VOLUME 5 ISSN 2456-9704

CYBER LAW IN INDIA

By Siddharth Sundar & Parth Saluja
From Symbiosis Law School, Hyderabad

ABSTRACT

In India, "Cyber Laws" are handled under the 'Information Technology Act , 2000'(IT ACT, 2000), which came into force on October 17, 2000. The primary objective of which, is providing recognition to electronic commerce(also known as e-commerce) and facilitating the filing of electronic records with the Government. It is pertinent to keep in mind that all the laws that are existing in India are enacted way back. It was virtually impossible to imagine the idea of something called the 'Internet' keeping in mind the socio-economic, cultural, political, and technological scenario(s) of the relevant time. The arrival of the internet gave emergence to a various number of technical glitches and legal loopholes which exist due to the so-called 'cyberspace' required the enactment of Cyber Laws. In a country where the society is becoming more and more dependent on technology, crime which is based on electronic law-breaking will increase inevitable and lawyers need to go the extra mile to provide justice. In this paper, the author shall take a look at the vigorous efforts taken by the law makers to ensure that the 'technology' available is used for the better, ethical, and legal purposes and not for committing crime. The author shall take a look at the laws established to curb the increasing committing of cyber crime from the Indian Technology Act, 2000 to various institutions like Indian Computer Emergency Response Team(CERT-In) , Centre for Development of Advanced Computing(CDAC), and Data Security Council of India (DSCI) in order to enhance the security of Information Technology Systems.

Keywords

Internet , Cyberspace , Cyber Law, E-Commerce, Data Security.

INTRODUCTION.

The Computer based world of Internet is also popularly known as the 'Cyberspace'. The laws that exist in this area are referred to as the 'Cyber laws'. Cyber law can also be defined as the law governing over computers inter-networked all over the world. The growth of economic-commerce, which touches almost all forms of commercial transactions and activities is due to the existence of Cyberspace. This has brought the need for the lawmakers to strengthen the legal infrastructure of the society. Cyber law encompasses laws relating to Intellectual Property, Data Security, and Cyber Crimes. In this article we shall take a brief look at the history of Cyber Law in India. We shall take a look at what Cyber Law is, What is it's need, and why to enforce and strengthen the legal framework related to Cyber Law in India?

II. CYBER LAW - A BRIEF INTRODUCTION.

The word 'Internet' is used in every day speech, before understanding what Cyber Law is, let us see what the Internet is. The internet is defined according to the business dictionary as "A means of connecting a computer to another computer anywhere in the world through dedicated routers and

servers."[1] Now when defined in such a way, the immediate question that pops up is, 'Why connect two computers?' The answer to this question is that when two computers are connected, they can share and access all kinds of information like text, audio, video, graphics, and other computer programs. This allows for the people working in the related field to create various opportunities on the 'Cyberspace'. The various online-shopping sites, streaming websites, etc., are only existing due to the Internet that has connected computers across the world. This has enabled commercial transactions with the click of a key. This is also termed as 'electronic-commerce' (also known as e-commerce). Now that we've taken a look at what the Internet is. Let us see the various ways in which cyber criminals function. Firstly, cyber crimes have been categorized into two for better understanding.

1) Using the Computer as a target.

a)Unauthorized hacking:

Unauthorized hacking is basically gaining access to another computer on the network by instructing or communicating with the logical, arithmetical and memory function resources of a computer. Entry without the permission of the owner or for unlawful purposes is called as Unauthorized hacking. Some hackers code programs that are designed to destroy computers, whereas some hackers code programs that steal credit card information, transfer money from various banks to their accounts.

b) Trojan Attack:

Programs that are proposed as healthy and useful to the user but turn out to be damaging to the computer are called 'Trojans'. They are usually disguised in the forms of excel sheets and games.

c) Virus Attack:

Programs that have the ability to access other programs and infect them resulting in the multiplication of these programs is called a virus.

d) Electronic Mail Attacks (E-mail):

E-mail spamming, bombing, spoofing etc., come under this category.

e) Denial of Service Attacks (DOS):

Flooding computers on the network with requests more than it can handle is called a 'Denial of Service' Attack. It is usually used to disrupt connection between two or more computers on the internet.

2) Using the Computer as a weapon.

Pornography, Cyber Terrorism, IPR Violations , Credit Card Frauds, etc., come under this category.

With the advent of the 'Internet' and 'Cyberspace', Cyber criminals are able to utilize all resources available to disrupt or alter the computers connected on the internet to gain access. With this access, they are able to extract personal information related to the owner and use it for their personal benefits. This is a pressing issue in today's technological based scenario. Almost everyone today uses Computers, Smart Phones and has access to the 'Internet' and is vulnerable to any form of attack. This has brought the need for the law makers to strengthen the legal framework related to

[1] http://www.businessdictionary.com/definition/internet.html

Cyber Law in order to provide justice. In short, Cyber Laws can be defined as the laws that govern over computers that are connected all over the world through the 'Internet'. Cyber Laws govern laws related to Intellectual Property, Data Security and Cyber Crimes in general.

III. WHY DO WE NEED CYBER LAW?

As the world is becoming more and more technology-dependent and digitally advanced, all commercial activities can now be done through the internet. The initial objective of the internet was only to use computers as information-sharing tools. As the internet developed, people managed to use the 'Internet' to satisfy their commercial needs and wants by e-commerce. Thus, all the legal issues that are raised when any form of illicit activity is committed on the internet are governed by the 'Cyber Laws'. There are a variety of reasons as to why we need Cyber Law. The first and foremost of which is the protection of the rights of internet users. Cyber crimes such as, Online Fraud, Share Trading Fraud, Credit Card Theft, Virus attacks etc., are becoming common by the minute. As all the businesses are using the 'Internet' to store electronic data and conduct commercial activities, it becomes quite easy for the Cyber Criminal to access this data through various methods, alter the data newly accessed and benefit from this. To curb the ever-so increasing criminal possibilities that have arisen with the advent of the 'Cyberspace' , the lawmakers need to strengthen the legal framework of the Constitution. Thus, we have Cyber Laws in place to represent and define the norms of the Cyber Society.

IV. CYBER LAW IN INDIA.

Cyber Law in India is governed under the Information Technology Act, 2000, which came into existence on October 17, 2000. Any Cyber Crime committed by any person with a computer , computer system, or a computer network located in India is brought under the purview of this act. Not a lot of cases have been recorded in this field as the Act itself was passed in the year 2000. However we have had a landmark breakthrough judgment in the year 2015. The case of Shreya Singhal vs. Union of India[2]. This case challenged the constitutional validity of Section 66A of the Information Technology Act, 2000 from the perspectives of the principles on which the Indian Constitution was drafted upon. The court declared it's judgment, marking the said section Unconstitutional. It was a landmark judgment because it upheld Section 69A and Section 79 of the Information Technology Act, 2000(intermediaries).

As we can see that there is a certain amount of legal progress in the field, let us take a look at the agencies and institutions set up in the country to curb Cyber Criminal activities and filter the internet.

As we are already aware of the fact that Cyber Crime can only be curbed with proper cooperation from different stakeholders like Internet Users, Service Providers, Industries etc., we need to have adequately staffed institutions set up everywhere in India. The Government has set up an Inter Departmental

[2] *W.P.*(Crl).*No. 167 of 2012*

Information Security Task Force(ISTF). Indian Computer Emergency Response Team(CERT - In) is the agency set up to respond to computer security incidents when they occur. Apart from these, there are a various number of other institutions that have been set up in order to monitor and apprehend Cyber Criminals. Some of these include:

1) National Cyber Coordination Centre (NCCC)
2) Cyber Command for Armed Forces
3) Crime and Criminal Tracking Network & Systems (CCTNS), in addition to the creation of sector-specific CERTs for power sector.
4) Centre for Development of Advanced Computing(CDAC)
5) Data Security Council of India (DSCI)

It is implied that Cyber Criminals can only be apprehended when they victims of the Crime be it an individual or an organization , co-ordinate with the law enforcement agencies for effective response. India, has to effectively improve its mechanisms to secure the Cyber Space and provide maximum Cyber Security. These institutions being set up show progress and help to curb the society of the Deep Web Criminals.

V. CONCLUSION

To sum up the above article, as the technology usage is increasing and effectively improving work-space scenario, it is pertinent to keep in mind that, establishing laws immediately would be the best way to go. The institutions set up by the government are formed primarily with that objective in mind. As this develops, it will be further easier to curb the criminal activities provided this is taken seriously and as an imminent threat. Technology is undoubtedly a double-edged sword, it can be used for good purposes (Businesses, White Hat Hackers etc.,) and for bad purposes(Black Hat Hackers, Online Frauds, Scammers etc.,). Hence, the law makers should take tenacious efforts in ensuring that these activities are minimized and the rate of Cyber Crime in the nation is reduced. villainous computer expert to spread viruses, trojans and malicious software over the internet. Cyber Crime is a threat that is becoming more and more dangerous by the minute. Countries, with inadequate security systems for these kinds of attacks will be immensely vulnerable in the future economy. The only solution for this, is that the governments should analyze their situation and determine if they are in a position to combat such criminal activities, and to the layman, self-protection is the only option, because who knows? You might be the next victim.

REFERENCES

1) https://blog.ipleaders.in/need-know-cyber-laws-india/
2) Shreya Singhal vs. Union of India (*W.P.*(Crl).*No. 167 of 2012)*
3) http://www.businessdictionary.com/definition/internet.html

4) http://www.ey.com/Publication/vwLUAssets/ey-strategic-national-measures-to-combat-cybercrime/$FILE/ey-strategic-national-measures-to-combat-cybercrime.pdf

*****