a threat to civil liberties by their very existence. Other countries have some notion of political ideology, religious case, etc. in their view of terrorism. Indian Law on Information and Communication Technology has been shoehorned into a clause that imposes the stiffest penalty within the entire ITA (life imprisonment) gives even more cause for concern.

4.4 Civil Liability for Corporate:

As mentioned above, anybody corporate who fails to

observe data protection norms may be liable to pay compensation if:

- It is negligent in implementing and maintaining reasonable security practices, and thereby
- Causes wrongful loss or wrongful gain to any person;

Claims for compensation are to be made to the adjudicating officer appointed under section 46 of the IT Act.

4.5 Cyber Crimes under IPC and Special Laws

4.5.1 The Indian Penal Code, 1860

Normally referred to as the IPC, this is a very powerful legislation and probably the most widely used in criminal jurisprudence, serving as the main criminal code of India. Enacted originally in 1860 and amended many a times since, it covers almost all substantive aspects of criminal law and is supplemented by other criminal provisions. In independent India, many special laws have been enacted with criminal and penal provisions which are often referred to and relied upon, as an additional legal provision in cases which refer to the relevant provisions of IPC as well.

The Indian Penal Code was amended by inserting the word 'electronic' thereby treating the electronic records and documents on a par with physical records and documents. The Sections dealing with false entry in a record or false document etc. (e.g. 192, 204, 463, 464, 464, 468 to 470, 471, 474, 476 etc.) have since been amended as 'electronic record and electronic document' thereby bringing within the ambit of IPC. Now, electronic record and electronic documents has been treated just like physical records and documents during commission of acts of forgery or falsification of physical records in a crime. After the above amendment, the investigating agencies file the cases/ charge-sheet quoting the relevant sections from IPC under section 463, 464, 468 and 469 read with the ITA/ITAA under Sections 43 and 66 in like offences to ensure the evidence and/or punishment can be covered and proved under either of these or under both legislation.

- Sending threatening messages by email - Sec 503 IPC
- Sending defamatory messages by email - Sec 499 IPC
- Forgery of electronic records - Sec 463 IPC
- Bogus websites, cyber frauds - Sec 420 IPC
- Email spoofing - Sec 463 IPC
- Web-Jacking - Sec. 383 IPC
- E-Mail Abuse - Sec.500 IPC

4.5.2 Cyber Crimes under the Special Acts

- Online sale of Drugs - Narcotic Drugs and Psychotropic Substances Act, 1985.
- Online sale of Arms – Arms Act, 1959.

***

Chapter 5

Cyber Crime : Landmark Judgements in India

1. ***Sanjay Kumar vs. State Of Haryana***[25]

Punjab-Haryana High Court (Section 65 and Section 66 of the IT Act, 2000)

Present criminal revision has been preferred by the petitioner against judgment dated 21.08.2012 passed by the learned Sessions Judge, Faridabad, whereby an appeal preferred by the petitioner has been dismissed and judgment of conviction dated 01.09.2011 and order of sentence dated 03.09.2011 passed by learned Judicial Magistrate First CRR No.66 of 2013 (O&M) 2 Class, Faridabad, has been upheld, vide which the petitioner has been convicted for offences punishable under Sections 420, 467, 468, 471 of the Indian Penal Code and Sections 65 and 66 of the Information & Technology Act, 2000 and sentenced to undergo rigorous imprisonment as follows:-

Under Section Period Fine 420 IPC Two years Rs.1,000/- 467 IPC Three years Rs.2,000/- 468 IPC Two years Rs.1,000/- 471 IPC Two years Rs.1,000/- 65 I.T. Act Two years Rs.1,000/- 66 I.T. Act Two years Rs.1000/- In default of payment of fine, the petitioner shall further undergo simple imprisonment for a period of two months. All the sentences were ordered to run concurrently.

Brief facts of the prosecution case are that the Senior Branch

Manager, Vijay Bank, NIT, Faridabad moved a complaint dated 11.02.2003 before the Police stating that the petitioner was deputed by M/s Virmati Software and

Telecommunication Ltd. to maintain the Software System supplied by them to the bank. He was also looking Software System of certain other banks. In connection with rendering such services, the petitioner was having access to their accounting system which was computerized and was also in a position to enter into ledgers and various other accounts. While reconciling the accounts, certain discrepancies were pointed out by the officials of the bank and in that process, it was revealed that the accused-petitioner, who was having SB Account No. 21499 in his CRR No.66 of 2013 (O&M) 3 personal name in their bank, manipulated the entries by forging and fabricating certain entries from one account to another, from the computer system by handling the software and got the entries pertaining to the amount of the the bank and withdrew the amounts from the bank on various dates by issuing cheques in his own favour and withdrew the amount from the cash counter of the bank as well as through transfer/clearing transactions. As per enquiry, it has been revealed that the accused by carrying out forgery, fabricating the entries in the computer system of the bank, illegally and wrongfully, withdrew Rs.17,67,409/- from the bank and thus, caused wrongful gain to himself and wrongful loss to the bank. The said Bank came to know regarding the fraud committed by the accused on 07.02.2003. thereafter, the accused was called to the bank and he was confronted with the details of the fraud but he gave evasive replies as only admitted having embezzled a sum of Rs. 17 lacs without giving further information or revealing the exact amount of fraud or the modus operandi of the same and also assured to pay back the amount to the bank.

Filing and Investigation

On receipt of the complaint, a case bearing FIR No. 165 dated 11.02.2003, under Sections 406, 420, 467, 468, 469, 471 of the Indian Penal Code and Sections 65, 66 and 72 of the Information and Technology Act, 2000 was registered against the petitioner. After completion of investigation, challan against the accused-petitioner was presented in the Court. Thereafter, charge was framed against the accused petitioner to which he pleaded not guilty and claimed trial.

The prosecution, in order to prove its case, examined PW1 A. CRR No.66 of 2013 (O&M)

Siridhar, PW2 Girish Kumar Verma, PW3 Maheshwar Rath, PW4 Ramesh Kumar Malik and PW5 Dalip Singh, DSP. Thereafter, statement of the accused was recorded under Section 313 Cr.P.C. All the incriminating circumstances were put to the accused. He denied the same and pleaded innocence.

The learned trial Court, after appreciation of the evidence, convicted and sentenced the petitioner as aforesaid vide judgment and order dated 01.09.2011 and 03.09.2011 respectively. Thereafter, the petitioner preferred an appeal, which was dismissed by the learned Sessions Judge, Faridabad vide judgment dated 21.08.2012. Hence, this criminal revision.

Learned counsel for the petitioner was heard and perused the record. Learned counsel for the petitioner contends that the petitioner has been falsely implicated in this case as the complainant and eye witness was inimical to the petitioner as they were having a dispute about 15/16 years prior to the occurrence. Learned counsel further contends that there is no direct evidence to connect the petitioner with the alleged offence in question, therefore, no *prima facie* case has been made out against the petitioner

The court considered the contentions of the learned counsel for the petitioner. From perusal of the judgments of both the Courts below, it transpires that the allegations against the petitioner are that the petitioner CRR No.66 of 2013 (O&M) 5 has manipulated the computerized Bank account, i.e., the interest entries and thereby cheated the complainant bank by forging electronic record in order to cause wrongful loss to the bank and wrongful gain to himself to the tune of Rs.17,67,409/-. It has come in the documentary evidence on record that the petitioner has forged the entries in the bank record and had thereby withdrawn a sum of Rs.17,67,409/-.

Courts' Observation

The learned Trial Court, after appreciating the evidence on record, observed as under:-

"1. All the prosecution witnesses have supported the prosecution case. The complainant PW-1 A. Siridhar and PW-2 Girraj Parshad Sharma have stated that the accused Sanjay Kumar Bhatia was the employee of M/s Virmati Software and Telecommunication Ltd. and have been appointed in their branch for the purpose of maintenance of Software System supplied by them to the bank. This fact stand corroborated by document Ex. P36 wherein in Team No. 7 the name of Sanjay has been mentioned along with his residence number and Pager number. Sanjay Kumar Bhatia has also opened an A/c No. 21499 in their bank as evident from the account opening form of the accused Sanjay Bhatia placed on record as Ex.P37 along with specimen signature Card Ex. P38 and the cheque book issued register Ex.P39. Further, from the bank statement of account no. 21499, Ex.P8, on 1.8.2001, Rs. 2,00,000/- was deposited by clearing and Rs. 1/- as interest. However, nothing is mentioned as to what is the basis of clearing. In this regard, PW-3 Maheshwar Rath stated that during his inquiry he could not find any supporting document or CRR No.66 of 2013 (O&M) 6 voucher. The accused has also not produced any evidence in this regard. Rather, Ex.PW1/D shows that even the amount of Rs.2,00,000/- has been transferred from interest account on 1.8.2001. This fact stand corroborated by the report Ex.P34 wherein it is mentioned that the accused has increased interest portion in his own account through first time creation to the extent of Rs.2,00,000/- and then applied interest along with other SB accounts and to mislead the Branch employees, the accused has splitted the transaction into 2 parts,one entry is shown as "by interest credit" as Rs.1.00 and the other by clearing as Rs.2,00,000/- and, therefore, the amount of Rs.2,00,000/- is reflected in account statement as `by clearing'.

2. Similarly, using the same modus operandi, accused forged the interest entries on 1.8.2002 and 2.8.2000 and got deposited Rs.3,00,000/- and Rs.4,20,000/- respectively in his account.

3. Further, the accused used the fixed deposit account of Sardar Jeet Singh. The account of Jeet Singh was opened on 8.3.2002 in which Rs.1,05,00,000/- was deposited on that day as evidence from Ex.P3. The statement of account of Sardar Jeet Singh Ex.P3 shows that an interest of Rs.8,46,489/- was deposited on 29.4.2002. However, the said interest calculated was an inflated one, calculated by forging entries to the effect as it the account of Jeet Singh was opened on a prior date. Thereafter, on 30.4.2002, accused transferred the amount of Rs.8,46,489/- to the account of Anil Kumar Sharma having A/c No. 22618 which had already been closed on 1.9.2001, as evident from Ex.P5, by forging the CRR No.66 of 2013 (O&M) 7 entries to the effect that it was changed in bank records form closed to o pen and on 8.5.2002, 13.5.2002 and 18.5.2002, accused transferred the amount of Rs.2,50,000/-, Rs. 2,50,000/- and Rs.3,47,409/- respectively from the account of Sh. Anil Kumar to his account as evident from Ex.P5 and Ex.P8 to Ex.P12. Further, PW-3 Sh. Maheshwar Rath has stated as also evident from his report Ex.P34 that the transaction rooted through the account of Jeet Singh and Anil Kumar has been deleted by accused using SRF files which were later recovered during Audit.

4. Moreover, Ex.P15 to Ex.P24 show that accused has withdrawn the said amount through cheques.

5. In this manner, the accused was dishonestly forged the bank records to cause wrongful loss to the bank and thereby cheated the concerned bank by depositing Rs.17,67,409/- in his account and thereafter withdrawing the same. Further, the accused has admitted his guilt vide letter Ex.P44. The signature of accused on the letter Ex.P44 are similar to the specimen signatures of accused on bank opening account card Ex.P38 as well as on the

bank opening Account form Ex.P37. Furthermore, from the bare perusal of the confessional statement Ex.P44, it clearly emanates that the manner in which the word `Sanjay' has been written is similar to the manner word `Sanjay' has been written by accused below his signatures by accused as he even returned in his statement under Section 313 Cr.P.C, 1973 Moreover, Ex.P47 and Ex.P48 show that accused has tendered Rs.3,50,000/- to the bank in respect of the amount fraudulently withdrawn by him which shows the CRR No.66 of 2013 (O&M) 8 admission of guilt as evident from Ex.P47 and Ex.P48.

6. On the other hand, the learned counsel for the accused during the course of arguments has argued that no specific password was allotted to Sanjay. However, no doubt password is given to an employee but it has surfaced in the testimonies of the prosecution witnesses that for the purpose of maintaining the software and in this manner had assess to all those files to which only the employee of the bank could have. Moreover, as the amount was deposited in the account of accused and he has withdrawn it, there is no force in said argument.
7. In this manner, the accused had cheated the bank and forged the electronic record to cause wrongful loss to bank and wrongful gain to himself. The prosecution has been able to prove beyond reasonable doubts, the ingredients of Sections 420, 467, 468 and 471 IPC.
8. Furthermore, clearly the accused has tampered with the computer source document and he has also altered in the information which resided in the computer resource and by doing so he committed the offences under Sections 65 and 66 of the Information & Technology Act, 2000. At the same time, it is pertinent to mention that although accused was having secured assess to electrical record of the bank and he forged the entries and cheated to cause wrongful gain to himself but there is no such breach of confidentiality by disclosing the information to any other person and as such he is acquitted of offence under Section 72 of the Information & Technology Act, 2000."

Conviction

The learned Trial Court was wholly justified in convicting the accused-petitioner and the learned Appellate court, as can be clearly seen, CRR No.66 of 2013 (O&M) 9 had not committed any error in upholding the conviction of the accused petitioner. Learned counsel for the petitioner failed to point out any misreading or non-reading of any evidence and could not point out any infirmity in the judgments of the Courts below. The findings of guilt, reached against the accused-petitioner does not, thus, suffer from any infirmity, legal or factual and does not therefore, warrant interference by this Court in exercise of this Court's revision jurisdiction.

In view of the above, there is no merit in the contentions raised by the learned counsel for the petitioner. Dismissed in limine.

2. Fatima Riswana vs. State Rep. by ACP, Chennai & Ors[26]

(In The High Court of Madras)

The appellant is a prosecution witness in S.C. No. 9 of 2004 wherein respondents 2 to 6 are the accused facing trail for offences punishable under Section 67 of Information Technology Act, 2000 r/w Section 6 of Indecent Representation of Women (prohibition) Act, 1986, Under Section 5 & 6 of Immoral Traffic (Prevention) Act, 1956, Under Section 27 of Arms Act, 1959 And Sections 120(B), 506(ii), 366, 306 & 376 I.P.C. The said trial relates to exploitation of certain men and women by one of the accused Dr. L. Prakash for the purpose of making pornographic photos and videos in various acts of sexual intercourse and thereafter selling them to foreign websites. The said session's trail came to be allotted to the foreign websites. The said Session's trial came to be allotted to the V Fast Track Court, Chennai which is presided over by a lay Judge. When the said trail before the V Fast Track Court was pending certain criminal revision petitions came to be filed by the accused against the orders made by the said court rejecting their applications for supply of copies of 74 Compact Discs (CDs) containing pornographic material on which the prosecution was relying. The said revision petitions

were rejected by the Madras High Court by its order dated 13th February, 2004 holding that giving all the copies of the concerned CDs might give room for copying such illegal material and illegal circulation of the same, however the court permitted the accused persons to peruse the CDs of their choice in the Chamber of the Judge in the presence of the accused, their advocates, the expert, the public prosecutor and the Investigating Office and also observed that the case be transferred to another court with competent jurisdiction presided by a male officer at the option of the sessions judge and taking the same the accused filed a revision petition for transferred to Fast track 4 court presided by the male officer and the Appellant alleged that she would be embarrassed if the trail is conducted by the male presiding officer and that the lady sessions judge didn't object or the trial of the case and the Appellant alleged that she would be embarrassed if the trial is conducted by the male presiding officer and that the Lady sessions judge didn't object to the trail of the case in the fast track 5 and the high court has erred in transferring the case and the Appellant was not given any opportunity of being heard before the alleged transfer. The learned counsel for the respondents contended that the Appellant learned though arrayed as witness is for all purpose an accused herself and law officer appearing in the case had expressed their embarrassment in conducting the trial before a lady Presiding Officer and even though the Presiding Officer did not expressly record her embarrassment, it was apparent that she too wanted the case to be transferred to another court, therefore, this Court should not interfere with the order of transfer. It was held that this appeal has to be allowed in the sessions case No. 9 of 2004 now transferred to the IV Fast Track Court Chennai be Transferred back to the V Fast Track Court, Chennai.

3. Avnish Bajaj vs. State (N.C.T.) of Delhi[27]

(In The High Court of Delhi)

Facts

Avnish Bajaj (Appellants), CEO of Baazee.com, an online

auction website, was arrested for distributing cyber pornography. The charges stemmed from the fact that someone had sold copies of a pornographic CD through the Baazee.com website.

The court granted him bail in the case. Factors considered by the court were:

1. There was no prima facie evidence that Mr. Bajaj directly or indirectly published the pornography,
2. The actual obscene recording/clip could not be viewed on Baazee.com,
3. Mr. Bajaj was of Indian origin and had family ties in India.

History of the case

Avnish Bajaj is the CEO of Baazee.com, a customer-to-customer website, which facilitates the online sale of property. Baazee.com receives commission from such sales and also generates revenue from advertisements carried on its web pages.

An obscene MMS clipping was listed for sale on Baazee.com on 27th November, 2004 in the name of "DPS Girl having fun". Some copies of the clipping were sold through Baazee.com and the seller received the money for the sale.

Avnish Bajaj was arrested under section 67 of the Information Technology Act, 2000 and his bail application was rejected by the trial court. He then approached the Delhi High Court for bail.

Issues raised by the Prosecution

1. The accused did not stop payment through banking channels after learning of the illegal nature of the transaction.
2. The item description "DPS Girl having fun" should have raised an alarm.

Issues raised by the Defence

1. Section 67 of the Information Technology Act relates to

publication of obscene material. It does not relate to transmission of such material.

2. On coming to learn of the illegal character of the sale, remedial steps were taken within 38 hours, since the intervening period was a weekend.

Findings of the court

1. It has not been established from the evidence that any publication took place by the accused, directly or indirectly.
2. The actual obscene recording/clip could not be viewed on the portal of Baazee.com.
3. The sale consideration was not routed through the accused.
4. *Prima facie* Baazee.com had endeavoured to plug the loophole.
5. The accused had actively participated in the investigations.
6. The nature of the alleged offence is such that the evidence has already crystallized and may even be tamper proof.
7. Even though the accused is a foreign citizen, he is of Indian origin with family roots in India.
8. The evidence that has been collected indicates only that the obscene material may have been unwittingly offered for sale on the website.
9. The evidence that has been collected indicates that the heinous nature of the alleged crime may be attributable to some other person.

Decision

1. The court granted bail to Mr. Bajaj subject to furnishing two sureties of Rs. 1 lakh each.
2. The court ordered Mr. Bajaj to surrender his passport and not to leave India without the permission of the Court.

3. The court also ordered Mr. Bajaj to participate and assist in the investigation.
4. *S. Sekar* vs. *The Principal General Manager (Telecom) (B.S.N.L.)*

(In The High Court of Madras)

Facts of the Case

The petitioner is an employee of the second respondent, B.S.N.L, working as a Telecom Technical Assistant (Switch). It so happened that while he was working in SIPCOT MBM Main Exchange, Keeranur, the B.S.N.L. higher officials suspected him and others for having committed offences in manipulating the computer system and thereby causing loss to B.S.N.L. The FIR in Crime No. 1 of 2004 was came to be registered on 06.01.2004 by the Police, Pudukottai, for the offences under Section 406, 420 and 468 I.P.C. and 43(g) of the Information Technology Act, 2000.

The main thrust of the grievance of the petitioner in this case is that when there is a special enactment namely, the Information Technology Act, 2000, which is in operation relating to the alleged misconduct attributed as against the petitioner, there is no question of invoking the penal sections under the Indian Penal Code, It is also his specific plausible argument that section 43(g) of the Information Technology Act, 2000, has been invoked without any basis. The Second respondent filed the computer which was adopted by the first respondent filed the computer which was adopted by the first respondent also, denying and refuting the allegations and the averments highlights that the FIR registered was proper and the Police is investigating into the matter properly.

The point for consideration is as to whether the FIR referred to supra, has to be declared null and void as prayed by the Writ petitioner?

Judgement

It was held that the Police to investigate thoroughly into the matter and add or delete the penal Sections under the

Information Technology Act, 2000, as well as IPC and ultimately, it is for the criminal court which would be seized of the matter to decide on that. The Section 43(g) of the Information Technology Act, 2000, invoked by the police and specified in the FIR is declared void. Accordingly, the Writ petition is ordered. No costs, connected M.P. are closed.

5. Syed Asifuddin and Ors. vs. The State of Andhra Pradesh And Another[29]

(In The High Court of Andhra Pradesh)

Facts

Tata Indicom employees were arrested for manipulation of the electronic 32-bit number (ESN) programmed into cell phones that were exclusively franchised to Reliance Infocomm.

The court held that such manipulation amounted to tampering with computer source code as envisaged by section 65 of the Information Technology Act, 2000.

Case

Reliance Infocomm launched a scheme under which a cell phone subscriber was given a digital handset worth Rs. 10,500/- as well as service bundle for 3 years with an initial payment of Rs. 3350/- and monthly outflow of Rs. 600/-. The subscriber was also provided a 1 year warranty and 3 year insurance on the handset.

The condition was that the handset was technologically locked so that it would only work with the Reliance Infocomm services. If the customer wanted to leave Reliance services, he would have to pay some charges including the true price of the handset. Since the handset was of a high quality, the market response to the scheme was phenomenal.

Unidentified persons contacted Reliance customers with an offer to change to a lower priced Tata Indicom scheme. As part of the deal, their phone would be technologically "unlocked" so that the exclusive Reliance handsets could be used for the Tata Indicom service.

Reliance officials came to know about this "unlocking" by Tata employees and lodged a First Information Report (FIR) under various provisions of the Indian Penal Code, Information Technology Act and the Copyright Act.

The police then raided some offices of Tata Indicom in Andhra Pradesh and arrested a few Tata Tele Services Limited officials for re¬programming the Reliance handsets.

These arrested persons approached the High Court requesting the court to quash the FIR on the grounds that their acts did not violate the said legal provisions.

Issues raised by the Defense in the case

1. It is always open for the subscriber to change from one service provider to the other service provider.
2. The subscriber who wants to change from Tata Indicom always takes his handset, to other service providers to get service connected and to give up Tata services.
3. The handsets brought to Tata by Reliance subscribers are capable of accommodating two separate lines and can be activated on principal assignment mobile (NAM 1 or NAM 2). The mere activation of NAM 1 or NAM 2 by Tata in relation to a handset brought to it by a Reliance subscriber does not amount to any crime.
4. A telephone handset is neither a computer nor a computer system containing a computer programmer.
5. There is no law in force which requires the maintenance of "computer source code". Hence section 65 of the Information Technology Act does not apply.

Courts Observation

1. As per section 2 of the Information Technology Act, any electronic, magnetic or optical device used for storage of information received through satellite, microwave or other communication media and the devices which are programmable and capable of retrieving any information by manipulations of electronic, magnetic or optical impulses is a computer which can be used as computer system in a computer network.

2. The instructions or programmed given to computer in a language known to the computer are not seen by the users of the computer/consumers of computer functions. This is known as source code in computer parlance.
3. A city can be divided into several cells. A person using a phone in one cell will be plugged to the central transmitter of the telecom provider. This central transmitter will receive the signals and then divert them to the relevant phones.
4. When the person moves from one cell to another cell in the same city, the system, i.e., Mobile Telephone Switching Office (MTSO) automatically transfers signals from tower to tower.
5. All cell phone service providers have special codes dedicated to them and these are intended to identify the phone, the phone's owner and the service provider.
6. System Identification Code (SID) is a unique 5-digit number that is assigned to each carrier by the licensor. Every cell phone operator is required to obtain SID from the Government of India. SID is programmed into a phone when one purchases a service plan and has the phone activated.
7. Electronic Serial Number (ESN) is a unique 32-bit number programmed into the phone when it is manufactured by the instrument manufacturer. ESN is a permanent part of the phone.
8. Mobile Identification Number (MIN) is a 10-digit number derived from cell phone number given to a subscriber. MIN is programmed into a phone when one purchases a service plan.
9. When the cell phone is switched on, it listens for a SID on the control channel, which is a special frequency used by the phone and base station to talk to one another about things like call set-up and channel changing.
10. If the phone cannot find any control channels to listen to, the cell phone displays "no service" message as it is out of range.

11. When cell phone receives SID, it compares it to the SID programmed into the phone and if these code numbers match, cell knows that it is communicating with its home system. Along with the SID, the phone also transmits registration request and MTSO which keeps track of the phone's location in a database, knows which cell phone you are using and gives a ring.
12. So as to match with the system of the cell phone provider, every cell phone contains a circuit board, which is the brain of the phone. It is a combination of several computer chips programmed to convert analog to digital and digital to analog conversion and translation of the outgoing audio signals and incoming signals.
13. This is a micro processor similar to the one generally used in the compact disk of a desktop computer. Without the circuit board, cell phone instrument cannot function.
14. When a Reliance customer opts for its services, the MIN and SID are programmed into the handset. If someone manipulates and alters ESN, handsets which are exclusively used by them become usable by other service providers like TATA Indicom.

Decision

1. A cell phone is a computer as envisaged under the Information Technology Act.
2. ESN and SID come within the definition of "computer source code" under section 65 of the Information Technology Act.
3. When ESN is altered, the offence under Section 65 of Information Technology Act is attracted because every service provider has to maintain its own SID code and also give a customer specific number to each instrument used to avail the services provided.
4. Whether a cell phone operator is maintaining computer source code, is a matter of evidence.
5. In Section 65 of Information Technology Act, 2000 the

disjunctive word "or" is used in between the two phrases-

a. "when the computer source code is required to be kept"

b. "maintained by law for the time being in force"

6. *D'zine Garage Pvt. Ltd. rep. by its Director Mr. Hari Sethuraman vs. D'zine Café FZE & D'zine Café FZE vs. D'zine Garage Pvt. Ltd. rep. by its Director Mr. Hari Sethuraman*[30]

(In The High Court of Madras)

Facts of the Case

Plaintiff registered proprietor of the service mark 'D'zine filed suit for permanent injection against Applicant-Defendant who was using the mark 'D'zine' café as a service mark and as part of their corporate name and domain name 'www.Dzinecafe.com'- Respondent/Plaintiff contended that the Applicant- Defendant has deliberately adopted a similar service mark/trade name D'zine café in a calculated attempt to cash in on the reputation and goodwill enjoyed by the Respondent/Plaintiff and to get illicit and quick gains without putting any substantial efforts. Interim injunction granted. Hence, application by Defendant to vacate interim injunction and to strike the pleadings and reject the plaint Applicant-Defendant contended that the Respondent-Plaintiff has no office in India and hence present Court has no jurisdiction to try the matter and therefore, the plaint was liable to be rejected. It was Held that to justify an Order of rejection of plaint, the Defendant would be required to show a very strong case in his favour and the power would be exercised sparingly and only in exception cases, since it would interface with the right of the party to proceed with the trial to get to it legitimate and according to the substantive merit of his case – Such a case has not been made out by the Defendant – it was held that application for rejection of plaint not maintainable.

Defendant sought vacation of interim injunction on the ground that the registration is for a logo only and that

'D'zine' was not a coined word, it is a corrupt from of design and is commonly used – Further contented that, D'zine' café were sufficiently different and not likely to mislead and many others are using it.

Judgement

Held, for granting interim injunction phonetic similarity cannot be ignored and prior user must be proved and dishonest intention must be there. In the instant case, there is phonetic similarity

Further, 'D'zine not a generic word, it cannot be said to carry distinctive reference to a particular trade, becoming publici jiris. As business of parties are almost same and the fact that one is 'Dzine' café and other is 'Dzine' garage, clientele is likely to be confused and they are the same – prior user established by Plaintiff – No specific denial of the charge that the Defendant is taking advantages of the plaintiff mark- Usage of the same word by others and others and that is a common word is no defence in an action for interim injunction – Interim injunction granted.

7. *Nirav Navinbhai Shah & ors.* vs. *State of Gujarat and Another*[31]

(In The High Court Of Gujarat)

Facts of the Case

The applicants, original accused in crime I.C.R. No. 54 of 2004 dated 26.02.2004 registered with sector 7 police station Gandhinagar for offences punishable under sections 381, 408, 415, 418, 420 read with sections 34 and 120B of the Indian Penal Code and section 66 and 72 of the Information Technology Act, 2000 (herein after referred to as 'the IT Act for short) have preferred this application under section 482 of the Code of Criminal Procedure 1973 (herein after referred to as 'the code' for short) for quashing of FIR I.C.R. No. 54 of 2004 dated 26.02.2004 registered with Sector No. 7 Police Station Gandhinagar and the resultant Criminal Case No. 54 of 2004 dated 26.02.2004 registered with sector No. 7 Police station Gandhinagar and the resultant Criminal case

No.3528 of 2004 pending before the judicial Magistrate First Class Gandhinagar, mainly on the grounds that the facts and allegation leading to lodging FIR show that the real dispute was a civil dispute and as the same has been amicably settled between the parties, no useful purpose would be served in continuing the criminal proceedings, rather continuation of same would be counterproductive to the interest of justice.

Judgment

The complaint also does not contain any essential ingredient for maintaining criminal proceeding for the alleged offences. As it is stated in the arguments of the learned counsels that the parties have filed civil suits also in respect of the same dispute. The entire dispute between the parties is resolved by amicable settlement. The alleged hacking is perpetrated on the Complainants computer system only which said to have data pertaining to its client. The Counsels have submitted that on same of the web sites these data are already available. The dispute appears to be private in nature. The offence alleged is not strictly affecting or infringing any other individual or citizen. Thus looking to the nature of the disputes, it can well be said that continuation of the same is not in interest of justice. It was held that the FIR 54 of 2004 registered at sector 7 Police Station Gandhinagar and resultant Criminal Case No. 3528 of 2004 pending before the JMFC Gandhinagar deserve to be quashed in the interest of just and hereby they are quashed. Rule is made absolute.

8. *SMC Pneumatics (India) Pvt. Ltd.* vs. *Jogesh Kwatra*[32]

(In The High Court of Delhi)

Facts : Cyber Defamation

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 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 employee could be indulging in the matter of sending abusive emails, the plaintiff terminated the services of the defendant.

Judgement

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.

9. *Nasscom* vs. *Ajay Sood & Others*

(In The High Court of Delhi)

Facts

In a landmark judgment in the case of National Association of Software and Service Companies vs Ajay Sood & Others, delivered in March, 2005, 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 pretend to represent online banks and siphon cash from e-banking accounts after conning consumers into handing over confidential banking details.

Judgement

The Delhi HC stated that even though there is no specific legislation in India to penalise 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 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 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 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 Rs. 1.6 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.

10. *State of Tamil Nadu* vs. *Suhas Kutti*[34]

Facts

Assistant Commissioner of Police, Cyber Crime Cell, C.C.B. Egmore, Chennai 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, 2000.

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 cited 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 Bangalore. At that time also, the 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.

Judgement

The 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.

11. *Google India Pvt. Ltd.* vs. *M/s.Visaka Industries Limited and another*

(In the High Court of Andhra Pradesh)

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 space in the form of articles for worldwide 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.

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.

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 thereunder 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,

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

(2) "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 much less 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.

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:

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 communication 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 theevidence 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.

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.

Accordingly, the Criminal Petition is dismissed.

12. *Microsoft Corporation* vs. *Yogesh Papat*[36]

(In the High Court of Delhi)

Facts

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.

Judgement

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 Rs. 1.98 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."

13. *Autodesk, Inc. & Another* vs. *Mr. Prashant Deshmukh & Others*[37]

(In the High Court of Delhi)

Facts

Autodesk, Inc. (hereinafter "Plaintiff 1") is a renowned U.S.-based design software and digital content company, providing design software to professionals, has several authorized resellers in India and also claims to be the owner of various trademarks in India, including AUTODESK and AutoCAD. Microsoft Corporation, (hereinafter "Plaintiff 2") owns software such as Microsoft Windows and Microsoft Office and is almost a household name regarding computer peripherals. It also has a subsidiary company in New Delhi. The plaintiffs claim that the software developed and marketed by them are computer programs as per Section 2(ffc) of the Copyright Act, 1957 and also covered as 'literary work' as per Section 2(o) of the Copyright Act. Moreover, the rights of authors of member countries of the Berne and Universal Copyright Conventions are protected under Indian Copyright laws since both India as well as U.S.A. are signatory to both these conventions. Based on information regarding large-scale use of unlicensed/pirated software by the defendants, plaintiffs have alleged infringement of their copyright and trademark rights by the defendants.

Issues raised in the case

Whether the defendants are guilty of having infringed the copyright and trademark right associated with the software that belong to the plaintiffs?

Remedies sought by plaintiffs

Injunction restraining the defendants from infringing the plaintiffs' copyright and registered trademarks, damages of Rs.20 lakhs and rendition of accounts and delivery up of the unlicensed/pirated software contained in hard disks, compact disks, floppies etc.

Decision

The defendants never tried to contest the suit by filing a

written statement. Evidence revealed that defendants 1 and 2 were not holding any license from Plaintiff 1, while defendant 3 (M/s Space Designers Syndicate) was a licensed user of AutoCAD LT 2005. Mr. Devesh J. Tiwari, the person who had informed the plaintiffs of the infringement, was an employee of M&S Consultancy Services (one of the defendants) as a computer service engineer. He revealed in the court that his employer company did not possess any legal licensed software and that his superiors were fully aware of the pirated software, including the Microsoft Windows 95/98 Operating System; Microsoft Office 97/2000 and Auto CAD Versions 12, 14 and 2000 etc. being used from printed CDs within the company. It was also contended on the plaintiff's behalf that the word Microsoft has been continuously and extensively used by Plaintiff 2 since long and has come to be identified and recognized exclusively with Plaintiff 2.

The person-in-charge of the IT Department of the Legal Representatives of the plaintiff companies also testified that mostly all licenses used by commercial entities regarding plaintiff's products can be used in perpetuity and that a software programme purchased by an entity anytime should reflect in the data base of the product purchase summary maintained by the plaintiff companies. Needless to say, the defendants' names were conspicuously absent from that data base.

With regard to applicability of the Act to work first published in any territory outside India such as U.S., the court referred to Section 40 of the Act and also to paragraphs 2 and 3 of the International Copyright Order, 1999 and held the provisions of the Act, especially S. 51 (dealing with infringement in the absence of a license), to be applicable vis-à-vis the rights associated with defendants' products in this case. Moreover, as per S. 14 of the Act, the court believed that by using pirated versions of the software copyrighted by the plaintiffs, the defendants were certainly guilty of infringement, besides having also caused trademark infringement.

Regarding the issue of punitive damages in matters of piracy and infringement, reference was made to precedents such as *Time Incorporated* vs. *Lokesh Srivastava & Anr.*, 2005 (30) PTC 3 (Del), *Hero Honda Motors Ltd.* vs. S*hree Assuramji Scooters*, 2006 (32) PTC 117 (Del), *Microsoft Corporation* vs. *Deepak Raval MIPR 2007 (1) 72,* and *Larsen and Toubro Limited* vs. *Chagan Bhai Patel* MIPR 2009 (1) 194, all of which favor the awarding of punitive damages for dissuading the infringers, even if the infringers decide not to appear in the suit proceedings at all. It was also argued that given the energy and resources spent by right-holders in infringement litigation, failure to award punitive damages would only foment encouragement for actions such as infringement and passing off.

The court also voiced concerns about increasing instances of piracy of software of reputed companies such as Microsoft and AutoCAD in the country, which might cause discouragement amongst the investors in the development of such software in the lack of dwindling license fees. Furthermore, the use of pirated software for commercial rather than personal purposes should, according to the court, be more heavily frowned upon, and therefore the court awarded the plaintiffs the permanent injunction sought for as also punitive damages amounting to Rs. 1 lakh against Defendant No. 2.

14. Travel India Times vs. India Times Travel[38]

(In the High Court of Delhi)

The fact situation in the Delhi High Court judgment in *Times Internet* vs. *M/s Belize Domian Whois Service Ltd. & Others* is a instance of cyber squatting. The judgment reaffirms the domain name-trademark / passing off principle. Contrary to oktatabyebye.com dispute where WIPO ruled in favour of Tata sons requiring Gurgaon-based travel portal MakeMyTrip to transfer the domain oktatabyebye.com to Tata, passing off in the instant case is evident.

Facts

Indiatimes.com is an e-commerce portal owned by the

plaintiff company, Times Internet. Since 2000, the website offers a wide range of services including travel services through travel.indiatimes.com. The defendant, M/s Belize Domain Whois Service Ltd. & Others registered Indiatimestravel.com in 2005. It carries some sponsored links.

Arguing that "indiatimestravel.com" is deceptively similar to that of platintiff's registered domain name "travel. indiatimes.com", plaintiff submitted that the defendant was trying to take advantage of its brand name. The plaintiff, citing revenue figures, submitted that its website enjoys reputation and signifies the services and products marketed through the website. The plaintiff sought for an injunction restraining the defendants from cyber squatting, using any other identical or deceptively similar name and transferring the domain name "indiatimestravel.com" to the plaintiff.

Judgment

The Court referred to the Supreme Court judgment in *Satyam Infoway Ltd.* vs. *Sifynet Solutions Pvt. Ltd.* which had a similar fact situation. In the instant case, Supreme Court observed that "a domain name .....is chosen as an instrument of commercial enterprise not only because it facilitates the ability of consumers to navigate the Internet to find websites they are looking for, but also at the same time, serves to identify and distinguish the business itself, or its goods or services, and to specify its corresponding online Internet location. Consequently a domain name as an address must, of necessity, be peculiar and unique and where a domain name is used in connection with a business, the value of maintaining an exclusive identity becomes critical." Comparing both the domain name and the trademark, Supreme Court held that a domain name can have all the characteristics of a trademark. Accordingly, domain names can be protected under Trademarks Act, 1999.

In the instant case, the High Court observed that the plaintiff owned the mark "indiatimes.com" way before the defendant created the mark "indiatimestravel.com". Further, "indiatimes" which was the essential component of the domain name, was used by the defendant without

any explanation. This can confuse an ordinary netizen and can result in associating defendant's portal with that of the plaintiff company. The use of impugned web portal by the defendant may also jeopardise the reputation of the plaintiff if the products and services which are advertised through the website lack quality. Further, as the defendant did not appear before the Court and contest the claims of the plaintiff, defendant's conduct was held to be in mala fide. Considering the above mentioned aspects, the instant dispute was held to be a clear case of "passing off". As the plaintiff was held to have the sole right to use the words "indiatimes", defendant was directed to transfer "indiatimestravel.com" to plaintiff.

15. *Cubby, Inc* vs. *CompuServe, Inc.*[40]

Where CompuServe is an online company providing access to over 150 special interest forums comprised of electronic bulletin boards, interactive online conferences, and topical databases. A newsletter called Rumorville was made available via the bulletin board. The plaintiff sued CompuServe for libel after allegedly defamatory statements were disseminated through the newsletter against it. Cubby argued that the court should consider CompuServe to be a "publisher" of the allegedly defamatory statements, and thus hold it liable for the statement.

The court held that CompuServe had "no more editorial control over such a publication than does a public library, bookstore, or newsstand". The court instead found CompuServe to be more akin to a "distributor" rather than a "publisher". Thus, because it was undisputed that CompuServe did not have knowledge of or reason to know of the allegedly defamatory statements made in the publication, especially given the large number of publications it carries and the speed with which publications are uploaded into its computer banks and made available to CompuServe subscribers, the court held that CompuServe could not be held liable to Cubby for the defamatory statements. The court noted that to impose on CompuServe the duty to examine every publication it carries for

defamatory statements would "impose an undue burden on the free flow of information".

16. *State Bank of India* vs. *Rizvi Exports Ltd.*[41]

(In The Debt Recovery Appellate Tribunal, Allahabad)

State Bank of India (SBI) (Appellants) had filed a case to recover money from some persons who had taken various loans from it Respondent: Rizvi Exports Ltd. As part of the evidence, SBI submitted printouts of statement of accounts maintained in SBI's computer systems.

The relevant certificates as mandated by the Bankers Books of Evidence Act (as amended by Information Technology Act) had not been attached to these printouts.

The Court held that these documents were not admissible as evidence Decided On: 01.10.2002

17. *Groff* vs. *America Online, Inc.*[42]

Facts

The plaintiff, an individual in Rhode Island who subscribed to America Online, sued the company in Rhode Island state court, alleging violations of state consumer protection legislation. The process of becoming a member of AOL includes a step in which the applicant must assent to AOL's terms of service by clicking an "I Agree" button. The terms of service "contains a forum-selection clause which expressly provides that virginia law and Virginia courts are the appropriate law and forum for the litigation between members and AOL." AOL moved to dismiss this suit from the Rhode Osland Superior Court for improper venue on the ground that a forum selection clause in the parties' contract mandated that the suit be brought in virginia, where AOL's base of operations was located. The court agreed, and dismissed the suit.

Judgement

The court held that the plaintiff assented to AOL's terms of service online by the click of an "I agree" button. The terms of service included a clause mandating that suits concerning

the service be brought in Virginia. AOL customers must first click on an "I agree" button indicating assent to be bound by AOL's terms of service before they can use the service. This button first appears on a web page in which the user is offered a choice either to read, or simply agree to be bound by, AOL's terms of service. It also appears at the foot of the terms of service, where the user is offered the choice of clicking either an "I agree" or "I disagree" button, by which he accepts or rejects the terms of service. The court held that a valid contract existed, even if the plaintiff did not know of the forum selection clause: "our Court stated the general rule that a party who signs an instrument manifests his assent to it and cannot later complain that he did not read the instrument or that he did not understand its contents. Here, plaintiff effectively "signed" the agreement by clicking. "I agree" not once but twice. Under these circumstances, he should not be heard to complain that he did not see, read, etc. and is bound to the terms of his agreement."

18. *Diebold Systems Pvt Ltd.* vs. *The Commissioner of Commercial Taxes*[43]

(Section 2 of Information Technology Act, 2000)

Facts

Diebold Systems Pvt. Ltd. Appellants manufactures and supplies Automated Teller Machines (ATM). Diebold sought a clarification from the Advance Ruling Authority (ARA) in Karnataka on the rate of tax applicable under the Karnataka Sales Tax Act, 1957 on sale of Automated Teller Machines.

The majority view of the ARA was to classify ATMs as "computer terminals" liable for 4% basic tax as they would fall under Entry 20(ii)(b) of Part 'C' of Second Schedule to the Karnataka Sales Tax Act.

The Chairman of the ARA dissented from the majority view. In his opinion, ATMs would fit into the description of electronic goods, parts and accessories thereof. They would thus attract basic rate of tax of 12% and would fall under Entry 4 of Part 'E' of the Second Schedule to the KST Act.

The Commissioner of Commercial Taxes was of the view that the ARA ruling was erroneous and passed an order that ATMs cannot be classified as computer terminals. Findings of the court:

1. The enlarged definition of "computers" in the Information Technology Act cannot be made use of interpreting an Entry under fiscal legislation.
2. An Automatic Teller Machine is an electronic device, which allows a bank's customer to make cash withdrawals, and check their account balances at any time without the need of human teller.
3. ATM is not a computer by itself and it is connected to a computer that performs the tasks requested by the person using ATM's. The computer is connected electronically to many ATM's that may be located from some distance from the computer.

Decision

ATMs are not computers, but are electronic devices under the Karnataka Sales Tax Act, 1957.

19. *Manish Kathuria* vs. *State*[44]

The first reported case of cyber-stalking in India and the reason for the 2008 amendment to the IT Act,5 the Manish Kathuria case involved the stalking of a woman named Ritu Kohli. Kathuria followed Kohli on a chat website, abused her by using obscene language and then disseminated her telephone number to various people.

Later, he began using Kohli's identity to chat on the website "www.mirc.com". As a result she started receiving almost forty obscene telephone calls at odd hours of the night over three consecutive days. This situation forced her to report the matter to the Delhi Police. As soon as the complaint was made, Delhi Police traced the IP addresses and arrested Kathuria under Section 509 of the Indian Penal Code. The IT Act was not invoked in the case, since it had not come into force at the time when the complaint was filed.

While there is no record of any subsequent proceeding, this

case made Indian legislators wake up to the need for a legislation to address cyber-stalking. Even then, it was only in 2008 that Section 66-A was introduced. As a result, now cases are being reported under this section as opposed to Section 509 of the Indian Penal Code, as was the case where a Delhi University student was arrested for stalking a woman from Goa by creating fake profiles on social networking websites, uploading pictures on them and declared her to be his wife. It is hoped that the decision in this would favour the victim.

In the case commonly known as Ritu Kohli Case is India's first case of cyber stalking. It was indeed an important revelation into the mind of the Indian cyber stalker. A young Indian girl being cyber stalked by a former colleague of her husband took a legal call against such stalking. Ritu Kohli's case took the imagination of India by storm. The case which got cracked however predated the passing of the Indian Cyber law and hence it was just registered as a minor offences under the Indian Penal Code.

20. *State of Maharashtra* vs. *Anand Ashok Khare*[45]

This case related to the activities of the 23-year-old Telecom engineer Anand Ashok Khare from Mumbai who posed as the famous hacker Dr Neuker and made several attempts to hack the Mumbai police Cyber Cell website.

21. *Firos* vs. *State of Kerala*[46]

Facts

The Government of Kerala issued a notification u/s 70 of the Information Technology Act declaring the FRIENDS application software as a protected system.

The author of the application software filed a petition in the High Court against the said notification. He also challenged the constitutional validity of section 70 of the IT Act.

The Court upheld the validity of both, section 70 of the IT Act, as well as the notification issued by the Kerala Government.

Decision

There is no conflict between the provisions of Copyright Act and Section 70 of IT Act.

Section 70 of the IT Act is not unconstitutional.

While interpreting section 70 of the IT Act, a harmonious construction with Copyright Act is needed.

Section 70 of the IT Act is not against but subject to the provisions of the Copyright Act.

Government cannot unilaterally declare any system as "protected" other than "Government work" falling under section 2(k) of the Copyright Act on which Govt.'s copyright is recognized under Section 17(d) of the said Act.

22. *State of Tamilnadu* vs. *Dr L. Prakash*[47]

Summary of the case

State of Tamilnadu v/s Dr L. Prakash was the landmark case in which Dr L. Prakash was sentenced to life imprisonment in a case pertaining to online obscenity. This case was also landmark in a variety of ways since it demonstrated the resolve of the law enforcement and the judiciary not to let off the hook one of the very educated and sophisticated professionals of India.

23. *Benususan Restaurant Corp.* vs. *King*[48]

Facts

Where a New York jazz club operator sued a Missouri club owner claiming trademark infringement, dilution and unfair competition over the use of the name "The Blue Note". The defendant maintained a web site promoting his Missouri "Blue Note" club and providing a Missouri telephone number through which tickets to the club could be purchased.

The issue, as framed by the Federal District Court, was whether the existence of the web site, without more, was sufficient to vest the court with personal jurisdiction over the defendant under New York's long-arm statute.

The court held that it did not. The court considered whether the existence of the web site and telephone ordering information constituted an "offer to sell" the allegedly infringing "product" in New York, and concluded it was not. The court noted that, although the web site is available to any new Yorker with Internet access, it takes several affirmation steps to obtain access to this particular site, to utilize the information contained there, and to obtain a ticket to the defendant's club.

24. *Ashcroft, Attorney General et al* vs. *Free Speech Coalition, et al.*[49]

Facts

The US Supreme Court affirmed the judgment of the Court of Appeals for the Ninth Circuit that the prohibitions of Ss.2256 (8) (B) and 2256(8) (D) are overboard and unconstitutional. Being part of the Child Pornography Prevention Act of 1996 (CPPA) S. 2256 (8) (B) bans a range of sexually explicit images, sometimes called "virtual child pornography," that appear to depict minors but were produced by means other than using real children, such as through the use of youthful-looking adults or computer-imaging technology and S.2256(8)(D) is aimed at preventing the production or distribution of pornographic material pandered as child pornography.

Justice Kennedy opined:

"Congress may pass valid laws to protect children from abuse, and it has. The prospect of crime. however, by itself does not justify laws suppressing protected speech..."

As a general principle, the First Amendment bars the government from dictating what see or read or speak or hear. The freedom of speech has its limits; it does not embrace certain categories of speech, including defamation, incitement, obscenity, and pornography produced with real children.

The Government submits "that virtual child pornography whets the appetites of pedophiles and encourages them to

engage in illegal conduct. This rationale cannot sustain the provision in question. The mere tendency of speech to encourage unlawful acts is not a sufficient reason for banning it. The government "cannot constitutionally premise legislation on the desirability of controlling a person's private thoughts." First Amendment freedom are most in danger when the government seeks to control thought or to justify its laws for that impermissible end. The right to think is the beginning of freedom, and speech must be protected from the government because speech is the beginning of thought." (Decided on April 16, 2002).

25. *State* vs. *Amit Prasad* [50]

State vs. *Amit Prasad*, was India's first case of hacking registered under Section 66 of the Information Technology Act, 2000. A case with unique facts, this case demonstrated how the provisions of the Indian Cyber law could be interpreted in any manner, depending on which side of the offence you were on.

26. *R* vs. *Graham Waddon* [51]

Facts

The defendant was charged with numerous counts of publishing obscene articles contrary to S. 2(1) of UK's Obscene Publications Act 1959. The defendant had created pornographic images, which were illegal under the UK's Obscene Publications Act. He ran a series of sites based in the US, hosting them on a US based Internet service provider. These images were accessible to anyone in the world via the Internet who became a subscriber by giving credit card details. He was charging UK customers 25 pounds a month for access. The subscriber was given a password and could log onto the various websites to obtain the images. It was submitted on behalf of the defendant that, because the Internet publication had necessarily occurred abroad, therefore the instant court did not have jurisdiction.

Hardy Christopher, J. held:

"Publishing an article under S. 1(3) (b) of the 1959 Act

included data stored electronically and transmitted. To transmit simply meant to send from one place or person to another. In the instant case, an act of publication took place when the data was transmitted by the defendant or his agent to the service provider, and the publication or transmission was in effect still taking place when the data was received. both the sending and receiving took place within the jurisdiction of the court and it was irrelevant that the transmission may have left the jurisdiction in between the sending and receiving".

27. The Arzika case[51]

Pornography and obscene electronic content has continued to engage the attention of the Indian mind. Cases pertaining to online obscenity, although reported in media, often have not been registered. The Arzika case was the first in this regard.

28. *Air Force Bal Bharti School & Anr.* vs. *Delhi School Tribunal & Ors.*[52]

The Air Force Bal Bharti School case demonstrated how Section 67 of the Information Technology Act, 2000 could be applicable for obscene content created by a school going boy.

A 16-year-old boy was arrested in April 2001 on the charge of creating a pornographic website containing obscene comments about some women teachers and girls of his school, Air Force Bal Bharati in Delhi. When he was released on bail, the school refused to take him back.

29. *Sri Prabhakar Singh* vs. *Union of India*[53]

P.R. Transport Agency through its partner Sri Prabhakar Singh Vs. Union of India (UOI) through Secretary, Ministry of Coal, Bharat Coking Coal Ltd. through its Chairman, Chief Sales Manager Road Sales, Bharat Coking Coal Ltd. and Metal and Scrap Trading Corporation Ltd. (MSTC Ltd.) through its Chairman cum Managing Director., Writ Petition No. 58468 of 2005.

History of the case

Bharat Coking Coal Ltd. (BCC) held an e-auction for coal in different lots.

P.R. Transport Agency's (PRTA) bid was accepted for 4000 metric tons of coal from Dobari Colliery.

The acceptance letter was issued on 19th July, 2005 by e-mail to PRTA's e-mail address. Acting upon this acceptance, PRTA deposited the full amount of Rs. 81.12 lakh through a cheque in favour of BCC. This cheque was accepted and encashed by BCC.

BCC did not deliver the coal to PRTA. Instead it e-mailed PRTA saying that the sale as well as the e-auction in favour of PRTA stood cancelled "due to some technical and unavoidable reasons".

The only reason for this cancellation was that there was some other person whose bid for the same coal was slightly higher than that of PRTA. Due to some flaw in the computer or its programmed or feeding of data the higher bid had not been considered earlier.

This communication was challenged by PRTA in the High Court of Allahabad. [Note: Allahabad is the state of Uttar Pradesh (UP)]

BCC objected to the "territorial jurisdiction" of the Court on the grounds that no part of the cause of action had arisen within U.P.

Issue raised by BCC

The High Court at Allahabad (in U.P.) had no jurisdiction as no part of the cause of action had arisen within U.P.

Issues raised by PRTA

1. The communication of the acceptance of the tender was received by the petitioner by e-mail at Chandauli (U.P.). Hence the contract (from which the dispute arose) was completed at Chandauli (U.P). The completion of the contract is a part of the "cause of action'.

2. The place where the contract was completed by receipt of communication of acceptance is a place where 'part of cause of action' arises.

Observation by the court:

1. In reference to contracts made by telephone, telex or fax, the contract is complete when and where the acceptance is received. However, this principle can apply only where the transmitting terminal and the receiving terminal are at fixed points.
2. In case of e-mail, the data (in this case acceptance) can be transmitted from anywhere by the e-mail account holder. It goes to the memory of a 'server' which may be located anywhere and can be retrieved by the addressee account holder from anywhere in the world. Therefore, there is no fixed point either of transmission or of receipt.
3. Section 13(3) of the Information Technology Act has covered this difficulty of "no fixed point either of transmission or of receipt". According to this section "...an electronic record is deemed to be received at the place where the addressee has his place of business."
4. The acceptance of the tender will be deemed to be received by PRTA at the places where it has place of business. In this case it is Varanasi and Chandauli (both in U.P.)

Decision

1. The acceptance was received by PRTA at Chandauli / Varanasi. The contract became complete by receipt of such acceptance.
2. Both these places are within the territorial jurisdiction of the High Court of Allahabad. Therefore, a part of the cause of action has arisen in U.P. and the court has territorial jurisdiction.

30. *Washington Post* vs. *Total News* [55]

History of the case:

Where the "totalnews.com" website used framing

technology to set a news story from other website within the overall Total News frame by blocking banner advertisements and other distinguishing features.

The U.S. District Court Southern District of New York passed an order of settlement stating that "the defendants agree permanently to cease the practice of framing plaintiff's websites". Plaintiffs agree that Defendants may link from the Totalnewa.com website or any other website to nay plaintiff's website, provided that:

(1) Defendants may link to plaintiff's website only via hyperlinks consisting of the names of the linked sites in plain text, which may be highlighted;

(2) Defendants may not use on any website, as hyperlinks or in any other way, any of plaintiff's proprietary logos or other distinctive graphics, video or audio material, nor may defendants otherwise link in any manner reasonably likely to: (i) imply affiliation with, endorsement or sponsorship by any plaintiff; (ii) cause confusion, mistake or deception; (iii) dilute Plaintiff's marks; or (iv) otherwise violate state or federal law;

(3) Each plaintiff's agreement to permit linking by defendants remains revocable, on 15 business days notice, at each Plaintiff's sole discretion. Revocation by any plaintiff shall not affect any other terms and conditions set forth herein. If defendants refuse to cease linking upon notice, and any plaintiff brings an action to enforce its rights under this subparagraph, it shall be an affirmative defense that defendants conduct does not otherwise infringe or violate plaintiffs rights under any theory of any intellectual property, unfair competition or other law.

***

Chapter 6

Cyber Laws – Recent Trends

Cyber Law of India: The Information Technology Act, 2000 (IT Act 2000) still governs the cyber law of India and related issues. IT Act, 2000 has become an redundant and draconian law that needs to be repealed. The telegraph and cyber law of India remained outdated, colonial and draconian in the year 2014 as well.

India must ensure techno legal measures to regulate Indian cyberspace. Similarly, regulations and guidelines for effective investigation of cyber crimes in India is also need of the hour. The Indian Government has assured in the year 2014 that the IT Act, 2000 could be amended to accommodate e-commerce concerns.

The technological development has given rise to a cyber world constituting cyber space. Cyber space is witnessing considerable advancement with the rapid increase in the information technology.

It is always hard to determine or predict something in the future in an accurate manner.

There is a possibility to consolidate the technological advancements in the past. The internet users are increasing tremendously every year and at the same time there is also rise in the number of people using mobiles and smart phones.

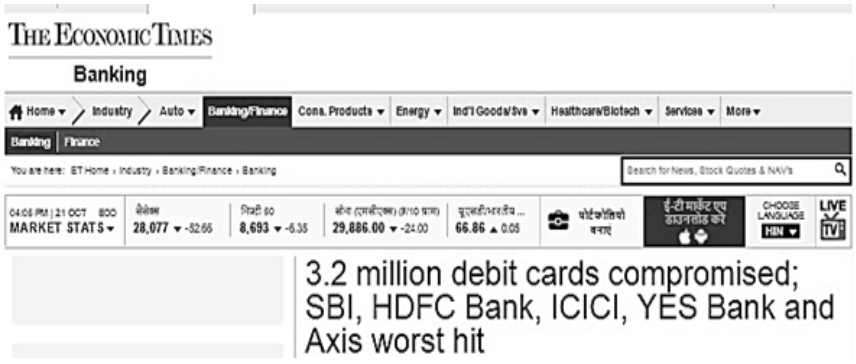
The cyber law trends and developments of India are as follows:

1. *Cyber Crimes Prevention Strategy* : Cyber crimes have significantly increased in India in last few years. Reacting to the same, Indian Government had now decided to formulate a cyber crimes prevention strategy for India. However, till date, the proposed strategy has not been formulated.
2. *Cyber Crimes Investigation Training*: With increased cyber crimes in India, a need was felt to provide cyber crimes

investigation training to law enforcement agencies of India. India needs to enhance cyber crimes investigation capabilities so that cyber crimes can be effectively tackled. Similarly, modernisation of police force of India is urgently needed with a special focus upon techno legal skills development for them.

3. *Encryption Laws* : Almost six years back the Standing Committee on Information Technology pulled Department of Telecommunication (DOT) over encryption issues. The encryption laws and regulations in India need clarity. Legal risks for websites development companies in India would also increase due to improper use of encryption for such websites. A dedicated encryption policy of India and techno legal encryption law in India is need of the hour.

4. *Bank ATMs Compromised* : Recently, on October 20, 2016, it was reported that around 3.2 million debit cards of the bank consumers were compromised. Among many, SBI, HDFC Bank, ICICI, YES Bank and Axis Bank were worst at hit. Banks in India will either replace or ask users to change security codes for more than 3.2 million debit cards.


THE ECONOMIC TIMES

Banking

Home | Industry | Auto | Banking/Finance | Cons. Products | Energy | Ind'l Goods/Svs | Healthcare/Biotech | Services | More

Banking | Finance

You are here: ET Home › Industry › Banking/Finance › Banking

Search for News, Stock Quotes & NAVs

04:05 PM | 21 OCT BSE MARKET STATS | सेंसेक्स 28,077 ▼ -52.65 | निफ्टी 50 8,693 ▼ -6.35 | मोद (एमसीएक्स) (प्र/10 ग्राम) 29,886.00 ▼ -24.00 | यूएसडी/आरएसए... 66.86 ▲ 0.05 | पोर्टफोलियो बनाएं | ई-दी मार्केट एप डाउनलोड करें | CHOOSE LANGUAGE HIN | LIVE TV

3.2 million debit cards compromised; SBI, HDFC Bank, ICICI, YES Bank and Axis worst hit

Reproduced from The Economic Times

5. *Corporate Scam Investigations* : Although the Companies Act, 2013 has been formulated to curb corporate frauds yet a dedicated fraudulent MLM regulations is need of the hour. The powers of Serious Fraud Investigation Office (SFIO) were also enhanced so that they can effectively deal with corporate frauds and crimes in India. SEBI has also notified

the Securities and Exchange Board of India (Procedure for Search and Seizure) Regulations, 2014.

6. *Cyber Insurance:* Cyber insurance in India became a reality in the year 2014 and many companies and individuals have started taking cyber insurance policies in India. However, the business of cyber insurance would raise many novel techno legal issues in this regard that all stakeholders must be well prepared to deal with.
7. *Cloud Computing* : The cloud computing legal issues in India are still not clear and this has resulted in limited adoption of cloud computing in India. The cloud computing legal and regulatory requirements in India for businesses and entrepreneurs must be analysed in advance before launching a project. Cloud computing service providers in India are Internet intermediary within the meaning of IT Act, 2000 and they are also required to comply with cyber law due diligence requirements.
8. *E-Mail Policy* : The e-mail policy of India has still not been implemented despite strict warnings by Delhi High Court. So bad is the situation that the Delhi High Court has accused central government of sitting over e-mail policy of India. The Delhi High Court has also directed Central Government to issue notification regarding electronic signature under Information Technology Act 2000. The encryption policy of India is also missing till date though it is need of the hour. However, Madhya Pradesh has given legal recognition to e-mail communications among Government Departments.
9. *Online Payments* : Online and mobile payments witnessed an increase in India in last decade. However, legal and regulatory issues were not taken seriously by various mobile payment providers in India. There are many legal issues of e-commerce in India that various online payment service providers of India must comply with. It has already specified the cyber law due diligence requirements for Paypal and online payment transferors in India. Similarly, we have also outlined the e-commerce and online business legal compliances for online payment market of India. Further, payment gateway and POS terminal services providers must

also keep in mind the cyber law due diligence requirements in India.

10. *Online Gambling in India* : Online gambling laws in India have remained in a state of suspension. Online gambling in India is still punishable in almost all of the cases with few selective exceptions. The matter is pending before the Supreme Court of India and it has referred the matter for the opinion of Central Government. However, the Central Government has not given a conclusive opinion on this issue so far.

11. *Websites Blocking in India* : Websites blocking in India was another development that resulted in many protests as well. For instance, Tamil website Savukku was ordered to be blocked by Madras High Court. However, immediately after the blocking of the Savukku website, it became available through proxy servers making the blocking redundant. In the year 2013, the Indian Government blocked 39 Internet sites on ground of pornography. The Supreme Court of India also sought the response of Indian Government in this regard in 2013. However, Indian Internet Service Providers (ISPs) told the Supreme Court that they cannot block pornographic websites unilaterally and voluntarily.

12. *Bitcoins* : The legality of bitcoins in India was a major questioning the year 2014. The Enforcement Directorate (ED) searched and raided few Bitcoin exchanges to see whether they were violating Indian laws or not. ED believed that Bitcoins can be used for criminal activities including money laundering, hawala transactions and funding of terrorist activities. Indian Laxmicoin had even sought clarifications from regulatory authorities of India before its launch. Cyber attacks also targeted Bitcoin users and Bitcoin Exchanges in the year 2014. According to some reports, Bitcoin website Mt. Gox's disappeared due to sophisticated cyber attacks and stealing of Bitcoins. RBI informed that they cannot regulate Bitcoins.

13. *Mobile Applications* : Mobile applications also saw a tremendous increase in India in the recent years. However, most of the mobile application developers are violating Indian Laws and may be prosecuted in future.

14. *Cyber Law Due Diligence* : Cyber Law Due Diligence Requirements in India are neglected by various stakeholders. Indian Government has remained indifferent while Cyber Law Due Diligence requirements are being flouted by Telecom Companies, E-commerce Websites, etc.
15. *Internet Intermediary Liability* : Internet Intermediary Liability in India is closely related to the Cyber law Due Diligence Compliances. As many stakeholders failed to ensure Cyber Law Due Diligence Compliances, they violated the Information Technology (Intermediaries Guidelines) Rules, 2011 of India.
16. *Telecom Companies Violations* : Tata Teleservices Limited (TTL) and Airtel are Violating Indian Cyber Law and Internet Intermediary Rules of India. Complaints against Tata and Airtel are already pending before the Department of Telecommunication and Telecom Regulatory Authority of India (TRAI).
17. *E-Discovery Requirements* : The need for E-Discovery for Indian companies has significantly increased and it would even increase further in the years too. The Cyber Law Non-Compliances have given rise to an increased demand for E-Discovery in India.
18. *Corporate Frauds in India* : Corporate Frauds Investigations in India have become multi disciplinary in nature. Besides the traditional corporate frauds, now Cyber Crimes and Technology Frauds have also become part of Corporate Frauds Investigation in India.
19. *Indo American Cyber Crimes Cooperation* : An Indo-American alert, watch and warn network for real time information sharing in Cyber Crime Cases has been established to deal with Cyber Crimes cases falling within Indian and American jurisdictions.
20. *Corruption And Technology Related Due Diligence* : Besides Cyber Law Due Diligence, the scope of Indian and Foreign Corruption and Technology related due diligences in India has also increased. With the passage of Lokpal and Lokayuktas Act, 2013 by the Indian Parliament, a stress upon corruption free environment has been made. Even Central

Government permission is not required by CBI anymore to prosecute senior bureaucrats for corruption cases monitored by Supreme Court of India.

21. *Cyber Harassment And Cyber Stalking* : Cases of Cyber Harassment and Cyber Stalking have increased in India. Websites like OLX are becoming a breeding ground for Cyber Harassment and Cyber Stalking. Further, allegations of selling stolen goods were also leveled against OLX.
22. *E-Commerce Compliances*: Websites providing E-Commerce services in India are not complying with Indian Laws. The e-Commerce Websites must be regulated in India as they are operating with great disregard to Indian Laws. Although Indian Government has assured that E-Commerce in India would be regulated by comprehensive guidelines yet till date no such sign has been shown by the Government.
23. *Legality of Bitcoins* : The Bitcoin craze has finally started fading away as the Reserve Bank of India (RBI) issued a Warning Advisory against use of Bitcoins in India citing Cyber Security and Legal Risks. The Enforcement Directorate (ED) also searched Seven Digital Cash LLP office and website for selling and buying Bitcoins in India. The Legality of Bitcoins in India was always in doubts. Many countries like China, France, Thailand, Norway, etc. have either regulated the use of Bitcoins or they have completely banned them in their jurisdictions.
24. *Conflict of Laws in Cyberspace* : Another problem that Indian Government is not willing to resolve pertains to Conflict of Laws in Indian Cyberspace. For long Companies like Google, Facebook, etc. are violating Laws of India. Indian Government has not taken a tough stand against such Foreign Companies that although operating in India for profit yet are not complying with Indian Laws. For instance, G-Mail is abetting and encouraging commission of various Cyber Crimes in India yet Indian Government has allowed it to operate so far.
25. *E-Mail Policy of India* : There is no operational E-Mail Policy of India. The Delhi High Court is analyzing E-Mail Policy of India and complaint mechanism to Facebook. The Delhi

High Court has also directed Central Government to issue Notification regarding Electronic Signature under Information Technology Act, 2000. An Advisory by Maharashtra Government to use Official E-Mails has already been issued. Even an Email Policy of India is in pipeline.

26. *Cyber Crimes and Wildlife* : Cyber Criminals are not leaving any opportunity to indulge in Cyber Crimes in India. The Cyber Criminals tried to crack the Iridium GPS Satellite Collar of a Tiger. The attempt to crack the collar was committed from Pune whereas the tiger with collar was located at a great distance at the tiger reserves of Madhya Pradesh. The Wildlife Crime Control Bureau (WCCB) has also recently traced at least 200 websites all over the country, which are being used by people to trade in animal parts. So the Cyber Crimes in India are evolving and Law Enforcement Agencies of India must be well equipped to deal with such Crimes.

27. *Child Porn Nuisance* : Child Pornography in India is becoming a big nuisance. An Advisory by Home Ministry of India on Preventing and Combating Cyber Crime against Children in India has also been issued. Recently Interpol helped India in tracking child porn surfers. We also need such Techno Legal Framework so that child pornography can be curbed to the maximum possible extent in India.

28. *Online Gambling in India* : Although we have no dedicated Online Gambling Laws in India yet online gambling is fairly regulated in India under various Legislations. By indulging in gambling in online and offline manner, the concerned person or company would be violating the Laws of India. Many online gambling rackets were busted in the year 2013 and Indian Government must seriously consider regulation of Online Gambling in India.

29. *Online Pharmacies in India* : Online Pharmacies in India are under regulatory scanner around the world, including India. Online sales of prescribed medicines in India are by and large unregulated and open for abuses. In fact, illegal and unregulated online sales of prescribed medicines in India are flourishing like a plague. Indian Government must give a serious thought to this area. Meanwhile, various stake-

holders must understand various aspects of Telemedicine and Online Pharmacies Laws in India and their legal implications and liabilities.

30. *MLM Companies Frauds* : Multi Level Marketing (MLM) frauds have significantly increased in India. Indian Government has even considered blocking of websites of MLM companies in India that are engaging in fraudulent behaviour. More clarity in this regard is needed.

31. *Civil Liberties Protection in Cyberspace* : Civil Liberties Protection in Cyberspace is gaining importance in India and worldwide Even at the United Nations (UN), Civil Liberties Protection in Cyberspace were considered. The United Nations even passed a resolution approving Right to Privacy in the Digital Age. However, India is in no mood of complying with that Resolution.

32. *E-Surveillance in India* : E-Surveillance in India has increased tremendously despite the UN Resolution. India has launched Illegal and Unconstitutional Projects like Aadhar, Central Monitoring System (CMS), national Intelligence Grid (Natgrid), crime And Criminal Tracking Networks and Systems (CCTNS), Internet Spy System Network And Traffic Analysis System (NETRA), etc without any Parliamentary Oversight and Legal Frameworks. E-Surveillance, Civil Liberties Protection in Cyberspace and Conflict of Laws are some of the crucial issues that United Nations and India must consider on a priority basis.

33. *Internet Governance and India* : In view of its growing Indian Cyber Security concerns, India has decided to challenge the U.S. government's control over the Internet and ensure that the trio of the U.S., Russia and China does not ignore India's concerns while developing an International Regime for Internet Governance. India will also push for storing all Internet Data and VoIP Services within the Country, besides ensuring control and management of servers.

34. *ICANN Free Domain Name Protection in India* : The Policies and Agreements of Internet Corporation for Assigned Names and Numbers (ICANN) are in active violation of Indian Laws. Thus, Domain Name Protection in India must

be free from ICANN's influence and must be judged independently of ICANN's Polices and Agreements.

35. *Challenges in Mobile Laws* : Today, there are lots of activities in the mobile ecosystem. The increasing competition has introduced new models of mobile phones, personal digital assistors, tablets and other communication devices in the global market. The intensive use of mobile devices has widened the mobile ecosystem and the content generated is likely to pose new challenges for cyber legal jurisprudence across the world. There are no dedicated laws dealing with the use of these new communication devices and mobile platforms in a number of jurisdictions across the world as the usage of mobile devices for input and output activities is increasing day by day. With the increasing mobile crimes, there is an increasing necessity to meet the legal challenges emerging with the use of mobile devices and ensure mobile protection and privacy.

36. *Legal issues of Cyber Security* : The other emerging cyber law trend is the need for enacting appropriate legal frameworks for preserving, promoting and enhancing cyber security.

    The cyber security incidents and the attacks on networks are increasing rampantly leading to breaches of cyber security which is likely to have serious impact on the nation. However, the challenge before a lawmaker is not only to develop appropriate legal regimes enabling protection and preservation of cyber security, but also to instil a culture of cyber security amongst the net users. The renewed focus and emphasis is to set forth effective mandatory provisions which would help the protection, preservation and promotion of cyber security in use of computers, allied resources and communication devices.

37. *Cloud computing and law* : With the growth in internet technology, the word is moving towards cloud computing. The cloud computing brings new challenges to the law makers. The distinct challenges may include data security, data privacy, jurisdiction and other legal issues. There pressure on the cyber legislators and stakeholders would

be to provide appropriate legal framework that could benefit the industry and enable effective remedies in the event of cloud computing incidents.

38. *Privacy & Data Protection* : As the world moves towards more ubiquitous computing at 24x7 accesses to various kinds of resources and communication devices, online privacy and data protection will continue to be important topics as far as growth of cyber law jurisprudence is concerned. Different countries are likely to come up with their own enabling frameworks so as to not only preserve and protect online privacy but also provide for stringent methodologies for protecting data in the digital and mobile ecosystems.

39. *Social media & legal problems* : The social media is beginning to have social and legal impact in the recent times raising significant legal issues and challenges. A latest study indicates the social networking sites responsible for various problems. Since the law enforcement agencies, intelligence agencies target the social media sites; they are the preferred repository of all data. The inappropriate use of social media is giving rise to crimes like cyber harassments, cyber stalking, identity, theft etc. The privacy in social media is going to be undermined to a great extent despite the efforts by relevant stake holders. The challenge to the cyber legislators would be to effectively regulate the misuse of social media and provide remedies to the victims of social media crimes. Social Media Litigations are also likely to increase concerning the association or nexus with the output of social media. The litigations regarding defamation, matrimonial actions are popularly increasing and with the data, information resident on social media networking there is an emerging trend of various other litigations in the coming years.

40. *Spam laws* : There is considerable growth of spam in emails and mobiles. Many countries have already become hot spots for generating spam. As the number of internet and mobile users increase the spammers make use of innovative methods to target the digital users. It is therefore necessary to have effective legislative provisions to deal with the menace of spam.

These are some of the trends in Cyber Law which are based on the analysis of emerging cyber law jurisprudence. With the growing pace of technology, it may not be possible to overrule any new trend in the technology which might have direct or indirect impact on Cyber Law.

With the ongoing advancing technology, more emerging trends are bound to occur. This creates a huge responsibility to update the legal protection and regulation of these cyber issues at par with global standards.

***

Chapter 7

Conclusion and Recommendations

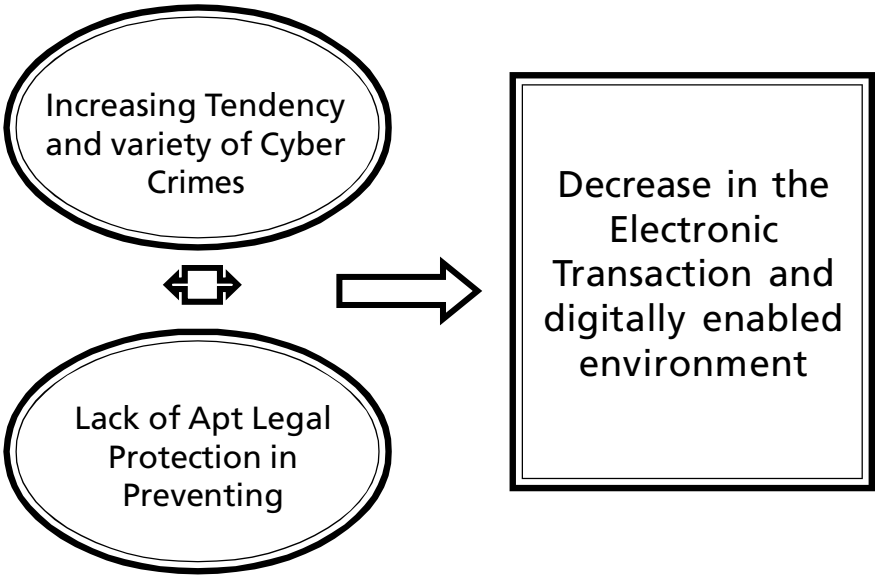
7.1 Cyber Law: A Need to Retake

From the above discussion it seems quite clear that with the advancement of Information and Communication Technology, the frequency of cybercrimes is also increasing.

With the ongoing advancement of technology, varieties of cyber crimes are taking place. New categories of cyber crimes from email hacking to software piracy, from cyber stalking to cyber terrorism are taking place in the qualified world of information and communication technology.

It is reported again and again that on an average crime through cyber world is increasing at the rate of 1.4% every year. It is surprising to know is that majority of cyber crimes are conducted by the qualified people. From Pune Bank fraud case to Bangalore's cyber defamation case, qualified engineers in this technology are marked as accused. They are tending to commit crime as they are well aware about principles and computer ethics for their use in proper manner or their misuse towards impairing the societal peace.

The issues discussed in the various cases by the courts in India demarcates the fact that the Indian law on Information Technology is not robust and the doubts left in the provisions are reason for the escape of the accused. The Information Technology Act is objectifying the promotion of electronic transactions rather than prevention of cyber misuse. It was only in year 2008 when the Amendment Act of 2008 has brought few specific categories of cyber crimes.



The above fugure makes it clear that 1) Increase in the frequency and variety of Cyber Crimes plus the 2) Low level of protection in preventing and regulating the emerging cyber crimes is equal to the 3) decrease in the growth of electronic transactions and digitally enabled environment.

This might adversely affect the inclusive growth of our country too.

It is quite clear that increasing tendencies of cyber crime without legal recourse are detrimental to the growth of electronic transactions in our country at par with global standards. Therefore, a balanced law on preventing and regulating cyber crime is need of the hour.

The law on cyber crime needs to be strong in order to prevent future cyber crime. Law should change it recourse to ensure a safe, secure and trustworthy computing environment. It is crucial not only to our national sense of well-being, but also to our national security and economy.

Though India has taken a lot of steps to stop cybercrime but the cyber law cannot afford to be static, it has to change with the changing times.

7.2 Recommendation

Therefore to combat cyber crimes effectively and efficiently

in line with the emerging trends in cyber laws, following recommendations are submitted:

National Plan to Combat Cybercrime

It is suggested that alike the developed countries, Indian government should also initiate a National Plan to combat cyber crimes.

This national plan should intent to work on the following objectives and key priorities:

(i) Educating the Community to Protect Themselves;

(ii) Partnering with industry to tackle the shares problem of Cyber Crime;

(iii) Fostering Intelligence led approach and sharing information;

(iv) Improving the capacity and capability of agencies to address cyber crime;

(v) Improving international cooperation on cyber crime;

(vi) Ensuring effective Criminal Justice System

Cyber Crime Prevention Guide to Users

Rightly said prevention is better than cure therefore, it is suggested that the government should issue cyber crime prevention guidelines to citizens at large so that users can follow guidelines in protecting themselves from the Cyber Crimes.

Best practice to prevent Cyber Crime should include following directions to users:

a. Updating the Computer System Regularly;

b. Selecting strong passwords which cannot be guessed. One should avoid using passwords like date of birth, date of marriage anniversary and alike;

c. Keep changing the passwords regularly;

d. Protecting Computers with security Softwares and Physical Firewalls.

e. Protecting ones personal information;
f. Keeping an eye on phony email messages;
g. Regular signing out of online accounts and transactions;
h. Avoid sharing credit card and debit card details;
i. Stop responding to emails and messages asking for personal information;
j. Pay attention to privacy policies;
k. Guarding ones email addresses;
l. Regularly reviewing bank and credit card statements and
m. alike

Comprehensive Law on Cyber Crime

The present law on Information technology should be amended comprehensively keeping in mind the recent changes and prospective changes in the cyber arena. Possible categories of cyber crime should be well defined with the variables of constituting crime, possibilities of prevention and clear demarcations on punishment for the cyber crime.

This will facilitate the courts to administer the justice quickly and the clear punishment will prevent people towards committing the crime.

Specialized Agency to Investigate Cyber Crime

Investigation plays important role in getting the real culprit to be punished for his deed. Cyber Crime being a specialized and intellectual crime requires experts in investigating the crime. Therefore, it is suggested that specialized agencies should be appointed in investigating the crime so that the victim can get equated justice.

Promoting Cyber Literacy

Last but not the least; the government should start campaigns in promoting literacy about cyber world and cyber crime specifically to make the people more aware about the use and misuse. It is further recommended that cyber illiteracy should start from grassroots level; institutes, computer centers, schools & individuals.

Unless the people recognize the power of Information and Communication Technology in the construction and nation building and the adverse effect of its misuse in destroying the inclusive development of the society as a whole, no law will be able to remedy the nusance of cyber crime.

Therefore, along with strengthening the legal protection on cyber crimes, the government should enhance the awareness amongst masses about the use and misuse of Information and Communication Technology and its recompense and effects in the inclusive development of nation as a whole. This will surely commence us towards a true "Digital India."

References

1. Audit of Fraud,Fraud Detection Technique& Forensic Audit, Case Study on Cyber Crimes. Indian Audit & Accounts Departments; (unpublished).
2. Barkha and U. Ram Mohan, Cyber Laws and Crimes, 3rd Edition, Delhi Law House.
3. Basha K.N.;"Seminar and Workshop on Detection of Cyber Crime and Investigation," (unpublished).
4. Boateng and Amanor (2014); "Phishing,Smishing & Vishing: An Assessment of Threats against Mobile Devices", Vol. 5, April 2014, pp.297-307.
5. Bramhe Manoj (2011);"SMS Based Secure Mobile Banking", Vol. 3, pp.472- 479.
6. Common Cyber Crimes and Government Laws and Rules in Information Security" Unit 3, Information Technology Act, 2000.
7. Crime in India: 2011-Compendium (2012), National Crime Records Bureau, Ministry of Home Affairs, Government of India,New Delhi, India.
8. CSIS: Securing Cyberspace for the 44th Presidency, CSIS Commission on Cybersecurity, US Center for Strategic and International Studies (CSIS), Washington DC, December 2008.

9. Dr.Muthukumaran B. (2008), Chief Consultant, Gemini Communication Ltd., "Cyber Crime Scenario in India", Criminal Investigation Department Review.
10. Dr. Prasanna A., "Cyber Crimes: Laws And Practice", IMG, Thiruvananthapuram.
11. Dudeja V.D (2011); Cyber Crimes and Law: Crimes in Cyber Space – Scams and Frauds, Vedams eBooks (P) Ltd (New Delhi, India), Published by Commonwealth (2002-09-24) ISBN 10: 8171697089 / ISBN 13: 9788171697083.
12. Ghosh Arjita and Sen Sandip, "Agent-Based Distributed Intrusion Alert System", University of Tulsa, Tulsa OK 74104, USA
13. Goyal Mohit (2012); "Ethics and Cyber Crime in India", International Journal of Engineering and Management Research, Vol. 2, Issue-1.
14. Guinier D, Dispositif (2006); Continuity Planning – BRP/BCP: a legal requirement for some and a vital necessity for all). Expertises, no. 308, Nov. 2006, pp. 390-396.
15. Gupta Nikhil A. (2014); "Mobile Cell Phones and Cyber Crimes in India- How Safe are we" Vol. 4, February, pp. 427-429.
16. Hassan Anah Bijik et al. (2012), "Cybercrime in Nigeria: Causes, Effects and the Way Out", ARPN Journal of Science and Technology, ISSN 2225-7217, Vol. 2, No. 7.
17. Indian Institute of banking and Finance (2012); IT Security, Taxmann India Private Limited, New Delhi India.
18. Kamath Nandan (2012); Law relating to Computer, Internet and e-Commerce (A Guide to Cyber Laws) 5th Edition, Delhi Book House.
19. Kandpal & Singh (2013); "Latest Face of Cybercrime and Its Prevention in India, Vol. 2, pp.150-156.
20. KPMG (2014); Cyber Crime: Survey Report – 2014, Forensic Technology Services, KPMG India.
21. KPMG International (2011); Issues Monitor "Cyber Crime – A Growing Challenge for Governments July, Vol. 8.

22. Kumar D. Vinay (2012) Cyber Crime Prevention and Role of Libraries, Vol. 3, pp 222-224.

23. Kumar Shiva V., (2015); "Cyber Crime Prevention and Detection", Andhra Pradesh Police Academy.

24. Malik Kulwant (2011), "Emergence of Cyber Crime in India", International Referred Research Journal, Vol. 2, ISSUE 22, ISSN-0975-3486, RNI: RAJBIL 2009/30097.

25. Mathew et al.; "Cyber security solutions for DLMS meters using GSM/GPRS Technology".

26. Mistry Nilay, et al. (2014); "Preventive Actions to Emerging Threat in Smart Devices Security",Vol.1, May, pp. 20-26.

27. Nagpal Rohas (2008) Introduction to Indian Cyber Law, Asian School of Cyber Laws, Pune, India

28. Nagpal Rohas (2010); "Cyber Crime & Digital Evidence – Indian Perspective"; Real World Cyber Crime Cases, Asian School of Cyber Crime.

29. Lasheng Yu and Chantal Mutimukwe (2009); "Agent Based Distributed Intrusion Detection System (ABDIDS)" ISBN 978-952-5726-07-7 (Print), 978-952-5726-08-4 (CD-ROM) Proceedings of the Second Symposium International Computer Science and Computational Technology (ISCSCT'09) Huangshan, P. R. China, 26-28, pp. 134-138.

30. Peiravi Ali and Peiravi Mehdi (2010), "Internet security - Cyber Crime Paradox", Journal of American Science; Vol. 6, No. 1, pp. 15-24 (ISSN: 1545-1003).

31. Petri Daniel; An Introduction to Trojan Horse VIRUS", (unpublished).

32. Pladna Brett, "The Lack of Attention in the Prevention of Cyber Crime and How to improve it", East Carolina University, ICTN6883.

33. Saini Hemraj et al. (2013); Cyber-Crimes and their Impacts: A Review", Vol. 2, March April, pp.202-209.

34. Scarfone and Mell (2007) "Guide to Intrusion Detection and Prevention Systems (IDPS)", National Institute of Standards and Technology Special Publication 800-94, pp. 94, 127.

35. Shankar Rao et al. (2012); "Cyber-Crimes and Their Impacts: A Review", International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 2, 2012, pp.202-209 ISSN: 2248-9622. Source: www.ijera.com.

36. Sheakh Taraq Hussain (2012), "Cyber Law: Provisions and Anticipation", Vol. 53, Sep, pp. 10-12.

37. Singh Talwant, (2011) Cyber Law & Information Technology, New Delhi, India.

38. Singh Yatinder (Justice), Cyber Law, Delhi Book House, New Delhi.

39. Suri and Chhabra, (2003) Cyber Crime Pentagon Press, New Delhi, India.

40. Sylvester Gerard (2007), "Cyber Crime", The SAMACHAR, pp. 40, 43.

41. Tanwar Ashwani (2012),"Legal Perspective of Cyber Crimes in India," Vol. 3, Feb, pp. 35-36.

42. Thapa Anju and Dr. Kumar Raj (2011); "Cyber Stalking: Crime and Challenge at the Cyberspace", Vol. 2, pp. 2229- 6166.

43. Threat from the Internet-Cyber war (2010); "It is time for countries to start talking about arms control on the internet", The Economist, Available at http:/ www.economist.com/node/16481504 (Last Accessed: October 24, 2016).

44. Verizon (2011): 2010 Data Breach Investigations Report, Verizon/US Secret Services, 2011.

***

End Notes

1. See ITU on Global ICT Data and ICT Development Index. Available at http://www.itu.int/net/pressoffice/press_releases/2015/57.aspx#.V_SZfvl97IU
2. Indian Express. Report on "India Ranks 131 on Global Index of Information And Communication Technology Access" Available at http://indianexpress.com/article/india/india-news-india/india-ranks-131-on-global-index-of-information-and-communication-technology-access-report/ (December 1, 2015)
3. Internet Live Data, Available at http://www. internetlivestats.com/internet-users/
4. Internet World Stat – Usage and Population Statistics, Available at http://www.internetworldstats.com/top20.htm
5. See https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/
6. NCRB Report on Cyber Crime. Available at http://ncrb.nic.in/StatPublications/CII/CII2014/chapters/Chapter%2018.pdf
7. Big Box Breach: The Inside Story of WalMart's Hacker Attack; Available at https://www.wired.com/2009/10/walmart-hack/
8. IRCTC Website Hacked, Personal Data of 1 Crore User at Risk. Source : http://daily.bhaskar.com/news/TOP-irctc-website-hacked-data-of-lakhs-leaked-5316549-PHO.html?ref=bkh
9. Inside Story: Government Websites at the mercy of hackers. Source : http://www.rediff.com/news/slide-show/slide-show-1-inside-story-govt-websites-at-the-mercy-of-hackers/20130314.htm
10. *Avnish Bajaj* v. *State (N.C.T.) of Delhi*

11. 2006, Cri LJ, 3463, Raj 2411
12. AIR 2006 Ker 279, 2006 (3) KLT 210, 2007 (34) PTC 98 Ker.
13. 2006 (1) ALD Cri 96, 2005 CriLJ 4314
14. 2003 VIIAD Delhi 1, 107 (2003) DLT 385, 2003 (71) DRJ 178, 2003 (3) JCC 1669
15. S. 43: Penalty and compensation for damage to computer, computer system, etc
16. [1988] 1 AC 1063 (HL)
17. (1997)20/11/1997
18. Jun 11, 2010 - No. 2003 of 2010
19. Email Threat to BSE. Source: http://timesofindia.indiatimes.com/india/Email-threat-for-BSE/articleshow/4483587.cms
20. 4680 of 2004 Criminal Complaint.
21. 4680 of 2004 Criminal Complaint.
22. (2005) 3 CompLJ 364 Del
23. 2008 (1) Bom.C.R 670. Bench: P J.N., S A.A.
24. 1973 AIR 106, 1973 SCR (2) 757
25. 10th Jan, 2013 CRR No.66 of 2013 (O&M)
26. AIR 2005 712
27. (2005) 3 Comp LJ 364 (Del)
28. MANU/TN/9663/2007
29. 2005 Cri LJ 4314
30. 2008 (36) PTC 614 Mad
31. 2005 Cri L J 4314
32. Suit No. 1279/2001, Delhi High Court
33. 119 (2005) DLT 596, 2005 (30) PTC 437 Del
34. 4680 of 2004 Criminal Complaint.
35. Crl.P.No.7207 OF 2009 19-04-2011

36. 118 (2005) DLT 580, 2005 (30) PTC 245 Del
37. (2011 (46) PTC 38 (Del.)
38. 2010
39. 2004 (28) PTC 566 (SC)
40. 776 F. Supp. 135 (S.D.N.Y.1991)
41. II (2003) BC 96
42. 1998 WL 307001 (1998)
43. [2006] 144 STC 59 (Kar)
44. 2008
45. 2001
46. AIR2006 Ker 279, 2006
47. 7313 of 2002 and W.P.M.P.No. 10120 of 2002
48. 937 F.Supp. 295 (SDNY, 1996)
49. No 00-795
50. 2011
51. Southwark [Crown Court, 30/6/1999].
52. 2009
53. 2013
54. 2005
55. 97 CIF. 1190 (PKL)
56. Source : The Economic Times, October 20, 2016. http://economictimes.indiatimes.com/industry/banking/finance/banking/3-2-million-debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-and-axis-worst-hit/articleshow/54945561.cms

Web - Resources

1. https://cybercrimelawyer.wordpress.com/category/66c-punishment-for-identity-theft/
2. www.met.police.uk/pceu/documents/ACPOecrime strategy.pdf
3. www.cyberlawsindia.net
4. www.economictimes.indiatimes.com/
5. http://www.enotes.com/research-starters/social-impacts-cyber-crime
6. http://en.wikipedia.org/wiki/Computer_crime
7. http://in.norton.com/
8. http://ncrb.nic.in/
9. www.ncpc.org
10. http://deity.gov.in/
11. http://cybercellmumbai.gov.in/
12. http://ncrb.gov.in/
13. http://catindia.gov.in/Default.aspx
14. http://www.cert-in.org.in/
15. http://cca.gov.in/rw/pages/index.en.do
16. www.safescrypt.com
17. www.nic.in
18. www.idrbtca.org.in
19. www.tcs-ca.tcs.co.in
20. www.mtnltrustline.com

21. www.ncodesolutions.com

22. www.e-Mudhra.com

23. www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_ activity _Interface2008/567_prov guidelines _ provisional 2_3April2008_fr.pdf

24. www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/103537.pdf

25. http://userpage.fu-berlin.de/~jmueller/its/conf/Madrid02/abstracts/Ghernaouti-Helie.pdf

***