A Pathway to Cyber Crime Free Digital Society with Human Rights Measures

Dr Kamal K Vyas, Director SIET, Sikar (Raj), profkamalkvyas@gmail.com
Mr Om Pal, Assistant Professor, SIT Sikar,
Dr Sandhya Vyas, HOD (Deptt of Social Sc), BBV Pilani (Raj), *profsandhyavyas@gmail.com*

***Key-words** : Cyber Crime, e-Banking, Information Technology Act 2000, Knowledge Society, Hacker, Human Right, Digital Signature, National Security Agency, IT Acts, Cyber Crime Offences.*

*****

Introduction:

Digital Society has paved a way to a new world of Knowledge based services, business networking and e-banking, budding as a solution to reduce costs, change the sophisticated economic affairs to more easier, speedy, efficient, and time saving method of transactions. Internet has emerged as un-beatable mass-media for the present pace of life but at the same time also resulted in various threats to the Users and Financial institutions. Various criminals like - hackers, crackers have been able to enter their way to interfere with the internet accounts through various techniques like hacking the Domain Name Server (DNS), spoofing, phishing, etc. Those have been successful in gaining “unauthorized access” to the user’s confidential accounts and stolen useful data to gain huge profits from customers secrete information.

These unwanted intruders in Cyber world act as Cyber Terrorists for producing destructive and harmful effects to tangible and intangible property of others, this act is called as “Cyber Crime”. Cyber Crime is an international problem with no national boundaries. Hacking attacks can be launched from any corner of the world without any fear of being traced or prosecuted easily. Cyber terrorist can collapse the economic structure of a country from a place where that country might not have any option like “Extradition Treaty” to catch that criminal. The only safeguard would be to keep protection using better technology to combat such situation.

This exploratory paper contributes an understanding of the effects of negative use of Information technology, and how far the present law in India is successful in dealing with such issues or threats, and in what way the legal structure lagging to curb the Cyber Crime. In such situation, timely updates are major requirement of the system to combat “Cyber Terrorism Disaster”. There are many protocols & techniques evolved to curb the criminal activities of these Cyber Terrorists, but still the problem persists in Legal System, because it is failed to keep pace with Technology Advancement thus produce a deterring effect on the criminals. If the suggestions are undertaken time to time, along with better co-ordination among various National and International agencies to make the system more efficient.

This paper briefly revealing the informative briefing about Information Technology Act 2000, Popular Offences under Cyber Crime, How to Curb it Nationally & Internationally and last but not least, a small discussion about “What Precaution should be taken during Curbing so it should not violate Human Rights”.

In today’s world of cyberspace which is largely dependent upon the internet and use of technology, the incidents of cyber crime have increased. To protect one from the cybercrime, there was a need for cyber laws and so, the implementation of cyber laws in India began in the year 2000, with the IT Act as an introduction to Indian Cyber Law. The laws governing the crimes of the virtual world or the cyberspace are popular as **Cyber laws in India**.

Definition of Cyberlaws states that it's a subset of law which specifically deals with the inter-network technology. Meaning cyber law of India deals with the crime done through a computer or any other digital device. *Before knowing about Indian cyber laws and cyber crimes' rules with their applicability,*

what are cyber crimes?

- Cyber crimes are not defined anywhere in the information technology law of India or in the 2013 policy on National Cyber Security or under any other laws, cyber crime rules or regulation in India.
- However, cyber crime has been dealt with under various cybersecurity laws such as Indian IT law, Indian Penal Code etc.
- Cyber crime has been identified as a crime which is essentially a combination of computer and crime. Thus, an offence done with the computer is cyber crimes.
- IT Acts in India include data, information, computer and computer network as a part of the cyber crime.

To know what is cyberlaw, it is necessary to understand that **what is cyber law in India** and what it deals with.

Importance of Cyber Law in India

Cyber laws of India or Cybercrime law in India is important because of the prime reason that cyber crime act in India encompasses and covers all the aspects which occur on or with the internet **-** transactions and activities which concern the internet and cyberspace.

Cyber Crime laws in India are important because it concerns everyone who uses or does anything with the internet. Every activity done on the internet comes under the purview of cyber laws in India.

Types of Cyber crimes

Different types of cyber crimes have different types of cyber crime punishment in India. That in itself is an elaborate section. However, let's

- **Identity theft -** ***When personal information of a person is stolen with the purpose of using their financial resources or to take a loan or credit card in their name then such crime is known as Identity theft.***
- **Cyberbullying -** ***When the teenager or adolescent harass, defame, embarrass or intimidate somebody else with the use of the internet, phone, chat rooms, instant messaging or any other social network then the person is said to be committing the crime of Cyberbullying. When the same crime is done by the adults it is known as Cyberstalking.***
- **Cyberterrorism -** ***When a threat of extortion or any kind of harm is being subjected towards a person, organization, group or state, it is known as the crime of Cyber Terrorism. Generally, it includes the well-planned attack strategies on the Government and corporate computer system.***
- **Hacking -** ***The most common cyber crime is Hacking. In this crime, the person gets access to other person's computers and passwords to use it for their own wrongful gain.***

Evolution of Cyber Law in India

With an increase in the dependency on the use of technology, the need of cyber law was necessary. Much like every coin has two sides, therefore, the dependency on the technology had its own pros and cons.

Thus, the rise of the 21st century marked the evolution of cyberlaw in India and Information Technology Act, 2000. It was popularly familiar as the **IT Laws in India**, which set the way for the evolution of Cyber Law Act.

The first ever cyber crime was recorded in the year 1820. The objective of Information technology laws in India is as follows:

- ***To protect the legal recognition to E-transactions***
- ***Legal recognition to a digital signature as a valid signature to accept agreements online***
- ***Protection of online privacy and stopping cyber crimes***
- ***To give legal recognition to keeping accounting books in electronic form by bankers as well as other organizations***
- ***The Indian IT law updated the Reserve Bank of India Act and the Indian Evidence Act.***

Though with the evolution of cyber law almost all the online activities came under scrutiny.

However, one thing about cyber law is that there are certain areas on which **cybercrime laws in India** do not apply such as:

- ***Negotiable Instrument being other than cheque***
- ***Power of Attorney (PoA)***
- ***Will***
- ***The contract for Sale or Conveyance of Immovable Property***
- ***Central Government notified documents or transactions.***

The Need of Cyber Laws

In the present world which is a more tech-savvy world the cyber law and cyber crimes has also become more sophisticated.

Internet and technology were launched for research purpose and making the life of humans easy but as the use and number of people on the internet increased the **need of cyber law in India** was felt.

As the nature of the internet is anonymous it is easy to commit cyber crimes. Thereby many could so misuse this aspect largely. Hence, there were the needs of cyber law in India.

What is the Information Technology Act, 2000?

When the emphasis was on the need for cyber law or cyber security laws, then, it was imperative to implement an IT law in India. This is the Information Technology Act, 2000, or also known as the Indian Cyber Act or the **Internet Law in India**.

Since the enactment of the Indian Internet Laws was to bring in view all the electronic records and online or electronic activities to legal recognition.

Therefore, the Cybercrime Act in India today provides with the much needed legal framework for cyber law and cyber crimes. It also provides for the provisions to deal with cyber crimes.

The Internet Laws in India not only validates the digital signatures but also provides how the authentication of the documents can be done which has been accepted and generated by using the digital signatures.

The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions.

Since, the **Cyber Act in India** has given a legal definition to the concept of secure digital signatures, so that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.
As IT Act is a cyber security law to secure the cyberspace, the information technology law was amended:

- ***the Indian Penal Code,***
- ***the Indian Evidence Act,***
- ***the Banker's Book Evidence Act, and***
- ***the Reserve Bank of India***

The prime focus of **laws for cyber crime** or cybercrime laws in India is to prevent:

- ***computer crime,***
- ***forgery of electronic data & record in e-commerce, and***
- ***electronic transaction.***

IT Act, 2000 went through amendments in the year 2008. These were made in the laws on cyber crime - IT Act, 2000 by way of IT Act, 2008. As they were enforced at the beginning of 2009 to strengthen the cyber security laws.

How to Prevent Cyber Crime?

No doubt that the Cyber security laws or Cyber laws in India provide protection from cyber crime. However, prevention is always better than cure. Therefore, one should take the following steps for preventing a cyber crime:

- **Unsolicited text message** - ***We all get text messages from an unknown number. One should be cautious and try to avoid responding to text message or automated voice message from an unknown number.***
- **Downloads on the mobile phone** - ***Download everything on the mobile phone from a trustworthy source only.***
- **Online buying** - ***Always use a legitimate and trusted payment service. Hence, it's important to always use a credit card, because then, the charges can be disputed if there is a problem.***
- **Rating and feedback** - ***Always check for seller's rating and feedback of customer for the seller. Be sure that you are checking current feedbacks. Also, beware of feedbacks that are 100% seller favouring or have an entry on the same date.***
- **Personal Information Request** - ***Everyone must have received a call or mail. In which, the person on the other side asks for personal information. This includes your card CVV or a mail containing an attachment, which requires you to click on embedded links. Be sure to never respond to such emails or calls.***

Human Rights and Cyber Space

Human Rights and Cyber SpaceDay in and day out we find human rights violations and privacy of an individual is at stake with the recent advancements in the cyber space. A sincere effort is made to focus on the asserted boundlessness" of cyber space in order to examine how and to what extent the activities are centered round. Before we go deep into the subject, it is appropriate and necessary to understand the meaning and scope of cyber space.
In the Indian Constitution, the justiciable human rights broadly speaking, were included in part-III, while the non-justiciable social and economic rights were set forth in part-IV in the Directive Principles of State PolicyThe Directive Principles of State Policy are mentioned in part-IV of the Constitution of India covering Articles from 36 to 51. The Directive Principles of State Policy are not enforceable. Universal Declaration of Human Rights speaks of similar rights.

<u>Impact of Cybersecurity on Human Rights</u>

Cybersecurity laws and policies have a direct impact on human rights, particularly the right to privacy, freedom of expression, and the free flow of information. Policymakers have created several national policies with the intention of protecting the Internet and other information communication technologies (ICTs) systems against malicious actors. However, many of these policies are overly broad and ill-defined, and lack clear checks and balances or other democratic accountability mechanisms, which can lead to human rights abuses and can stifle innovation. For example, extreme cybersecurity laws can be used to censor dissidents, monitor communications, and criminalize online users for expressing their views.

References

[1]. https://www.myadvo.in/blog/what-is-the-cyber-law-in-india/
[2]. https://en.wikipedia.org/wiki/Information_Technology_Act,_2000
[3]. http://www.iibf.org.in/documents/cyber-laws-chapter-in-legal-aspects-book.pdf
[4]. https://www.youthkiawaaz.com/2018/06/common-cyber-crime-scenarios-and-applicability-of-legal-sections/
[5]. http://docs.manupatra.in/newsline/articles/Upload/C4971E8F-86E8-48E1-886B-CEF0B774397F.pdf