ARYAVART SHODH VIKAS PATRIKA
RNI TITLED NO. UPBIL04292
RNI REG. NO. UPBIL/2014/66218 PP. NO.- 264-268

ISSN NO.-2347-2944 (Print)
e-ISSN NO.-2582-2454 (Online)
Vol.-15, No.- III, Issues-25, YEAR- July-Sept.-2022

Critical Analysis of Cyber Crime in India

DR. Gaurav Kaushik

Assistant Professor- Department of Law Agra College, Agra (Dr B R Ambekar University) (Residence:- A 703 Manglam Shila, 100 Feet Road Dayal Bagh) Agra (U.P.) India

Received-10.09.2022, Revised-15.09.2022, Accepted-20.09.2022 E-mail: drgauravkaushik76@gmail.com

Abstract: ***The development of computers has provided fraudsters with additional opportunities. The increasing reliance on computers in modern life is the root of the evil known as cyber-crime. Without a question, computers and informatics have significantly transformed society at all levels. India has seen a lot of cybercrime instances over the last several years, and this is cause for significant concern because it directly affects people's social and economic well-being. A difficult and expanding topic of law is cyber law. The Information Technology Act 2000 and the Indian Penal Code 1860 handle the task of penalizing an online offender in the Indian context. These laws make sure that no one is exempt from responsibility and punish violators appropriately. Growing exploitation will accompany increasing use, so it's important to be watchful. The legal system will continue to develop in ways that will ensure that it meets current needs. This type of behavior typically entails the use of computers to alter a traditional crime. Cybercrime is distinct from other types of crime that take place in society. The reason is because it has no geographical limits and that no one knows who the cybercriminals are. It has an impact on all parties involved, including the government, industry, and individuals. The number of cybercrime cases is steadily rising across India's states and cities. The number of people detained in relation to the reported cybercrime instances is substantially lower. Indian cyber laws still need to be improved, as the Information Technology Act of 2000 cannot fully protect our online environment. Therefore, proper enforcement of cyber laws is necessary, along with awareness and wise policy development. This study article aims to investigate numerous cyberlaws issues.***

Key Words: Cybercrime, Information and Communication Technology, IT Act, Indian Penal Code.

Internet exchanges of vast amounts of information are essential in this age of information and technology. It affects all aspects of human life as well as all male age groups. Even if the internet has radically altered our society, there is still a risk of unauthorized access to and damage to the information available online. Information security and safety is now the biggest concern facing society today. Due to the exponential growth in users, cybercrime instances are likewise rising and are not constrained by any national or geographic borders. India has seen a lot of cybercrime instances over the last several years, and this is cause for significant concern because it directly affects people's social and economic well-being.

Crimes performed utilizing electronic equipment, such as smart phones or networked computers, are referred to as cybercrimes or digitalized crimes. Cybercrime can refer to any unlawful or unethical behavior carried out online or using a computer as a tool.

Types of cybercrimes- Cyber-attacks are among the most widespread types of cybercrime, and some of the others are listed below:

1. Distributed denial of Service Attack: "It brings down the server (any server). It is known as the flooding machine with requests in an attempt to overload systems. This attack causes inconvenience, hanging of servers, failure in showing results etc."
2. Spamming: "The act of spamming is a cybercrime which involves sending of unwonted and requested bulk message via email ID or two in individual. There are various types of spamming such as engine spamming, blogs spamming, ad spamming, social spamming etc."
3. Hacking: "It is an act of first identifying a backdoor into others computer in order to gain unlawful and

Corresponding Author / Joint Authors

ISSN NO.-2347-2944 (Print)
e-ISSN NO.-2582-2454 (Online)
Vol.-15, No.- III, Issues-25, YEAR- July-Sept.-2022

unauthorized access to the data inside such computer".

4. Phishing: "Fishing is a kind of cybercrime in which the victim or the target is approved by way of sending spam emails, telephonic calls, SMS by someone who impersonated himself to be a legitimate person or organization in order to gain your personal information".

5. E-Mail Spoofing: "A spoofed e-mail may be said to be one, which misrepresents its origin. It shows its origin to be different from which actually it originates".

6. SMS Spoofing: "Spoofing is a blocking through spam which means the unwanted uninvited messages".

7. Child Pornography: "It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children".

8. Identity Theft: "This is an act of stealing personal information of a targeted individual and later using such information to impersonate him/her".

9. Distribution of pirated software: "It means distributing pirated software from one computer to another intending to destroy the data and official records of the government".

10. 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".

11. Piracy Violation and IPR Infringement: "Most people download movies, games and other digital content from websites and providers such as TORRENT which is pirated material".

12. Malware: "This can be considered as a wide term used for various types of viruses or program that are designed to access the information of the victim without his knowledge and consent".

13. Transmitting Virus: "Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network".

14. Cyber Defamation: "This occurs when defamation takes place with the help of computers and / or the Internet. It is an act of imputing any person to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account".

Causes of cybercrime-

There are "four main causes which lead to the commission of cybercrime" as bellow:-

1. Breach Because of Mobile Devices
2. Embedding Malware Into Legitimate Applications
3. Exploiting Unauthorized Products
4. Unlimited Internet Access

Cyber Legislation in India-

Because of the widespread use of the internet nowadays, a new category of crimes called cybercrimes is growing every day. To stop internet-related criminal activity The Information Technology Act of 2000 was passed primarily with the intention of fostering a business-friendly environment for I.T. The acts that have been rendered punishable are listed in the IT Act. Cybercrimes are now covered by an amendment to the Indian Penal Code, 1860. The following is a list of the numerous online offenses that are punishable under the IT Act and the IPC:

Cybercrimes under the IT Act-

1. Tampering with Computer source documents - Sec.65
2. Hacking with Computer systems, Data alteration - Sec.66
3. Publishing obscene information - Sec.67
4. Unauthorized access to protected system Sec.70
5. Breach of Confidentiality and Privacy - Sec.72
6. Publishing false digital signature certificates - Sec.73

ISSN NO.-2347-2944 (Print)
e-ISSN NO.-2582-2454 (Online)
Vol.-15, No.- III, Issues-25, YEAR- July-Sept.-2022

Cyber Crimes under IPC and Special Laws-

1. Sending threatening messages by email - Sec 503 IPC
2. Sending defamatory messages by email - Sec 499 IPC
3. Forgery of electronic records - Sec 463 IPC
4. Bogus websites, cyber frauds
5. Email spoofing - Sec 463 IPC
6. Web-Jacking - Sec. 383 IPC
7. E-Mail Abuse - Sec.500 IPC

Cyber Crimes under the Special Acts-

1.Online sale of Drugs under Narcotic Drugs and Psychotropic Substances Act

2. Online sale of Arms Act-

Landmark Cases- The Indian legal framework governing cyberspace does not end with the IT Act. Several court rulings have significantly advanced India's system of cyber law. It is important to note the following seminal cyber law cases in India in order to fully comprehend the breadth of the regime-

1. Shreya Singhal v. UOI - "In the instant case, the validity of Section 66A of the IT Act was challenged before the Supreme Court. Two women were arrested under Section 66A of the IT Act after they posted allegedly offensive and objectionable comments on Facebook concerning the complete shutdown of Mumbai after the demise of a political leader. Section 66A of the IT Act provides punishment if any person using a computer resource or communication, such information which is offensive, false, or causes annoyance, inconvenience, danger, insult, hatred, injury, or ill will. The women, in response to the arrest, filed a petition challenging the constitutionality of Section 66A of the IT Act on the ground that it is violative of the freedom of speech and expression. The Supreme Court said that Section 66A condemns offensive statements that may be annoying to an individual but not affecting his reputation. However, the Court also noted that Section 66A of the IT Act is not violative of Article 14 of the Indian Constitution because there existed an intelligible difference between information communicated through the internet and through other forms of speech. Also, the Apex Court did not even address the challenge of procedural unreasonableness because it is unconstitutional on substantive grounds".

2. Shamsher Singh Verma v. State of Haryana- "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. The Supreme Court held that a Compact Disc is also a document. It further observed that it is not necessary to obtain admission or denial concerning a document under Section 294 (1) of CrPC personally from the accused, the complainant, or the witness".

3. Shankar v. State - "The petitioner approached the Court under Section 482, CrPC to quash the charge sheet filed against him. The petitioner secured unauthorized access to the protected system of the Legal Advisor of Directorate of Vigilance and Anti-Corruption (DVAC) and was charged under Sections 66, 70, and 72 of the IT Act. The Court observed that the charge sheet filed against the petitioner cannot be quashed with respect to the law concerning non-granting of sanction of prosecution under Section 72 of the IT Act".

4. Avnish Bajaj v. State (NCT) of Delhi- "Avnish Bajaj, the CEO of Bazee.com was arrested under Section 67 of the IT Act for the broadcasting of cyber pornography. Someone else had sold copies of a CD containing pornographic material through the bazee.com website. The Court noted that Mr. Bajaj was nowhere involved in the broadcasting of pornographic material. Also, the pornographic material could not be viewed on the Bazee.com website. But Bazee.com receives a commission from the sales and earns revenue for advertisements carried on via its web pages. The Court further observed that the evidence collected indicates that the offence of cyber pornography cannot be attributed to Bazee.com but to some other person. The Court granted bail to Mr. Bajaj subject to the

ISSN NO.-2347-2944 (Print)
e-ISSN NO.-2582-2454 (Online)
Vol.-15, No.- III, Issues-25, YEAR- July-Sept.-2022

furnishing of 2 sureties Rs. 1 lakh each. However, the burden lies on the accused that he was merely the service provider and does not provide content".

5. State of Tamil Nadu v. Suhas Katti - "The accused opened a false e-mail account in the name of the victim and posted defamatory, obscene, and annoying information about the victim. A charge-sheet was filed against the accused person under Section 67 of the IT Act and Section 469 and 509 of the Indian Penal Code, 1860. The Additional Chief Metropolitan Magistrate, Egmore convicted the accused person under Section 469 and 509 of the Indian Penal Code, 1860 and Section 67 of the IT Act. The accused was subjected to the Rigorous Imprisonment of 2 years along with a fine of Rs. 500 under Section 469 of the IPC, Simple Imprisonment of 1 year along with a fine of Rs. 500 under Section 509 of the IPC, and Rigorous Imprisonment of 2 years along with a fine of Rs. 4,000 under Section 67 of the IT Act".

6. CBI v. Arif Azim (Sony Sambandh case)- "A website called www.sony-sambandh.com enabled NRIs to send Sony products to their Indian friends and relatives after online payment for the same. In May 2002, someone logged into the website under the name of Barbara Campa and ordered a Sony Colour TV set along with a cordless telephone for one Arif Azim in Noida. She paid through her credit card and the said order was delivered to Arif Azim. However, the credit card agency informed the company that it was an unauthorized payment as the real owner denied any such purchase. A complaint was therefore lodged with CBI and further, a case under Sections 418, 419, and 420 of the Indian Penal Code, 1860 was registered. The investigations concluded that Arif Azim while working at a call center in Noida, got access to the credit card details of Barbara Campa which he misused. The Court convicted Arif Azim but being a young boy and a first-time convict, the Court's approach was lenient towards him. The Court released the convicted person on probation for 1 year. This was one among the landmark cases of Cyber Law because it displayed that the Indian Penal Code, 1860 can be an effective legislation to rely on when the IT Act is not exhaustive".

7. Pune Citibank Mphasis Call Center Fraud - "In 2005, US $ 3,50,000 were dishonestly transferred from the Citibank accounts of four US customers through the internet to few bogus accounts. The employees gained the confidence of the customer and obtained their PINs under the impression that they would be a helping hand to those customers to deal with difficult situations. They were not decoding encrypted software or breathing through firewalls, instead, they identified loopholes in the Mphasis system. The Court observed that the accused in this case are the ex-employees of the Mphasis call center. The employees there are checked whenever they enter or exit. Therefore, it is clear that the employees must have memorized the numbers. The service that was used to transfer the funds was SWIFT i.e. society for worldwide interbank financial telecommunication. The crime was committed using unauthorized access to the electronic accounts of the customers. Therefore this case falls within the domain of 'cyber crimes". The court held that section 43(a) of the IT Act, 2000 is applicable because of the presence of the nature of unauthorized access that is involved to commit transactions. The accused were also charged under section 66 of the IT Act, 2000 and section 420 i.e. cheating, 465,467 and 471 of The Indian Penal Code, 1860".

8. SMC Pneumatics (India) Pvt. Ltd. vs. Jogesh Kwatra- "In this case, Defendant Jogesh Kwatra was an employee of the plaintiff's company. He started sending derogatory, defamatory, vulgar, abusive, and filthy emails to his employers and to different subsidiaries of the said company all over the world to defame the company and its Managing Director Mr. R K Malhotra. In the investigations, it was found that the email originated from a Cyber Cafe in New Delhi. The Cybercafé attendant identified the defendant during the enquiry. On 11 May 2011, Defendant was terminated of the services by the plaintiff. The plaintiffs are not entitled to relief of perpetual injunction as prayed because the court did not qualify as certified evidence under section 65B of the Indian Evidence Act. Due to the absence of direct evidence that it was the defendant who was sending these emails, the court was not in a position to accept even the strongest evidence. The court also restrained the defendant from publishing, transmitting any

ISSN NO.-2347-2944 (Print)
e-ISSN NO.-2582-2454 (Online)
Vol.-15, No.- III, Issues-25, YEAR- July-Sept.-2022

information in the Cyberspace which is derogatory or abusive of the plaintiffs".

Steps To Prevent Cyber Crimes

1. Avoid downloading files from scam emails.
2. Avoid clicking on links from dubious websites and spam emails.
3. Withhold personal information until you are certain of its accuracy.
4. Avoid sending any photos online, especially to strangers and chat friends, as there have been instances of photos being used inappropriately.
5. To prevent unauthorized use of your credit card information, never enter it on an unsecure website.

Conclusion- Cybercrime is a side effect of the remarkable development of the information society and its reliance on internet use worldwide, but especially in India. Because internet is a free-flowing, borderless, and global problem, cybercriminals are not confined by regional boundaries. India has experienced a large number of cybercrime cases during the last few years.

It is a serious issue because it directly affects people's social and economic lives. These scams are spreading widely over the world, but especially in India. This is primarily a result of ignorance on the part of some states, banks, and other institutions. You can find life-altering experiences in the vast pool of cyberspace. More than ever, everyone uses the internet daily.

Both the user and the government play a crucial role in ensuring a secure and enjoyable online experience. The subscriber needs to be vigilant enough to stay current on cybercrime that is common in cyberspace. On the other side, the government creates the necessary laws to make sure that no criminal escapes their responsibility. The biggest problem with cybercrime is that it is constantly changing due to the ongoing development of digital technologies. As a result, new cybercrime strategies and tactics are used.

Because of this, cybercrime should be treated with the same seriousness as other crimes that take place in our society, such as theft, rape, and murder. The Cyber Law regime, however, is still unable to effectively address all of the Cyber Crimes that are now being committed. Cybercrimes are continually changing, and new categories of cybercrimes are being added to the Cyber Law regime every day as the nation moves toward the "Digital India" movement. India's Cyber Law legislation is less strict than those in other countries. As a result, India's Cyber Law framework need significant modifications in order to address the enormous increase in Cyber Crimes each year.

REFERENCES

1. Shreya Singhal v. UOI (2013) 12 SCC 73
2. Shamsher Singh Verma v. State of Haryana 2015 SCC SC 1242
3. Shankar v. State Rep Crl. O.P. No. 6628 of 2010
4. Avnish Bajaj v. State (NCT) of Delhi (2008) 150 DLT 769
5. State of Tamil Nadu v. Suhas Katti CC No. 4680 of 2004
6. CBI v. Arif Azim (Sony Sambandh case) www.sony-sambandh.com
7. Pune Citibank Mphasis Call Center Fraud https://indiankanoon.org/doc/72601833/
8. SMC Pneumatics (India) Pvt. Ltd. vs. Jogesh Kwatra CM APPL. No. 33474 of 2016
9. K.D.Gaur ,Criminology and Penology ,(Deep and Deep publication ,New Delhi,2003)
10. Indian Penal Code 1860 Bare Act 2022 Professional Book Publishers
11. Information Technology Act 2000 Bare Act Universal's New Delhi 2020
12. Types of Cyber Crime and its Causes by Priyanjali karmakar website https://www.legalserviceindia.com/legal/article-3042--types-of-cyber-crime-and-its-causes.html

*****