CYBER CRIMES AGAINST WOMEN IN INDIA: AN ANALYTICAL STUDY WITH SPECIAL REFERENCE TO INFORMATION TECHNOLOGY LAWS

By Dasvinder Singh[*]

ABSTRACT

The Indian civilization is one of the world's oldest civilizations still in existence. In this country, the position of women has been elevated to a higher level. They have been accorded the status of goddesses. However, as a result of the modernization of society, their fundamental rights have been trampled. The sector of information technology in India is experiencing rapid development. People are reliant on computers for a variety of reasons, their day-to-day goings-on and doings. The year 2000 is remembered as a watershed moment in the history of technological advancement. Because of the extensive usage of computer technology, there has been an uptick in cybercrime. In addition, the majority of victims of crimes committed online are female. In this nation of ours, the newest form of criminal activity is known as cybercrime. Different types of illegal activity committed online include cyberstalking, morphing and slander in the digital realm. Emails are being used to harass women in this world today. They have to deal with the issue of cyberbullying. It is quite typical in today's society. The Information Technology Act of 2000 was passed in order to prevent crimes of this nature, but that law will not be particularly successful on its own until people change the way they think about it.

Keywords- Cybercrimes, Digital, India, Information technology, Women etc.

[*] Ph.D. Research Scholar, Panjab University, Chandigarh.

I. INTRODUCTION

Women have been revered as goddesses from ancient times. They have a unique position in the community. Despite occupying a special position within society, they are among the most marginalized groups. Since women's welfare was a top priority for the drafters of the constitution, they are granted a number of rights that are included in the list of fundamental rights. The criminal laws are in place to safeguard women's dignity as well. The crime against women is evolving together with the times. These days, crime is not just restricted to physical harm. People are disseminating pornographic material and harming women's reputations in the name of freedom of speech and expression. One of the most recent forms of crime against women is cybercrime.

Any unauthorised computer-related action is considered cybercrime. While traditional crimes can also be performed while using a computer, cybercrime includes more specialised crimes like viruses and phishing schemes.[1]

In terms of vulnerability to ransomware, spam, and malware in the digital sphere, India is one of the most vulnerable countries. Traditional crimes are not at all like cybercrime. Even while technology is supposed to improve society, it is actually making things worse, especially for women. Cybercrime against women includes instances such as cybertrolling on social media and email harassment, among other things. Additionally, India has created a distinct law to deter cybercrime against women.[2] The Information Technology Act of 2000 makes a good effort to stop cybercrime against women.

II. MEANING OF CYBERCRIME

In a broader sense, cybercrime refers to any illegal activity conducted through or in connection with a computer system or network, including offences like unlawful information distribution and possession.

Hackers trying to get into computer networks were the first to commit cybercrime. A few people did it. Some only to experience the rush of breaking into top-secret networks, but others aimed to obtain private, confidential substance. Eventually, thieves began to introduce computer viruses into networks, which resulted in malfunctions on desktop and laptop

[1] Abhinav Sharma, *Cyber Crimes against Women: A Gloomy Outlook of Technological Advancement* , 1 IJLMH 9, 11 (2018).
[2] *Id.* at 10.

computers. When computers were introduced in the late 1960s, crimes were primarily concerned with physical harm to phone and computer networks. Computer viruses are malicious software or code that has the ability to replicate and cause harm or destruction to systems and data. Where widespread usage of computer viruses occurs, such as banks, governments, or hospitals networks, these activities could be under the heading of cyber terrorism. Cybercriminals also partake in phishing frauds such as credit card theft and requesting bank account numbers.[3]

The word "hacking" is used to characterize the process of changing a product or process to make it work differently or to address an issue. The phrase is said to have started in the 1960s, when it was applied to the actions of some MIT model train enthusiasts who changed the way their trains ran. Those found methods to modify specific features without having to completely redesign the apparatus. When the first computerized phones were introduced in the 1970s, a malevolent link between hacking and systems came under attack. The novel form of criminal activity posed a challenge to law enforcement partly as a result of a lack of laws to support criminal prosecution and a scarcity of investigators knowledgeable about the technologies being compromised. It was evident that criminal behaviour could easily access computer systems, and as consumers gained access to increasingly sophisticated communications, more Cybercrime opportunities increased.[4]

III. OBLIGATIONS ON A GLOBAL SCALE TO COMBAT CYBERCRIME

Investigations into cybercrimes usually take international human rights law into account when analyzing privacy issues. According to human rights standards, laws must be sufficiently explicit to provide a sufficient indication of the situations in which authorities are authorized to employ an investigative measure, as well as that sufficient and there must be strong safeguards against misuse.[5]

Budapest, Nov. 23, 2001 - The Convention is the first international agreement on crimes perpetrated through computer networks, including the Internet. It specifically addresses copyright violations, fraud involving computers, the use of child pornography, and breaches of network security. It also includes a number of authorities and protocols, including as interception and computer network searches. As stated in the preamble, its primary goal is to

[3] G. Tanuja Reddy, *Regulation of Cyber Crimes Against Women – A Critique*, 8 IJIRT 82, 84 (2022).
[4] Dr. Sharmila Rudra, *Cyber Crime Against Women In India*, 28 IOSR-JHSS 26, 28, (2023).
[5] Akhil Bhatt, *Rise of Cyber Crimes against Women in India*, 2 IJRPR 130, 132, (2021).

seek a common criminal policy intended to protect society against cybercrime, particularly by enacting suitable laws and promoting global collaboration. The first and only agreement of its kind on a global scale is the agreement on Cybercrime, 2003. It aims to combat crimes involving computers and the internet by establishing global collaboration among member states, harmonizing national cybercrime legislation, and advancing investigative methods. That was signed on November 23, 2001, in Budapest, and became operative on July 1, 2004. The Accord features an Additional Protocol was implemented on March 1st, 2006. Even if the Convention is a project of the European Union, numerous non-European nations have ratified the same for example, Australia, Canada, Japan, South Africa, Sri Lanka, United States of America et cetera.[6]

India has not yet acceded to the Convention. Bangladesh ought to ratify this Convention as well, as it will enable the nation to participate in the global development of cyber laws. Approval of this Convention will assist the nation in enhance and harmonise national laws pertaining to cybercrimes with global norms and will make it easier for Bangladesh's authorities to contact overseas authorities in order to address cybercrimes. with assurance and efficiency.[7]

IV. DIVERSE FORMS OF CYBERCRIME TARGETING WOMEN

The following are some examples of cybercrimes that target women particularly, among the many other crimes committed against people and society at large:

1. One of the most talked-about online crimes in the modern world is **cyber stalking**. "Stalking" is defined by the Oxford Dictionary as "pursuing stealthily". Cyber stalking is tracking a person's online activities by sending unsolicited and occasionally threatening messages on the message boards the victim frequents, joining the chat rooms the victim frequents, sending unsolicited emails to the victim, etc. Cyber stalking often happens to women who are stalked by males, or to kids who are stalked by pedophiles or adult predators. The victim of a cyber stalker is usually a novice online, unfamiliar with netiquette and Internet security. More than 75% of the victims are female, making them their primary target.

[6] Saumya Uma, *Outlawing Cyber Crimes Against Women In India*, BLR 103, 110 (2017).
[7] Subhra Rajat Balabantaray, *A Sociological Study of Cybercrimes Against Women In India: Deciphering The Causes And Evaluating The Impact On The Victims*, 19 IJAPS 24, 39 (2023).

2. **Email-based harassment** is not a novel idea. It's a lot like sending unsolicited letters. Blackmailing, threatening, harassing, and even email cheating are examples of harassment. E-harassments are comparable to letter harassment; however they frequently cause issues when they are submitted from fictitious identities. The main reasons why people engage in cyber stalking are sexual harassment, love, obsession, retaliation, hatred, ego, and power trips. Cyber stalkers use chat rooms and websites to harass and target their victims. Accessibility in addition to the anonymity these chat rooms and forums offer, free email and website space has also to the rise of online harassment known as "cyber stalking."[8]
3. 3. **Cyber bullying**: With the press of a button, people can now contact with each other anywhere in the world, posing new risks due to technology. Cyber bullying refers to the intentional use of ICT (information and communication technology), especially mobile phones and the internet, to cause distress to another person. Willful and repeated harm inflicted through the use of cyber bullying is by using cellphones, laptops, or other electronic devices, by making menacing or scary communications. India ranks third in the world for cyber bullying, also known as online bullying, behind China and Singapore. Situation of suicides connected to cyber bullying has increased during the previous ten years.[9]
4. Bullies on the internet specifically target women in the same way that they target young teens. In contrast to cyber bullying, which is a recent Asia, in essence, trolls deflect attention from publications. In essence, the posts made by trolls are provocative designed to elicit a significant number of pointless replies.
5. **Morphing** is the process of an unauthorized user altering the original image. Morphing is the process by which an unauthorized person using a false identity downloads the victim's photos, edits them, and then uploads or reloads them. It has been noted that phone users have been observed to download images of women from websites, modify them, and then repost or upload them again on other websites using fictitious profiles. This is equivalent to breaking The IT Act of 2000. The offender may also be charged with criminal trespass under Section 441 of the IPC; Section 290 for causing a public disturbance and Section 292A for publishing or printing obscene or slanderous material subject or topic meant to extort and under Section 501 for defamation.[10]

[8] *Id.* at 41.
[9] Priya Gupta, *Cyber Crime Against Women in Indian Context: An Overview*, 8 JRHSS 75, 76 (2020).
[10] *Id* at 77.

6. One could define a fake email as one that falsely claims to originate from Legal India. It demonstrates how its true source differs from its place of origin. Scamming people online is common and involves email spoofing. The phrase "**email spoofing**" refers to fraudulent email activity wherein the sender's address and other email header components are changed to make it seem as though the email came from a recognized or approved source. Through altering the email's header, from, reply-to, and return-path fields, among other attributes, it is possible for users to make an email appear to be from someone other than the sender.[11]
7. **Cyber torts**, such as libel and defamation, are another prevalent crime committed online against women. While any gender can experience this, women are more susceptible. This happens whenever someone publishes libelous content online or through the use of computers, disparaging remarks about a person on the internet or sends all of their friends vilifying emails.

V. LEGAL FRAMEWORK TO REGULATE CYBERCRIMES

The constitution's Article 19(1)(a) guarantees the basic right to free speech and expression. Article 19(2) mentions reasonable constraints that can be placed on this right, making it non-absolute. Following its 2008 modification, the Information Technology Act of 2000 established such reasonable limitations. These take the form of authority given to state or federal governments to provide directives for interception, observation, or decryption of any data via any Indian computer source.

For millions of internet users, the freedom of expression has been extended since the invention of the internet. The internet encourages speech and expression as a fundamental right, and information wants to be freely available. The case of *Neelam Mahajan Singh* v. *Commissioner of Police* concerns the equilibrium between the rights to free speech and right to know. It was decided that in the sake of free speech and public morality, we shouldn't try to pander to everyone who can read or write. Public space and the right to free speech and expression should coexist in harmony. But the former must yield when the latter is gravely violated.[12]

Ritu Kohli's otherwise flawless wedded life in New Delhi was flipped upside down when she began getting several emails from an unidentified sender. She initially disregarded the emails.

[11] Sameera Khan, *Cyber Crimes against Women in India: A Torment in Society*, 3 IJLSI 170, 179 (2021).
[12] Jaspreet Singh, *Violence Against Women In Cyber World: A Special Reference To India*, 4 IJARMSS 60, 72, (2015).

Stalker posted her home phone number and other personal information online, using foul and offensive language, urging people to give her a call. Consequently, she began to receive several lewd calls at strange hours from all over the place, and then she became frightened. Kohli, distraught, reported the incident to the police. Thankfully, Delhi police moved quickly to stop it. They located the hacker's IP address, or Internet Protocol address, in a cybercafé. Manish Kathuria, the cyberstalker, was later taken into custody by the Delhi police and was charged for insulting the modesty of a person under section 509 of the Indian Penal Code. women and in accordance with the 2000 IT Act (Information Technology Act). [13]

Neha Ghai, a 28-year-old woman, was horrified in another instance of cyber stalking that was reported. On her cell phone, she received offensive calls and texts, and her mailbox even contained lewd emails. She discovered when she went to the cyber cell to file a complaint against the accused that she has become a target of cyber stalking, where the stalker amassed all of her personal information put on offensive gateways. These days, cyber stalking has grown to be a significant problem, and victims should contact the police right away. By following the IP (internet protocol) address of the system being used for the accused, the police can locate the criminal behavior.

The right to privacy is closely related to how information is shown in the digital sphere. The internet is becoming a necessary tool for communication, and people utilise it to exercise their right to free expression and The Indian Constitution guarantees freedom of expression. However, because this freedom is not unrestricted, adjustments are also contemplated in the IT Act. The entire IT Act's Section 66A was invalidated by the court in *Shreya Singhal* v. *Union of India* in 2015, claiming that because of the language employed in Article 19(2) of the Constitution, it was not spared terms like "menacing", "grossly offensive", "annoying", and "causing annoyance" in this section. Other than not tripping within any of the classifications that speech restrictions can be applied to, section 66A was overturned due to vagueness, excessive width, and chilly impact.[14]

The Indian Cyber Law is the name given to the Information Technology act of 2000. It is the primary piece of legislation in India that governs the use of computers, computer networks, computer systems, communication devices, and electronic data and information.

[13] *Id.* at 74.
[14] Syed Fahad Hussain, *Cyber Crime against Women in India: Issues and Challenges*, 10 ANTHRO. BULL.75, 77 (2018).

This law has addressed a number of criminal justice issues, including network provider liability and cybercrimes. The aforementioned act was modified in 2008. As a result of the legislation, all types of phones, tablets, and personal digital data have been included in the scope of cyber legislation. The act primarily addresses internet business, but a few of its clauses address offences against the human body. The Act's principal provisions are listed below.[15]

Section 67 of the Information Technology Act prohibits the publication and transmission of pornographic materials on the internet that could cause disturbances to public morality and public order. It is predicated on IPC Sec. 292. However, the IT Act of 2000 imposes harsher penalties. This crime is subject to bail.

Sending insulting communications through communication devices was prohibited by Section 66 A. computer assets. It becomes illegal under Section 66A if it is sent via a computer resource. Anything that is blatantly offensive Anything that has a frightening quality Any information that you are aware is untrue yet is delivered with the intention of offending would fall under this section. It is crucial that 66A attempts to address the issue of spam in a limited way. However, this clause was declared unconstitutional by the hon'ble Supreme Court of India.[16]

Identity theft is now a crime according to Section 66 C. This offence qualifies as a bailable offence in which the Bail is a legal right for those who are accused, even in the event of an arrest.[17]

If someone uses a computer system, computer networks, computer resources, or communication devices to impersonate someone who has previously passed away, that person is considered to have committed the section 66 D crime of cheating. To further define the charge of privacy breach, Section 66E has been expanded. The necessary actions are as follows capturing publishing and transmitting. Transmit refers to sending a visual image electronically.

To avoid cybercrimes, the National Cyber Security Policy of 2013 is there. India now has a policy that lays out the legal foundation for the country's efforts to promote cyber security. There are 14 goals to establish an Indian cyber ecosystem. One of the main goals is to make national monitoring easier and the expansion of cyber infrastructure.

[15] *Id* at 78.
[16] Dr. Shalini Kashmiria, *Mapping Cyber Crimes Against Women In India*, 1 IRJCL 22, 32 (2014).
[17] *Id.* at 34.

VI. CONCLUSION AND SUGGESTIONS

Cybercrime against women is growing rapidly, with new offences including gender bullying and trolling emerging and becoming a more prevalent type of cybercrime. However, such offences are not covered by the IT Act 2000, and the procedure for an investigation is not necessary. Act does not address gender bullying or cyber trolling, which is one of the Act's shortcomings. For the study, a separate unit must be established. Particular instruction is required be assigned to the police to handle online offences against women. The nation's judicial system ought to attempt to successfully address the issue of cybercrimes against women.

REFERENCES

- Abhinav Sharma, *Cyber Crimes against Women: A Gloomy Outlook of Technological Advancement*, 1 IJLMH 9, 11 (2018).
- Akhil Bhatt, *Rise of Cyber Crimes against Women in India*, 2 IJRPR 130, 132, (2021).
- Dr. Shalini Kashmiria, *Mapping Cyber Crimes Against Women In India*, 1 IRJCL 22, 32 (2014).
- Dr. Sharmila Rudra, *Cyber Crime Against Women In India*, 28 IOSR-JHSS 26, 28, (2023).
- G. Tanuja Reddy, *Regulation of Cyber Crimes Against Women – A Critique*, 8 IJIRT 82, 84 (2022).
- Jaspreet Singh, *Violence Against Women In Cyber World: A Special Reference To India*, 4 IJARMSS 60, 72, (2015).
- Priya Gupta, *Cyber Crime Against Women in Indian Context: An Overview*, 8 JRHSS 75, 76 (2020).
- Sameera Khan, *Cyber Crimes against Women in India: A Torment in Society*, 3 IJLSI 170, 179 (2021).
- Saumya Uma, *Outlawing Cyber Crimes Against Women In India*, BLR 103, 110 (2017).
- Subhra Rajat Balabantaray, *A Sociological Study of Cybercrimes Against Women In India: Deciphering The Causes And Evaluating The Impact On The Victims*, 19 IJAPS 24, 39 (2023).
- Syed Fahad Hussain, *Cyber Crime against Women in India: Issues and Challenges*, 10 ANTHRO. BULL.75, 77 (2018).

****