UNIT – 1

INTRODUCTION OF CYBER SPACE IN INDIA

STRUCTURE

1.1 INTRODUCTION

Cyber Law is the law, which is governing cyber space. Cyber space is a very wide term which includes computers, networks, software, data storage devices, the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc. The law governing all the instruments included in the cyber space is called Cyber law.

Cyber-crime is the latest and perhaps the most complicated problem in the cyber world. Cyber-crimes are unlawful acts where 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.

Crime is both a social and economic phenomenon and is as old as human society. Crime in any form adversely affects all the members of the society. Cyber-crime is not defined in Information Technology Act 2000 nor in the I.T. Amendment Act 2008 nor in any other legislation in India.

The primary source of cyber law in India is the Information Technology Act, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government. This unit presents the legislation in India dealing with offences relating to the use of or concerned with the abuse of computers or other electronic gadgets- the law that governs the cyber space in India.

1.2 OBJECTIVES

After reading this unit you are able to understand the following:

- Cyber space
- Cyber-crime
- What is cyber law
- Cyber law in India
- Information Technology Act, 2000
- Information Technology Amendment Act, 2008
- Other relevant legislations in the nation that deal with cybercrimes in various sectors
- Legislations in other nations

1.3 SUBJECT

1.3.1 CYBER SPACE

The term cyber or cyberspace has today come to signify everything related to computers, the Internet, websites, data, emails, networks, software, data storage devices (such as hard disks, USB disks etc.) and even electronic devices such as cell phones, ATM machines etc. Thus a simplified definition of cyber law is that it is the “law governing cyber space”. The issues addressed by cyber law includes cyber-crime, electronic commerce, Intellectual Property in as much as it applies to cyber space and Data protection & privacy.[1]

The word cyberspace have been coined by author William Gibson in his science-fiction novel 'Neuromancer', written in 1984, in the following words,

"A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematically concepts…….A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity, lines of light ranged in the non-space of the mind, clusters and constellations of data".[2]

1.3.2 CYBER-CRIME

Crime is both a social and economic phenomenon. Kautilya's Arthashastra written around 350 BC, considered to be an authentic administrative treatise in India, discusses the various crimes, security initiatives to be taken by the rulers, possible crimes in a state etc. and also advocates punishment for the list of some stipulated offences. Different kinds of punishments have been prescribed for listed offences and the concept of restoration of loss to the victims has also been discussed in it.

Crime in any form adversely affects all the members of the society. In developing economies, cyber-crime has increased at rapid strides, due to the rapid diffusion of the Internet and the digitisation of economic activities. Thanks to the huge penetration of technology in almost all walks of society right from corporate governance and state administration, up to the lowest 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 man cannot spend a day without computers or a mobile. Snatching some one's mobile will tantamount to dumping one in solitary confinement!

Cyber Crime is not defined in Information Technology Act 2000 nor in the I.T. Amendment Act 2008 nor in any other legislation in India. In fact, it cannot be too. Offence or crime has been dealt with elaborately listing various acts and the punishments for each, under the Indian Penal Code, 1860 and quite a few other legislations too. Hence, to define cyber-crime, we can say, it is just a combination of crime and computer. To put it in simple terms 'any offence or crime in which a computer is used is 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 a computer or an information stored in a computer used (or misused) by the fraudster. The I.T. Act defines a computer, computer network, data, information and all other necessary ingredients that form part of a cyber-crime. In a cyber-crime, computer or the data itself the target or the object of offence or a tool in committing

[1]http://www.slideshare.net/bharadwajchetan/an-introduction-to-cyber-law-it-act-2000-india

[2] New York: Berkley Publishing Group, 1989, p. 128

some other offence, providing the necessary inputs for that offence. All such acts of crime will come under the broader definition of cyber-crime.[3]

1.3.3 WHAT IS CYBER LAW

The area of law dealing with the use of computers and the Internet and the exchange of communications and information thereon, including related issues concerning such communications and information as the protection of intellectual property rights, freedom of speech, and public access to information. It is also known as ‘Internet law’ and ‘Computer law’.

In simple words, law encompasses the rules of conduct: that have been approved by the government, and which are in force over a certain territory, and which must be obeyed by all persons on that territory. Violation of these rules will lead to government action such as imprisonment or fine or an order to pay compensation.

Cyber law is fundamentally different from laws that geographic nations use today. The unique structure of the Internet has raised several judicial concerns. There is a substantial literature and commentary that the Internet is not only "regulable," but is already subject to substantial law regulations, both public and private, by many parties and at many different levels. Since the Internet defies geographical boundaries, national laws can not apply globally and it has been suggested instead that the Internet can be self-regulated as being its own trans-national "nation".[4]

Cyber law stands for collectively several laws like computer law, internet law and information technology law.

There is no single definition of the term “cyber law”. One of the definition of cyber law given in 1996, which is broadly accepted as follows:-

‘Simply speaking, cyber law is a generic term, which refers to all the legal and regulatory aspects of Internet and the World Wide Web. Anything concerned with or related to or emanating from any legal aspects or issues concerning any activity of citizens and others, in Cyberspace comes within the ambit of Cyber law.’[5]

1.3.4 CYBER LAW IN INDIA

Internet was commercially introduced in India after 49th year of its independence. The need for cyber laws was propelled by numerous factors:[6]

- The coming of internet led to the emergence of numerous ticklish legal issues and problems, which necessitated the enactment of cyber laws.
- The existing laws could not be interpreted in the light of the different activities in cyberspace.

---

[3] http://iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf
[4] wiekipedia
[5] Pavan Duggal, Textbook on cyber Laws, Universal Law Publishers, 2014 Edition, p. 2
[6] ibid

- There was no law in India which gave legal validity and sanction to the activities in cyberspace (for example, e-mail).
- The General Assembly of the United Nations adopted the United Nations Commission on International Trade laws (UNCITRAL) Model Law on Electronic Commerce on January 30, 1997.

Inspired by UNCITRAL law on e-commerce, Government of India decided to enact a law that would make e-commerce legal, electronic records admissible in evidence and which would make cosmetic changes to some other existing laws. On 17th may, parliament passed India's first Cyber law, namely, The Information Technology Act, 2000 (IT Act, 2000). After receiving President's assent on June 9, it was implemented on October 17, 2000. To overcome the loopholes and drawbacks of this law parliament passed the Information Technology (Amendment) Act, 2008. The new amendment sought to remove procedural difficulties in the implementation of the law, making the legislation technology 1998'Aimedtofacilitatetotheadded various new cybercrimes in the IT Act, 2000.

1.3.5 THE DRAFT ELECTRONIC COMMERCE ACT, 1998

The Electronic Commerce Act, 1998 aimed to 'facilitate the development of a secure regulatory environment for electronic commerce by providing a legal infrastructure governing electronic contracting, security and integrity of electronic transaction, the use of digital signatures and other issues related to electronic commerce'[7]. Another draft known as Electronic Commerce Support Act, 1998 had 8 sections which were mainly concerned with necessary amendments to other Act to bring the latter in complete harmony with Electronic Commerce Act, 1998[8].

The above drafts had been prepared by the Ministry of Commerce. Parallel drafts also been prepared by the Department of Electronics. Out of these four drafts the Law Ministry had to make a final draft and to pull it before Parliament.

However, with the birth of the Ministry of Information Technology, the job was undertaken by it, and what came forth was the Information Technology Bill, 1999. The Bill was introduced in Parliament in December 1999, was passed in May, 2000[9].

1.3.6 INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act, 2000 aimed to 'provide legal recognition for transaction carried out by means of electronic data exchange and other means of electronic communication, commonly referred to as 'electronic commerce', which involves the use of alternatives to paper based methods of communication and storage of information, to facilitate electronic filing of

[7]The Act had 62 sections divided over fifteen parts. This Act- as is clear from the drafts of Electronic Commerce Act, 1998 – was not apply to the State of Jammu and Kashmir.
[8] This Act also was not apply to the State of Jammu and Kashmir.
[9]Mishra J.P., An Introduction to Cyber laws, Central law Publications: First Edition: 2012, p. 14.

documents with the Government agencies'. To this end, it also had to amend the Indian Penal Code, the Indian Evidence Act, Banker's books Act and the Reserve Bank of India Act.[10] The act has 13 chapters with 94 sections and four schedules. The IT Act, 2000 expended to whole of India and in some cases outside India too. Following the passage of Negotiable Instrument Amendment Act, 2002, the IT Act, 2000 underwent some major changes with effect from February 06, 2003.[11]

1.3.7 INFORMATION TECHNOLOGY AMENDMENT ACT, 2008

In the year 2001, the UNCITRAL had come out with its model law on electronic signature with an aim to make it technology-natural. On the domestic front also, the problems had surfaced on a scale that had made the amendment in the IT Act, 2000 inevitable. The draft of Information Technology (Amendment) Bill, 2006 was introduced on December 15, 2006 in the Loksabha. This bill was further amended by the Information Technology (Amendment) Bill, 2008; and on the process, the underlying Act was renamed as the Information Technology Amendment Act, 2008 (IITA, 2008). This act was passed in the Lower House of the Parliament on December 22, 2008 and by Upper House December 23, 2008.

Latter the Government has come out with the Cyber Appellate Tribunal (Salary, Allowances and other Term and Conditions of Service of Chairperson and Members) Rules 2009; the Cyber Appellate Tribunal (Procedure for Investigation of Misbehaviour in Capacity of Chairperson and Members) Rules, 2009; the Information Technology (Procedure and Safeguard foe Interception, Monitoring and Decryption of Information) Rules, 2009; the Information Technology (Procedure and Safeguard for Blocking for Access of Information by Public) rules, 2009; and Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic data or Information) Rules, 2009.

The latest rules notified by the government in the year 2011 include: the Information Technology (Electronic Service Delivery) Rules, 2011; the Information Technology (Reasonable security practice and procedures and sensitive personal data or information) Rules, 2011; the Information Technology (intermediaries guidelines) rules, 2011; and the Information Technology (Guidelines for Cyber Café) Rules, 2011.

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.

IT Act, 2000 has amended the sections dealing with records and documents in the IPC 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

[10] Preamble of the act
[11] Mishra J.P., An Introduction to Cyber laws, Central law Publications: First Edition: 2012, p. 15

IPC, all crimes to an electronic record and electronic documents just like physical acts of forgery or falsification of physical records.

In practice, however, the investigating agencies file the cases quoting the relevant sections from IPC in addition to those corresponding in ITA like offences under IPC 463,464, 468 and 469 read with the ITA/ITAA Sections 43 and 66, to ensure the evidence or punishment stated at least in either of the legislations can be brought about easily.

The Indian Evidence Act 1872: This is another legislation amended by the ITA. Prior to the passing of ITA, all evidences in a court were in the physical form only. With the ITA giving recognition to all electronic records and documents, it was but natural that the evidentiary legislation in the nation be amended in tune with it. In the definitions part of the Act itself, the "all documents including electronic records" were substituted. Words like 'digital signature', 'electronic form', 'secure electronic record ''information' as used in the ITA, were all inserted to make them part of the evidentiary mechanism in legislations.

Admissibility of electronic records as evidence as enshrined in Section 65B of the Act assumes significance. This is an elaborate section and a landmark piece of legislation in the area of evidences produced from a computer or electronic device. Any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by computer shall be treated like a document, without further proof or production of the original, if the conditions like these are satisfied: (a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly.... By lawful persons... (b)the information derived was regularly fed into the computer in the ordinary course of the said activities; (c) throughout the material part of the said period, the computer was operating properly and a certificate signed by a person .Responsible etc.

To put it in simple terms, evidences (information) taken from computers or electronic storage devices and produced as print-outs or in electronic media are valid if they are taken from system handled properly with no scope for manipulation of data and ensuring integrity of data produced directly with or without human intervention etc. and accompanied by a certificate signed by a responsible person declaring as to the correctness of the records taken from a system a computer with all the precautions as laid down in the Section.

However, this Section is often being misunderstood by one part of the industry to mean that computer print-outs can be taken as evidences and are valid as proper records, even if they are not signed. We find many computer generated letters emanating from big corporates with proper space below for signature under the words "Your faithfully" or "truly" and the signature space left blank, with a PostScript remark at the bottom "This is a computer generated letter and hence does not require signature".

The Act does not anywhere say that 'computer print-outs need not be signed and can be taken as record'.

The Bankers' Books Evidence (BBE) Act 1891: Amendment to this Act has been included as the third schedule in ITA. Prior to the passing of ITA, any evidence from a bank to be produced in a court, necessitated production of the original ledger or other register for verification at some stage with the copy retained in the court records as exhibits. With the passing of the ITA the definitions part of the BBE Act stood amended as: "'bankers' books' include ledgers, day-books, cash-books, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device". When the books consist of printouts of data stored in a floppy, disc, tape etc., a printout of such entry ...certified in accordance with the provisions ....to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and (b) a certificate by a person in-charge of computer system obtaining a brief description of the computer system and the particulars of the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorised persons; the safeguards adopted to prevent and detect unauthorised change of data ...to retrieve data that is lost due to systemic failure or .....

In short, just like in the Indian Evidence Act, the provisions in Bankers Books Evidence Act make the printout from a computer system or a floppy or disc or a tape as a valid document and evidence, provided, such print-out is accompanied by a certificate stating that it is a true extract from the official records of the bank and that such entries or records are from a computerised system with proper integrity of data, wherein data cannot be manipulated or accessed in an unauthorised manner or is not lost or able to temper due to system failure or such other reasons.

Here again, let us reiterate that the law does not state that any computerised print-out even if not signed, constitutes a valid record. But still even many banks of repute (both public sector and private sector) often send out printed letters to customers with the space for signature at the bottom left blank after the line "Yours faithfully" etc. and with a remark as Post Script reading: "This is a computer generated letter and hence does not require signature". Such interpretation is grossly misleading and sends a message to public that computer generated reports or letters need not be signed, which is never mentioned anywhere in nor is the import of the ITA or the BBE.

The next Act that was amended by the ITA is the **Reserve Bank of India Act, 1934.** Section 58 of the Act sub-section (2), after clause (p), a clause relating to the regulation of funds transfer through electronic means between banks (i.e. transactions like RTGS and NEFT and other funds transfers) was inserted, to facilitate such electronic funds transfer and ensure legal admissibility of documents and records therein.

1.3.8 OBSERVATIONS ON INFORMATION TECHNOLOGY ACT, 2000 AND INFORMATION TECHNOLOGY AMENDMENT ACT, 2008[12]

Awareness: There is no serious provision for creating awareness and putting such initiatives in place in the Act. The government or the investigating agencies like the Police department (whose job has been made comparatively easier and focused, thanks to the passing of the IT Act), have taken any serious step to create public awareness about the provisions in these legislations, which is absolutely essential considering the fact that this is a new area and

[12] http://iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf

technology has to be learnt by all the stake-holders like the judicial officers, legal professionals, litigant public and the public or users at large. Especially, provisions like scope for adjudication process is never known to many including those in the investigating agencies.

Jurisdiction: This is a major issue which is not satisfactorily addressed in the ITA or ITAA.

Jurisdiction has been mentioned in Sections 46, 48, 57 and 61 in the context of adjudication process and the appellate procedure connected with and again in Section 80 and as part of the police officers 'powers to enter, search a public place for a cybercrime etc. In the context of electronic record, Section13 (3) and (4) discuss the place of dispatch and receipt of electronic record which may be taken as jurisprudence issues.

However some fundamental issues like if the mail of someone is hacked and the accused is a resident of a city in some state coming to know of it in a different city, which police station does he go to? If he is an employee of a Multi-National Company with branches throughout the world and in many metros in India and is often on tour in India and he suspects another individual say an employee of the same firm in his branch or headquarters office and informs the police that evidence could lie in the suspect's computer system itself, where does he go to file he complaint. Often, the investigators do not accept such complaints on the grounds of jurisdiction and there are occasions that the judicial officers too have hesitated to deal with such cases. The knowledge that cyber-crime is geography-agnostic, borderless, territory-free and sans all jurisdiction and frontiers and happens in 'cloud' or the 'space' has to be spread and proper training is to be given to all concerned players in the field.

Evidences: Evidences are a major concern in cyber-crimes. Pat of evidences is the 'crime scene 'issues. In cyber-crime, there is no cyber-crime. We cannot mark a place nor a computer nor a network, nor seize the hard-disk immediately and keep it under lock and key keep it as an exhibit taken from the crime scene.

Very often, nothing could be seen as a scene in cyber-crime. The evidences, the data, the network and the related gadgets along with of course the log files and trail of events emanating or recorded in the system are actually the crime scene. While filing cases under IT Act, be it as a civil case in the adjudication process or a criminal complaint filed with the police, many often, evidences may lie in some system like the intermediaries' computers or some times in the opponent's computer system too. In all such cases, unless the police swing into action swiftly and seize the systems and capture the evidences, such vital evidences could be easily destroyed. In fact, if one knows that his computer is going to be seized, he would immediately go for destruction of evidences (formatting, removing the history, removing the cookies, changing the registry and user login set ups, reconfiguring the system files etc.) since most of the computer history and log files are volatile in nature.
There is no major initiative in India on common repositories of electronic evidences by which in the event of any dispute (including civil) the affected computer may be handed over to a common trusted third party with proper software tools, who may keep a copy of the entire disk and return the original to the owner, so that he can keep using it at will and the copy will be produced as evidence whenever required. For this there are software tools like 'Encase' with a global recognition and our own C-DAC tools which are available with much retrieval

facilities, search features without giving any room for further writing and preserving the original version with date stamp for production as evidence.

Non coverage of many crimes: While there are many legislations in not only many Western countries but also some smaller nations in the East, India has only one legislation -- the ITA and ITAA. Hence it is quite natural that many issues on cyber-crimes and many crimes per se are left uncovered. Many cyber-crimes like cyber-squatting with an evil attention to extort money. Spam mails, ISP's liability in copyright infringement, data privacy issues have not been given adequate coverage.

Besides, most of the Indian corporate including some Public Sector undertakings use Operating Systems that are from the West especially the US and many software utilities and hardware items and sometimes firmware are from abroad. In such cases, the actual reach and import of IT Act Sections dealing with a utility software or a system software or an Operating System upgrade or update used for downloading the software utility, is to be specifically addressed, as otherwise a peculiar situation may come, when the user may not know whether the upgrade or the patch is getting downloaded or any spyware getting installed. The Act does not address the government's policy on keeping the backup of corporates including the PSUs and PSBs in our county or abroad and if kept abroad, the subjective legal jurisprudence on such software backups.

We find, that most of the cyber-crimes in the nation are still brought under the relevant sections of IPC read with the comparative sections of ITA or the ITAA which gives a comfort factor to the investigating agencies that even if the ITA part of the case is lost, the accused cannot escape from the IPC part.

To quote the noted cyber law expert in the nation and Supreme Court advocate Shri Pavan Duggal, "While the lawmakers have to be complemented for their admirable work removing various deficiencies in the Indian Cyber law and making it technologically neutral, yet it appears that there has been a major mismatch between the expectation of the nation and the resultant effect of the amended legislation. The most bizarre and startling aspect of the new amendments is that these amendments seek to make the Indian cyber law a cyber-crime friendly legislation; - a legislation that goes extremely soft on cyber criminals, with a soft heart; a legislation that chooses to encourage cyber criminals by lessening the quantum of punishment accorded to them under the existing law; ….. a legislation which makes a majority of cybercrimes stipulated under the IT Act as bailable offences; a legislation that is likely to pave way for India to become the potential cyber-crime capital of the world……"

Let us not be pessimistic that the existing legislation is cyber-criminal friendly or paves the way to increase crimes. Certainly, it does not. It is a commendable piece of legislation, a landmark first step and a remarkable mile-stone in the technological growth of the nation. But let us not be complacent that the existing law would suffice. Let us remember that the criminals always go faster than the investigators and always try to be one step ahead in technology. After all, steganography was used in the Parliament Attack case to convey a one-line hidden message from one criminal to another which was a lesson for the investigators to know more about the technology of steganography. Similarly Satellite phones were used in the Mumbai attack case in November 2008 after which the investigators became aware of the technological perils of such gadgets, since until then, they were relying on cell phones and the directional tracking by the cell phone towers and Call Details Register entries only.

Hopefully, more and more awareness campaign will take place and the government will be conscious of the path ahead to bring more and more legislations in place. Actually, bringing more legislations may just not be sufficient, because the conviction rate in cybercrime offences is among the lowest in the nation, much lower than the rate in IPC and other offences. The government should be aware that it is not the severity of punishment that is a deterrent for the criminals, but it is the certainty of punishment.

It is not the number of legislations in a society that should prevent crimes but it is the certainty of punishment that the legislation will bring.

1.3.9 OTHER RELEVANT LEGISLATIONS IN THE NATION THAT DEAL WITH CYBERCRIMES IN VARIOUS SECTORS

1.3.9.1 PREVENTION OF MONEY LAUNDERING ACT:

Black money has always been a serious evil in any developing economy. Nation builders, lawmakers and particularly the country's financial administrators have always taken persistent efforts to curb the evil of black money and all sorts of illegally earned income. A major initiative taken in this direction in India is the Anti-Money Laundering Act 2002. A main objective of the Act was to provide for confiscation of property derived from, or involved in, money laundering.

Money laundering though not defined in the Act, can be construed to mean directly or indirectly attempting to indulge in any process or activity connected with the proceeds of crime and projecting it as untainted property. The Act stipulates that whoever commits the offence of money laundering shall be punishable with rigorous imprisonment for a term which shall not be less than three years but may extend to seven years and also be liable to a fine which may extend to five lakh rupees.

Money laundering involves a process of getting the money from illegal sources, layering it in any legal source, integrating it as part of any legal system like banking and actually using it. Since the banking as an industry has a major and significant role to play in the act of money laundering, it is now a serious responsibility on the part of banks to ensure that banking channel is not used in the criminal activity.

Much more than a responsibility, it is now a compliance issue as well.

1.3.9.2 E-RECORDS MAINTENANCE POLICY OF BANKS

Computerisation started in most of the banks in India from end 80's in a small way in the form of standalone systems called Advanced Ledger Posting Machines (Separate PC for every counter/activity)which then led to the era of Total Branch Automation or Computerisation in early or mid90's. TBA or TBC as it was popularly called, marked the beginning of a networked environment on a Local Area Network under a client-server architecture when records used to be maintained in electronic manner in hard-disks and external media like tapes etc. for backup purposes.

Ever since passing of the ITA and according of recognition to electronic records, it has become mandatory on the part of banks to maintain proper computerized system for electronic records. Conventionally, all legacy systems in the banks always do have a record maintenance policy often with RBI's and their individual Board approval stipulating the period of preservation for all sorts of records, ledgers, vouchers, register, letters, documents etc.

Thanks to computerisation and introduction of computerized data maintenance and often computer generated vouchers also, most of the banks became responsive to the computerized environment and quite a few have started the process of formulating their own Electronic Records Maintenance Policy.

Indian Banks' Association took the initiative in bringing out a book on Banks' e-Records Maintenance Policy to serve as a model for use and adoption in banks suiting the individual bank's technological setup.

Hencebanksshouldensurethate-recordsmaintenancepolicywithdetailsof e-records, their nature, their up keep, the technological requirements, off-site backup, retrieval systems, access control and access privileges initiatives should be in place, if not already done already.

On the legal compliance side especially after the Rules were passed in April 2011, on the "Reasonable Security Practices and Procedures" as part of ITAA 2008 Section 43A, banks should strive well to prove that they have all the security policies in place like compliance with ISO 27001 standards etc. and-records are maintained. Besides, the certificate to be given as an annexure to e-evidences as stipulated in the BBE Act also emphasizes this point of maintenance of e-records in a proper ensuring proper backup, ensuring against tamper ability, always ensuring confidentiality, integrity, availability and Non Repudiation.

This policy should not be confused with the Information Technology Business Continuity and Disaster Recovery Plan or Policy nor the Data Warehousing initiatives. Focus on all these three policies (BCDRP, DWH and E-records Maintenance Policy) are individually different, serving different purposes, using different technologies and maybe coming under different administrative controls too at the managerial level.

1.3.10LEGISLATIONS IN OTHER NATIONS

As against the lone legislation ITA and ITAA in India, in many other nations globally, there are many legislations governing e-commerce and cyber-crimes going into all the facets of cyber- crimes. Data Communication, storage, child pornography, electronic records and data privacy have all been addressed in separate Acts and Rules giving thrust in the particular area focused in the Act.

In the US, they have the Health Insurance Portability and Accountability Act popularly known as HIPAA which inter alia, regulates all health and insurance related records, their upkeep and maintenance and the issues of privacy and confidentiality involved in such records.

Companies dealing with US firms ensure HIPAA compliance insofar as the data relating to such corporate are handled by them. The Sarbanes-Oxley Act (SOX) signed into law in 2002and named after its authors Senator Paul Sarbanes and Representative Paul Oxley, mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures, and combat corporate and accounting fraud. Besides, there are a number of laws in the US both at the federal level and at different states level like the Cable Communications

Policy Act, Children's Internet Protection Act, and Children's Online Privacy Protection Act etc.

In the UK, the Data Protection Act and the Privacy and Electronic Communications Regulations etc. are all regulatory legislations already existing in the area of information security and cyber-crime prevention, besides cyber-crime law passed recently in August 2011. Similarly, we have cyber-crime legislations and other rules and regulations in other nations.[13]

1.4 SUMMARY

The term cyber or cyberspace has today come to signify everything related to computers, the Internet, websites, data, emails, networks, software, data storage devices (such as hard disks, USB disks etc.) and even electronic devices such as cell phones, ATM machines etc. Thus a simplified definition of cyber law is that it is the "law governing cyber space".

Cyber Crime is not defined in law. The I.T. Act defines a computer, computer network, data, information and all other necessary ingredients that form part of a cyber-crime

Cyber law is fundamentally different from laws that geographic nations use today. Cyber law stands for collectively several laws like computer law, internet law and information technology law.

Internet was commercially introduced in India after 49th year of its independence. The need for cyber laws was propelled by numerous factors: Inspired by UNCITRAL law on e-commerce, Government of India decided to enact a law that would make e-commerce legal, electronic records admissible in evidence and which would make cosmetic changes to some other existing laws. On 17th may, parliament passed India's first Cyber law, namely, The Information Technology Act, 2000 (IT Act, 2000). Latter the Government has come out with the Cyber Appellate Tribunal (Salary, Allowances and other Term and Conditions of Service of Chairperson and Members) Rules 2009; the Cyber Appellate Tribunal (Procedure for Investigation of Misbehaviour in Capacity of Chairperson and Members) Rules, 2009; the Information Technology (Procedure and Safeguard foe Interception, Monitoring and Decryption of Information) Rules, 2009; the Information Technology (Procedure and Safeguard for Blocking for Access of Information by Public) rules, 2009; and Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic data or Information) Rules, 2009.

The latest rules notified by the government in the year 2011 include: the Information Technology (Electronic Service Delivery) Rules, 2011; the Information Technology (Reasonable security practice and procedures and sensitive personal data or information) Rules, 2011; the Information Technology (intermediaries guidelines) rules, 2011; and the Information Technology (Guidelines for Cyber Café) Rules, 2011.

The IT Act, 2000 also had to amend the Indian Penal Code, the Indian Evidence Act, Banker's books Act and the Reserve Bank of India Act. The IT Act, 2000 expended to whole of India and in some cases outside India too. Following the passage of Negotiable Instrument

[13] http://iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf

Amendment Act, 2002, the IT Act, 2000 underwent some major changes with effect from February 06, 2003.

There is no serious provision for creating awareness and putting such initiatives in place in the Act. The government or the investigating agencies like the Police department (whose job has been made comparatively easier and focused, thanks to the passing of the IT Act), have taken any serious step to create public awareness about the provisions in these legislations, which is absolutely essential considering the fact that this is a new area and technology has to be learnt by all the stake-holders like the judicial officers, legal professionals, litigant public and the public or users at large.

Jurisdiction is a major issue which is not satisfactorily addressed in the ITA or ITAA. Some fundamental issues like if the mail of someone is hacked and the accused is a resident of a city in some state coming to know of it in a different city, which police station does he go to? If he is an employee of a Multi-National Company with branches throughout the world and in many metros in India and is often on tour in India and he suspects another individual say an employee of the same firm in his branch or headquarters office and informs the police that evidence could lie in the suspect's computer system itself, where does he go to file he complaint. Often, the investigators do not accept such complaints on the grounds of jurisdiction and there are occasions that the judicial officers too have hesitated to deal with such cases. The knowledge that cyber-crime is geography-agnostic, borderless, territory-free and sans all jurisdiction and frontiers and happens in 'cloud' or the 'space' has to be spread and proper training is to be given to all concerned players in the field.

Evidences are a major concern in cyber-crimes. Part of evidences is the 'crime scene' issues. Very often, nothing could be seen as a scene in cyber-crime. The evidences, the data, the network and the related gadgets along with of course the log files and trail of events emanating or recorded in the system are actually the crime scene. In all such cases, unless the police swing into action swiftly and seize the systems and capture the evidences, such vital evidences could be easily destroyed. In fact, if one knows that his computer is going to be seized, he would immediately go for destruction of evidences (formatting, removing the history, removing the cookies, changing the registry and user login set ups, reconfiguring the system files etc.) since most of the computer history and log files are volatile in nature.

While there are many legislations in not only many western countries but also some smaller nations in the East, India has only one legislation -- the ITA and ITAA. Hence it is quite natural that many issues on cyber-crimes and many crimes per se are left uncovered. Many cyber-crimes like cyber-squatting with an evil attention to extort money. Spam mails, ISP's liability in copyright infringement, data privacy issues have not been given adequate coverage.

Hopefully, more and more awareness campaign will take place and the government will be conscious of the path ahead to bring more and more legislations in place. Actually, bringing more legislations may just not be sufficient, because the conviction rate in cyber-crime offences is among the lowest in the nation, much lower than the rate in IPC and other offences. The government should be aware that it is not the severity of punishment that is a deterrent for the criminals, but it is the certainty of punishment.

It is not the number of legislations in a society that should prevent crimes but it is the certainty of punishment that the legislation will bring.

As against the lone legislation ITA and ITAA in India, in many other nations globally, there are many legislations governing e-commerce and cyber-crimes going into all the facets of cyber- crimes. Data Communication, storage, child pornography, electronic records and data privacy have all been addressed in separate Acts and Rules giving thrust in the particular area focused in the Act.

In the US, they have the Health Insurance Portability and Accountability Act popularly known as HIPAA which inter alia, regulates all health and insurance related records, their upkeep and maintenance and the issues of privacy and confidentiality involved in such records.

In the UK, the Data Protection Act and the Privacy and Electronic Communications Regulations etc. are all regulatory legislations already existing in the area of information security and cyber-crime prevention, besides cyber-crime law passed recently in August 2011.

Technology is always a double-edged sword and can be used for both the purposes – good or bad. Steganography, Trojan Horse, Scavenging (and even DoS or DDoS) are all technologies and per se not crimes, but falling into the wrong hands with a criminal intent who are out to capitalize them or misuse them, they come into the gamut of cyber-crime and become punishable offences. Hence, it should be the persistent efforts of rulers and law makers to ensure that technology grows in a healthy manner and is used for legal and ethical business growth and not for committing crimes. It should be the duty of the three stake holders viz.(i) the rulers, regulators, law makers and investigators (ii) Internet or Network Service Providers or banks and other intermediaries and (iii) the users to take care of information security playing their respective role within the permitted parameters and ensuring compliance with the law of the land.

1.5 GLOSSARY

1. NETIZENS- a user of the Internet, especially a habitual or keen one.
2. ENCASE- **Encase** is a suite of digital forensics products by Guidance Software. The software comes in several forms designed for forensic, cyber security and e-discovery use
3. C-DAC TOOLS- Introduction. Dictionary Tagging Tool is a language resource development software developed by GIST, **C-DAC** Pune.
4. USB DISKS –**USB disks** let you add unlimited storage to your desktop or laptop (especially laptops!) for movies, songs, images, backups, and other bulky data.
5. CYBER SQUATTING- The practice of registering names, especially well-known company or brand names, as Internet domains, in the hope of reselling them at a profit.

1.6 SAQS

1. TICK THE CORRECT ANSWERS

(i) The IT Act, 2000 expended to

(a) Whole of India
(b) Whole of India except Jammu and Kashmir
(c) Whole of the world
(d) Whole of India and in some cases outside India too.

(ii) The General Assembly of the United Nations adopted the United Nations Commission on International Trade laws (UNCITRAL) Model Law on Electronic Commerce on
(a) January 29, 1997
(b) January 30, 1997
(c) January 31, 1997
(d) January 1, 1997

(iii) Cyber space is a very wide term which includes the following
(a) Computers, networks, software, data storage devices.
(b) The Internet, websites, emails.
(c) Electronic devices such as cell phones, ATM machines etc.
(d) All of the above

(iv) Which of the following legislation is/are amended by the ITA-
(a) The Indian Evidence Act 1872
(b) The Indian Penal Code, 1860
(c) The Bankers' Books Evidence (BBE) Act 1891
(d) All of the above
(e) None of the above

(v) Which of the following legislation/legislations in the nation that deal with cybercrimes in various sectors:
(a) Prevention of Money Laundering Act:
(b) e-Records Maintenance Policy of Banks:
(c) both of the above
(d) none of the above

2. TRUE/ FALSE STATEMENT-

(i) Cyber Crime is not defined in Information Technology Act 2000. True/ false
(ii) The word cyberspace have been coined by author William Gibson. True/ false
(iii) Cyber Law is the law that is governing cyber space. True/ false
(vi) There is provision for creating awareness and putting such initiatives in IT Act. True/ false

1.7 REFERENCES

1. Mishra J.P., An Introduction to Cyber laws, Central law Publications: First Edition: 2012
2. Pavan Duggal, Textbook on cyber Laws, Universal Law Publishers, 2014 Edition,
3. http://iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf
4. http://www.slideshare.net/bharadwajchetan/an-introduction-to-cyber-law-it-act-2000-india
5. http://iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf

1.8 SUGGESTED READINGS

1. Mishra J.P., An Introduction to Cyber laws, Central law Publications: First Edition: 2012.
2. Pavan Duggal, Textbook on cyber Laws, Universal Law Publishers, 2014 Edition.
3. Gupta & Agarwal, Cyber Law; 1st edition, Premiere Publishing Company
4. Cyber and E-Commerce laws, P. M. Bakshi and R. K. Suri

1.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

1. What do you understand by the cyber-crime?
2. Give a brief account of the legislation amended by the Information technology Act, 2000.
3. Write a short note on the cyber laws of other nations.
4. Do you find ITA and ITAA successful against the cyber-crime? Critically analyse your answer.

1.10 ANSWER SAQS

1. (i) (d); (ii) (b); (iii) (d); (iv) (d) (v) (c)
2. (i) True (ii) True (iii) True (iv) False