CYBER OFFENCES AGAINST WOMEN AND LEGAL PROTECTION

Written by ***Mohit* & Sanjeev*****

** LL.M., Rajiv Gandhi National University of Law, Punjab, B.A. LL.B (Hons.), National Law University Odisha, India*

*** LL.M., Rajiv Gandhi National University of Law, Punjab, B.A. LL.B (Hons.), National Law University and Judicial Academy, Assam, India*

RESEARCH METHODOLOGY

Objectives of the Study

- To understand the meaning of cyber-crime against women.
- To find out causation behind the victimization of women.
- To analyze law dealing with in checking cyber-crime against women in India, and to find out the loopholes in the law if there is any.
- To find the gap between legal actions & technological advancement.
- To situate the growing threat of cyber-crime against women and girls within the broader context and challenge of cyber-crime, Internet growth and governance.

Hypothesis

Cyber Law and its enforcement are effective to curb the cyber-crime against women in India.

Method of Research

For the research work the doctrinal methodology will be used by researcher. Researcher will analyze case law decided by the Supreme Court, High Courts' and cyber appellate tribunal. Law library resources will also be taken into account for the study.

Sources of Data Collection

- Primary Sources: Information Technology Act, 2000, provisions, statutes, amendments etc.
- Secondary Sources: Websites, articles, books, journals etc.

Scope of the Study

The researcher has used doctrinal method and relied on the secondary sources for the content of the research paper. Owing to the large number of topics that could be included in the project, the scope of this research paper is very vast. Though the researcher has tried his level best to not to left any stone unturned in doing his research work to highlight the various aspects relating to the topic.

INTRODUCTION

Women can use cyberspace to exercise their rights, from obtaining information to freely and anonymously expressing themselves. Cyber-crime, on the other hand, is a worldwide problem, and women are the most vulnerable victims of this new kind of crime. Women's vulnerability and safety are among the most serious problems of any criminal or penal legislation, yet women remain defenceless in cyberspace. Cybercrime against women is at an all-time high, and it might represent a grave danger to an individual's overall security. Users may share material in the form of photos, text, videos, and audio over the World Wide Web. Women are especially harmed by the widespread distribution of such information. There have been several incidents in recent years of women getting unsolicited email that includes rude and abusive language.

Cybercrime against women is on the rise, and women have been disproportionately attacked online. Some perpetrators attempt to defame women by sending obscene emails, stalking women through chat rooms, websites, and other means, creating pornographic videos in which women are depicted in compromising positions, usually without their consent, spoofing e-mails, and morphing images for pornographic content, and so on. Sex offenders hunt for victims on social networking sites, as well as employment and marriage websites, where individuals upload personal information in the hopes of a brighter future. Women have become

increasingly vulnerable to cybercrime as a result of the disclosure of personal information. It is clear that female victimisation leads to cybercrime and vice versa.

On the one hand, the internet is a gift, but it has also made women's lives unsafe owing to an increase in cybercrime in the virtual world. With the advent of the internet, women of all ages and backgrounds are at risk. While many women are harassed online, the issue of what distinguishes Indian women emerges. Women who are assaulted in India, which is largely patriarchal and conservative, are often blamed, and online victims are no exception. There have been cases when women's marriages have been halted as a result of their internet persecution. In addition, compared to their western counterparts, they have less legal protection, and Indian women victims do not get sufficient answers from ISPs controlled mostly from a western cultural viewpoint. India is among one of the few countries to have passed the Information Technology Act, 2000 to tackle cyber-crime. This Act covers a broad range of commercial and economic offences. Despite the fact that women's problems are still not addressed in the Act.

When a man's email id or personal data kept on websites, as well as personal computers, is viewed and updated in an unlawful manner, he might continue to live by contacting the police and his friends. He may neither be exposed to widespread humiliation by society, as a woman victim is, nor may he be degraded to a simple "sex object," as his female counterpart is. His persecution can only be assessed in terms of financial damages. A woman victim, on the other hand, may be shunned by society. She may not be able to handle the online humiliation as well as her male counterpart; it may envelop her in feelings of shame and contempt for herself. A woman victim may find it very difficult to reclaim her social and professional standing, in addition to the prospect of being reduced to a sex avatar. More than digitally robbed men or digitally jeopardised national security, virtual vandalised ladies delight the globe.

It is fair to say that research on this topic has stalled. With the exception of a few investigations from European viewpoints, the most of the studies were conducted from a US perspective. The state has enacted various regulations for financial crimes, property crimes, and crimes against children, but women victims do not get immediate assistance from the state because crime patterns go unnoticed and are eclipsed by broader trends in cybercrime.

DEFINITION AND CLASSIFICATION OF CYBER CRIME

Norbert Wiener invented the word '**cybernetics**' in the year 1948 and characterised it as '*the study of communication as a way of managing machines and society*,' which became widely used by the 1980s.[i] The word "cyber" refers to the cyber space, also known as "virtual space," which is the informational space represented by a computer and in which different objects or symbol pictures of information may be found. As a result, it is the location where computer programmes and data are processed.[ii]

The phrase "cyber crime" is misleading.[iii] It is a catch-all word for any illicit operations carried out via computers, the Internet, cyberspace, and the global web. In India, no legislation has yet provided a meaning for the word "cyber crime." Even after being amended by the Information Technology (Amendment) Act, 2008, the Indian Penal Code, 1860, does not utilise the phrase "cyber crime" anywhere.

"Any criminal conduct encouraged or enabled through a computer system, whether it is in itself a crime's object, a tool used through which crime is committed, or an act as an evidence repository which is somehow linked to a crime," according to one definition of cyber crime.[iv] "A crime committed on a computer network," according to an internet dictionary. "Crimes aimed against a computer or a computer system" is a simple definition of cybercrime. However, the complexity of cybercrime cannot be adequately represented in such narrow and basic words. Cybercrime, according to Pavan Duggal, refers to any operations carried out with illegal intent over the internet. These might be traditional criminal acts or actions that have emerged as a result of the new medium's development. Cybercrime may be defined as any activity that offends human sensibilities in some way.[v]

In everyday speech, the terms "**cybercrimes**" and "**computer crimes**" are interchangeable. The term "computer crimes" encompasses not just crimes done on the Internet, but also crimes conducted in connection with or with the assistance of computers. The distinction between cybercrime and computer crime is often misunderstood. Even the writers of cybercrime do not always properly differentiate the concepts.[vi] As a result, it's critical to distinguish between cybercrime and computer crime. Computer crimes are those committed with the use of a computer or computers, whereas cybercrimes are those committed with the use of a computer network.[vii]

Donn B. Parker makes a distinction between computer crime and cyber crime. The perpetrator of a computer crime employs particular knowledge of computer technology, while the perpetrator of a cyber crime uses unique knowledge of cyberspace.[viii] Cybercrime does not, in general, need sophisticated computer operating abilities. In cybercrime, a suspect and a victim could connect using Web-based chat rooms, Microsoft Network Messenger (MSN), or e-mail, for example. When a criminal earns the confidence of a prospective victim, he or she is in a position to conduct a crime against that person. Even while the Internet most likely facilitated the suspect in interacting with the victim in this instance, this does not indicate that technology or the Internet were to blame for the murder.

The four types of cybercrime may be roughly categorised.[ix] They are as follows:

1. **Cybercrime Against Individuals**: Crimes done by cyber criminals against an individual or person. Examples: Harassment through electronic mail; dissemination of obscene content; cyber-stalking etc.

2. **Property Crimes**: These crimes include computer vandalism, intellectual (copyright, trademark, patented, etc.) online threatening, property crimes, and so on. Examples: Computer vandalism; virus transmission etc.

3. **Crimes against Organizations**: Crimes which committed intending to pose a danger to foreign governments or other organisations over the net. Organizational cyber-crime is the name given to certain types of cyber-crimes.

4. **Cybercrime Against Society**: Cybercrime Against Society refers to cybercrimes that have an impact on society as a whole. Examples: child pornography, indecent exposure of polluting the young, financial crimes etc.[x]

CYBER CRIMES AGAINST WOMEN: INDIAN SCENARIO

Cyber-crime makes use of the internet and information technology to carry out illicit actions that are banned and punished under the State's law. While cybercrime may be perpetrated against people, property, or the government, this initiative concentrates mainly on cybercrime against women. Essentially, India has two key laws that handle cybercrime against women to

a big range: **The Indian Penal Code (*hereinafter* 'IPC'), 1860 (amended several times, most recently in the year 2013) and the Information Technology (*hereinafter* IT) Act of 2000 (which was significantly updated in 2008**.[xi] The IPC is a broad criminal law that identifies a wide range of offences and provides punishments for them. It is vital to emphasise that they are mainly meant to address crimes committed in the actual / tangible / real world. Legislative revisions and court interpretations have made such IPC sections relevant to cyber-crimes against women.[xii]

Unlike the IPC, the IT Act is a separate legislation that covers a wide range of issues related to the use of information technology, including the crime's commission. The fundamental goal of the legislation is in establishing an atmosphere that encourages the use of information technology. The 2008 Amendment Act included certain offences / cyber-crimes as a result of the experience in dealing with offences connected to the abuse of information technology from 2000 to 2007. In tackling cyber-crime against women, these laws complement and support one other.[xiii] Women, particularly young girls who are inexperienced in the online world and who have been just exposed to the internet and do not comprehend the internet's vices, are particularly vulnerable to falling prey to cyber crooks and bullies. Cybercrime and cyberbullying can in a variety of forms, including:

1. ***Cyber Harassment:*** Cyber harassment is a pattern of behaviour designed to annoy or agitate a person via the use of the internet. Sexual harassment is a kind of harassment that is sexual in character, and it covers a variety of activities, the most common of which is repeated and unwelcome sexual advances. Sexual harassment is now defined in Indian law as physical contact and approaches including uninvited and explicit sexual overtures, as specified by the Criminal Law Amendment (Bill) 2013.

In the cyber world, harassment such as blackmail, threatening, bullying, and even cheating is often done through e-mailing. **Sections 67 A and 67 B of the IT Act** provide sexual harassment in respect of offences of publishing or transmitting material containing sexually explicit act and child pornography in electronic form.

2. ***Cyber Stalking:*** Although stalking isn't always sexual in nature, it however tortures, terrorises, intimidates and harasses the victim. The stalker strives to create a connection with the victim without her agreement, which is a flagrant invasion of her privacy. Stalking may

take place in person or via technological methods, such as cyber-stalking.[xiv] One amongst the most often reported cyber-crimes against females is cyber stalking, which is tracking and monitoring woman's offline as well as online activities and movements invisibly.[xv]

S. 354D of IPC, which punishes and defines stalking, covers internet stalking. Stalking is defined as a male following a female and continuously contacting or attempting to interact with her for intimate connection despite the lady's evident indifference. When he utilises the Internet for these intentions, he is committing cyber stalking.

A first conviction for stalking may result in up to three years in jail and a fine, while a second conviction can result in up to 5 years in prison and a fine.[xvi] The first conviction in a cyber stalking case against a female occurred in July 2015,[xvii] when the accused was found guilty under S. 509 of IPC (words, gestures, or actions designed to offend a lady's modesty) and S. 66E of IT Act, 2008 (penalty for privacy's invasion). The present cyber laws in India do not encompass cyber stalking. The culprit may only be booked remotely for violation of secrecy and privacy under the provisions of Sections 66, 72, 72 A of the IT Act.

3. ***Cyber Pornography:*** It is the act of creating, publishing, or disseminating pornographic items through the use of internet. Charge of 'obscenity' has traditionally dealt with pornography legislation. Any content is deemed obscene if it is lewd or appeals to racy interests, or if it has the effect of depraving and corrupting those who utilise it.[xviii] An act like this may result in a sentence of up to 5 years in jail and with a fine up to Rs. 5000.

In addition, **S. 354A IPC**, which deals with sexual harassment and was enacted in 2013, covers a male who shows pornographic material to a female without her consent. Further legal recourse is provided by **Section 67A of the IT Act**, which forbids publishing, sending, or causing it to be published or even if transmitted in any electronical form any content containing sexually overt act or behaviour, and classifies such activities as penal crimes. The penalties under IT Act are significantly extra severe: up to 5 years in jail and a fine up to Rupees 10 lakhs for a first offence, and up to7 years in prison and a fine of up to Rupees 10 lakhs for consecutive offences.

4. ***Voyeurism:*** Voyeurism, mainly directed at intimate acts of females, have become perceptible in the purview of frequent developments in the field of information technology that

allow photos and videos to be taken very easily using a smartphone and dispersed widely through social networking and pornographic websites on the internet.[xix] In the **IPC**, voyeurism is defined under **S. 354 C** and punished by a sentence of 1 to 3 years in jail with fine for first conviction, and 3 to 7 years in prison with fine in case of consecutive convictions. **S. 66E of IT Act** additionally supplements the IPC prohibition on voyeurism.

5. ***Cyber Defamation***: It is also another widespread online crime towards women, which includes both defamation and libel. This is committed when defamation is carried out through Internet.[xx] Defamation is dealt with under Section 499 of the IPC, and it is punished in Section 500. Sections 469 and 503 also deal with a person's reputation. A person who has been defamed in cyberspace may file a complaint with the cyber crime investigation cell under the IT Act.

6. ***Morphing***: Morphing is the process of altering an image and making it seem wholly or mostly different. The criminally minded sections of cyber world often grab images of females from sites like Facebook & then morph them with some another picture of a woman in a compromising setting to make it seem as though those ladies were engaging in such behaviour. Following this, the threat of exposing the modified photographs and lowering the women's social position is often used to blackmail them.[xxi] Such modified photographs are often used to smear the victim woman's image and defame her reputation.[xxii] **S. 43 (which encompasses actions of unlawful, copying, downloading, destroying, and extracting or altering data) & S. 66 IT Act might be used to prosecute such behaviour (which spells out certain types of computer related offences).** In addition, the perpetrator may be charged with public nuisance under Section 290, obscenity under Section 292A, sexual harassment under Section 354A and defamation under Section 501 of the IPC.

7. ***Email Spoofing:*** It is a term used for describing deceitful email activity in which the sender's address and all other parts of the e-mail header are changed to make it appear that the e-mail is sent from a verified company and source but in reality, it is not.[xxiii] Cyber thieves often utilise this tactic to collect personal information and intimate photographs from unsuspecting women, and then use those images and other information to blackmail those ladies. ***Gujarat Ambuja's Executive Case***,[xxiv] is the most well-known case of cyber spoofing; in this case, the offender purported to be a female in order to defraud and extort an Abu Dhabi-based NRI.

INTERNATIONAL SCENARIO OF CYBER CRIMES

Attempts to define 'cybercrime' have been made in a number of scholarly publications. National law, on the other hand, seems to be unconcerned with a precise definition of the term. Fewer than 5% of the over 200 pieces of national law indicated by nations in answer to the research questionnaire included the term "cyber-crime" in the title or scope of the legislation. Rather, 'electronic communications,' 'computer crimes,' 'information technology,' 'high-tech crimes' were more typically used in law. Many of these pieces of law, in effect, generated criminal offences that are included in the idea of cyber-crime, such as illegal accessing a computer system or data tampering. When national law included the term 'cyber-crime' in the title of any section or in any Act (for example, the 'Cybercrime Act,' the definitional portion of legislation seldom provided a definition for the term.[xxv]

Law is a very dynamic instrument which allows the State to adapt to newer social and security concerns, like finding the right balance between criminal control and privacy, or determining the scope of responsibility for service providers. In addition to national laws, international law, often known as the law of nations, governs state-to-state interactions in all of its forms.[xxvi] Cybercrime is covered by provisions in both national and international law.

Interpol, as an international law-enforcement organisation with 184 members, was one of the first to confront computer crime, coordinating law enforcement agencies and legislations, and making efforts to develop international counter-cybercrime capabilities. Interpol now has four working groups on information technology crime: **African, American, Asia-South Pacific, and European Working Parties** on Information Technology Crime. A Steering Committee for Information Technology Crime was formed in addition to these organisations in order to unify the various regional working-party actions. Interpol has offered technological assistance to law enforcement in the areas of cybercrime detection, investigation, and evidence collecting. Along with law enforcement efforts to fight cybercrime, Interpol also takes steps to prevent cybercrime, such as collaborating with credit card companies to combat fraud in payment by creating a database on Interpol's website.[xxvii]

The impact of cybercrime on women is more mental than physical, despite the fact that the emphasis of legislation safeguarding women's protection is more on physical than mental damage. It is becoming a worldwide issue as well.[xxviii]According to recent figures from the US

Department of Justice, 850,000 American adults, largely women, are victims of cyber-stalking every year, and 40% of women have encountered violence in terms of dating online.[xxix]

Several Member States have recently passed laws to combat cyber violence against girls and women; for example, measures which criminalise revenge porn is established in the United Kingdom, Germany, France, and Malta, with policies in Slovenia and Ireland presently pending. In the year 2013, the End Violence Against Women Coalition (EVAW) held a discussion on the enforcement & prosecution of online "harassment and violence," raising concerns that criminal justice establishments took a dissimilar, and not very much effective approach to online harassment and violence than they did offline. When reporting an internet crime, some participants said they received "wholly insufficient police answers."[xxx]

Sharing private sexual videos or images without the owner's agreement with the goal of causing pain to people targeted became a criminal crime in the UK in April 2015, with a potential sentence of two years in jail.[xxxi] Since the law's implementation, more than 200 persons have been prosecuted, according to a report released in September 2016. Meanwhile, in the year 2016, France passed the "Digital Republic Law," which makes anyone found guilty of revenge pornography face stiffer penalties. Perpetrators risk a two-year jail term or a €60,000 fine under new law. In 2014, a German court approved similar legislation, making it unlawful to preserve personal images of a former partner after they have requested that they be deleted. The National Centre for Cyber Stalking Research (NCCR), established in 2009 in the United Kingdom, intends to offers analysis and research regarding the occurrence, motives, affects, and assessment of risk of cyber offence against women and girls.[xxxii] The institute released the findings of a research on the prevalence, nature, and effect of cyber stalking in 2011, and it is now undertaking a survey on the effect and occurrence of revenge porn. Following that, in year 2015, a hotline for revenge porn victims was created, which received around 2000 calls in its first six months.[xxxiii]

CYBER SECURITY: IT'S PROTECTION AND PROCEDURAL ASPECTS IN INDIA

There isn't any separate cyber security law in India. The IT Act, as well as the rules & regulations passed under it, deals with cyber security and cyber-crime. The IT Act along with providing legal recognition and protection for transactions conducted via electronic data interchange & other forms of electronic communications, also have provisions aimed for safeguarding of electronic data, information, & records, as well as preventing unlawful or unauthorised use of computer system.[xxxiv]

The cyber violence perpetrated against females is gender specific and solely affects them. The IPC and certain Special and Local Laws control and punish certain offences (SLLs). The Indecent Representation of Women (Prohibition) Act of 1986 and the IT Act, 2000 are the two SLLs. The IT Act, unlike the other two acts, does not include gender-specific provisions, although it does have a few clauses that deals with issues which are gender specific and suggest penalties for such offences. The Indecent Representation of Women (Prohibition) Act, enacted in 1986, was designed to fight indecent depictions of females in commercials, publications, writings, paintings, and figures.[xxxv]

The IT Act of 2000 is not a statute that specifically addresses cybercrime against women, but it does include sections that address such offences & the penalties for their conduct. Defamation, cybersex, hacking, email spoofing, and trespass into individual's private domain are all typical cybercrimes today, yet they are not particularly included in the IT Act. **Sections 66A, 66E, 67, and 67A** principally deal with offences committed against women. The penalty for sending offensive communications via communication services is outlined in **Section 66A**, which includes any message or e-mail sent with the intent of inconveniencing or annoying the addressee or recipient, or deceiving or misleading the recipient in regard to origin of the messages.

The infringement of privacy is penalised under **Section 66E**, which states that the publishing of any photograph of the victim's private region without the victim's agreement is a serious offence.

Furthermore, **Section 67** establishes penalties for the electronic publishing or transfer of any sort of obscene content. The publishing or transfer of any material containing sexually explicit conduct in an electronic form is punishable under **Section 67A**. The majority of cyber-violence complaints are filed under the IT Act's Sections 67 and 67A. **Section 354 of the Indian Penal Code**, which oversees cybercrime to some degree, provides the penalty of voyeurism, sexual harassment, and stalking.

Many times, cybercrime against women happens inside marital relationships, when a husband who is separated from the bond publishes lewd images of his spouse; in such circumstances, proving the victim's permission becomes tough and convoluted. Another explanation for the lower number of reporting of complaints is that many females are unaware that such laws exist to safeguard their bodily privacy as well as the privacy of all physically intimate activities.[xxxvi] This scenario will play out the same way if law enforcement's function is confined to the registration of cases only and subsequently the investigation of those instances.[xxxvii]

The goal of legislation in contemporary times should be to defend women's dignity, security, and privacy, rather than to restrict the development of virtual material that may lead to uncontrolled sexual life. The usage of the adjectives "prurient" and "lascivious" interest in sexuality demonstrates the state's unfavourable attitude about sexuality. The female body is shown as a medium that has the ability to make individuals unprincipled and dishonest. Furthermore, there is a significant time gap in between the arrests of accused and suspects and the filing of charges. This lower rate of charge filing indicates a flawed investigating process.[xxxviii]

There is also a critical need for appropriate training of police personnel who investigate cyber crime cases, since such investigations often entail technology, making it difficult in tracking down the perpetrators and providing victims the justice they deserve.[xxxix] Furthermore, the police stations who are in charge of investigating cybercrime must cooperate closely with the Detective Department, women's police stations, and Criminal Investigation Department. This collaboration is critical since these agencies are qualified for investigating these situations, but it is currently lacking.

NGO's such as the All India Women's Conference, Sakshil Navjyoti, and others provide assistance in these areas. The judges must be educated on how to retain electronic records and

how to manage them. Aside from the court, even the police need to be better educated on how to deal with electronic documents. The absence of consistent evidence makes it harder to bring the victim to justice and convict the culprit.[xl]

JUDICIAL RESPONSES AND PRACTICES

***State of Maharashtra v. Yogesh Prabhu*[xli]**

M. R. Natu, Additional Chief Metropolitan Magistrate at that time, ruled the case in July of 2015. This was the first instance of internet stalking against a woman to result in a conviction. The lady first began conversing with accused Yogesh Prabhu on a social media website in 2009. Yogeshin ded to marry her and proposed her for that, but she declined the offer of marriage. She continued to get messages after that, but she stopped replying to them and disregarded them since she was suspicious of his peculiar behaviour. He couldn't locate her since she banned him on the internet. He continued following her, & after some months, he began sending her e-mails with pornographic photographs and video footage from a fake unknown account. Terrified by this act of Yogesh, she filed a police report, which was subsequently investigated by the Cyber Crime Investigation Cell. The device's IP address was traced, and was discovered to belong to a company called "Vashi," where Yogesh Prabhu worked. The inquiry was completed, and Yogesh was found guilty under **S. 509 of the IPC and S. 66E of the IT Act**, which were the laws in effect at the time.

***State of Tamil Nadu v. Suhas Katti*[xlii]**

In November of 2004, a Chennai court ruled on this matter. It was the first time a woman had been convicted of internet pornography. The victim was a divorced woman who began getting texts from the accused after she rejected down his marriage proposal. The accused individual utilised a bogus email ID in the identity of a female to send her filthy, irritating, and defamatory photographs in a Yahoo chat group. People on the phone were also calling the victim, believing she was requesting sexual activities. Then, the victim filed a police report alleging the aforementioned issues, which were later probed further by the Cyber Crime Cell of Chennai. Following the conclusion of the inquiry, the accused was sentenced to two years of harsh imprisonment & a punishment of Rs. 500, as well as one year of simple imprisonment with a

fine of Rs. 500, under **Sections 469 and 509 of the Indian Penal Code**, respectively. He was also sentenced to two years of solitary confinement and a fine of Rs. 4000 under **S. 67 of the IT Act**.

State v. Avnish Bajaj[xliii]

In May of 2008, Justice S. Muralidhar of the High Court of Delhi handed down his decision in this matter. It is also famously known as the MMS incident of Delhi Public School 2004 and is a well-known incidence of voyeurism. It considered the creation of a pornographic video recording of 2 high school students engaging in sexual behaviour, as well as its unauthorised distribution among pupils through MMS. The footage was also put up for sale on the eBay India website. The Chief Executive Officer of eBay India was then subjected to a legal investigation and convicted under the Information Technology Act.

State of Madhya Pradesh v. Saddam Hussain[xliv]

The case is significant because it demonstrates that courts treat cybercrime issues extremely seriously. The accused made the victim's modesty a point of contention. The accused recorded it on his phone and later on blackmailed her into doing sexual favours to him. The victim filed a criminal complaint under **S. 507 of the IPC, S. 354D of the IPC, and S. 66A of the IT Act**. Then, the petition was submitted at the Madhya Pradesh High Court, requesting that the conviction be overturned based on a settlement between the accused and the victim. The HC refused to do so, stating that these crimes have a broad impact on society and that any private settlement between the parties would not halt the case's progress.

Jogesh Kwatra v. SMC Pneumatics (India) Private Limited[xlv]

An employee of the firm began sending insulting, libellous, and obscene emails to the Managing Director. The emails were anonymous and frequent, and they were sent to a large number of the company's business contacts in order to destroy the company's image and goodwill. The firm was able to identify the guilty thanks to the help of a private computer expert. The employee was barred from sending, publishing, or transmitting emails that were defamatory or disparaging to the plaintiffs by the Delhi High Court.

CONCLUSION AND RECOMMENDATIONS

Several types of cybercrime targeting women are now being perpetrated in India. The internet's significance and need have made it a necessary part of everyone's life. People from all ages utilise the internet, which has both advantages and disadvantages. Cybercrime against women is not exclusive to India; it is a worldwide problem. It is also a major source of worry many governments because of its continued rise. The legislative requirements adopted to combat cybercrime are insufficient to properly combat the problem. These rules do not fully represent the reality of what women face when they are victims of cybercrime. The first step in providing victims with legal recourse is ensuring that women's online experiences of threat, harassment, abuse, or intimidation are accurately translated into written regulation via revisions to the two key legislation. Without a doubt The Indian Parliament approved the IT Act, 2000 with the goal of making it easier to fight cybercrime. There are, nevertheless, loopholes in Indian laws, such as:

1. The Information Technology Act of 2000 neither defines nor utilises the term "cyber crimes," but rather specifies and punishes specific offences. The IT Act, 2000 punishes just a few types of cybercrime and does not cover all of them.

2. The Indian Penal Code defines cyber defamation, while the IT Act of 2000 does not. If any public good defence is put up, such as object being of general interest or held for confidential religious reasons, S.67, 67A, 67B, and 67C cannot be argued to encompass pamphlet, book, paper writing, painting, drawing, representation, or figure in any electronic form.

3. Personal viewing is not an infraction under any provision of the IT Act 2000; nevertheless, even if it is shown that you have published, communicated, or caused to be publish in any electronic form, it may be an offence under Section 67.

4. Typical cyber-crimes such as morphing, cyber stalking, and email spoofing are not included in offences under the IT Act,2000.

In India, cybercrime against women is still seen as a minor offence, owing to a general lack of respect for women in our current culture, as well as the fact that many people are reluctant to accept the reality that merely publishing photographs of someone online is considered a crime. Cybercrimes such as morphing and e-mail spoofing lack moral support in society and are

therefore dismissed. This gets us to the most crucial component of the process: individuals must recognise the rights of others and understand what constitutes a crime. Many women are ignorant of their legal rights when it comes to cybercrime. The Indian government has prioritised boosting women's awareness as a means of both preventing and punishing such crimes.

Awareness in raising of legislation and building of perspective on cyber-crime against females among other criminal justice system stakeholders, including the Investigating Officers, judges, and public prosecutors is equally critical. It is also critical to recognise that the law doesn't have the capacity to address all aspects of the problem of cyber-crime against females in India. Women should be taught to take preventative measures such as being cautious when communicating with strangers online, and protection of passwords and other sensitive information that could compromise a woman's privacy and security. As a preventative strategy, women internet users in India need to be more aware of how to improve privacy settings on social networking sites.

BIBLIOGRAPHY

Books and Journals:

- Pawan Duggal, Cyber law- The Indian Perspective, 2002
- Norbert Weiner, "The Human Use of Human Beings: Cybernetics and Society" (1954) referred by T.P.S. Rathore, "Cyber Terrorism and Information Technology Act, 2000", International Journal of Language Studies, vol.5, Aug. 2014
- Sameer Hinduja, "Computer crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future", International Journal of Cyber Criminology, Vol. 1, No. 1, January, 2007
- B. Muthukumaran, "Cyber Crimes Scenario in India", Criminal Investigation Department Review, 2008, p. 17,
- United Nations Office on Drugs and Crime, Comprehensive Study on Cyber Crime, February 2013
- EU Decision on Attacks against Information Systems and Commonwealth of Independent States Agreement

- Xingan Li, "International Actions Against Cybercrime: Networking Legal Systems in the Networked Crime Scene", Vol. 4, September 2007
- EVAW (2013), "New Technology: Same Old Problems", Report of a roundtable on social media and violence against women and girls, 2013
- Mayura U. Pawar, Archana Sakure, "Cyber space and Women: A Research", International Journal of Engineering and Advance Technology, Vol. 8, September 2019
- Astha Srivastava, "Cyber Delinquency: Issues and Challenges under Indian Legal System", International Journal of Engineering and Advanced Technology (IJEAT) 2019

Websites:

- https://www.scribd.com/document/406103309/11-cha-pter
- http://www.naavi.org/pati/pati_cybercrimes_dec03.htm
- http://cybercrimejournal.com/sameer.pdf
- https://shodhganga.inflibnet.ac.in/bitstream/10603/188293/11/11_cha[pter%203.pdf
- https://blog.ipleaders.in/cyber-crimes-classification-and-cyber-forensics/
- https://docs.manupatra.in/newsline/articles/Upload/CE3E0AE8-DE2B-41EA-92A2-8A46035DECEB.pdf
- http://www.gcl.in/downloads/bm_cybercrime.pdf
- https://blog.ipleaders.in/cyber-defamation-india-issues/
- https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
- https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017DC0474
- https://www.webology.org/2007/v4n3/a45.html
- https://itforchange.net/e-vaw/wp-content/uploads/2018/01/Molly_Ghosh.pdf
- http://www.endviolenceagainstwomen.org.uk/resources/61/newtechnology-same-old-problems-dec-2013
- http://www.cps.gov.uk/legal/p_to_r/revenge_pornography/file:///C:/Users/HP/Downloads/cyber_violence_against_women_and_girls.pdf
- https://www.lexology.com/library/detail.aspx
- https://www.ijeat.org/wp-content/uploads/papers/v8i6S3/F13130986S319.pdf
- https://www.ijeat.org/wp-content/uploads/papers/v8i5C/E12040585C19.pdf
- https://www.ijeat.org/wp-content/uploads/papers/v8i6S3/F13130986S319.pdf

Statutes:

- Information Technology Act, 2000
- Information Technology (Amendment) Act, 2008
- Indian Penal Code
- Foreign Statutes

ENDNOTES

[i] Norbert Weiner, *The Human Use of Human Beings: Cybernetics and Society* (2nd edn, Garden City 1954).
[ii] ibid.
[iii] Parthasarathi Pati, 'Cyber Crimes' < https://www.naavi.org/pati/pati_cybercrimes_dec03.htm> accessed 31 October 2021.
[iv] Sameer Hinduja, 'Computer crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future' (2007) 1(1) International Journal of Cyber Criminology <http://cybercrimejournal.com/sameer.pdf> accessed 31 October 2021.
[v] Pavan Duggal, *Cyber law- The Indian Perspective* (1st edn, Saakshar Law Publications 2002) 256.
[vi] Ritu, 'Cyber Crimes National and International Perspective' (Doctor of Philosophy in Law Thesis, Kurukshetra University 2017) 57.
[vii] ibid.
[viii] Weiner (n 1) 8.
[ix] Diva Rai, 'Cyber Crimes: Classification and Cyber Forensics' <https://blog.ipleaders.in/cyber-crimes-classification-and-cyber-forensics/> accessed 31 October 2021.
[x] ibid.
[xi] Saumya Uma, 'Outlawing Cyber Crimes Against Women in India' [2017] Bharati Law Review <https://docs.manupatra.in/newsline/articles/Upload/CE3E0AE8-DE2B-41EA-92A2-8A46035DECEB.pdf> accessed 31 October 2021.
[xii] ibid.
[xiii] B Muthukumaran, 'Cyber Crimes Scenario in India' [2008] Criminal Investigation Department Review <http://www.gcl.in/downloads/bm_cybercrime.pdf> accessed 31 October 2021.
[xiv] Uma (n 11) 11.
[xv] Rajat Misra, 'Cyber Crime Against Women' [2013] SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2486125> accessed 31 October 2021.
[xvi] Indian Penal Code 1860 (IPC 1860), s 354D.
[xvii] *Yogesh Prabhu v State of Maharashtra* 2006 (3) MHLJ 691.
[xviii] IPC 1860, s 292.
[xix] Uma (n 11) 11.
[xx] Subodh Asthana, 'Defamation in the Internet Age: Laws and Issues in India' <https://blog.ipleaders.in/cyber-defamation-india-issues/> accessed 31 October 2021.
[xxi] Misra (n 15).
[xxii] Uma (n 11) 11.
[xxiii] Misra (n 15) 16.
[xxiv] *Gujarat Ambuja Cement & Ors v Union of India* AIR 2000 MP 194.
[xxv] United Nations Office on Drugs and Crime, *Comprehensive Study on Cyber Crime* (2013) <COMPREHENSIVE STUDY ON CYBERCRIME - Draft February 2013 (unodc.org)> accessed 31 October 2021.
[xxvi] Report from the Commission to the European Parliament and the Council, *Attacks against Information Systems and Commonwealth of Independent States Agreement* (2017) <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017DC0474> accessed 31 October 2021.
[xxvii] Xingan Li, 'International Actions Against Cybercrime: Networking Legal Systems in the Networked Crime Scene' (2007) 4(3) Webology <https://www.webology.org/2007/v4n3/a45.html> accessed 31 October 2021.

[xxviii] Molly Ghosh, 'National Dialogue on Gender-based Cyber Violence' (2018) <https://itforchange.net/e-vaw/wp-content/uploads/2018/01/Molly_Ghosh.pdf> accessed 31 October 2021.
[xxix] ibid.
[xxx] End Violence Against Women, *New Technology: Same Old Problems* (End Violence Against Women Coalition, 2013) <-) (endviolenceagainstwomen.org.uk)> accessed 31 October 2021.
[xxxi] 'Revenge Pornography - Guidelines on prosecuting the offence of disclosing private sexual photographs and films' (The Crown Prosecution Service, 2017) < Revenge Pornography - Guidelines on prosecuting the offence of disclosing private sexual photographs and films | The Crown Prosecution Service (cps.gov.uk)> accessed 31 October 2021.
[xxxii] European Institute for Gender Equality, *Cyber Violence Against Women and Girls* (2017) <Cyber violence against women and girls | European Institute for Gender Equality (europa.eu)> accessed 31 October 2021.
[xxxiii] ibid.
[xxxiv] Aprajita Rana and Rohan Bagai, 'Cybersecurity in India' (Lexology, 2020) <Cybersecurity in India - Lexology> accessed 31 October 2021.
[xxxv] Mayura U Pawar and Archana Sakure, 'Cyber space and Women: A Research' (2019) 8(6S3) International Journal of Engineering and Advance Technology (IJEAT) <https://www.ijeat.org/wp-content/uploads/papers/v8i6S3/F13130986S319.pdf> accessed 31 October 2021.
[xxxvi] Astha Srivastava and Shivangi Sinha, 'Cyber Delinquency: Issues and Challenges under Indian Legal System' (2019) 8(5C) IJEAT <https://www.ijeat.org/wp-content/uploads/papers/v8i5C/E12040585C19.pdf> accessed 31 October 2021.
[xxxvii] Pawar and Sakure (n 35) 22.
[xxxviii] ibid.
[xxxix] ibid.
[xl] ibid.
[xli] *Yogesh Prabhu v State of Maharashtra* 2006 (3) MHLJ 691.
[xlii] *Suhas Katti v State of Tamil Nadu* CC No 4680 of 2004.
[xliii] *Avnish Bajaj v State (NCT) of Delhi* (2005) 3 Comp LJ 364 Del.
[xliv] *Saddam Hussain v State of Madhya Pradesh* CRA 3370 of 2014
[xlv] *SMC Pneumatics (India) Private Limited v Jogesh Kwatra CS (OS) No 1279/2001 Del.*