CYBERLAW, ITS TRENDS AND CHALLENGE IN THE DIGITAL GENERATION

Aarti Singh*

"*Law & Technology seldom mix like oil & water. There is consistent criticism that the development of technology is not met by equivalent movement in the law. Non- recognition of Technology within the sphere of law is only a disservice to the inevitable."* - **N.V. RAMANA.**

ABSTRACT

Cyber laws are made to protect internet users from cybercrime. As we know, with the advancement of technology, with every new invention in technology, cybercrime is also continuously increasing day by day. In this article, the main focus is on cyber law, the need and importance of cyber law, and cyber law in India including the Information Technology Act, 2000. We also have discussed cyber security, types of cyber security, and judicial activism on cyber security.

Keywords: Cyber Law, Cyber Security, Types Of Cyber Security, Cyberattack, Cybercrime, Fraud, Judicial Activism.

INTRODUCTION

In today's times, any kind of data can send and receive via audio, e-mail or video in just a few seconds. But how do we ensure that all data is safe? The answer to this question lies in cyber security. Various changes are taking place in mankind due to these latest technologies but we are impotent to protect our privacy. Computers are the main tools for cyber fraud or cyber crimes. With the help of the internet, various tasks are now performed online. Computers and cell phones now became a part of our day-to-day life. But with the perks of cyber developments, the issue of cybercrime also came. It includes various things like cyberbullying, cyberstalking, cyber terrorism, virtual pornography, identity theft, cyber espionage, phishing, cyber extortion, computer virus programs, computer fraud, computer hacking, spam attacks, etc. There are various categories of cybercrimes. Cybercrimes can be against the individual, against companies, against society, and against the government. Trends in cyber crimes are Ransomware attacks, Pandemic related Phishing, Mobile malware, an Increase in business e-mail compromise attacks, Artificial Intelligence in

*RAJASTHAN SCHOOL OF LAW FOR WOMEN, JAIPUR.

cybercrime, Internet of Things (IoT) in cybercrime, cyber activism, Supply chain attacks, and Data breaches.

CONCEPT OF CYBER LAW

Cyberlaw or Laws of the Internet are the laws that provide legal protection against cybercrime. The legal issues and complexities due to communication technology, particularly the internet are emerging nowadays. Cyber laws provide protection to users. Cyber laws protect internet users from all the illegal or unlawful activities happening in cyberspace. It attempts to face and solve the challenges in cyberspace, created by the misuse of the internet. It tries to investigate criminal activities with the laws or legal system. Cyber laws prevent internet users from cyber-criminal activities by protecting access to information from unauthorized people, e-mail, hardware, websites, software, etc. Cyber laws vary from country to country. Also, cyber laws are different according to jurisdiction. Thus, it is important for a person to know about the cyber law of their respective country. It is important so that they can know which activity is legal and which is not on their network and can prevent unauthorized activities.

AREAS INVOLVING CYBER LAW

Fraud: To protect users from online fraud, cyber laws exist. The most common online frauds are identity theft and credit card. There are state and federal criminal charges for any person who does or attempts to commit online fraud.[1]

Copyright: Copyright basically protects the original works from copying or making a profit from them. In the digital field, cyber laws prevent the infringement of copyright and protect them by encouraging copyright protection.

Defamation: Defamation basically means the communication of false statements by a person about another person and hence, affecting his reputation or injuring the reputation of the other person. Cyber laws provide protection against online defamation.

[1] Preethiga Narasimman, 'Cyber Security Laws and Regulations of 2023' (KknowledgeHut,14 June,2023) https://www.knowledgehut.com/blog/security/cyber-security-laws accessed 25 June, 2023

NEED FOR CYBER LAWS

In this technocrat environment, when the world is shifting to the digital aspects in every field, digitalisation is coming with the increasing rate of crimes. As we all know, initially, the internet was an information-sharing and research tool and was not in so regulated manner. Eventually, with time, especially post-pandemic, everything just shifted to the digital. Everything and anything can be done online with the help of the internet whether it's a business, transaction, or governance; we have the option of e-business, e-transaction, e-governance, e-commerce et cetera.In fact, with the increase in online transactions or e-transactions, online business is made easy. When we are shopping online, online shopping offers various options at times different according to quality, and price. It is more customer friendly as it becomes easy for users to choose one from thousands of products in a single place. Due to all of this, every entrepreneur has his business both online and offline.

But all these benefits come with a risk, a risk of getting fooled by some fake label or product. A risk of online fraud that's why a person should only order from a trusted website or app. As we say, "precaution is better than cure".

All these legal issues related to cybercrime 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 momentum.[2]All the valuable data is on the network whether it's related to any company, government department et cetera. which if hacked, can lead to the stealing of data ultimately resulting in heavy loss and the rise of a great problem. Transactions, signatures, contracts et cetera everything, so, to protect the users from cybercrime related to any online activity the cyber laws developed. Cyber law is important because it touches almost all aspects of transactions in activities and on involving the internet, the world wide web and cyberspace. Every action and reaction in cyberspace has some legal and cyber legal angles.[3]

[2] 'Need for Cyber law in India- Indian Cyber Security' (indiancybersecurity.com) https://www.indiancybersecurity.com/need_for_cyber_law.php accessed 25 June, 2023
[3] Vinit Verma, 'Importance of Cyber Law in India' (Legal Service India) https://www.legalserviceindia.com/legal/article-1019-importance-of-cyber-law-in-india.html accessed 25 June, 2023

CYBER LAWS IN INDIA

Cyber laws are important for the countries like India where we have extreme internet use. The most important act is Information Technology Act, 2000. Information Technology Act, 2000 is the first act that the Indian Parliament approves. The Act defines its object as:

"to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic methods of communication and storage of information, to facilitate electronic filing of documents with the government agencies and further to amend the Indian Penal Code, 1860; Indian Evidence Act, 1872; the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act 1934 and for matters connected therewith or incidental thereto."[4]

With the misuse of technology by humans, cyber-attacks are becoming more dangerous. That's why, the legislation brings various amendments. Various sanctions have been enacted to protect the e-commerce, e-banking and e-governance sectors. Now, it includes almost all the communication devices latest in nature, as its scope has been broadened. Information Technology Act, 2000 provides a safe environment on the internet for internet users in India. There are some important provisions of the act, which are:

Section 43 - Penalty for damage to the computer, computer system, etc[5]

Section 66 - Hacking with the computer system.[6]

Section 66B - Punishment for dishonestly receiving stolen computer resources or communication devices.[7]

Section 66C - Punishment for identity theft.[8]

Section 66D - Punishment for cheating by personation by using computer resources.[9]

Section 66E - Punishment for violation of privacy.[10]

[4]Information Technology Act 2000
[5]Information Technology Act 2000, s 43
[6]Information Technology Act 2000, s 66
[7]Information Technology Act 2000, s 66B
[8] Information Technology Act 2000, s 66C
[9]Information Technology Act 2000, s 66D
[10] Information Technology Act 2000, s 66E

Section 66F-Punishment for cyber terrorism.[11]

Section 67-Punishment for publishing or transmitting obscene material in electronic form.[12]

Technicality in Information Technology (IT) Act, 2000: The act provides a regulatory framework for cyberspace use, also misuse in India. But as we know, Information Technology is an ever-growing field and it is constantly changing, due to which there are some loopholes or technicalities in the Information Technology Act, 2000. First, there are no provisions for spamming and spamming is a major problem nowadays. There are spam emails and messages. Also, there are no provisions for phishing. It is a process in which cybercriminals attempt to acquire information, sensitive in nature, of a person by using electronic means. There are no provisions for the protection of privacy of a person and identity theft which are almost a global problem now. All other developed countries including the USA have strict rules and regulations for the same. There is no mechanism of data protection in Internet banking. The law of Information Technology Act should deal with cyber attacks by providing a regulatory mechanism.

CYBER SECURITY

A practice by which we protect networks, programs, and systems from digital attacks is called cyber security. Cyber security also known as electronic information security or information technology security, usually defends computers, servers, electronic systems, mobile devices, data, and networks from malicious attacks. It is necessary to protect the valuable data and records of an organisation as cybercrime and cyber attacks are growing day by day and nowadays become common. Thus, cyber security is required to protect the users. To safeguards networks, data, and computers from weaknesses, attacks, and unlawful admittance by the internet the technologies and procedures are denoted by cyber security.

TYPES OF CYBERSECURITY

The cyber security is divided into various types:

Network Security: We need network security to protect the users and blog the cyber attacks as most attacks occur over the network.

[11]Information Technology Act 2000, s 66F
[12]Information Technology Act 2000, s 67

Cloud Security: As cloud computing has been increasingly adopted, that's why we need a strategy to control cyber attacks on the cloud.

Mobile Security: The work of mobile security is to protect smartphones and tablets from cyber attacks as they have access to zero-day, corporate data, threats, or business threats from malicious apps, phishing et cetera.

Endpoint Security: By endpoint security, the companies secured their users' data must be end-to-end encrypted.

Internet of Things Security: Internet of Things (IoT) Security protects the devices so that they don't expose their organisation to cyber threats while using the Internet of Things (IoT).

Application Security: Application security prevents users from many malicious apps. As we often see, when we download any app or application on our smartphones or tablets or laptops etc. the application is checked by the security application installed in our communication device. It protects the users from downloading any application which can be used by hackers to hack our data.

JUDICIAL ACTIVISM ON CYBER SECURITY

Here are a few case laws on cyber security:

Avinash Bajaj v. State (N.C.T) of Delhi:[13] In the case of ***Avnish Bajaj v. State*** *(N.C.T) of Delhi*[14], Mr. Avnish Bajaj filed a petition under Section 482 before the Delhi High Court seeking the quashing of the summoning order. A summoning order was issued by the competent Court against the accused, after the prosecution filed a charge sheet against the then Managing Director of Bazee, which was later taken over by E-Bay, accusing he had committed offences under Section 292 of the Indian Penal Code (advertisement/sale of obscene objects) and Section 67 of the Information Technology Act (causing publication of obscene objects on the internet). The court observed a prima facie case for the offence under Section 292 (2) (a) and 292 (2) (d) IPC made out against the website both in respect of the listing and the video clip respectively and held that since the Indian Penal Code does not

[13]Avnish Bajaj v. State (NCT of Delhi), (2005) 116 DLT 427: (2005) 79 DRJ 576
[14]*Ibid*

recognize the concept of an automatic criminal liability attaching to the directory where the company is an accused, the petitioner can be acquitted under Sections 292 and 294 of IPC.[15]

State of Tamil Nadu v. Suhas Kutti:[16] The accused man was the friend of the victim. He desired to get married to the victim, Ms. Roselind, but she got married to someone else rejecting him. Later then she got divorced after which he tried to allure her again. After this rejection was infuriated, and he started to harass the woman by sharing her number and also by posting obscene messages on various groups with the motive of offending her and making people believe that she was a woman of wrongful nature. After which she started to receive messages from unknown people and she was very much insulted. The accused created a fake account in the name of the victim, Ms. Roselind with the intention of harming the reputation of the victim. Based on the above situations, the victim filed a complaint under section 67 of the IT Act, 2000 and under sections 469 and 509 of the Indian Penal Code, 1860.[17]Based on the examination of the facts and circumstances of the case, the honourable judges have passed the judgement by sentencing the accused under section 67 of the Information Technology Act, 2000, section 509 and 469 of the Indian Penal Code, 1860 for his acts which was not only against the legality of the country but also against the morality, posting obscene material and talking ill about women which is shameful and it should be noted that these kinds of acts should be completely stopped in order to protect the woman from various unhealthy remarks.[18]

CONCLUSION

Cybercrime is a very vast topic. Nowadays, everyone is becoming more and more dependent on the internet, this is a very good opportunity for cybercriminals. Computers, tablets, smartphones, etc. are very useful in today's time. Any task can be performed online but at the same time, it attracts criminal activities. So, the government and the lawmakers must create strong laws and acts which help the users to protect their privacy, data, etc. Cyber security aims to protect all internet users by creating useful applications which help in detecting malicious apps. Thus, we need cyber laws and cyber laws must contain strict rules and regulations and also strict punishments for cybercriminals.

[15]Arya Jha, 'Avinash Bajaj v. State (N.C.T) of Delhi' (Indian Law Portal, 24 September, 2020) https://indianlawportal.co.in/avinsh-bajaj-v-state-nct-of-delhi-bazee-com-case/ accessed 25 June, 2023
[16]Suhas Katti v. State of Tamil Nadu (2004), C No. 4680 of 2004
[17]Nagarjun. S, 'Suhas Katti v. State of Tamil Nadu' (Indian Law Portal, 1 January, 2021) https://indianlawportal.co.in/suhas-katti-v-state-of-tamil-nadu/ accessed 25 June, 2023
[18]*Ibid*