CYBER LAW IN INDIA & OTHER COUNTRIES

| Authored By : Ms. Tavleen Sood |

As we all know that this is the era where most of the things are done usually over the internet starting from online dealing to the online transaction. Since the web is considered as worldwide stage, anyone can access the resources of the internet from anywhere. Self-protection, while essential, is not sufficient to make cyberspace a safe place to conduct business. The rule of law must also be enforced. Countries where legal protections are inadequate will become increasingly less able to compete in the new economy. As cyber crime increasingly breaches national borders, nations perceived as havens run the risk of having their electronic messages blocked by the network. National governments should examine their current status to determine whether they are sufficient to combat the kinds of crimes discussed in this report. Where gaps exist, governments should draw on best practices from other countries andwork closely with industry to enact enforceable legal protections against these new crimes. In order to stop or to punish the cyber criminals the term "Cyber Law" was introduced. We can define cyber law as it is the part of the legal systems that deals with the Internet, cyberspace, and with the legal issues. It covers a broad area, encompassing many subtopics as well as freedom of expressions, access to and utilization of the Internet, and online security or online privacy. Generically, it is alluded as the law of the web.

3.1. Introduction to cyber law in India and other countries

The invention of Computer has made the life of humans easier, it has been using for various purposes starting from the individual to large organizations across the globe. In simple term we can define computer as the machine that can stores and manipulate/process information or instruction that are instructed by the user. Most computer users are utilizing the computer for the erroneous purposes either for their personal benefits or for other's benefit since decades . This gave birth to "Cyber Crime". It doesn't have a fixed definition, but in a simple term we can defined it as the law that governs the cyberspace. Cyber laws are the laws that govern cyber area. Cyber Crimes, digital and electronic signatures, data protections and privacies etc are comprehended by the Cyber Law . The UN's General Assembly recommended the first IT Act of India which was based on the "United Nations Model Law on Electronic Commerce"

(UNCITRAL) Model . 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. These crimes are discussed in detail further in this chapter. A comprehensive discussion on the Indian law relating to cyber crimes and digital evidence is provided in the ASCL publication titled "Cyber Crimes & Digital Evidence – Indian Perspective. The most common cyber-crimes are cyber thefts which also includes identity thefts, fraud, forgery, defamation, pornography and hacking. Reports show that forgery was done mostly by youngsters in the age group of 18-30 years, whereas cyber frauds were committed mostly by middle aged people in the age group of 30-45 years.

3.2. Aim & objectives of cyber law in India and other countries

When more and more people are using the digital format whether in the form of mobile phones as also communication devices and computers, it is but natural to expect that they would be facing large number of cutting-edge legal issues in cyberspace.

The aims and objectives of the Cyber law are as follows:-

- To create more awareness about cyber legal issues and challenges
- To provide advice, inputs as also guidance to people on their day-to-day legal issues concerning the use of cyberspace
- To work on research and development on cutting-edge issues and challenges in cyberspace
- To contribute to the global debate on evolving Cyber Law jurisprudence
- Dedicated encryption laws need to be formulated.
- The concept of Cloud computing should be given a legal acceptance.
- E-mail policy has to be formulated and implemented.
- Legal issues of online payments
- The legal aspects of online gambling and online pharmacies need to be reconsidered.
- The legal aspects of Bitcoins need to be reconsidered.
- Framework for blocking websites
- Regulation of mobile applications

3.3. What is the need and importance of cyber law and security?

Cyber Law deals with the legal issues of the internet usage and all devices connected over the network, their proper use in order to prevent and control cyber crimes. Since the internet is all over the world the rules and regulations are a bit cloudy but we need to keep in mind a few things to ensure that we are using the internet in a proper and safe manner without causing any trouble.

1. The internet's jurisdictional boundaries may not be clear but the users are bound by the jurisdictional laws of the area in which they reside.
2. Do not access web sites that may not be approved by the jurisdiction in your area.
3. Do not post any offensive material that may cause an outrage among other internet users. Articles with an offensive tone on sensitive subjects like religion, politics etc., Uploading child pornography and other offensive materials is considered a crime in many countries and is punishable depending upon the country's laws.
4. Illegally downloading and distributing protected items like intellectual property and copyrighted articles is a cyber crime and those who are caught engaging in such acts can be prosecuted.
5. Duplication of content or software from CDs and DVDs that are copyrighted and distribution of these on the internet is punishable.
6. Stealing user information (phishing) and impersonating a user (ID theft) are serious cyber-crimes.
7. Sending bulk messages that can affect networks and jam mailboxes is called spamming. The US introduced CAN-SPAM Act t in 2003 that allows prosecution of spammers.
8. Illegal bank transactions through internet, to any dangerous individuals who might threaten national security is a cyber-crime that will be considered as a breach of national security and those caught engaging in such acts can be punished by the government.

Even though the Cyber Laws are not very clear to everyone the increase in cyber-crime rate has pushed many governments to introduce Acts that would govern the cyber space at least within their jurisdictions. The governments of USA, UK, Canada and China have enforced Cyber Laws to control Cyber-crimes. The other nations that have followed in introducing Cyber laws are India, Australia, Malaysia, Iran, Iraq, Indonesia, Thailand etc. Among all these nations China emerges to be the strictest in its laws regarding the use of the internet.

3.4. History of cyber law in India

The information Technology Act is an outcome of the resolution dated 30th January 1997 of the General Assembly of the United Nations, which adopted the Model Law on Electronic Commerce, adopted the Model Law on ElectronicCommerce on International Trade Law. This resolution recommended, inter alia, that all states give favourable consideration to the said Model Law while revising enacting new law, so that uniformity may be observed in the laws, of the various cyber-nations, applicable to alternatives to paper based methods of communication and storage of information.The Department of Electronics (DoE) in July 1998 drafted the bill. However, it could only be introduced in the House on December 16, 1999 (after a gap of almost one and a half years) when the new IT Ministry was formed. It underwent substantial alteration, with the Commerce Ministry making suggestions related to e-commerce and matters pertaining to World Trade Organization (WTO) obligations. The Ministry of Law and Company Affairs then vetted this joint draft.After its introduction in the House, the bill was referred to the 42-member Parliamentary Standing Committee following demands from the Members. The Standing Committee made several suggestions to be incorporated into the bill. However, only those suggestions that were approved by the Ministry of Information Technology were incorporated. One of the suggestions that was highly debated upon was that a cyber café owner must maintain a register to record the names and addresses of all people visiting his café and also a list of the websites that they surfed. This suggestion was made as an attempt to curb cyber crime and to facilitate speedy locating of a cyber criminal. However, at the same time it was ridiculed, as it would invade upon a net surfer's privacy and would not be economically viable. Finally, this suggestion was dropped by the IT Ministry in its final draft. The Union Cabinet approved the bill on May 13, 2000 and on May 17, 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President on 9th June 2000 and came to be known as the Information Technology Act, 2000. The Act came into force on 17th October 2000.This led to the passage of the Information Technology (Amendment) Act, 2008 which was made effective from 27 October 2009. The IT (Amendment) Act, 2008 has brought marked changes in the IT Act, 2000 on several counts.

3.5. Information Technology Act 2000

Information Technology Act, 2000 is India's mother legislation regulating the use of computers, computer systems and computer networks as also data and information in the electronic format. This legislation has touched varied aspects pertaining to electronic

authentication, digital (electronic) signatures, cyber crimes and liability of network service providers.

The Preamble to the Act states that it aims at providing legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information and aims at facilitating electronic filing of documents with the Government agencies.

This Act was amended by Information Technology Amendment Bill, 2008 which was passed in Lok Sabha on 22nd December, 2008 and in Rajya Sabha on 23rd December, 2008. It received the assent of the President on 5th February 2009 and was notified with effect from 27/10/2009.

The IT Act of 2000 was developed to promote the IT industry, regulate ecommerce, facilitate e-governance and prevent cybercrime. The Act also sought to foster security practices within India that would serve the country in a global context. The Amendment was created to address issues that the original bill failed to cover and to accommodate further development of IT and related security concerns since the original law was passed. The IT Act, 2000 consists of 90 sections spread over 13 chapters [Sections 91, 92, 93 and 94 of the principal Act were omitted by the Information Technology (Amendment) Act 2008 and has 2 schedules.[Schedules III and IV were omitted by the Information Technology (Amendment) Act 2008].

3.6. Information Technology Act Amendment 2008

The term **'digital signature'** has been replaced with 'electronic signature' to make the Act more technology neutral.

i. 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.

ii. 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.

iii. The damages of Rs. One Crore prescribed under section 43 of the earlier Act of 2000 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'

iv. 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

v. Sections 66A to 66F has been added to Section 66 prescribing punishment for offences such as obscene electronic message transmissions, identity theft, cheating by impersonation using computer resource, violation of privacy and cyber terrorism.

vi. Section 67 of the IT Act, 2000 has been 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 Rs.100,000 to Rs. 500,000. Sections 67A to 67C have also been inserted. While Sections 67A and B deals with penal provisions in respect of offences 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.

vii. 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 69A 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.

viii. Section 79 of the 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;

ix. 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.

3.7. Present Scenario

India is trying to implement the Digital India project to the best of its capabilities. The success of Digital India project would depend upon maximum connectivity with minimum cyber security risks. This is also a problem for India as India has a poor track record of cyber security.

According to Home Ministry statistics, as many as 71,780 cyber frauds were reported in 2013, while 22,060 such cases were reported in 2012. There have been 62,189 incidents of cyber frauds till June 2014. In 2013, a total of 28,481 Indian websites were hacked by various hacker groups spread across the globe. The numbers of hacking incidents were 27,605 in 2012 and 21,699 in 2011. As per the cyber-crime data maintained by National Cyber Records Bureau, a total of 1,791, 2,876 and 4,356 cases were registered under the Information Technology Act in 2011, 2012 and 2013, respectively. A total of 422, 601 and 1,337 cases were registered under cyber-crime related sections of the Indian Penal Code in 2011, 2012 and 2013, respectively. There has been an annual increase of more than 40 per cent in cyber-crime cases registered in the country during the past two-three years,

3.8. 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. The Bank NSP Case

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

company lost a large number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

3. 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.

3.9. Conclusion

The rise and proliferation of newly developed technologies begin star to operate many cybercrimes in recent years. Cybercrime has become great threats to mankind. Protection against cybercrime is a vital part for social, cultural and security aspect of a country. The Government of India has enacted IT Act, 2000 to deal with cyber-crimes. The Act further revise the IPC, 1860, the IEA (Indian Evidence Act), 1872, the Banker's Books Evidence Act 1891 and the Reserve Bank of India Act, 1934. Any part of the world cyber-crime could be originated passing national boundaries over the internet creating both technical and legal complexities of investigating and prosecuting these crimes. The international harmonizing efforts, coordination and co-operation among various nations are required to take action towards the cyber-crimes. Our main purpose of writing this paper is to spread the content of cyber-crime among the common people. At the end of this paper “A brief study on Cyber Crime and Cyber Law’s of India” we want to say cyber-crimes can never be acknowledged. If anyone falls in the prey of cyber-attack, please come forward and register a case in your nearest police station. If the criminals won’t get punishment for their deed, they will never stop.