ABHIDHVAJ LAW JOURNAL

[www.abhidhvajlawjournal.com]

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

Editor In chief – Assistant Professor Mr. Janmejay Singh

Publisher & Founder – Vaibhav Sangam Mishra

Frequency – Quarterly (4 Issue Per year)

ISSN : 2583-6323 (Online)

CYBER LAW IN INDIA AND THEIR EFFECTIVENESS

AUTHOR'S NAME – Avirup Mondal, LL.B, First Year.

INSTITUTION NAME – MIES R.M. Law College Sonarpur, Kolkata, West Bengal.

ABSTRACT :

Indian law and cybercrime are becoming more and more important challenges as the nation transactions to a digital economy. Although the Information Technology Act of 2000 offers a legal framework to control cyber activity in the nation, its efficacy in preventing cybercrime is still up for question. This article gives a general overview of cybercrime and the law in India and assesses how well the legal system works to combat online threats. Beginning with a definition of cybercrime, the article goes on to explain the numerous cyber threats that are commonly found In India. Except for Information Technology Act measures pertaining to cybercrime have been also added to the Indian Penal Code and the Indian Evidence Act. These laws outline the penalties for transgressions such as child pornographic dissemination, cyberstalking, and online fraud. The Indian government has established numerous organizations including the Cyber Crime Investigation Unit and Cyber Swachhta Kendra, to carry out the enforcement of laws related to cyber offenses. These organizations strive to deter, examine, and inform the public about safe online conduct. Generally, the Indian Government is acting to combat cybercrime and defend its people from threats online. Yet it is crucial for individuals to also take responsibility for their own online safety by exercising good cybersecurity behaviors and being attentive to potential damages.

INTRODUCTION :

No one can deny the fact that the internet and technologies have changed our day-to-day activity dramatically. It made our life easier and more comfortable. It is surely a blessing but it can turn into a curse for some people because of Cyber Crimes. With the Increasing usage of the internet, Cyber Crimes are also increasing day by day. Cyber Crime means committing a crime using the internet and network. Hackers commit this type of crime. To prevent this kind of crime Cyber Laws were introduced through Information Technologies Act which came into action on October 17, 2000. In this article, we will discuss Cyber Crime and Cyber Crime laws in India and how effective it is.

WHAT IS CYBERCRIME :

Using the network, computer, or network-based devices as a tool to commit crimes or do criminal activities can be called Cyber Crimes. People who use the internet carelessly can be the target of cybercrime anytime. Cyber Crimes include committing fraud, identity theft, privacy breaching, stealing debit card & credit card information, spyware installing, ransomware attacks, phishing, child pornography and intellectual property trafficking, cyber terrorism, etc. These crimes are often committed by hackers or cyber criminals who want to make money. This kind of crime is not only a threat to individuals, it can be a threat to the whole nation's security & financial health. Cyber Crime is pretty much a global issue, sometimes it may even hurt a Nation's reputation.[1]

CYBERCRIME LAWS IN INDIA :

Cyber Crime laws are part of the Information Technologies Act, of 2000, and the Indian Penal Code of 1860. The main purpose of cyber law is to protect the legal status of electronic transactions and regulate them. Cyber laws in India have various benefits. It not only helps to grow e-commerce in India but also safeguards the nation & its citizens from cyber threats.

Some important cyber offense sections covered by the Information Technologies Act, of 2000

Section 43[2] – Applicable to cases when someone harms a computer system without the owner's consent. The owner is entitled to claim reimbursement for the total harm[3].

Section 65[4] – Relevant to cases when one manipulates computer source documents intentionally. If proven guilty, the penalty is up to 3 years in Prison and/or a fine of up to Rs. 2 lacks.

Section 66[5] – If someone is discovered dishonestly or fraudulently committed one of the acts listed in section 43, shall be punished with a maximum of three years imprisonment and/or a fine of Rs. 5 lacks.

[1] INFOSECAWARNESS, https://infosecawareness.in/cyber-laws-of-india#:~:text=In%20Simple%20way%20we%20can,to%20the%20Indian%20Penal%20Code, (Last visited Mar 20, 2023)
[2] Information Technologies Act, of 2000, 43, No,21, act of parliament (India)
[3] Nikunj Arora\Cyber crime laws in India\ Blog ipleaders\ (Mar. 27, 2023, 9:29 PM), https://blog.ipleaders.in/cyber-crime-laws-in-india/
[4] Information Technologies Act, of 2000, 65, No,21, act of parliament (India)
[5] Information Technologies Act, of 2000, 66, No,21, act of parliament (India)

Section 66A[6] – Applicable to cases if someone sends displeasing information through a computer or any other communicative device. In 2015 this section was removed as unconstitutional by the Supreme Court.

Section 66B[7] – If any person dishonestly retains a stolen electronic device or computer punishable under this section. Punishment shall be imprisonment up to 3 years or a fine of Rs. 1 lack or both.

Section 66C[8] – If any person is found using an electronic signature, password, or other unique identification feature of another person shall be punished with imprisonment up to 3 years and a fine which can extend up to Rs. 1 lack.[9]

Section 66D[10] – Any individual caught using a communication device or a computer resource to impersonate someone else is punishable with imprisonment up to 3 years and/or a fine up to Rs. 1 lack.[11]

Section 66E[12] – Publishing and spreading images of private areas of the body of someone without their consent shall be punished under this section with imprisonment up to 3 years and/or a fine up to Rs. 2 lacks.[13]

Section 66F[14] – If anyone is found of doing acts of cyber terrorism shall be charged under this section with imprisonment which may extend up to life. It's a nonbailable offense.

Section 67[15] – Applicable to cases when someone publishes or spreads obscene information through computer or electronic devices shall be punished with imprisonment up to 5 years and a fine up to Rs. 10 lacks.

[6] Information Technologies Act, of 2000, 66A, No,21, act of parliament (India)
[7] Information Technologies Act, of 2000, 66B, No,21, act of parliament (India)
[8] Information Technologies Act, of 2000, 66C, No,21, act of parliament (India)
[9] ICLG\ https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india\ Last Visited 31/03/2023
[10] Information Technologies Act, of 2000, 66D, No,21, act of parliament (India)
[11] OP Manocha Ex Senior Scientist\ Violating these cyber laws can land you in jail!\ Times of India\ (Mar. 27, 2023, 9:29 PM)\ https://timesofindia.indiatimes.com/blogs/livesimply/violating-these-cyber-laws-can-land-you-in-jail/
[12] Information Technologies Act, of 2000, 66E, No,21, act of parliament (India)
[13] *Id.* at 3.
[14] Information Technologies Act, of 2000, 66F, No,21, act of parliament (India)
[15] Information Technologies Act, of 2000, 67, No,21, act of parliament (India)

Section 67A[16] – If anyone publishes or transmits any material that contains sexually explicit acts shall be charged under this section with a fine up to Rs. 10 lacks and imprisonment which may extend up to 7 years.

Section 67B[17] – Anyone who publishes, transmits, or encourages the publication or transmission of any electronic content that shows children engaging in sexually explicit acts shall be charged under this section. It also includes encouraging child abuse or luring kids into an online relationship with one or more kids engaging in sexually explicit behavior and providing context text or photos that suggest such behavior. For the first event, such a person shall be punished with imprisonment up to 5 years and a fine up to Rs. 10 lacks. In case of the second incident, such a person shall be charged with imprisonment up to 7 years and a fine up to Rs. 10 lacks.[18]

Some important provisions of cybercrime law covered by IPC

Section 464[19] – Forgery

Section 468[20] – Forgery Pre-Planned Cheating

Section 465[21] – False documentation

Section 471[22] – Presenting a forged document as genuine

Section 469[23] – Reputation damages[24]

Some famous cases of cybercrime in India and its judgments :

[16] Information Technologies Act, of 2000, 67A, No,21, act of parliament (India)
[17] Information Technologies Act, of 2000, 67B, No,21, act of parliament (India)
[18] Jhan_vl3, *Law and Cyber Crimes*, LEGAL SERVICE IN INDIA , (Mar 20, 2023), https://www.legalserviceindia.com/legal/article-6911-law-and-cyber-crimes.html
[19] Indian Penal Code 1860, 464, NO, 45, Acts of parliament (India)
[20] Indian Penal Code 1860, 468, NO, 45, Acts of parliament (India)
[21] Indian Penal Code 1860, 465, NO, 45, Acts of parliament (India)
[22] Indian Penal Code 1860, 471, NO, 45, Acts of parliament (India)
[23] Indian Penal Code 1860, 469, NO, 45, Acts of parliament (India)
[24] Jhan_vl3, *Law and Cyber Crimes*, LEGAL SERVICE IN INDIA , (Mar 20, 2023), https://www.legalserviceindia.com/legal/article-6911-law-and-cyber-crimes.html

- Shreya Singhal v. UOI AIR 2015 SC 1523[25]

In this case, two women were held guilty under Section 66A because of posting unpleasant comments on Facebook. The Supreme Court held that Section 66A violates the fundamental rights of freedom of speech of citizens & and the section was struck down by The SC.[26]

- CBI v. Arif Azim (Sony Sambandh Case)[27]

In this case, Arif Azim used the credit card information of someone else for ordering Sony Colour TV and cordless headphone. He was charged under Sections 418, 419, and 420 of IPC. The court showed sympathy towards the defendant believing he was only 24 years old and it was his first offense. The Court gave him 1 year of probation.

- Avnish Bajaj v. State (NCT) of Delhi[28]

In this case, Avnish Bajaj was the CEO of Bazee.com& he was detained under Section 67 of the IT Act for transmitting cyberpornography. Someone else had sold copies of a CD containing sexual content on Bazee.com.[29] The Court granted him bail in exchange for the production of two sureties worth Rs. 1 lakh each. The Court stated that he was not involved in transmitting pornographic content and further stated owner of such CD was someone else.

- State of Tamil Nadu v. Suhas Katti[30]

In this case, the accused created a fake email in the name of the victim and posted offensive, irritating, and defamatory information about the victim. The defendant was charged under Section 67 of the IT Act and Sections 469 and 509 of the IPC. The court sentenced the accused person to 2 years of rigorous imprisonment along with a fine of Rs. 500.[31]

EFFECTIVENESS OF CYBER LAWS IN INDIA :

[25] Shreya Singhal v. UOI AIR 2015 SC 1523
[26] CYBER LEGAL SERVICES, https://www.cyberralegalservices.com/detail-casestudies.php, (last visited Mar 20, 2023)
[27] CBI v. Arif Azim (Sony Sambandh Case)
[28] Avnish Bajaj v. State (NCT) of Delhi
[29] ashwin\Landmark Cyber Law cases in India\Enhelion\ (Mar. 27, 2023, 9:29 PM)\ https://enhelion.com/blogs/2021/03/01/landmark-cyber-law-cases-in-india/
[30] State of Tamil Nadu v. Suhas Katti
[31] Muskan Sharma, *Landmark Cyber Law Cases in India*, ENHELION, (Mar 20, 2009), https://enhelion.com/blogs/2021/03/01/landmark-cyber-law-cases-in-india/

In the era of technology and the internet cyber crime is a major problem. Cybercrime laws are becoming more and more significant in nations like India, for having extraordinarily high internet users. The usage information, software, e-commerce & online financial activities all are supervised by strict legal cyber laws. Cyberlaw has instilled fear in the hearts of cybercriminals and it makes them hesitate to do such actions out of fear of legal ramifications. A legal framework for authenticating, monitoring, and securing digital records through digital signatures, encryption techniques, etc has been established under IT Act 2000. Cyber laws give e-commerce enterprises the foundation and infrastructure they need to operate legally and safely. One most significant things are the digital signature which was introduced by the IT Act. Digital signature has significantly increased data protection for businesses and it has also improved genuine security in online transactions. Corporate entities or professionals are engaging in the business of serving as a "Certifying Authority" for digital signatures because of cyber laws. Cyber laws also ensure a more secure and simple electronic transaction process. Whenever anybody attempts cyber crime the Act protects corporations by issuing legislative recourse and legal support in the form of monetary compensation or jail.

The IT Act 2000's Chapter XI specifies methods and strategies for dealing with such offenses. Nowadays individuals to organizations are carrying out many transactions over the internet and cyberspace, which can help their business, as well as makes life more convenient and provide them with uncountable knowledge. Notwithstanding some shortcomings, these cyber laws offer effective defenses against cybercrimes.

But as technology always evolves cybercriminals also discovering new ways to bring threats into cyberspace. So Acts also have to be updated from time to time. Indian Cyber Laws still have a broad opportunity for reformation, both provisions and implementations of such provisions to keep the safe internet space for everyone. To combat cybercrimes it is necessary nation is well equipped with strict legal weapons i.e. strict Cyber Laws. Except law people also have to be aware of various cyber threats and how they can keep them safe and how laws are there available for cybercrime victims.[32]

CONCLUSIONS :

[32] MYADVO, https://www.myadvo.in/blog/How-effective-are-Cyber-Laws-in-India/, (last visited Mar 20, 2023)

The purpose of Cyber Crime Laws is to handle offenses like hacking, online fraud, cyberstalking, and phishing, among others. The Information Technology Act of 2000, was revised in 2008 to give more comprehensive coverage of cybercrimes and enhance the punishments for offenders. The effectiveness of these rules has been put to the test recently as cybercrime has greatly increased. The usefulness of laws in preventing cybercrimes is debatable, despite the fact that they have aided to some extent in reducing the frequency of such crimes. The lack of technical expertise among law enforcement officers is one of the main obstacles to the implementation of these regulations. The police and other authorities frequently lack the specific expertise and abilities needed to effectively prosecute many cybercrimes. Investigations are delayed as a result, and laws are not enforced effectively. The complexity of cybercrimes, which frequently cross national and international borders and involve several authorities, is another difficulty. This makes it challenging to find offenders and prosecute them. Also, cybercriminals are always changing their strategies and coming up with new ways to exploit weaknesses. As a result, it's possible that soon the rules and regulations won't be sufficient to deal with new risks. Therefore, even though India's cybercrime laws have been crucial in combating the rising tide of cybercrime, much effort needs to be done to assure their effectiveness. To effectively tackle cybercrime, law enforcement organizations must improve their technical capabilities and work more closely with other organizations and foreign partners. In order to stay up with the changing threat environment, policymakers must also continuously update and strengthen the laws.