Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777796

ADVANCE TECHNOCRATIC NATURE OF INDUSTRIAL SOCIETY AND THE CYBER CRIME AGAINST WOMEN OCCUPIED IN LEGAL FRAMEWORK

Manjeet Singh

Ph.D. Management, Amity Business School, Amity University Chhattisgarh

Dr Satyendra Patnaik

Professor & Dean, Amity Business School, Amity University Chhattisgarh

Abstract

As of June 2016, the use of the internet is recognised as a human right by the United Nations Human Rights Council. The number of people using the internet is also increasing quickly in India, and the concept of a modern India has placed a heavy emphasis on science and technology as the means to the end of complete and all-encompassing development. The authors of this study want to investigate whether or not the rise of internet and social media has contributed to the epidemic of cybercrime against women in India. In Industrial society ,women online are more vulnerable to cyber-crimes, which occur when illegal activity is conducted online. To stay one step ahead of such criminals, the judicial system, together with the police and investigative agencies, should be equipped with cutting-edge web-based apps. Cybercrime has been highlighted, and the legal remedies available under several pieces of law dealing with the threat of cybercrime have been highlighted as well. The article also discusses in depth the government's participation in the present legal system, as well as the government's responsibility for its actions. Focus will also be given to the causes and consequences of the rise in cybercrime directed towards women. In light of the paper's findings, it is concluded that neither the provisions of the Indian Criminal Code, 1860 nor the Information Technology Act, 2000 adequately deal with such offences and fail to give sufficient precautions to prevent the same. Finally, the author(s) proposes a set of required steps that must be adopted to comprehensively and effectively address the problem of cybercrimes against women.

Keywords: *women, cybercrime, Information, technology, legal.*

1. INTRODUCTION

It's no secret that cybercrime affects countries all over the world. Cybercrime and the targeting of women have increased dramatically since the rise of digital technologies, and both constitute a serious risk to individual safety. India is one of the few nations to pass legislation to tackle cybercrime, however despite this, the IT Act of 2000 makes no mention of women's difficulties. Act has defined as crimes such as hacking, disseminating obscene content online, and tampering with data. While this Act does a lot to protect women's safety, it does not address every possible danger that they face. Children are not immune to the effects of cyberbullying. The goal of Safety Web is to help parents keep their children safe while using the internet. We

are taking both legal and technical steps to secure our digital infrastructure from harm. Yet, modern technology does not recognise national borders; it flows more readily over the globe, which means that criminals are increasingly situated in locations remote from the sites of their actions' consequences. Cybercrime refers to any illegal behaviour in which a computer or network is utilised in any way (as a source, tool, or target). Cyberspace is the next frontier of machine-controlled information[1]. The idea of cybercrime targeting women is very fresh in India. When India first began its foray into the realm of IT, the Information Technology Act of 2000 prioritised safeguarding electronic commerce and communications above cyber socialising and communications. Cyber Victimization of Women and Cyber Laws in India revealed the Act to be an incomplete piece of legislation. The goal of this research was to bring attention to the problem of cybercrime against women in India. In a nation like India, where the incidence of crime committed against women is growing like a coconut tree, the safety of women has always been a concern. In the past, this only occurred on roadways or in foreign locations. Once upon a time, a woman's own home was the best location to avoid becoming a victim, but times have changed. Their own neighbourhood is becoming as criminal as the streets outside. Nevertheless, they only have access to what's on their displays. This is of extreme importance. An individual woman may experience an increase in insecurity due to the rising frequency of cybercrime directed at women. These people are no longer able to go anyplace and feel secure. When we consider the bigger picture, we see that it has much greater consequences for people and for society at large.[2]

2. MEANING AND ORIGIN OF CYBERCRIME

In its broadest sense, the term "cybercrime" refers to any sort of illicit activity that is carried out through or in connection with a computer system or network[3]., Hackers' attempts to penetrate computer systems marked the beginning of cybercrime. Some did it for fun, simply to see what it was like to hack into top-secret networks, while others had more sinister motives. In the end, thieves began deliberately infecting computers with viruses, which caused widespread system failures in homes and businesses.[4] When computers first appeared in the late 1960s, most crimes included the destruction of hardware, such as computer systems or telephone lines.

Computer viruses are malicious software or pieces of code that may replicate themselves and do severe harm to a computer's files and operating system. Cyberterrorism may be committed when computer viruses are employed on a big scale, such as with bank, government, or hospital networks. Phishing schemes, in which the victim is tricked into disclosing personal information such as bank account or credit card data, are another common tactic used by computer criminals.[5] The word "hacking" refers to the practise of making unauthorised changes to software or hardware in order to improve performance or address a specific issue. The phrase was supposedly coined in the 1960s to characterise the actions of a subset of model railroad

[1] Desai, M. and Jaishankar, K (2007). Cyber Stalking-Victimization of Girl Students: An Empirical Study.
[2]Shobhna Jeet, "Cyber-crimes against women in India: Information Technology Act, 2000" Elixir Criminal Law 47 (2012) 8891-8895, Elixir International Journal.
[3] . Tiwari; Garima, Understanding Laws Cyber Laws & Cyber Crimes(Lexis Nexis Publication), 2014, Pg no. 8
[4]https://study.com/academy/lesson/what-is-cybercrime-definition-history-types-laws.html
[5] https://study.com/academy/lesson/what-is-cybercrime-definition-history-types-laws.html

fans at Massachusetts Institute of Technology who altered the way their trains worked. They figured various methods to modify the device's performance without having to redesign it from the ground up. The 1970s saw the first attacks against computerised phone systems, cementing the negative connotation that has since followed the practise.[6] Law enforcement agencies had a hard time dealing with this novel kind of crime because there was a dearth of laws to help in criminal prosecution and an absence of detectives with expertise in the technology being hacked. It was obvious that computers might be used for illegal activities, and as consumers gained access to more sophisticated forms of communication, the potential for cybercrime increased.[7]

3. VARIOUS KINDS OF CYBER CRIME AGAINST WOMEN

Some examples of cybercrime that disproportionately affects women are listed below: –

- Cyber-stalking.
- Harassment via e-mails.
- Cyber Bullying
- Morphing.
- Email spoofing.
- Cyber Defamation.
- Trolling and Gender Bullying

Categories of Online Violence Against Women: –

Cyberstalking: One of the most often discussed types of online crime nowadays is cyberstalking. Stalking is defined as "stealthy pursuit" in the Oxford lexicon. Cyberstalking is the practise of keeping tabs on a person online and harassing them via various means, such as accessing chatrooms they frequent, sending them unwanted emails, putting threatening remarks on message boards they visit, etc. Women are disproportionately targeted by male cyber stalkers, whereas male paedophiles target youngsters. The victim of a cyber stalker is often a novice Internet user who is unaware of basic online safety practises. Their primary objective in doing so is Women make up over 75% of the casualties.

HarassmentEmail harassment is not a novel phenomenon. It's quite close to letter-based harassment. Email may be used for all kinds of abusive purposes, from blackmail to threats to bullying to even infidelity. Similar to snail mail harassment, e-mail harassment may become problematic when submitted under a bogus identity. Cyberstalking might be motivated by sexual harassment, infatuation with a romantic partner, vengeance and hatred, or a desire for

[6] https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/
[7] https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/

power and control. Cyberstalkers harass their victims using a variety of online mediums, including but not limited to websites, chat rooms, discussion forums, open publishing websites (such as blogs and Indie media), and email. Free email and web hosting, together with the anonymity offered by online chat rooms and message boards, have all led to the rise of cyber stalking as a form of harassment.

Cyber Bullying-Now, individuals from all over the globe may instantly share information and ideas with one another, but this convenience also brings new vulnerabilities. According to Childnet International, "cyberbullying" occurs when one person uses ICT (especially mobile phones and the internet) with the intent to cause distress to another. Bullying in the digital era is defined as "the intentional and repetitive damage caused via the use of computers, mobile phones, or other electronic devices by sending messages of an intimidating or threatening character." As compared to China and Singapore, India ranks third in the world when it comes to cyber bullying, also known as online bullying [Simhan]. Instances of suicide attributed to cyberbullying have increased over the previous decade.

Morphing-Images that have been morphed have had unlawful changes made to them. Morphjacking occurs when a hacker uses a false identity to obtain a victim's photos, alters them, and then reuploads or reloads them. False users have been seen stealing images of women off the internet, modifying them, and then uploading them to other sites under fictitious identities. There has been a clear breach of the Information Technology Act of 2000. In addition to Section 501 for defamation, Section 441 for criminal trespass, Section 290 for public nuisance, Section 292A for printing or publishing grossly indecent or scurrilous matter, or matter intended to blackmail, and Section 501 for defamation are all possible charges against the offender under the Indian Penal Code.

Email Spoofing-A faked email is one that falsely claims to have come from a different address [Legal India]. It reveals that the true origin of the item is not where it claims to have come from. Spoofing emails is a common kind of internet fraud. Email spoofing refers to a kind of email fraud in which the sender's address and other portions of the email header are changed to make it look as if the email came from a trusted or legitimate sender. By altering the email's header, from, Return-Path, and Reply-To fields, etc., malicious individuals may make the email seem to be sent by someone else.

Cyber Defamation-Another prevalent online crime against women is cyber tort, which includes slander and defamation. Although both sexes are susceptible, women are often hit harder. Online defamation happens when an offender uses a computer or the Internet to spread false information about another person to a large group of people, for as when they post false information about someone on a website or send a chain email to everyone in their contact list.

Trolling and Gender Bullying-Gender bullying and trolling[8] are two forms of cybercrime against women that have received surprisingly little attention in India. Women experience cyberbullying at the same rates as younger teens[9]. Cyberbullying, on the other hand, is a

[8] Halder Debarati, Jaishanker,H; Cyber Crimes Against Women In India,pg. no. 43
[9] Ibid

relatively recent development in India. Trolls essentially detracts from the primary purpose of publishing. The primary goal of the troll's postings is to spark a flood of irrelevant comments.[10]

The National Crime Records Bureau (NCRB) of India has made available crime data for the previous calendar year. The NCRB has supplied crime statistics expressed as crimes per one lakh of the population to facilitate meaningful comparisons. Also, the Bureau has separated information on crimes like murder and violence against women. Lucknow has the highest incidence of violence against women (279 cases per 100,000 residents), followed by Delhi (52), Indore (130), Jaipur (128) and Kanpur (129). (118). Coimbatore(7), Chennai(15), Surat(28), and Kolkata(32) have the lowest recorded rates (29). As can be seen from the above, the four Indian cities of Delhi, Jaipur, Lucknow, and Indore have the highest overall crime rates.

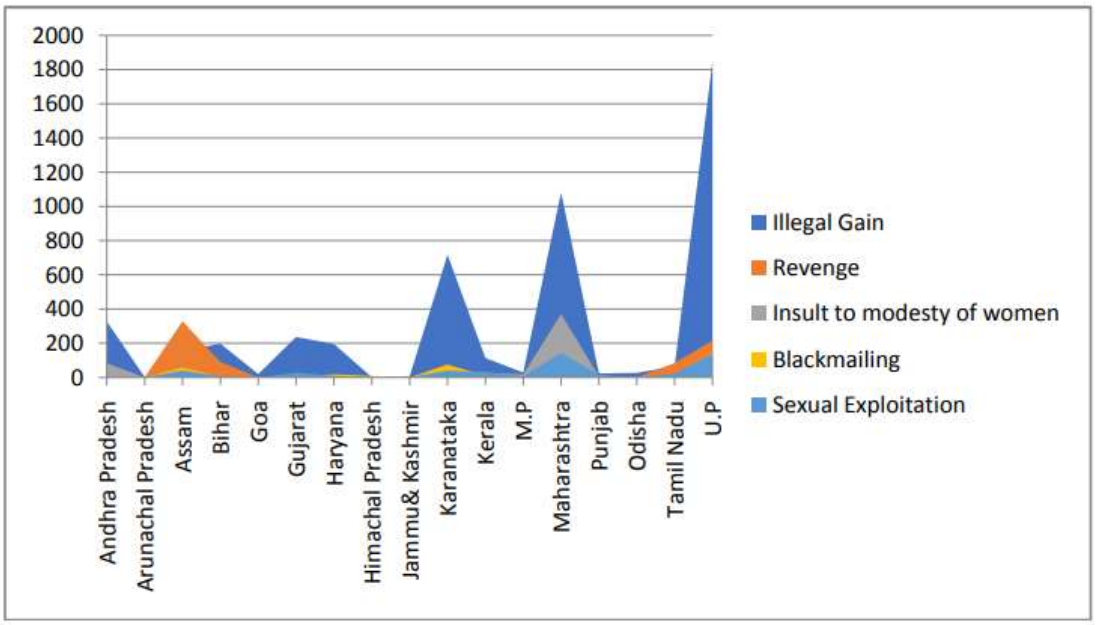

Fig 1: Crime Rate in India

4. IMPACT OF CYBER-CRIME

Women have been hit harder than males by the current wave of technological progress. Nowadays, digital interventions—that is, computer technical interventions—are present in every aspect of human existence. When seen in this way, both the benefits and drawbacks become apparent. The problem of cybercrime is widespread. With the rise of modern technology come new dangers, including an increase in cybercrime and the targeting of women, both of which represent serious threats to individual safety. Increasing cybercrime poses a challenge to individuals' right to privacy and safety online[11]. The Internet is a massive network and informational superhighway that spans the globe. Internet use statistics reveal the consequences of the expanding base of users as telecommunications infrastructure expands into

[10] Ibid pg 62
[11] http://www.legalserviceindia.com/artic les/etea.htm

more rural areas. With the Internet's incorporation into the globalisation process, which is plainly washing away old realities and certainties and giving rise to new possibilities and problems connected with living in a compact globe, this statement is no longer true. Cyberspace is a gift to modern humanity. The advent of the internet has allowed communication amongst individuals all over the world. Human beings can't help but be curious about the world around them. The need to find the untraveled road has been amplified by the curiosity about the world's inhabitants. Because of this, the Internet and other cyberspace have become more widely known.[12]

- The social networking websites have developed a new arena for socializing.
- All segments of society's female population, regardless of demographics, are celebrating their newfound freedom with equal fervour.
- It has simplified many aspects of life for women in India, including shopping, banking, travelling, and even filing taxes.
- Within the limits of their culture, it has empowered women to struggle for equality.
- They may now tell the world about their trials and triumphs; doing so inscribes new domains of authority alongside the information they acquire.
- Although there are many positive effects of the internet, the increasing prevalence of cybercrime has made it unsafe for women to use the internet alone.
- The emergence of the internet has created a dangerous environment for women of all ages and social classes.
- As compared to other women, what distinguishes Indian women as targets of internet violence?
- Victims of any kind of violence, especially those committed against women, are often held responsible in India, a nation where patriarchy and orthodoxy prevail.
- Information and communication technology penetration provides several advantages, and the number of users who take use of these benefits grows steadily.
- The decrease in the price of Internet-capable gadgets has also contributed to this expansion.
- Because of the widespread use of ICT, the market for related goods and services has expanded rapidly.

[12] Fabio Marturana, Simone Tacconi and Giuseppe F. Italiano (2013). Cybercrime and Cloud Forensics: Applications for Investigation Processes (pp. 313-330).

- The information and communication technology industry, which influences many facets of the economy.

- A major player on a global scale as a leading supplier of cutting-edge ICT-enabled solutions and services; excels across several measures of success, including economic prosperity, social cohesion, and ethnic and gender balance.

- programmes that rely on information technology to function, such as those provided by the government to its citizens, public distribution networks, healthcare networks, educational networks, banking networks, etc.[13]

The survey queried female social media users about the specific cybercrime issues that had arisen for them. 5.45% of users have had their profiles hacked, 3.9% of their photos morphed, 28.4% of their emails contained offers, 5.15 % of them fell victim to romance or dating scams, 6.75 % of them were victims of cyberbullying, 4.6% of them were victims of information trolling, and 1.2% were victims of link baiting. The majority of respondents have experienced problems while utilising social networking sites, such as scams, hacking, cyberbullying, cyberromance, and link baiting.

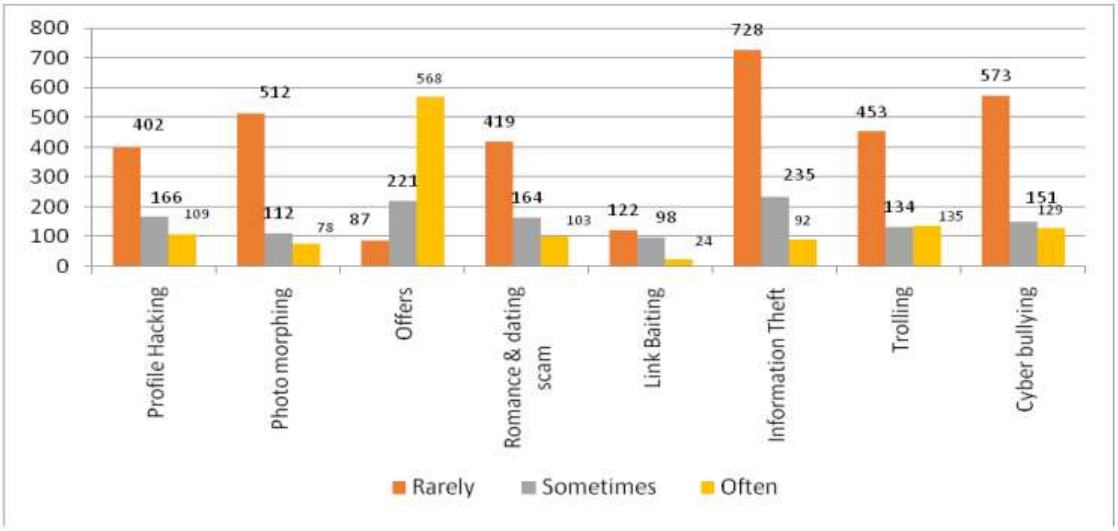

Fig 2: Social Media Crime among Women

Women have been surveyed on their familiarity with the laws that protect them from being victimised by cybercriminals on social media platforms. There were around 78.4% "No" responses and 21.6% "Yes" responses. Seventy-four percent of those in Chennai who responded said no, while just twenty-five and a half percent said yes. The majority (82.5%) residents said "No," while just 17% agreed. Most women online do not know they have legal recourse when cyber-crime occurs on social media.

[13]Sarabjot Singh Anand, Arshad Jhumka and Kimberley Wade (2011). International Journal of Digital Crime and Forensics (pp. 16-34).

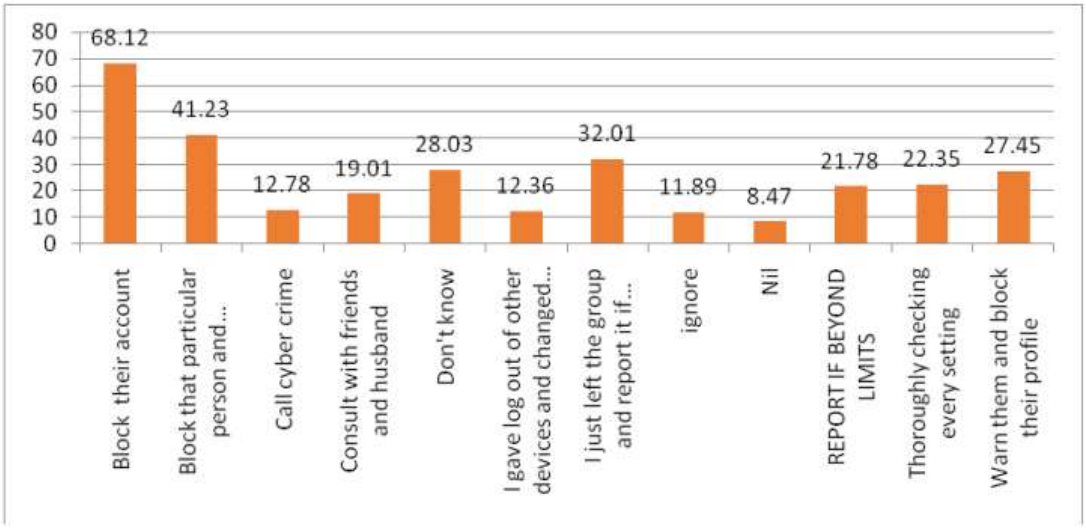

Fig 3: Women Familiar with the Laws

5. LEGAL PROTECTION (REMEDIES)

Case of *Suhas Katti v. State of Tamil Nadu*, decided in 2004 by a Chennai Court, resulted in the first conviction in India for cyber pornography.[14] When she declined the man's marriage proposal, the divorcee reported him to the police because he was sending her offensive, slanderous, and irritating comments in a Yahoo messaging group. The defendant allegedly created a fake email account in the woman's name and forwarded messages sent to it. Many individuals who thought the victim was asking for sex called her, assuming she was. A First Information Report was filed with the police in February of 2004, and a conviction was reached by the Chennai Cyber Crime Unit only seven months later. Katti was given two years of rigorous imprisonment and a fine of Rs. 500 for violating Section 469 of the Indian Penal Code (forgery with the intent to cause damage to someone's reputation), one year of simple imprisonment and a fine of Rs. 500 for violating Section 509 of the Indian Penal Code (words, gestures, or acts intended to insult the modesty of a woman), and two years of rigorous imprisonment and a fine of Rs. 4000 for violating Section 67 of the (punishment for publishing or transmitting obscene material in electronic form)

SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra was the first case of internet defamation in India. Defendant[15], an employee of the firm, was accused of cyber defamation after sending offensive and libellous emails regarding the company's Managing Director. These were anonymous and frequent, sent to many of their business partners, and intended to damage the plaintiff's reputation. After consulting a private computer specialist, the plaintiff was able to identify the responsible party and file suit in Delhi's High Court. The court issued a preliminary injunction barring the employee from writing, publishing, or transmitting any e-mails that are disparaging or defamatory of the plaintiffs. As a result, the judicial system has also been instrumental in establishing a safe and secure online environment. They must have trust in the

[14] Order passed on 5th Nov'2014 in CC No. 4680 of 2014
[15] 2 http://cyberlaws.net/cyberindia/defamation.htm

judicial system as a whole. The judiciary is a public good, and it will always be an integral part of any functional society. These are some of the legal options open to victims of cybercrime:

- ***Online/Mobile Harassment/Cyber Bullying and Cyber Stalking***

Harassment by electronic means is punished by imprisonment for a duration which may extend to 3 years and with fines if the harassed person sends very unpleasant or threatening material or repeatedly causes irritation, harm, insult, etc.[16]

- ***Sending offensive messages through a computer resource or communication device: Section66A, IT Act***

It includes:

For the intent to cause annoyance, inconvenience, danger, obstruction, enmity, hatred, ill will, insistently by making use of such computer resource or a communication device, any information that is grossly offensive or has menacing character; or Any information which he knows to be false, but for the purpose of achieving such an end.

Any electronic mail or electronic mail message sent with the intent to irritate, inconvenience, or deceive the addressee or receiver into thinking the communication originated from a source other than the intended sender.

A fine and/or imprisonment of up to three years is possible for such an offence. [17]

- ***Sexual Harassment: Section-354A IPC***

If a guy does any of the following, he is considered:

a. Harassment may take the form of unwanted and overtly sexual approaches, as well as physical contact.

b. A request for sexual favours or a demand for them;

c. Against a woman's wishes, displaying pornographic material;

using sexually suggestive language,

Shall be guilty of the offence of sexual harassment.

a. For the first three instances of sexual harassment, the offender faces severe imprisonment for a period that may extend to three years, or a fine, or both.[18]

[16] Section-66A. Information Technology Act, 2000.
[17] ibid.
[18] Section-354A Indian Penal Code, 1860.

b. The maximum penalty for a repeat offence of sexual harassment is one year in jail, a fine, or both.[19]

- ***Stalking: Section-354D IPC***

A person who:

a. harasses a lady by following her about and making numerous efforts to start up a conversation with her when she's clearly not interested;

b. Stalks a woman by keeping tabs on her online activity, whether via e-mail, the web, or other technological means.

Anybody found guilty of stalking for the first time faces a maximum of three years in jail and a fine of up to $250,000, depending on the severity of the crime.[20]

- **Violation of Body Privacy: Section-66E IT Act**

The crime of photographing a person's private parts carries a maximum sentence of three years in jail and a fine of up to two million rupees (depending on the severity of the offence).[21]

- ***Voyeurism: Section-354C IPC***

On first conviction, a man will face imprisonment of either description for a term which shall not be less than one year, but which may extend to three years,[22] and will also be subject to a fine. This is because women have a right to privacy in intimate situations, and men who observe or record such situations are breaking that right.[23]If the victim gives permission to record an act, but not to share it with anyone else, and that recording or act is shared with others nevertheless, it is a crime under this provision.[24]

- ***Punishment for publishing or transmitting obscene material in electronic form: Section-67 IT Act***

Anyone who publishes, transmits, or arranges for the publication of any material that is lascivious, appeals to the prurient interest, or has the tendency to deprave and corrupt people who are likely, in light of all relevant circumstances, to read, see, or hear the matter contained or embodied in it, will be punished on first conviction with either type of imprisonment for a term that may extend to three years and with a fine that is up to 5 lakhs[25]

- ***Material containing sexually explicit act, etc. in electronic form: Section-67A IT Act***

[19] ibid.
[20] Section-354D Indian Penal Code, 1860.
[21] Section-66E. Information Technology Act, 2000.
[22] Section-354C Indian Penal Code, 1860.
[23] Ibid.
[24] ibid
[25] Section-67. Information Technology Act, 2000.

On first conviction, anybody who publishes, transmits, or causes to be published or transmitted in the electronic medium any content that comprises sexually explicit acts or behaviour faces up to five years in jail and a fine up to 10 lakh rupees.[26]

LOOPHOLES IN THE CURRENT LEGAL SCENARIO

Although the rising number of crimes committed against women is a serious issue for any country, cybercrime compounds the problem by allowing offenders to assume false identities and behave unlawfully online. In response, the government should impose stringent regulations on ISPs, as they are the only entities with a comprehensive log of all the information accessible by everybody browsing the net. Internet service providers (ISPs) should be required to disclose any unusual user behaviour in an effort to prevent crimes from happening in their early stages. As many of those who use cyber cafes do so in order to engage in illegal activity without fear of having their own IP addresses disclosed in the course of an inquiry, the government needs to impose stronger regulations on the businesses that provide these services. In this way, one may hide one's true identity with the other methods. Individuals should be humble and watch for signs that they are being videotaped at all times. People also need to have a better understanding of the benefits and drawbacks of cyber culture. Individuals must be educated about their legal protections. Research shows that many Indians who use the internet are unaware of their legal protections in this area.

Procedural issues in the court system, such as a conflict of jurisdiction, the loss of evidence, and the absence of a cyber army and a cyber-savvy judge, pose significant challenges in the fight against cybercrimes against women. The involvement of the judiciary is crucial because it influences the passage of laws designed to address the problems. Because of the expanding reach of the internet, traditional notions of territorial jurisdiction, such as those envisioned in Section 16 of the Criminal Procedure Code and Section 2 of the International Penal Code, are becoming increasingly irrelevant in the context of issues relating to cybercrime and will need to make way for more flexible approaches to conflict resolution. There is no provision in the Information Technology Act of 2000 (the "Act") that makes the private viewing of material that may violate the rights of others illegal. A violation of the law may only be shown if it can be shown that the offending material was published, communicated, or induced to be published in electronic form (IPC, section 292). Cyberstalking, morphing, and email spoofing are all considered crimes under the Information Technology Act, 2000. Women in India who encounter cybercrime often delay reporting it out of shame and fear of repercussions. Even though there have been more and more of these events, few victims have come forward to seek redress. Thus, the primary causes of the inability to reduce such crimes against women include:

a. stereotypes of law enforcement and the criminal justice system.

b. Victim mentality.

c. A patriarchal culture.

[26] Section-67A. Information Technology Act, 2000.

d. Anxiety over facing the truth about the past.

e. concerns about personal privacy

Cybercriminals' methods and doggedness are the industry's biggest challenge. Ahead of such criminals, the judicial system, together with the police and investigation organisations, should be bolstered by cutting-edge web-based apps. To prevent new technologies from being used for exploitation or harassment, the legal system and regulatory bodies must keep up with them. Human rights, including the rights of women in particular, must be safeguarded online just as they are in the real world, and governments may do so via legal action. Laws should do more than only safeguard users; they should also teach and instruct all demographics on how to make full use of their freedom of expression. Additionally, people need to be more aware, both online and offline, of the safeguards they may take in cyber space and the options they have if their rights are abused. Nevertheless, the Criminal Law Amendment Bill (2013) has addressed most of the remaining issues in dealing with cybercrimes, such as the loss of evidence and the absence of a cyber army. Several improvements, such as more technically aware judges, are still necessary, nevertheless. It is possible to say that eliminating cybercrimes would need adequate application of legislation, public awareness, and education of women about their rights and legal remedies. The best way to stop these kinds of atrocities is not only by making more laws. Similarly, focusing just on the need to safeguard societal norms is not sufficient. The development of digital technology has outpaced the rules enacted to regulate it. Hence, the current legal framework is inadequate to address the issue. The threat of cybercrime is not limited to India; rather, it is global. Because of this, the global community as a whole must work together. Also, it is important to revitalise and promote grievance redressal processes and organisations so that people may more quickly and easily file complaints and face swift investigations and prosecutions.

6. SUGGESTIONS/TIPS TO FOLLOW TO STAY SAFE FROM CYBERBULLYING:

- Cybercrime exacerbates the difficulty of combating the rising tide of crimes against women in any given country, because of the ease with which perpetrators may assume new identities online and use them for criminal purposes. To combat this, the government should enact harsher rules to be applied on Internet Service Providers(ISP), since they are the only entities with a comprehensive record of all the data obtained by everybody browsing the net. Internet service providers (ISPs) should be required to disclose any unusual user behaviour in an effort to prevent crimes from happening in their early stages.

- People frequently use cyber cafes to engage in illegal activities without fear of having their own IP addresses revealed in any future investigation, so there is a need for legislation to make stricter regulation for cyber cafes, who should keep a record of their customers who utilised their internet services. In this way, one may hide one's true identity with the other methods.

- The public has to exercise caution while in public places with cameras present, as they should behave modestly. People also need to have a better understanding of the benefits and drawbacks of cyber culture. Research shows that many Indian internet users are unaware of their legal protections and must be educated on the topic.

- You shouldn't be afraid to report online harassment to the police.

- As the primary protocol for delivering emails, Simple Mail Transfer Protocol (SMTP), does not include an authentication method, email spoofing is conceivable. While an SMTP client may negotiate a security level with a mail server using an SMTP service extension, this measure is not always followed. In order to avoid any problems, ladies should always use the SMTP service extension while sending emails through the SMTP client.

Women online in India are still less likely to report cybercrime or cyberabuse than males are. Cybercriminals' methods and goals provide the biggest challenge when it comes to combating this kind of crime. The anonymity that the internet affords is often abused by its users. Due to the anonymous nature of the internet, criminals may easily flee and conceal themselves after committing a cybercrime. Thus, appropriate measures must be made to guarantee accurate crime reporting and the privacy of victims and witnesses.

7. CONCLUSION

Other forms of cybercrime, such as trolling and gender-based abuse, are rapidly expanding as a problem for women online. Yet such offences are not covered by the IT Act of 2000, and the investigative procedure is not suitable. One of the act's flaws is that it doesn't address online tolling or gender-based bullying. The probe requires its own secure holding facility. The cops who deal with cybercrimes against women need specialised training. The country's judicial system should make an effort to combat the growing issue of cybercrimes against women.

REFERENCES

[1] M. Dasgupta, Cyber Crime in India- A Comparative Study (Eastern Law House, Lucknow, 2009).

[2] Dr. Vishwanath Paranjape, Legal Dimensions of Cyber Crimes and Preventive Laws with Special Reference to India, (Central Law Agency Publication, Allahabad, 2010).

[3] Rodney D. Ryder, Guide to Cyber Laws (Information Technology Act, 2000, E-Commerce, Data Protection and the Internet), (Wadhwa Publication, New Delhi, 2001).

[4] Vakul Sharma, Information Technology: Law and Practice, (Universal Law Publication Co., Uttar Pradesh, 2010).

[5] Ratanlal and Dhirajlal, The Indian Penal Code, (Wadhawa and Co. Nagpur, 28th Ed. 2002)

[6] Suresh T. Vishwanathan, The Criminal Aspect in Cyber law in The Indian Cyber Law, (Bharat Law House ltd., New Delhi, 2001).

[7] Farooq Ahmad, Cyber Law in India- Law on Internet, (New Era Publication, Delhi, 2008).

[8] M.P.Shahi, Crime and Corruption in the Digital Age, (Authorspress, Delhi, 2000).

[9] Pavan Duggal Cyber Law-the Indian Perspective (Saakshar Law Publications, New Delhi, 2nd Edn.,2002)

[10] Rastogi A. Cyber Law, Law of Information Technology and Internet, (Lexis Nexis; 1st Edn. 2014).