AN INTRODUCTION TO CYBER LAWS WITH SPECIFIC REFERENCE TO INDIA

Rajkumar S. Adukia
B.Com (Hons.), FCA, ACS, AICWA, LLB
098200 61049
rajkumarfca@gmail.com
www.carajkumarradukia.com

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

The term "Cyber" is understood as computer and the mathematical analysis of the flow of information. The word "Cyber" comes from the Greek word for navigator originating in kybernété s meaning "helmsman

Internet and World Wide Web

The Internet is a global system of interconnected computer networks that use the standardized Internet Protocol Suite (TCP/IP). It is a network of networks that consists of millions of private and public, academic, business, and government networks of local to global scope that are linked by copper wires, fiber-optic cables, wireless connections, and other technologies. The Internet carries a vast array of information resources and services, most notably the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support electronic mail, in addition to popular services such as online chat, file transfer and file sharing, online gaming, and Voice over Internet Protocol (VoIP) person-to-person communication via voice and video.

The origins of the Internet reach back to the 1960s when the United States funded research projects of its military agencies to build robust, fault-tolerant and distributed computer networks. This research and a period of civilian funding of a new U.S. backbone by the National Science Foundation spawned worldwide participation in the development of new networking

technologies and led to the commercialization of an international network in the mid 1990s, and resulted in the following popularization of countless applications in virtually every aspect of modern human life. As of 2009, an estimated quarter of Earth's population uses the services of the Internet.

The terms Internet and World Wide Web are often used in everyday speech without much distinction. However, the Internet and the World Wide Web are not one and the same. The Internet is a global data communications system. It is a hardware and software infrastructure that provides connectivity between computers. In contrast, the Web is one of the services communicated via the Internet. It is a collection of interconnected documents and other resources, linked by hyperlinks and Uniform Resource Locator [URLs]

The World Wide Web was invented in 1989 by the English physicist Tim Berners-Lee, now the Director of the World Wide Web Consortium, and later assisted by Robert Cailliau, a Belgian computer scientist, while both were working at CERN in Geneva, Switzerland. In 1990, they proposed building a "web of nodes" storing "hypertext pages" viewed by "browsers" on a network and released that web in December

Cyber Law

Cyber law is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less a distinct field of law in the way that property or contract are, as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to apply laws designed for the physical world to human activity on the Internet.

There is no one exhaustive definition of the term “Cyberlaw”. Simply speaking, Cyberlaw is a generic term which refers to all the legal and regulatory aspects of Internet and the World Wide Web.

A Law encompasses the rules of conduct:

1. That have been approved by the government, and

2. Which are in force over a certain territory, and

3. Which must be obeyed by all persons on that territory

Violation of these rules could lead to government action such as imprisonment or fine or an order to pay compensation**.**

Cyber law encompasses laws relating to:

1. Cyber Crimes
2. Electronic and Digital Signatures
3. Intellectual Property
4. Data Protection and Privacy

Need for Cyber law

In today's techno-savvy environment, the world is becoming more and more digitally sophisticated and so are the crimes. Internet was initially developed as a research and information sharing tool and was in an unregulated manner. As the time passed by it became more transactional with e-business, e-commerce, e-governance and e-procurement etc. All legal issues related to internet crime are dealt with through cyber laws. As the number of internet users is on the rise, the need for cyber laws and their application has also gathered great moment

Key words related to cyber crimes

Cyber Defamation: This occurs when defamation takes place with the help of computers and or the Internet e.g. someone published defamatory matter about someone on a websites or sends e-mail containing defamatory information to all of that person's friends.

Cyber Pornography: This would include pornographic websites; pornographic magazines produced using computer and the Internet (to down load and transmit pornographic pictures, photos, writings etc.)

Cyber Stalking: Cyber stalking involves following a person's movements across the Internet by posting messages on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim

Data diddling: This kind of an attack involves altering the raw data just before it is processed by a computer and then changing it back after the processing is completed

Denial of Service: This involves flooding computer resources with more requests than it can handle. This causes the resources to crash thereby denying authorized users the service offered by the resources.

E-Mail bombing: Email bombing refers to sending a large amount of e-mails to the victim resulting in the victims' e-mail account or mail servers.

E-Mail spoofing: A spoofed email is one that appears to originate from one source but actually has been sent from another source. This can also be termed as E-Mail forging

Financial Claims: This would include cheating, credit card frauds, money laundering etc.
Forgery: Counterfeit currency notes, postage and revenue stamps, mark sheets etc., can be forged using sophisticated computers, printers and scanners.

Internet Time Theft: This connotes the usage by unauthorized persons of the Internet hours paid for by another person.

Logic bombs: These are dependent programs. This implies that these programs are created to do something only when a certain event occurs, e.g. some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date.

Online gambling: There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

"Phishing" is derived from the word "fishing", and it means luring or enticing an unwary customer of a Banking or Financial Institution to pass on sensitive information pertaining to their account. Scamsters then use this information to siphon off funds or, undertake transactions that are billed to the original customer.

Physically damaging a computer system:
This crime is committed by physically damaging a computer or its peripherals.

Salami attacks: 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.

Sale of illegal articles: This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, bulletin boards or simply by using e-mail communications.

Theft of information contained in electronic from: This includes information stored in computer hard disks, removable storage media etc.

Trojan horse: A Trojan as this program is aptly called, is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

Unauthorized access to computer system or network: This activity is commonly referred to as hacking. The Indian Law has however given a different connotation to the term hacking.

Virus/worm: 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. Worms, unlike viruses don not need the host to attach themselves to.

Chapter 2

CYBER CRIMES

Cyber crimes are unlawful acts where the computer is used either as a tool or a target or both. The enormous growth in electronic commerce (e-commerce) and online share trading has led to a phenomenal spurt in incidents of cyber crime.

United Nations' Definition of Cybercrime

At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined thus:

a. Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

b. Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

Of course, these definitions are complicated by the fact that an act may be illegal in one nation but not in another.

There are more concrete examples, including

i. Unauthorized access

ii Damage to computer data or programs

iii Computer sabotage

iv Unauthorized interception of communications

v Computer espionage

First recorded cyber crime

The first recorded cyber crime took place in the year 1820! That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around

since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage.

In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber crime!

Common types of Cyber Crimes may be broadly classified in the following groups:-

1 Against Individuals: -

a. Against Person: -

i. Harassment through e-mails.

ii. Cyber-stalking.

iii. Dissemination of obscene material on the Internet.

iv. Defamation.

v. Hacking/cracking.

vi. Indecent exposure.

b. Against property of an individual: -

i. Computer vandalism.

ii. Transmitting virus.

iii. Internet intrusion.

iv. Unauthorised control over computer system.

v. Hacking /cracking.

2 Against Organisations: -

a. Against Government, Private Firm, Company, Group of Individuals: -

i. Hacking & Cracking.

ii. Possession of unauthorised information.

iii. Cyber terrorism against the government organisation.

iv. Distribution of pirated software etc.

3. Against Society at large: -

i. Pornography (especially child pornography).

ii. Polluting the youth through indecent exposure.

iii. Trafficking.

Cyber crimes in India - Snapshots 2007 [National crimes records bureau [Ministry of home Affairs]

- Cyber Crimes (IT Act + IPC Sections) increased by 22.7% in 2007 as compared to 2006 (from 453 in 2006 to 556 in 2007)
- Cyber Forgery 64.0% (217 out of total 339) and Cyber Fraud 21.5% (73 out of 339) were the main cases under IPC category for Cyber Crimes.
- 63.05 of the offenders under IT Act were in the age group 18-30 years (97 out of 154) and 55.2% of the offenders under IPC Sections were in the age group 30-45 years (237 out of 429).

INTERNATIONAL INITIATIVES

To meet the challenge posed by new kinds of crime made possible by computer technology including telecommunication, many countries have also reviewed their respective domestic criminal laws so as to prevent computer related crimes. Some of these countries are USA, Austria, Denmark, France Germany, Greece, Finland, Italy, Turkey, Sweden, Switzerland, Australia, Canada, India, Japan, Spain, Portugal, UK, Malaysia and Singapore.

In 1997, The G-8 Ministers agreed to ten "Principles to Combat High-Tech Crime" and an "Action Plan to Combat High-Tech Crime"

Principles to Combat High-Tech Crime

1. There must be no safe havens for those who abuse information technologies.
2. Investigation and prosecution of international high-tech crimes must be coordinated among all concerned States, regardless of where harm has occurred.
3. Law enforcement personnel must be trained and equipped to address high-tech crimes.
4. Legal systems must protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized.
5. Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.
6. Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.
7. Trans-border electronic access by law enforcement to publicly available (open source) information does not require authorization from the State where the data resides.
8. Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed and employed.
9. To the extent practicable, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence.
10. Work in this area should be coordinated with the work of other relevant international fora to ensure against duplication of efforts.

Action Plan to Combat High-Tech Crime

In support of the PRINCIPLES, we are directing our officials to:

1. Use our established network of knowledgeable personnel to ensure a timely, effective response to transnational high-tech cases and designate a point-of-contact who is available on a twenty-four hour basis.

2. Take appropriate steps to ensure that a sufficient number of trained and equipped law enforcement personnel are allocated to the task of combating high-tech crime and assisting law enforcement agencies of other States.

3. Review our legal systems to ensure that they appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes.

4. Consider issues raised by high-tech crimes, where relevant, when negotiating mutual assistance agreements or arrangements.

5. Continue to examine and develop workable solutions regarding: the preservation of evidence prior to the execution of a request for mutual assistance; transborder searches; and computer searches of data where the location of that data is unknown.

6. Develop expedited procedures for obtaining traffic data from all communications carriers in the chain of a communication and to study ways to expedite the passing of this data internationally.

7. Work jointly with industry to ensure that new technologies facilitate our effort to combat high-tech crime by preserving and collecting critical evidence.

8. Ensure that we can, in urgent and appropriate cases, accept and respond to mutual assistance requests relating to high-tech crime by expedited but reliable means of communications, including voice, fax, or e-mail, with written confirmation to follow where required.

9. Encourage internationally-recognized standards-making bodies in the fields of telecommunications and information technologies to continue providing the public and private sectors with standards for reliable and secure telecommunications and data processing technologies.

10. Develop and employ compatible forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions.

Convention on Cybercrime

Representatives from the 26 Council of Europe members, the United States, Canada, Japan and South Africa in 2001 signed a convention on cybercrime in efforts to enhance international cooperation in combating computer-based crimes.

The Convention on Cybercrime, drawn up by experts of the Council of Europe, is designed to coordinate these countries' policies and laws on penalties on crimes in cyberspace, define the formula guaranteeing the efficient operation of the criminal and judicial authorities, and establish an efficient mechanism for international cooperation

ROLE OF INTERPOL

http://www.interpol.int/default.asp

The Interpol General Secretariat has harnessed the expertise of its members in the field of Information Technology Crime (ITC) through the vehicle of a 'working party' or a group of experts. In this instance, the working party consists of the heads or experienced members of national computer crime units. These working parties have been designed to reflect regional expertise and exist in Europe, Asia, America and in Africa. All working parties are in different stages of development. It should be noted that the work done by the working parties is not Interpol's only contribution to combating ITC, but it certainly represents the most noteworthy contribution to date.

Regional Working Parties

1. European Working Party on Information Technology Crime
2. African Regional Working Party on Information Technology Crime
3. Asia - South Pacific Working Party on Information Technology Crime
4. Latin America Working Party on Information Technology Crime

Chapter 3
ELECTRONIC SIGNATURES

Electronic signatures are used to authenticate electronic records. Digital signatures are one type of electronic signature. Digital signatures satisfy three major legal requirements

i. signer authentication
ii. message authentication and
iii. Message integrity.

History

Since well before the American Civil War began in 1861, morse code was used to send messages electronically by telegraphy. Some of these messages were agreements to terms that were intended as enforceable contracts. An early acceptance of the enforceability of telegraphic messages as electronic signatures came from the New Hampshire Supreme Court in 1869.[6]
In the 1980s, many companies and even some individuals began using fax machines for high-priority or time-sensitive delivery of documents. Although the original signature on the original document was on paper, the image of the signature and its transmission was electronic.[7]
Courts in various jurisdictions have decided that enforceable electronic signatures can include agreements made by email, entering a personal identification number (PIN) into a bank ATM, signing a credit or debit slip with a digital pen pad device (an application of graphics tablet technology) at a point of sale, installing software with a clickwrap software license agreement on the package, and signing electronic documents online.[citation needed]
The first agreement signed electronically by two sovereign nations was a Joint Communiqué recognizing the growing importance of the promotion of electronic commerce, signed by the United States and Ireland in 1998

An electronic signature may incorporate a digital signature if it uses cryptographic methods to assure, at the least, both message integrity and authenticity. Cryptography (or cryptology; from Greek κρυπτός, kryptos, "hidden, secret"] is the practice and study of hiding information.
In modern times cryptography is considered a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering.

A technical definition of 'cryptography', is often referred to as "the art and science of keeping messages secure".

Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords and electronic commerce which all depend on cryptography.

Until modern times cryptography was referred almost exclusively to encryption.

Encryption means the process of converting ordinary information (plaintext) into a difficult-to-interpret format (unintelligible gibberish i.e., ciphertext), a sa mechanism for protecting its confidentiality, integrity and sometimes its authenticity. Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext.

Encryption uses a cryptographic algorithm and a key to encode a message into ciphertext. The intended recipient uses a key to decode, the message back into its original form. If the cryptographic algorithm is strong, and the key properly selected and kept secret, it is infeasible for an unauthorized party to intercept the ciphertext and decrypt it back into plaintext.

Public-Key Cryptography

Asymmetric cryptography, also called public key cryptography, is a relatively new field, it was invented by Diffie and Hellman in 1976.

Whitfield Diffie and Martin Hellman proposed the notion of public-key (also, more generally, called asymmetric key) cryptography in which two different but mathematically related keys are used — a public key and a private key.

A public key system is so constructed that calculation of one key (the 'private key') is computationally infeasible from the other (the 'public key'), even though they are necessarily related. Instead, both keys are generated secretly, as an interrelated pair.

In public-key cryptosystems, the public key may be freely distributed, while its paired private key must remain secret. The public key is typically used for encryption, while the private or secret key is used for decryption.

An emerging form of electronic signatures is defined as “Biometric Signature” or “Dynamic Signature”. The term stands for handwritten signatures that are digitized throughout the writing process – including static characteristics and biometric (dynamic) signals”. Instead of replacing the handwritten signature these kind of e-signing solutions seek to transfer the signing ceremony into the digital world. “Biometric Signatures” require a hardware device for

signature capturing and a software which is able to combine the signature data, encrypt it and allows to detect later manipulation by creating a hash value.
Another approach is to attach some biometric measurement to a document as evidence of signature. For instance, fingerprints or iris patterns or and geometry (finger lengths and palm size) or even retinal patterns. All of these are collected using electronic sensors of some kind. Since each of these physical characteristics has claims to uniqueness among humans, each is to some extent useful as a signature method.

A digital signature is a type of electronic signature that arises from applying public-key cryptography to ensure, user authentication and contains additional functionality, to further ensure message authentication.

There is a subtle difference between "digital signature" and "electronic signature". A digital signature, is distinguished as a *species*, of its *genus* the more generic, 'electronic signature', which is used to describe any form of electronic authentication.

Digital Signatures- Indian Legislation

The Information Technology Act, 2000 provides for use of Digital Signatures on the documents submitted in electronic form in order to ensure the security and authenticity of the documents filed electronically. This is the only secure and authentic way that a document can be submitted electronically. As such, all filings done by the companies under MCA21 e-Governance programme are required to be filed with the use of Digital Signatures by the person authorised to sign the documents.
The Information Technology (Amendment) Act 2008, substitutes the words "electronic signature" for the words "digital signature" used in the Information Technology Act 2000.

"Electronic Signature" as per section 2(ta) of the IT(A) Act 2008, means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature"

"Electronic Record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

Certification Agencies: Certification Agencies are appointed by the office of the Controller of Certification Agencies (CCA) under the provisions of IT Act, 2000. There are a total of seven Certification Agencies authorised by the CCA to issue the Digital Signature Certificates (DSCs). The details of these Certification Agencies are available on the portal of the Ministry **www.mca.gov.in**

Class of DSCs: The Ministry of Company Affairs has stipulated a Class-II or above category certificate for e-filings under MCA21. A person who already has the specified DSC for any other application can use the same for filings under MCA21 and is not required to obtain a fresh DSC.

Validity of Digital Signatures: The DSCs are typically issued with one year validity and two year validity. These are renewable on expiry of the period of initial issue.

Costing/ Pricing of Digital Signatures: It includes the cost of medium (a UBS token which is a onetime cost), the cost of issuance of DSC and the renewal cost after the period of validity. The company representatives and professionals required to obtain DSCs are free to procure the same from any one of the approved Certification Agencies as per the web site. The issuance costs in respect of each Agency vary and are market driven.

Chapter 4

INTELLECTUAL PROPERTY

Intellectual property is refers to creations of the human mind e.g. a story, a song, a painting, a design etc. The facets of **intellectual property** that relate to cyber space are covered by Cyber law includes:

a) copyright law in relation to computer software, computer source code, websites, cell phone content etc,

b) software and source code licences

c) trademark law with relation to domain names, meta tags, mirroring, framing, linking etc

d) semiconductor law which relates to the protection of semiconductor integrated circuits design and layouts,

e) patent law in relation to computer hardware and software

The Indian Legislations on the above are

a) The Copyrights Act, 1957 and The Copyrights Rules, 1958
b) The Patents Act, 1970 and The Patents Rules, 2003
c) The Semiconductors Integrated Circuits Layout-Design Act, 2000 and The Semiconductors Integrated Circuits Layout-Design Rules, 2001
d) The Trade Marks Act, 1999 and The Trade Marks Rules, 2002

Copyright Law and Computer Software

According to section 2(ffc) of the Copyright Act,1957 a **computer program** is a "set of instructions expressed in words, codes, schemes or in any other form, including a machine readable medium, capable of causing a computer to perform a particular task or achieve a particular results".
Computer **software** is "computer program" within the meaning of the Copyright Act, 1957.Computer programs are included in the definition of **literary work** under the Copyright Act, 1957

Sec 2 (o) "literary work" includes computer programmes, tables and compilations including computer "literary data bases;

Sec 14 of the Copyright Act,1957 defines "copyright" to mean the exclusive right subject to the provisions of this Act, to do or authorise the doing of any of the following acts in respect of a work or any substantial part thereof, namely:-
14 (b) in the case of a computer programme
(i) to reproduce the work in any material form including the storing of it in any medium by electronic means;
(ii) to issue copies of the work to the public not being copies already in circulation;
(iii) to perform the work in public, or communicate it to the public;
(iv) to make any cinematograph film or sound recording in respect of the work;
(v) to make any translation of the work;

(vi) to make any adaptation of the work;

(vii) to do, in relation to a translation or an adaptation of the work, any of the acts specified in relation to the work

Punishment for copyright infringement

Knowingly using the infringing copy of a computer program on a computer is punishable with:

1. Imprisonment for a term between 7 days and 3 years and
2. Fine between Rs. 1 lakh and Rs. 2 lakh

In case the infringement has not been made for commercial gain, the Court may impose no imprisonment and may impose a fine up to Rs 50,000.

The offence can be tried by a magistrate not below the rank of a Metropolitan Magistrate or a Judicial Magistrate First Class.

In case of offences by companies, persons in charge of the company are also liable unless they prove that the offence was committed:

1. Without their knowledge or
2. despite their due diligence to prevent it.

Chapter 5

DATA PROTECTION AND PRIVACY LAWS

Data protection and privacy laws aim to achieve a fair balance between the privacy rights of the individual and the interests of data controllers such as banks, hospitals, email service providers etc. These laws seek to address the challenges to privacy caused by collecting, storing and transmitting data using new technologies.

Data Protection relates to issues relating to the collection, storage, accuracy and use of data provided by net users in the use of the World Wide Web. Visitors to any website want their privacy rights to be respected when they engage in e-Commerce. It is part of the confidence-creating role that successful e-Commerce businesses have to convey to the consumer

Any transaction between two or more parties involves an exchange of essential information between the parties. Technological developments have enabled transactions by electronic means. Any such information/data collected by the parties should be used only for the specific purposes for which they were collected. The need arose, to create rights for those who have their data stored and create responsibilities for those who collect, store and process such data. The law relating to the creation of such rights and responsibilities may be referred to as 'data protection' law.

The world's first computer specific statute was enacted in the form of a Data Protection Act, in the German state of Hesse, in 1970.The misuse of records under the Nazi regime had raised concerns among the public about the use of computers to store and process large amounts of personal data.[The Data Protection Act sought to heal such memories of misuse of information. A different rationale for the introduction of data protection legislation can be seen in the case of Sweden which introduced the first national statute in 1973.Here, data protection was seen as fitting naturally into a two hundred year old system of freedom of information with the concept of subject access (such a right allows an individual to find out what information is held about him) being identified as one of the most important aspects of the legislation.In 1995, the European Union adopted its Directive (95/46/EC) of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter, the Directive), establishing a detailed privacy regulatory structure.The Directive is specific on the requirements for the transfer of data. It sets down the principles regarding the transfer of data to third countries and states that personal data of EU nationals cannot be sent to countries that do not meet the EU "adequacy" standards with respect to privacy.In order to meet the EU "adequacy" standards, US developed a 'Safe Harbour' framework, according to which the US Department of Commerce would maintain a list of US companies that have self-certified to the safe harbor framework. An EU organization can ensure that it is sending information to a U.S. organization participating in the safe harbor by viewing the public list of safe harbor organizations posted on the official website.

Data protection has emerged as an important reaction to the development of information technology. In India data protection is covered under the Information Technology Act, 2000

GLOBAL LAWS ON DATA PROTECTION AND INFORMATION SECURITY

- UK Data Protection Act 1998 makes new provisions for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. The European Union Data Protection Directive (EUDPD) requires that all EU members must adopt national regulations to standardize the protection of data privacy for citizens throughout the EU.

- The Computer Misuse Act 1990 is an Act of the UK Parliament making computer crime (e.g. hacking) a criminal offence. The Act has become a model upon which several other countries including Canada and the Republic of Ireland, have drawn inspiration when subsequently drafting their own information security laws.
- EU Data Retention laws requires Internet service providers and phone companies to keep data on every electronic message sent and phone call made for between six months and two years.
- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232 g; 34 CFR Part 99) is a USA Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record.

- Health Insurance Portability and Accountability Act (HIPAA) requires the adoption of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. And, it requires health care providers, insurance providers and employers to safeguard the security and privacy of health data.
- Gramm-Leach-Bliley Act of 1999(GLBA), also known as the Financial Services Modernization Act of 1999, protects the privacy and security of private financial information that financial institutions collect, hold, and process.

- Sarbanes-Oxley Act of 2002 (SOX). Section 404 of the act requires publicly traded companies to assess the effectiveness of their internal controls for financial reporting in annual reports they submit at the end of each fiscal year. Chief information officers are responsible for the security, accuracy and the reliability of the systems that manage and report the financial data. The act also requires publicly traded companies to engage independent auditors who must attest to, and report on, the validity of their assessments.
- Payment Card Industry Data Security Standard (PCI DSS) establishes comprehensive requirements for enhancing payment account data security. It was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

- State Security Breach Notification Laws (California and many others) require businesses, nonprofits, and state institutions to notify consumers when unencrypted "personal information" may have been compromised, lost, or stolen.
- Personal Information Protection and Electronics Document Act (PIPEDA) - An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act Thant is in fact the case.

Chapter 6

CYBER TERRORISM

Cyber crime and cyber terrorism are both crimes of the cyber world. The difference between the two however is with regard to the motive and the intention of the perpetrator.

While a cyber crime can be described simply as an unlawful act wherein the computer is either a tool or a target or both, cyber terrorism deserves a more detailed definition. One can define cyber terrorism as a premeditated use of disruptive activities or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives.

Cyber terrorist prefer using the cyber attack methods because of many advantages for it.

a) The action is very difficult to be tracked.
b) They can hide their personalities and location.
c)They can do it remotely from anywhere in the world.
d) a big number of targets can be attacked

Cyber terrorism may take the form of Privacy violations; Secret information appropriation and data theft; Demolition of e-governance base and network damage and disruptions

Chapter 7

CYBER SECURITY STANDARDS

They are security standards which enable organizations to practice safe security techniques in order to minimize the number of successful cyber security attacks. These guides provide general outlines as well as specific techniques for implementing cyber security. For certain specific standards, cyber security certification by an accredited body can be obtained. There are many advantages to obtaining certification including the ability to get cyber security insurance

International Organization for Standardization (ISO) is a consortium of national standards institutes from 157 countries with a Central Secretariat in Geneva Switzerland that coordinates the system. The ISO is the world's largest developer of standards. The ISO-15443: "Information technology - Security techniques - A framework for IT security assurance", ISO-17799: "Information technology - Security techniques - Code of practice for information security management", ISO-20000: "Information technology - Service management", and ISO-27001: "Information technology - Security techniques - Information security management systems" are of particular interest to information security professionals.

The USA National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. The NIST Computer Security Division develops standards, metrics, tests and validation programs as well as publishes standards and guidelines to increase secure IT planning, implementation, management and operation. NIST is also the custodian of the USA Federal Information Processing Standard publications (FIPS)].

The Internet Society (ISOC) is a professional membership society with more than 100 organization and over 20,000 individual members in over 180 countries. It provides leadership in addressing issues that confront the future of the Internet, and is the organization home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). The ISOC hosts the Requests for Comments (RFCs) which includes the Official Internet Protocol Standards and the RFC-2196 Site Security Handbook.

The Information Security Forum is a global nonprofit organization of several hundred leading organizations in financial services, manufacturing, telecommunications, consumer goods, government, and other areas. It provides research into best practice and practice advice summarized in its biannual Standard of Good Practice, incorporating detail specifications across many areas.

Chapter 8

Cyber Forensics

Forensic – as per the dictionary definition relates to the use of science and technology for establishment of facts or evidence in a court of law. Similarly Cyber Forensic helps extract information from computer storage and other media to establish facts in a manner that can be presented in the court of law.

Cyber Forensics is a new and developing field, which can be described as the study of digital evidence resulting from an incidence of crime. Cyber Forensics professionals are not just

required by enterprises for their information security, but also by government agencies to keep track of nation's cyber security and preserve it from malicious attacks.

There are many reasons to employ the techniques of computer forensics:

- In legal cases, computer forensic techniques are frequently used to analyze computer systems belonging to defendants (in criminal cases) or litigants (in civil cases).
- To recover data in the event of a hardware or software failure.
- To analyze a computer system after a break-in, for example, to determine how the attacker gained access and what the attacker did.
- To gather evidence against an employee that an organization wishes to terminate.
- To gain information about how computer systems work for the purpose of debugging, performance optimization, or reverse-engineering.

Chapter 9

INDIAN LEGAL FRAMEWORK

Need for cyber law in India

Firstly, India has an extremely detailed and well-defined legal system in place. Numerous laws have been enacted and implemented and the foremost amongst them is The Constitution of India. We have inter alia, amongst others, the Indian Penal Code, the Indian Evidence Act 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934, the Companies Act, and so on. However the arrival of Internet signaled the beginning of the rise of new and complex legal issues. All the existing laws in place in India were enacted way back keeping in mind the relevant political, social, economic, and cultural scenario of that relevant time. Nobody then could really visualize about the Internet. The coming of the Internet led to the emergence of numerous ticklish legal issues and problems which necessitated the enactment of Cyber laws.

Secondly, the existing laws of India, even with the most benevolent and liberal interpretation, could not be interpreted in the light of the emerging cyberspace, to include all aspects relating to different activities in cyberspace. In fact, the practical experience and the wisdom of judgment found that it shall not be without major perils and pitfalls, if the existing laws were to be interpreted in the scenario of emerging cyberspace, without enacting new cyber laws.

Thirdly, none of the existing laws gave any legal validity or sanction to the activities in Cyberspace. For example, the Net is used by a large majority of users for email. Yet till today, email is not "legal" in our country. There is no law in the country, which gives legal validity, and sanction to email. Courts and judiciary in our country have been reluctant to grant judicial recognition to the legality of email in the absence of any specific law having been enacted by the Parliament. As such the need has arisen for Cyber law.

Fourthly, Internet requires an enabling and supportive legal infrastructure in tune with the times. This legal infrastructure can only be given by the enactment of the relevant Cyber laws as the traditional laws have failed to grant the same. E-commerce, the biggest future of Internet, can only be possible if necessary legal infrastructure compliments the same to enable its vibrant growth.

All these and other varied considerations created a conducive atmosphere for the need for enacting relevant cyber laws in India.

Matters relating to Cyber Laws, administration of the Information Technology Act 2000 (21 of 2000) and other IT related laws are controlled by the Department of Information Technology, Ministry of Communications & Information Technology Government of India.

A) Emergence of Information Technology Act, 2000

In India the Information Technology Act 2000 was enacted after the United Nation General Assembly Resolution A/RES/51/162, dated the 30th January, 1997 by adopting the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. This was the first step towards the Law relating to e-commerce at international level to regulate an alternative form of commerce and to give legal status in the area of e-commerce. It was enacted taking into consideration UNICITRAL model of Law on e- commerce 1996.

The IT Act 2000 was enacted on 9th June 2000 and was notified in the official gazette on 17th October 2000.

The IT Act, 2000 consists of 90 sections [Sections 91, 92, 93 and 94 of the principal Act were omitted by the Information Technology (Amendment) Act 2008 and has 2 schedules.[III AND IV Schedules were omitted by the Information Technology (Amendment) Act 2008]

Some important provisions of the Act are listed below:

- Chapter-I deals with the applicability of the Act and important definitions. The IT Act, 2000 will not apply to –
    - a negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881;
    - a power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;
    - a trust as defined in section 3 of the Indian Trusts Act, 1882;
    - a will as defined in clause *(h)* of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called;
    - any contract for the sale or conveyance of immovable property or any interest in such property; and
    - any such class of documents or transactions as may be notified by the Central Government in the Official Gazette
- Chapter-II of the Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by use of a public key of the subscriber.
- Chapter-III of the Act details about Electronic Governance and provides inter alia amongst others that where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is –
    - Rendered or made available in an electronic form and
    - Accessible so as to be usable for a subsequent reference.

This chapter also deals with the legal recognition of digital signatures.

- Chapter-IV of the Act deals with attribution, acknowledgement and dispatch of electronic records.
- Chapter-V of the Act deals with secure electronic records, secure digital signatures and the security procedure involved in such transactions.
- Chapter-VI of the said Act gives a scheme for Regulation of Certifying Authorities. The Act envisages a Controller of Certifying Authorities who shall perform the function of exercising supervision over the activities of the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities as also specifying the various forms and content of Digital Signature Certificates. The Act recognizes the need for recognizing foreign Certifying Authorities and it further details the various provisions for the issue of license to issue Digital Signature Certificates.
- Chapter-VII of the Act details about the scheme of things relating to Digital Signature Certificates.
- Chapter-VIII deals with the duties of subscriber of the Digital Signature Certificate.
- Chapter-IX of the said Act talks about penalties and adjudication for various offences. The penalties for damage to computer, computer systems etc. has been fixed as damages by way of compensation not exceeding Rupees One Crore to affected persons. The Act talks of appointment of any officers not below the rank of a Director to the Government of India or an equivalent officer of state government as an Adjudicating Officer who shall adjudicate whether any person has made a contravention of any of the provisions of the said Act or rules framed there under. The said Adjudicating Officer has been given the powers of a Civil Court.
- Chapter-X of the Act talks of the establishment of the Cyber Regulations Appellate Tribunal, which shall be an appellate body where appeals against the orders passed by the Adjudicating Officers, shall be preferred.
- Chapter-XI of the Act talks about various offences and the said offences shall be investigated only by a Police Officer not below the rank of the Deputy Superintendent of Police. These offences include tampering with computer source documents, publishing of information, which is obscene in electronic form, and hacking.

- Chapter XII deals with cases where the network service providers will not be liable for offences or contraventions under the Act.
- The Act also provides for the constitution of the Cyber Regulations Advisory Committee, which shall advice the government as regards any rules, or for any other purpose connected with the said act. The said Act also proposes to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the IT Act.

Key definitions- Sec 2(1)

(i) **"Computer"** means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

(j) **"computer network"** means the interconnection of one or more computers through—
(i) the use of satellite, microwave, terrestrial line or other communication media; and
(ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

(k) **"computer resource"** means computer, computer system, computer network, data, computer data base or software;

(l) **"computer system"** means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

(o) "**data**" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

(p) "**digital signature**" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

(q) "**Digital Signature Certificate**" means a Digital Signature Certificate issued under subsection (4) of section 35;

(r) **"electronic form"** with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

(t) **"electronic record**" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

(v) **"information"** includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche:

(w**) "intermediary"** with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;

Provisions under The Information Technology Act, 2000 on Penalty and Contraventions

- Sec.43 Damage to Computer system etc.-Compensation for Rupees 1crore.
- Sec.66 Hacking (with intent or knowledge) -Fine of 2 lakh rupees, and imprisonment for 3 years.
- Sec.67 Publication of obscene material in e-form -Fine of 1 lakh rupees, and imprisonment of 5years, and double conviction on second offence
- Sec.68 Not complying with directions of controller -Fine upto 2 lakh and imprisonment of 3 years.

- Sec.70 attempting or securing access to computer-Imprisonment upto 10 years.
- Sec.72 For breaking confidentiality of the information of computer -Fine upto 1 lakh and imprisonment up to 2 years
- Sec.73 Publishing false digital signatures, false in certain particulars-Fine of 1 lakh, or imprisonment of 2 years or both.
- Sec.74 Publication of Digital Signatures for fraudulent purpose -Imprisonment for the term of 2 years and fine for 1 lakh rupee

RULES FOR INFORMATION TECHNOLOGY

1. Information Technology (Certifying Authorities) Rules, 2000.

These rules prescribe the eligibility, appointment and working of Certifying Authorities (CA). These rules also lay down the technical standards, procedures and security methods to be used by a CA. These rules were amended in 2003, 2004 and 2006.

One of the most important compliance under this Rule is that the Certifying Authority should get its operations audited annually by an auditor and such audit shall include:

(i) security policy and planning;

(ii) physical security;

(iii) technology evaluation;

(iv) Certifying Authority's services administration;

(v) relevant Certification Practice Statement;

(vi) compliance to relevant Certification Practice Statement;

(vii) contracts/agreements;

(viii) regulations prescribed by the Controller;

(ix) policy requirements of Certifying Authorities Rules, 2000.

The Certifying Authority should also conduct half yearly audit of the Security policy, physical security and planning of its operations and repository.

Information Technology (Certifying Authority) Regulations, 2001 came into force on 9 July 2001. They provide further technical standards and procedures to be used by a Certifying Authority.

Two important guidelines relating to Certifying Authority were issued.

i. Guidelines for submission of application for license to operate as a Certifying Authority under the IT Act. These guidelines were issued on 9th July 2001.

ii. **Guidelines** for submission of certificates and certification revocation lists to the Controller of Certifying Authorities for publishing in National Repository of Digital Certificates. These were issued on 16th December 2002.

2. Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000

These rules prescribe the appointment and working of the Cyber Regulations Appellate Tribunal (CRAT) whose primary role is to hear appeals against orders of the Adjudicating Officers.

The **Cyber Regulations Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Presiding Officer) Rules**, 2003 prescribe the salary, allowances and other terms for the Presiding Officer of the CRAT.

Information Technology (Other powers of Civil Court vested in Cyber Appellate Tribunal) Rules 2003 provided some additional powers to the CRAT.

On 17th March 2003, the **Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules**, 2003 were passed.

These rules prescribe the qualifications required for Adjudicating Officers. Their chief responsibility under the IT Act is to adjudicate on cases such as unauthorized access,

unauthorized copying of data, spread of viruses, denial of service attacks, disruption of computers, computer manipulation etc. These rules also prescribe the manner and mode of inquiry and adjudication by these officers.

B) Information Technology (Amendment) Act 2008

The Government of India proposed major amendments to **Information Technology Act**, 2000 in form of the Information Technology (Amendment) Bill, 2006. The Bill was renamed as Information Technology (Amendment) Bill, 2008 and passed by Indian Parliament in December 2008 notified as the IT (Amendment) Act 2008 and received the assent of the President on the 5th Feb, 2009.

A review of the amendments indicates that there are several provisions relating to data protection and privacy as well as provisions to curb terrorism using the electronic and digital medium that have been introduced into the new Act.

Some of the salient features of the Act are as follows:

- The term "digital signature" has been replaced with "electronic signature" to make the Act more technology neutral.
- A new section has been inserted to define "communication device" to mean cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text video, audio or image.[Sec 2 (ha)]
- A new section has been added to define "cyber café" as any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.[Sec 2 (na)]
- A new definition has been inserted for "intermediary". "Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes, but does not include a body corporate referred to in Section 43A.[Sec 2 (w)]

- A new section 10A has been inserted to the effect that contracts concluded electronically shall not be deemed to be unenforceable solely on the ground that electronic form or means was used.
- The damages of Rs. One Crore (approximately USD 200,000) prescribed under section 43 of the earlier Act for damage to computer, computer system etc has been deleted and the relevant parts of the section have been substituted by the words, "he shall be liable to pay damages by way of compensation to the person so affected".
- A new section 43A has been inserted to protect sensitive personal data or information possessed, dealt or handled by a body corporate in a computer resource which such body corporate owns, controls or operates. If such body corporate is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, it shall be liable to pay damages by way of compensation to the person so affected.
- A host of new sections have been added to section 66 .Sections 66A to 66F prescribe punishment for offenses such as obscene electronic message transmissions, identity theft, cheating by impersonation using computer resource, violation of privacy and cyber terrorism.
- Section 67 of the old Act is amended to reduce the term of imprisonment for publishing or transmitting obscene material in electronic form to three years from five years and increase the fine thereof from Indian Rupees 100,000 (approximately USD 2000) to Indian Rupees 500,000 (approximately USD 10,000). A host of new sections have been inserted as Sections 67 A to 67C.
- While Sections 67 A and B insert penal provisions in respect of offenses of publishing or transmitting of material containing sexually explicit act and child pornography in electronic form, section 67C deals with the obligation of an intermediary to preserve and retain such information as may be specified for such duration and in such manner and format as the central government may prescribe.
- In view of the increasing threat of terrorism in the country, the new amendments include an amended section 69 giving power to the state to issue directions for interception or monitoring of decryption of any information through any computer resource.

- Further, sections 69 A and B, two new sections, grant power to the state to issue directions for blocking for public access of any information through any computer resource and to authorize to monitor and collect traffic data or information through any computer resource for cyber security.
- Section 79 of the old Act which exempted intermediaries has been modified to the effect that an intermediary shall not be liable for any third party information data or communication link made available or hosted by him if; (a) the function 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; (b) the intermediary does not initiate the transmission or select the receiver of the transmission and select or modify the information contained in the transmission; (c) the intermediary observes due diligence while discharging his duties.
- However, section 79 will not apply to an intermediary if the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act or upon receiving actual knowledge or on being notified that any information, data or communication link residing in or connected to a computer resource controlled by it is being used to commit an unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.
- A proviso has been added to Section 81 which states that the provisions of the Act shall have overriding effect. The proviso states that nothing contained in the Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957

The Department of Information Technology has prepared following draft rules under the IT (Amendment) Act., 2009 :

1. Section 52 – Salary, allowances and other terms and conditions of service of Chairperson and Members.

2. Section 54 – Procedure for investigation of misbehavior or incapacity of Chairperson and Members.

3. Section 69 - Directions for Interception, Monitoring and Decryption of Information
4. Section 69A - Blocking for public access of any information generated, transmitted, received, stored or hosted in a computer resource
5. Section 69B - Monitoring and Collecting Traffic Data or information
6. Section 70B(1) - Appoint an agency of the Government to be called the Indian Computer Emergency Response Team
7. Section 70B (5) - The manner in which the functions and duties of agency shall be performed.

C) Indian Penal Code, 1860

Indian Penal Code came into force in 1862 (during the British Raj) and is regularly amended, such as to include section 498-A. The Code has a total of 511 sections covering various aspects of the Criminal Law. Some of the relevant sections regarding cyber crime are listed below.

Sending threatening messages by email	Sec 503
Sending defamatory messages by email	Sec 499
Forgery of electronic records	Sec 463, 464, 468, 469
Bogus websites, cyber frauds	Sec 420
Email spoofing	Sec 463
Web-Jacking	Sec. 383
E-Mail Abuse, On line Defamation	Sec.500, 509
Criminal Intimidation by E- mail/ chat	Sec 506,507
Theft of computer Hardware	Sec 378,379

D) Indian Evidence Act, 1872

The Indian Evidence Act, identified as Act no. 1 of 1872, and called the Indian Evidence Act, 1872, has eleven chapters and 167 sections, and came into force 1st September 1872.

Information Technology Act 2000 made extensive changes in Indian Evidence Act, 1872. The amendments included:

(i) Sec 3 - Evidence - "Evidence" means and includes:

- All documents including electronic records produced in Court are called documentary evidence.
- "Electronic records" has the same meaning as assigned in IT Act,2000, i.e.:
- image or sound stored, received or sent in an electronic form; or
- micro film or computer generated micro fiche;

(ii) Sec 17- Admission defined - An admission is a statement, oral or documentary or contained in **electronic form** which suggests any inference as to any fact in issue or relevant fact.

(iii) **Sec 27-How much of information received from accused may be proved -** When any fact is discovered in consequence of information received from a person accused of any offence, in the custody of a police officer, *so much of such information, as relates distinctly to the fact thereby discovered, may be proved.*

(iv) When oral admissions as to contents of electronic records are relevant:

Sec 22A- Oral admissions as to the *contents of electronic records are not relevant*, unless the genuineness of the electronic record produced is in question.

Sec 59- Proof of facts by oral evidence - All facts, except the contents of documents or electronic records, may be proved by oral evidence**.**

Sec 39- How much evidence to be given when statement forms part of electronic record:

- When any statement of which evidence is given forms part of an electronic record, then
- Evidence shall be given of so much and no more of the electronic record, as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made. Opinion as to digital signature where relevant

Sec 47A When the Court has to form an opinion as to the digital signature of any person, the opinion of the *Certifying Authority which has issued the Digital Signature Certificate is a relevant fact.*

(v) **Proof as to digital signature**

Sec 67A Except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record, *the fact that such digital signature is the digital signature of the subscriber must be proved*

(vi) Proof as to verification of digital signature

Sec 73A In order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct-

(a) that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;
(b) any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person.

(vii) Admissibility of electronic records

Sec 65B (1) Any information contained in an *electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media* produced by a computer shall be deemed to be also a document, if certain conditions are satisfied.

It shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

Sec 65 B (2) The conditions are as following:

(a) the computer output was produced during the period when it was used regularly to store or process information for the purposes of any activities regularly carried on by a person having lawful control over the computer;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) Throughout the said period, computer was operating properly or, if not, then that part of the period was not such as to affect the electronic record or the accuracy of its contents; and

(d) The information contained in the electronic record reproduced or is derived from such information fed into the computer in the ordinary course of the said activities.

(viii) Presumption as to electronic agreements

Sec 85A The Court shall presume that every electronic record purporting to be an agreement containing the digital signatures of the parties was so concluded by affixing the digital signature of the parties.

(ix) Presumption as to electronic records and digital signatures:

Sec 85B (1) the Court shall presume that *the secure electronic record has not been altered* since the specific point of time to which the secure status relates.

(2) In proceedings involving secure digital signature, the Court shall presume that the *secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record.*

(x) Presumption as to electronic messages:

Sec 88A.The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission;

but the Court shall not make any presumption as to the person by whom such message was sent.

(xi) Presumption as to electronic records five years old

Sec 90A.Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the digital signature which purports to be the digital signature of any particular person was so affixed by him or any person authorised by him in this behalf.

Guidelines issued by Reserve Bank of India

1. Internet Banking in India – Guidelines- DBOD.COMP.BC.No.130/ 07.03.23/ 2000-01 dated June 14, 2001

2. Credit/Debit Card transactions-Security Issues and Risk mitigation measures issued by RBI on February 18, 2009 under Section 18 of Payment and Settlement Systems Act 2007. – mandates Additional security code other than the card number, the expiry date and card security code known as Card Verification Value (CVV)

Chapter 10

ROLE OF CHARTERED ACCOUNTANTS IN COMBATING CYBER CRIMES AND IN THE CYBER ENVIRONMENT

1. Technological measures-Public key cryptography, Digital signatures ,Firewalls,
2. Cyber investigation- Computer forensics is the process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in courts of law.
3. Information systems audit
4. Cyber Law Compliance officer
5. Initiate training of employees on Cyber Law Compliance
6. use authentication procedures suggested in law
7. Maintain data retention as suggested under Section 67C
8. Identify and initiate safeguard requirements indicated under Sections 69 and 69A, 69B

9. Initiate global standards of data privacy on collection, retention, access, deletion etc.

Chapter 11

Cyber Crime Cells in India

Mumbai

Address:

Assistant Commissioner of Police
Cyber Crime Investigation Cell
Office of Commissioner of
Police office,
Annex -3 Building,
1st floor,
Near Crawford Market,
Mumbai-01.

Contact Details:

+91-22-22630829
+91-22-22641261

Web site: http://www.cybercellmumbai.com
E-mail id: officer@cybercellmumbai.com

Chennai

Address:

Assistant Commissioner of Police
Cyber Crime Cell
Commissioner office Campus
Egmore,
Chennai- 600008
Contact Details: +91-40-5549 8211
E-mail id: s.balu@nic.in

For Rest of Tamil Nadu,

Address: Cyber Crime Cell, CB, CID, Chennai
E-mail id: cbcyber@tn.nic.in

Bangalore

(for whole of the Karnataka)

Address:

Cyber Crime Police Station
C.O.D Headquarters,
Carlton House,
1, Palace Road,

Hyderabad

Address:

Cyber Crime Police Station
Crime Investigation Department,
3rd Floor, D.G.P. Pffice
Lakdikapool,

Bangalore - 560 001 **Contact Details:** +91-80-2220 1026 +91-80-2294 3050 +91-80-2238 7611 (FAX) **Web site:**http://www.cyberpolicebangalore.nic.in/ **Email-id:** ccps@blr.vsnl.net.in,ccps@kar.nic.in	Hyderabad – 500004 **Contact Details:** +91-40-2324 0663 +91-40-2785 2274 +91-40-2329 7474 (Fax) **Web site:**http://www.cidap.gov.in/cybercrimes.aspx **E-mail id:** cidap@cidap.gov.in,info@cidap.gov.in
Delhi **CBI Cyber Crime Cell:** Superintendent of Police, Cyber Crime Investigation Cell Central Bureau of Investigation, 5th Floor, Block No.3, CGO Complex, Lodhi Road, New Delhi – 3 **Contact Details:** +91-11-4362203 +91-11-4392424 **Web site:** http://cbi.nic.in/ **E-Mail:** cbiccic@bol.net.in	**Thane** **Address:** 3rd Floor, Police Commissioner Office Near Court Naka, Thane West, Thane 400601. **Contact Details:** +91-22-25424444 **Web site:** www.thanepolice.org **E-Mail:** police@thanepolice.org
Pune Assistant Commissioner of Police Cyber Crime Investigation Cell	**Gujarat** DIG, CID, Crime and Railways Fifth Floor

Police Commissioner Office of Pune 2, Sadhu Vaswani Road, Camp, Pune 411001 **Contact Details:** +91-20-2612 7277 +91-20-2616 5396 +91-20-2612 8105 (Fax) **Website:** http://punepolice.com/crime branch.html **E-Mail:** punepolice@vsnl.com	Police Bhavan Sector 18, Gandhinagar 382 018 **Contact Details:** +91-79-2325 4384 +91-79-2325 3917 (Fax)
Gurgaon Superintendent of Police Gurgaon	

Chapter 12

Important Case laws

1. Pune Citibank MphasiS Call Center Fraud

some ex employees of BPO arm of MPhasis Ltd MsourcE, defrauded US Customers of Citi Bank to the tune of RS 1.5 crores has raised concerns of many kinds including the role of "Data Protection".

The crime was obviously committed using "Unauthorized Access" to the "Electronic Account Space" of the customers. It is therefore firmly within the domain of "Cyber Crimes".
ITA-2000 is versatile enough to accommodate the aspects of crime not covered by ITA-2000 but covered by other statutes since any IPC offence committed with the use of "Electronic Documents" can be considered as a crime with the use of a "Written Documents". "Cheating",

"Conspiracy", "Breach of Trust" etc are therefore applicable in the above case in addition to section in ITA-2000.

Under ITA-2000 the offence is recognized both under Section 66 and Section 43. Accordingly, the persons involved are liable for imprisonment and fine as well as a liability to pay damage to the victims to the maximum extent of Rs 1 crore per victim for which the "Adjudication Process" can be invoked.

2. Bazee.com case

CEO of Bazee.com was arrested in December 2004 because a CD with objectionable material was being sold on the website. The CD was also being sold in the markets in Delhi.

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

3. State of Tamil Nadu Vs Suhas Katti

The Case of Suhas Katti is notable for the fact that the conviction was achieved successfully within a relatively quick time of 7 months from the filing of the FIR. Considering that similar cases have been pending in other states for a much longer time, the efficient handling of the case which happened to be the first case of the Chennai Cyber Crime Cell
going to trial deserves a special mention.

The case related to posting of obscene, defamatory and annoying message about a divorcee woman in the *yahoo message group*. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting.

Based on a complaint made by the victim in February 2004, the Police traced the accused to Mumbai and arrested him within the next few days. The accused was a known family friend of the victim and was reportedly interested in marrying her. She however married another person. This marriage later ended in divorce and the accused started contacting her once again. On her reluctance to marry him, the accused took up the harassment through the Internet.

On 24-3-2004 Charge Sheet was filed u/s 67 of IT Act 2000, 469 and 509 IPC before The Hon'ble Addl. CMM Egmore by citing 18 witnesses and 34 documents and material objects. The same was taken on file in C.C.NO.4680/2004. On the prosecution side 12 witnesses were examined and entire documents were marked as Exhibits.

The Defence argued that the offending mails would have been given either by ex-husband of the complainant or the complainant her self to implicate the accused as accused alleged to have turned down the request of the complainant to marry her.

Further the Defence counsel argued that some of the documentary evidence was not sustainable under Section 65 B of the Indian Evidence Act. However, the court relied upon the expert witnesses and other evidence produced before it, including the witnesses of the Cyber Cafe owners and came to the conclusion that the crime was conclusively proved.

Ld. Additional Chief Metropolitan Magistrate, Egmore, delivered the judgement on 5-11-04 as follows:

" 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 RI for 2 years under 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 RI 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 as the first case convicted under section 67 of Information Technology Act 2000 in India.

4. The Bank NSP Case

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

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

In India's first case of cyber defamation, a Court of Delhi assumed jurisdiction over a matter where a corporate'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 employ could be indulging in the matter of sending abusive emails, the plaintiff terminated the services of the defendant.

After hearing detailed arguments of Counsel for Plaintiff, Hon'ble Judge of the Delhi High Court passed an ex-parte ad interim injunction observing that a prima facie case had been made out by the plaintiff. Consequently, the Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails either to the plaintiffs or to its sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing departments. Further, Hon'ble Judge also restrained the defendant from publishing, transmitting or causing to be published any information in the actual world as also in cyberspace which is derogatory or defamatory or abusive of the plaintiffs.

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

6. PARLIAMENT ATTACK CASE

Bureau of Police Research and Development at Hyderabad had handled some of the top cyber cases, including analysing and retrieving information from the laptop recovered from terrorist, who attacked Parliament. The laptop which was seized from the two terrorists, who were gunned down when Parliament was under siege on December 13 2001, was sent to Computer Forensics Division of BPRD after computer experts at Delhi failed to trace much out of its contents.

The laptop contained several evidences that confirmed of the two terrorists' motives, namely the sticker of the Ministry of Home that they had made on the laptop and pasted on their ambassador car to gain entry into Parliament House and the the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal.

The emblems (of the three lions) were carefully scanned and the seal was also craftly made along with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop.

7. Andhra Pradesh Tax Case

Dubious tactics of a prominent businessman from Andhra Pradesh was exposed after officials of the department got hold of computers used by the accused person.

The owner of a plastics firm was arrested and Rs 22 crore cash was recovered from his house by sleuths of the Vigilance Department. They sought an explanation from him regarding the unaccounted cash within 10 days.

The accused person submitted 6,000 vouchers to prove the legitimacy of trade and thought his offence would go undetected but after careful scrutiny of vouchers and contents of his computers it revealed that all of them were made after the raids were conducted.

It later revealed that the accused was running five businesses under the guise of one company and used fake and computerised vouchers to show sales records and save tax.

8. SONY.SAMBANDH.COM CASE

India saw its first cybercrime conviction recently. It all began after a complaint was filed by Sony India Private Ltd, which runs a website called www.sony-sambandh.com, targeting Non Resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online.

The company undertakes to deliver the products to the concerned recipients. In May 2002, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless head phone.

She gave her credit card number for payment and requested that the products be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency and the transaction processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim.

At the time of delivery, the company took digital photographs showing the delivery being accepted by Arif Azim.

The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase.

The company lodged a complaint for online cheating at the Central Bureau of Investigation which registered a case under Section 418, 419 and 420 of the Indian Penal Code.

The matter was investigated into and Arif Azim was arrested. Investigations revealed that Arif Azim, while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company's site.

The CBI recovered the colour television and the cordless head phone.

In this matter, the CBI had evidence to prove their case and so the accused admitted his guilt.

The court convicted Arif Azim under Section 418, 419 and 420 of the Indian Penal Code — this being the first time that a cybercrime has been convicted.

The court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. The court therefore released the accused on probation for one year.

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

9. Nasscom vs. Ajay Sood & Others

In a landmark judgment in the case of National Association of Software and Service Companies vs Ajay Sood & Others, delivered in March, '05, the Delhi High Court declared `phishing' on the internet to be an illegal act, entailing an injunction and recovery of damages. Elaborating on the concept of 'phishing', in order to lay down a precedent in India, the court stated that it is a form of internet fraud where a person pretends to be a legitimate association, such as a bank or an insurance company in order to extract personal data from a customer such as access codes, passwords, etc. Personal data so collected by misrepresenting the identity of the legitimate party is commonly used for the collecting party's advantage. court also stated, by way of an example, that typical phishing scams involve persons who pretend to represent online banks and siphon cash from e-banking accounts after conning consumers into handing over confidential banking details.

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

The plaintiff in this case was the National Association of Software and Service Companies (Nasscom), India's premier software association.

The defendants were operating a placement agency involved in head-hunting and recruitment. In order to obtain personal data, which they could use for purposes of headhunting, the defendants composed and sent e-mails to third parties in the name of Nasscom.

The high court recognised the trademark rights of the plaintiff and passed an ex-parte adinterim 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 Rs1.6 million to the plaintiff as damages for violation of the plaintiff's trademark rights. The court also ordered the hard disks seized from the defendants' premises to be handed over to the plaintiff who would be the owner of the hard disks.

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

Chapter 13

Useful Links

1. Department of Information Technology

http://www.mit.gov.in/

2. Controller of Certifying Authorities

http://cca.gov.in/

3. Controller General of Patents, Designs and Trademarks- Department of Industrial Policy and Promotion

http://www.ipindia.nic.in/

4. Reserve bank of India

http://www.rbi.org.in/