IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AN ANALYSIS OF EFFICACY OF CYBER LAWS TO COMBAT CYBER CRIMES IN INDIA

Dattatray Bhagwan Dhainje[i]

Abstract:

In the recent era humans have become increasingly dependent on the internet for all of their needs as technology improves as an internet facility like social networking, online shopping, data storage, gaming, online schooling, and online jobs are all examples of online activities. But in the other hands the crimes also increased in relation to technology like Cyber Crime, Cyber Crime is distinct from any other type of crime that occurs in society, which does not have territorial boundary it includes phishing, Credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, cyber terrorism etc. For this on International as well as National level they formed different types of law for protecting the Cyber Crimes. However, in India There are a lot of statutes and regulations enacted by various authorities that penalize cybercrime. The Indian Penal Code, 1860 and the Information Technology Act, 2000 both laws are penalizing a variety of cybercrimes and unsurprisingly, many clauses in the IPC and the IT Act overlap. This Research paper will focus on analysis of the various types of Cyber Crime and Legislative framework towards cybercrime in India with the help of Judicial decisions.

Key words: Cyber Crime, Types of Cyber Crime, Information Technology, Indian Penal Code, Judicial Decision.

I. Introduction:

The development of technology is the need of hour in the recent days; hence all the men are mostly dependant on the technology because it gets life easier to all in all manner from ordering to accessing everything the internet is also one of the parts of technology. It has been using for various purposes across the world which start from individual to large organisations. Since from last decades, most internet users have been using internet for erroneous goals, either for their own gain or for the benefit of others.[ii] This is the main reason of increasing the Cyber Crime in the world. While the introduction of digital technology or internet propelled mankind into the twenty-first century, criminals did the same. This is a new sort of crime that has spread to

practically every area of people's lives on the Internet.[iii] The term cybercrime is such a broad phrase; it is impossible to characterise it in just one or two sentences.

Cyber Crime refers to all the activities done with criminal intent in cyberspace. These could be either the criminal activities in the conventional sense or could be activities, newly evolved with the growth of the new medium. Because of the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace.[iv] The field of Cybercrime is just emerging and new forms of criminal activities in cyberspace are coming to the forefront with the passing of each new day.

Cybercrime refers to all activities carried out in cyberspace with the goal of committing a crime. These might be traditional criminal activities or activities that have emerged in response to the emergence of the new media. Because of the Internet anonymous character, it is possible to participate in a wide range of illegal actions with impunity, and those with intellect have been badly utilising this element of the Internet to continue illicit operations in cyberspace. The field of cybercrime is still developing, and new types of illegal activity in cyberspace are appearing with each passing day.[v] As in Indian law does not define the phrase "cybercrime" as such; nonetheless, a statute known as the Information Technology Act 2000 or the IT Act 2000 was enacted to combat these sorts of crimes.

II. Etymology of Cyber Crime:

The term Cyber Crime has a long historical development since 3500 B.C., Japan, China, and India have had primitive computers, but Charles Babbage's analytical engine is considered the beginning of modern computers.[vi] In the year 1820, the first Cyber Crime was registered. The loom was invented in France in 1820 by a textile merchant named Joseph Marie Jacquard.[vii] This equipment allows for a continuous succession of processes in the weaving of unique textiles or materials. As a result, Jacquard workers are extremely concerned that their livelihoods and conventional job are being jeopardised, and they choose to sabotage in order to deter Jacquard from using the new technology in the future.[viii] Further there are many incidences on Cyber Crime recently in 2017 Equifax case, in this case Equifax is compromised, revealing 143 million customer accounts, one of the biggest US credit bureaus. Social Security numbers, birth dates, addresses, driver's license numbers, and certain credit card numbers are part of the confidential leaked info.[ix] When social media first became popular in the early 2000's, cybercrime exploded. The inflow of individuals placing all the information they could into a profile database resulted in a deluge of personal information and an increase in ID theft. Thieves exploited the information to get access to bank accounts, create credit cards, and commit other types of financial crime. The criminal activity of cybercriminal is increase day by day.

The term Cyber Crime is defined as illegal conduct in which a computer is utilised as a tool, a target, or both. The following are some definition of Cyber Crime. According to Oxford Dictionary Cyber Crime means "Criminal activities carried out by means of computers or the Internet."[x] Further it can be defined by various authors according to Dr. Debarati Halder and Dr. K. Jaishankar define cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and

mobile phones (SMS/MMS)"[xi] in short it can be say that the Cyber Crime is an offence which can be carried out from the against Individual, criminal motive , through computer or internet for mental and physical harm. The nature of crime is a socially correlated phenomenon. No one has ever lived in a society without Cyber Crime, no matter how hard it tries. In reality, after a crime rate has been reduced to a reasonable level in the real world, how will it be feasible to do so in the virtual world, which is considerably more unreal, eternal, and legally less controllable? However, the nature, breadth, and meaning of crime in a particular culture evolves with time. The concept of a crime-free society is a fantasy, because crime cannot be separated from civilization. As a result, the type of a crime is determined by the nature of a community.

III. Types of Cyber Crime:

There are various types of Cyber Crimes but it basically divided in the three main types, Crime against Individual, Society and government i.e., also called as Cyber Termism. This kind of activities usually involves a modification of conventional crime by using informational technology. Here is the list of prevalent Cyber Crimes, some of them widely spread and some are not prevalent on larger scale. The main Cyber Crimes are discussed as:

Cyber-stalking presents a tangible danger, causing people to be afraid of using computer technology like the internet, e-mail, phones, text messages, webcams, websites, or movies[xii].

Dissemination of Obscene Material the Indecent exposure or Pornography essentially child pornography and hosting of a web site containing this forbidden content are all examples of dissemination of obscene material. These filthy topics have the potential to affect an adolescent's psyche by depraving or corrupting it.[xiii]

Defamation is the act of impugning someone's dignity by hacking his email account and sending filthy messages to an unknown person's email account[xiv].

Hacking It means unauthorized control or access over computer system and act of hacking completely destroys the whole data as well as computer programmes. Hackers usually hacks telecommunication and mobile network.[xv]

Cracking is one of the most serious cyber crimes that has been identified to yet. Cracking refers to a stranger breaking into your computer systems without your knowledge or authorization and tampering with sensitive information and data.[xvi]

Spoofing E-Mails A faked e-mail is one that misrepresents the sender's identity. It demonstrates that its origin is distinct from where it truly comes from.

SMS spoofing is the suppression of undesired unwelcome texts through spam. Wrongdoer obtains a person's mobile phone number and sends SMS over the internet, with the recipient receiving the SMS from the victim's cell phone number. It is a highly serious kind of cybercrime committed against an individual.[xvii]

Carding means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victims bank account mala-fidely. There is always unauthorized use of ATM cards in this type of cyber crimes.[xviii]

Cheating and Fraud The individual who commits cybercrime, such as stealing passwords and data storage, does it with a guilty conscience, resulting in fraud and cheating.

Assault Threatening a person's life or the lives of their family through the use of a computer network, such as E-mail, films, or phones, is known as assault by threat.

Cyber squatting occurs when two people claim ownership of the same domain name, either by claiming that they were the first to register it or by claiming that they were the first to use it or by claiming that they were the first to use anything similar to it. For example, www.yahoo.com and www.yaahoo.com are two identical domain names.[xix]

Vandalism on the Internet Vandalism is defined as the intentional destruction or damage of another's property. When a network service is interrupted or disrupted, cyber vandalism refers to the destruction or damage of data. Any form of physical injury done to a person's computer might fall under its scope. Theft of a computer, a component of a computer, or a computer peripheral are examples of these types of crimes.

Computer System Hacking Hacktivism targets well-known Twitter and blogging platforms by gaining illegal access to and control of computers. Data as well as the computer will be lost as a result of the hacking activity. Furthermore, research shows that such attacks were not just carried out for financial gain or to tarnish a certain person's reputation.[xx]

Transmitting Virus, Viruses that transmit themselves are programmes that attach themselves to a computer or a file and then spread to other files and computers on a network. They generally have an impact on a computer's data by modifying or removing it. Worm assaults have a significant role in influencing people's computer systems.

Cyber trespass Using a wireless internet connection to get access to someone's computer without the owner's permission and without disrupting, altering, misusing, or damaging data or system. [xxi]

Internet Time Thefts Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person. The person who gets access to someone elses ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other persons knowledge. You can identify time theft if your Internet time has to be recharged often, despite infrequent usage.

Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.[xxii]

Cyber Warfare Cyber Warfare is the term used to describe politically motivated hacking and surveillance. It is a type of information warfare that is sometimes compared to conventional warfare, albeit this comparison is debatable in terms of truth and political intent.

Distribution of pirated software This refers to the act of passing pirated software from one computer to another in order to erase government data and records.[xxiii]

Possession of Unauthorized Information It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.[xxiv]

With over 560 million internet users, India is the world's second biggest online market, after only China. By 2023, it is expected that the country would have over 650 million internet users. According to the latest national crime records bureau NCRB data, India saw a total of 27, 248 cybercrime instances in 2018.[xxv]

IV. Legislative framework:

Cyber laws, also known as internet laws and cybercrime laws, were created to keep track of crimes committed via the internet or using computer resources. By allowing the investigation and prosecution of online illegal activities, these rules assist to safeguard users from damage. Cyber laws include the whole legal system as it relates to the internet, cyberspace, and the legal concerns that arise from them. The usage of communicative, transactional, and distributive components of network information technology and devices are all covered by cyber law.[xxvi]

Cyber regulations are crucial in the development of new technology. In today's society, as time becomes increasingly digitally savvy, so are crimes. It gradually grew more accessible to e-business, e-commerce, e-governance, and e-procurement, among other things. It is concerned with all elements of activities and transactions that occur on the internet or through other forms of communication. These rules are required to safeguard businesses and individuals from dangerous online activity. The necessity for cyber regulations has grown in recent years as the number of internet users has increased.

The Information Technology Act, 2000[xxvii] governs cyber laws in India. The Principal goal of this Act is to provide electronic trade legal legitimacy and to make filing electronic records with the government easier. It encompasses a wide range of topics, including data protection, data security, digital transactions, electronic communication, freedom of speech, and online privacy, to name a few[xxviii].

This Act is based on the United Nations Model Law on Electronic Commerce is also known as UNCITRAL Model, which was recommended by the United Nations General Assembly in a resolution dated January 30, 1997. In India, the legislation establishes a legal foundation for e-commerce. It focuses on and addresses digital crimes, sometimes known as cybercrime, as well as electronic trade[xxix]. There are other laws also which deals with cyber crime i.e. Information Technology Amendment Bill of 2008[xxx] amended the statute. The Indian Penal Code of 1860[xxxi] and the Indian Evidence Act of 1872[xxxii]. These Act's were amended by the Information Technology Act of 2000 to take into account the fast changing technological landscape.

The various offenses related to internet which have been made punishable under the IT Act which are Section 65[xxxiii], 66[xxxiv], 67[xxxv], 70[xxxvi], 72[xxxvii],73[xxxviii] and the IPC are enumerated below:

The section 66 plays an important role, this section is extremely important as Right to Privacy has been recently held to be guaranteed as a fundamental right and protected under the Right to Life in Part III of the Constitution of India, in the landmark judgement in Justice K. S. Puttaswamy (Retd.) and Anr. V. Union of India and Ors[xxxix]. Sharing of any content that would be a breach to the privacy of a person, therefore, would also be violating Article 21 of the Constitution of India. Further the Indian Penal Code, 1860 have an important provisions dealing with the Cyber Crime as mentioned above which are Section 503[xl], 499[xli], 463[xlii], 420[xliii], 383[xliv], 500[xlv]. There are also many Act's like Online sale of Drugs under Narcotic Drugs and Psychotropic

Substances Act, Online sale of Arms Arms Act etc. which are dealing with the Cyber Crime in India and help full for eradicating the Cyber Crime from the society.

V. Judicial Decision on Cyber Crime:

India's legal framework for cyber law is established by the Information Technology Act of 2000 and the Rules enacted under it. The Information Technology Act is the primary piece of law that covers various sorts of cybercrime, as well as the fines that may be levied and the compliance requirements for intermediaries. In this sense, there are a number of cases involving cyber laws that are listed below.

The first cybercrime occurred in 1992 when the first polymorphic virus was released. The case of Yahoo v. Akash Arora[xlvi] was one of the earliest examples of cybercrime in India. The defendant, Akash Arora, was accused of utilizing the trademark or domain name 'yahooindia.com,' and a permanent injunction was sought in this case.

The case of Vinod Kaushik and others v. Madhvika Joshi and others[xlvii]is the other example in which the court held that according to Section 43 of the IT Act, 2000, accessing the e-mail accounts of the spouse and father-in-law without their consent is prohibited. In 2011, a decision was reached in this matter. All of these instances deal with the question of how cybercrime has evolved, with a focus on India.

Shreya Singhal v. UOI[xlviii] The Supreme Court's judgement was founded on three concepts: debate, advocacy, and provocation. It was pointed out that just discussing or even advocating for a topic, no matter how unpopular, is at the core of freedom of speech and expression. Section 66A was deemed to be capable of prohibiting all kinds of communication, with no distinction made between simple advocacy or discussion on a specific subject that is disagreeable to some and incitement by such words leading to a causal relationship to public disturbance, security, or health.

Shamsher Singh Verma v. State of Haryana[xlix] In this case, the accused preferred an appeal before the Supreme Court after the High Court rejected the application of the accused to exhibit the Compact Disc filed in defence and to get it proved from the Forensic Science Laboratory.

In the case of Syed Asifuddin and Ors. v. State of Andhra Pradesh and Anr[l]. Held that A "computer" is defined as any electronic, magnetic, optical, or other high-speed data processing device or system that performs logical, arithmetic, or memory functions by manipulating electronic, magnetic, or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities that are connected or related to the computer in a computer system or computer network, according to Section 2(1)(i) of the IT Act. As a result, a telephone handset falls under the definition of "computer" as stated in Section 2(1)(i) of the IT Act.

In the case of SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra[li] This case relates to cyber defamation. The motive behind was Just to malign the reputation of the company and its Managing Director all over the world. The defendant who was an employee of the plaintiff's company used to send derogatory, obscene, vulgar, and abusive emails to his employers and also to different subsidiaries of the said company all over the world.

In the case of Avnish Bajaj v. State (N.C.T.) of Delhi[lii] plaintiff was CEO of a company, which facilitates the online sale of property. An obscene MMS clipping was list for sale on his company with the name of "DPS Girl having fun". Some copies of the clipping were sell by his company and the seller receive the money for

the sale. Plaintiff was arrest under section 67 of the Information Technology Act, 2000. Plaintiff argued and hence court granted bail to him.

VI. Conclusion

The IT Act, 2000 and the Rules promulgated under it control the cyber legal system. The provisions of the Indian Penal Code, 1860, may be invoked where the IT Act is unable to provide for a specific type of offence or does not contain complete provisions for an offence. On the other hand, the current cyber law system is still incapable of dealing with the wide range of cybercrime that exists. As the country develops toward the 'Digital India' movement, cybercrime is continually growing, and new types of cybercrime are being added to the cyber law regime on a regular basis. As a result, a number of legislation adjustments are needed to reduce such offences.

Without prejudice to the efficiency of the current laws in place to prevent cybercrime, the efforts undertaken through legislation at regional, national, and international levels were needs to examined. The International agreement and there impact on the national legal system and on the types of conduct that constitute a cybercrime; the dearth of a global consensus on the legal definition of criminal conduct; the inadequacy of legal powers for investigation and access to computer systems, including the inapplicability of seizure powers to computerised data. The lack of uniformity between national procedural laws concerning cybercrime investigations; and the lack of extradition are all issues that need to be addressed. Challenges in drafting and executing cybercrime legislation.

But Indian legal system tries to prevent such crimes and speed up investigations, for this purpose government amended the laws with respect to crime as well as the as per the situation also the Central Government has made initiatives to raise awareness about cybercrime, issue alerts or advisories, expand capacity or train law enforcement prosecutors or judicial officials, improve cyber forensics capabilities, and so on. Complainants can register complaints against Child Pornography Child Sexual Abuse Material, rape/gang rape imageries, or sexually explicit information using the government's online cybercrime reporting system, www.cybercrime.gov.in. The Indian Cyber Crime Coordination Centre i.e. I4C has been established by the Central Government to manage matters relating to cybercrime in the country in a comprehensive and coordinated way[liii].

References:

[i] Ph. D Research Scholar, Maharashtra National Law University, Nagpur

[ii] Technology Digital World, *How the Internet Has Changed Everyday Life*, Available At Https://Www.Bbvaopenmind.Com/En/Articles/Internet-Changed-Everyday-Life/ Last Seen On 30/1/2022

[iii] United Nations Office On Drugs And Crime, *The Use Of The Internet For Terrorist Purposes*, Pg. 138 United Nations Publication, Available At Https://Www.Unodc.Org/Documents/Frontpage/Use_Of_Internet_For_Terrorist_Purposes.Pdf Last Seen On 29/12/2021

[iv] Vikaspedia, *Cyber Crime – Faqs* , Available At Https://Vikaspedia.In/Education/Digital-Litercy/Information-Security/Cyber-Crime-Faqs Last Seen On 26/12/2021

[v] Cyber Laws Of India, Available At Https://Www.Infosecawareness.In/Cyber-Laws-Of-India

[vi] Sauvik Acharjee, *The History Of Cybercrime: A Comprehensive* Guide, 2021, Available At Jigsawacademy.Com/Blogs/Cyber-Security/History-Of-Cybercrime/ Last Seen On 31/1/2022

[vii] Animesh Sarmah, Roshmi Sarmah , Amlan Jyoti Baruah, *A Brief Study On Cyber Crime And Cyber Law's Of India*, Pg. 2 International Research Journal Of Engineering And Technology (Irjet) E-Issn: 2395 -0056 Available At Https://Www.Southcalcuttalawcollege.Ac.In/Notice/50446irjet-V4i6303.Pdf Last Seen On 16/12/2021

[viii] The Bell Telephone Company Boots A Group Of Young Boys Off The Telephone Grid In New York For Repeatedly And Purposely Misdirecting And Disconnecting Customer Calls Two Years After Alexander Graham Bell Invented The Machine.

[ix] Irini Kanaris Miyashiro, *Case Study: Equifax Data Breach* , Available At Https://Sevenpillarsinstitute.Org/Case-Study-Equifax-Data-Breach/ Last Seen On 5/1/2022

[x] Oxford English And Spanish Dictionary, Synonyms, And Spanish To English Translator, Available At Https://Www.Lexico.Com/Definition/Cybercrime Last Seen On 5/12/2021

[xi] D. Halder, & K. Jaishankar, *Cyber Crime And The Victimization Of Women: Laws, Rights And Regulations*, Information Science Reference. See Also Rashmi Saroha, *Profiling A Cyber Criminal* , Pg. 2 International Journal Of Information And Computation Technology. Issn 0974-2239 Volume 4, Number 3 (2014), Pp. 253-258 Available At Http://Www.Ripublication.Com/Irph/Ijict_Spl/Ijictv4n3spl_06.Pdf Last Seen On 5/12/2021

[xii] Meryl Garcia, *Are You Being Stalked? Here's How You Can File A Complaint Without Visiting The Police Station,* Available At Https://Www.Thebetterindia.Com/45671/Stalking-India-Women-Complaint-Online/ Last Seen On 5/1/2022

[xiii] Monalisha Chowdhury, *India: Legal Provisions In India Against Sharing Of Obscene Content Online In Light Of The Bois Locker Room Incident*, S&A Law Offices, Available At Https://Www.Mondaq.Com/India/Publishing/959952/Legal-Provisions-In-India-Against-Sharing-Of-Obscene-Content-Online-In-Light-Of-The-Bois-Locker-Room-Incident Last Seen On 5/1/2022

[xiv] Kishan Tiwari, What Is Cyber Crime?, Available At Https://Legaldesire.Com/What-Is-Cyber-Crime/ Last Seen N 15/1/2022

[xv] Abhishek Jaiswal, *Cyber Hacking Law In India*, Available At Http://Www.Legalservicesindia.Com/Articles/Cyhac.Htm Last Seen On 30/1/2022

[xvi] Cyber Crime, Available At Https://Www.Shcollege.Ac.In/Wp-Content/Uploads/Naac_Documents_Iv_Cycle/Criterion-Ii/2.3.2/Ppt/Ms_Surabhighai_Cybercrime.Pdf Last Seen On 16/12/2021

[xvii] Neha Saini, *Sms Spoofing: How Scammers Are Using This Technique To Steal Money From Your Account*| Timesofindia.Com Available At Https://Timesofindia.Indiatimes.Com/Gadgets-News/Sms-Spoofing-How-Scammers-Are-Using-This-Technique-To-Steal-Money-From-Your-Account/Articleshow/85096378.Cms Last Seen On 16/12/2021

[xviii] Ibid

[xix] Email Frauds, Available At Http://Www.Cybercelldelhi.In/Emailfraud.Html Last Seen On 16/12/2021

[xx]Electronic Vandalism, *Rights And Responsibilities Of Participants In Networked Communities*, Available At Https://Www.Nap.Edu/Read/4814/Chapter/7 Last Seen On 19/12/2021

[xxi] Ernst L. Leiss, *Computer Viruses* , Encyclopedia Of Physical Science And Technology (Third Edition), 2003 Available At Https://Www.Sciencedirect.Com/Science/Article/Pii/B0122274105008425 Last Seen On 19/12/2021

[xxii] Ibid

[xxiii] Michael Robinsona , Kevin Jonesb , Helge Janick, *Cyber Warfare: Issues And Challenges* , Research Gate, Available At File:///C:/Users/Hp/Downloads/Cyberwarfare-Prepint.Pdf Last Seen On 25/1/2022

[xxiv] Ibid

[xxv]Neha Saini, *Sms Spoofing: How Scammers Are Using This Technique To Steal Money From Your Account*| Timesofindia.Com Available At Https://Timesofindia.Indiatimes.Com/Gadgets-News/Sms-Spoofing-How-Scammers-Are-Using-This-Technique-To-Steal-Money-From-Your-Account/Articleshow/85096378.Cms Last Seen On 16/12/2021

[xxvi] Prateek Singh, Cyber Laws In India: It Act,2ooo, Legal Service India.

[xxvii] The Information Technology Act, 2000, Available At Https://Www.Indiacode.Nic.In/Bitstream/123456789/13116/1/It_Act_2000_Updated.Pdf Last Seen On 5/1/2022

[xxviii] Vinitverma, *Importance Of Cyber Law In India* , Available At Https://Www.Legalserviceindia.Com/Legal/Article-1019-Importance-Of-Cyber-Law-In-India.Html Last Seen On 4/1/2022

[xxix] Diva Rai, *Model Law On Electronic Commerce* , Available At Https://Blog.Ipleaders.In/Model-Law-On-Electronic-Commerce/#:~:Text=It%20also%20helped%20in%20establishment,International%20trade%20law%20in%201996. Last Seen On 1/1/2022

[xxx] Techtarget Contributor, Information Technology Amendment Act 2008 (It Act 2008), Available At Https://Whatis.Techtarget.Com/Definition/Information-Technology-Amendment-Act-2008-It-Act-2008#:~:Text=Information%20technology%20amendment%20act%202008%20(It%20act%202008)&Text=The%20original%20act%20was%20developed,Country%20in%20a%20global%20context. Last Seen On 5/1/2022

[xxxi] The Indian Penal Code Of 1860, Available At Https://Blog.Ipleaders.In/The-Decriminalized-Sections-Under-The-Indian-Penal-Code-1860/ Last Seen On 5/1/2022

[xxxii] Indian Evidence Act Of 1872, Available At Https://Legislative.Gov.In/Sites/Default/Files/A1872-01.Pdf Last Seen On 15/12/2022

[xxxiii] Tampering With Computer Source Documents, Of Information Technology Act Of 2000

[xxxiv] Hacking With Computer Systems, Data Alteration, Of Information Technology Act Of 2000

[xxxv] Publishing Obscene Information, Of Information Technology Act Of 2000

[xxxvi] Un-Authorised Access To Protected System, Of Information Technology Act Of 2000

[xxxvii] Breach Of Confidentiality And Privacy, Of Information Technology Act Of 2000

[xxxviii] Publishing False Digital Signature Certificates , Of Information Technology Act Of 2000

[xxxix] (2017) 10 Scc 1, Air 2017 Sc 4161

[xl] Sending Threatening Messages By Email, Indian Penal Code, 1860

[xli] Sending Defamatory Messages By Email, Indian Penal Code, 1860

[xlii] Forgery Of Electronic Records, Indian Penal Code, 1860

[xliii] Bogus Websites, Cyber Frauds, Indian Penal Code, 1860

[xliv] Web-Jacking, Indian Penal Code, 1860

[xlv] E-Mail Abuse, Indian Penal Code, 1860

[xlvi] 1999 Iiad Delhi 229, 78 (1999) Dlt 285

[xlvii] In The Cyber Appellate Tribunal Appeal No 2/2010

[xlviii] Writ Petition (Criminal) No.167 Of 2012

[xlix] Criminal Appeal No. 1525 Of 2015

[l] 2006 (1) Ald Cri 96, 2005 Crilj 4314

[li] New Suit No. 65/14

[lii] (2005) 3 Complj 364 Del, 116 (2005) Dlt 427, 2005 (79) Drj 576

[liii] Press Information Bureau Government Of India Ministry Of Home Affairs, *Steps Taken To Deal With Cyber Crime And Cyber Security*, Available At Https://Pib.Gov.In/Pressreleaseshare.Aspx?Prid=1579226 Last Seen On 31/1/2022