ILE MULTIDISCIPLINARY JOURNAL [IF SCORE – 7.58]

VOLUME 4 AND ISSUE 1 OF 2025

APIS – 3920 – 0007 | ISSN - 2583-7230

Published by

Institute of Legal Education

https://iledu.in

PREVENTION OF CYBER CRIME AGAINST WOMEN IN INDIA

AUTHOR - DR. MANPREET KAUR, ASSISTANT PROFESSOR, UNIVERSITY INSTITUTE OF LAW, SANT BABA BHAG SINGH UNIVERSITY.

EMAIL ID: *DHANJALMANPREET07@GMAIL.COM*

BEST CITATION - DR. MANPREET KAUR, PREVENTION OF CYBER CRIME AGAINST WOMEN IN INDIA, ILE MULTIDISCIPLINARY JOURNAL, 4 (1) OF 2025, PG. 677-690, APIS – 3920-0007 | ISSN - 2583-7230.

ABSTRACT

The Internet has become a basic fact of everyday life for millions of people worldwide, from e-mail to online shopping. Ever faster and more accessible connections available on a wider range of platforms, such as mobile phones or person to person portable devices, have spurred new e-commerce opportunities. Online shopping and banking are increasingly widespread and over the next 10 years, the Net is expected to become as common as gas or electricity. The invention of the computers has opened new avenues for the fraudsters. It is an evil having its origin in the growing dependence on computers in modern life.

Keywords:- Cyber Crime, prevention of cyber crime, cyber crime against women, division of cyber crime, cyber attacks, hacking, cyber stalking, Cyber-victimisation, cyber harassment, Social Networking, computer, internet, cyber privacy.

INTRODUCTION

At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cyber-crime was broken into two categories and defined thus:

a. Cybercrime in a narrow sense (computer crime): Any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.

b. Cybercrime in a broader sense (computer-related crime): Any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network. The OECD Recommendations of 1986 included a working definition as a basis for the study: Computer-related crime is considered as any illegal, unethical or unauthorized behaviour relating to the automatic processing and the transmission of data.

CYBER CRIME

First Case of Cyber Crime The first recorded cyber-crime took place in the year 1820! That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage. In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics.

DIVISION OF CYBER CRIME

Cybercrime does not have a single exhaustive definition, but it generally includes activities that insult human feelings. Child pornography is one of the most serious cyber crimes, causing considerable damage to the younger

generations. Cybercrime can be classified as crimes against individuals, property and government.

Cybercrime against individuals includes offences such as cyberstalking, online harassment and invasion of privacy. Online harassment can take different forms - sexual, racial or religious - and cause considerable distress to the victims. Cyberstalking, a growing problem, reflects harassment in the real world and affects many people on the Internet, especially women. Privacy violations are another serious concern, as individuals value the safety and anonymity afforded by the Internet.

Cybercrime involves hacking, cyber intrusion and the spread of malicious programs. Hacking, one of the most dangerous cyber attacks, compromises confidential data without permission. No computer system is completely impenetrable to a hacker, which makes cyber attacks a serious risk. Software piracy is also a widespread cybercrime, involving the unauthorised distribution of pirated software.

Cybercrimes against governments include cyber terrorism, in which individuals or groups use cyberspace to pose a threat to national security. This crime is particularly dangerous when it is targeted at government or military websites. As cybercrime evolves, the legal framework needs to be reinforced to effectively tackle these threats. While the US legal system has begun to tackle cybercrime, more efforts are needed worldwide to regulate and prevent cybercrime.

CRIME AGAINST WOMEN IN INDIA

The role of information technology is remarkable in today's world. It has widened itself over the last two decades and has become the axis of today's global and technological development. The world of internet provides every user all the required information fastest communication and sharing tool making it the most valuable source of information. It has extended efficiency, cost effectiveness and accelerated productivity at individual as well as the business or governmental level. It has brought world under one umbrella. The expanding reach of computers and the internet has made it easier for people to keep in touch across long distances. The internet plays an important role in our day-to-day life activities from home to office like in connecting with friends, searching study materials and in attending important video conferences.

In this scenario, cybercrime has emerged as a major threat, especially for women. The rapid growth of cybercrime, such as cyber warfare, cyber terrorism, hacking, data theft, invasion of privacy, phishing, intellectual property theft and identity theft, is a cause for concern. Anonymous and the speed of the Internet make cyberspace an attractive medium for criminals. Technological progress has expanded cybercrime in all directions, and it is a serious threat to national security and to individual security, especially for women.

Although cyberspace gives women access to information and freedom of expression, it also exposes them to cybercrime. Women are often victims of harassment, cyberstalking, identity theft and online abuse. Many receive unsolicited e-mails containing obscene language, while others are victims of image-mapping, image-stealing and unauthorised pornography. Cyber criminals are using social networking sites and marriage websites to abuse women and misuse personal information to harass or defame them. This victimization is often exacerbated by India's patriarchal society, where victims are more often blamed than not...

India has adopted the Information Technology (IT) Act 2000 to fight cybercrime, but it mainly addresses economic crimes and neglects gender issues. Social networking platforms, while useful, have become a breeding ground for cyber harassment. Kerala registered 80,000 complaints about cybercrime in 2012 alone, of which 50,000 related to harassment of women. Internet abuse leaves women of all ages

vulnerable and perpetrators seek to damage reputations and create fear. Cyber-victimisation often arises from a broken relationship, harassment by a former partner, professional rivalry, male dominance and the misuse of digital technologies. Methods of cyber harassment include befriending victims under false identities, stalking online activities, or encouraging collective victimisation. The Internet allows for widespread harassment and exacerbates the distress of victims by publicising them.

Cybercrime against women has evolved in different digital eras:

a. **The Email Period (1990s):** This period marked the advent of cyber communication via e-mails. Lack of strong cyber-regulation meant that women faced online harassment mainly through e-mail. WHOA statistics from 2000 showed that 87 percent of victims were women, and that e-mail was the most common form of cyberstalking.

b. **The Chat-Room Period (Late 1990s - Early 2000s**): Public and private chat rooms have become widespread, allowing criminals to access personal information and interact with others in real time. Laws on digital communications have begun to be drafted, and studies of cyber psychology have gained importance as digital identities are increasingly abused.

c. **The Social Networking Period (Early 2000s - Present**): With the rise of platforms such as Six Degrees.com (1997) and other social networks, new threats have emerged, such as cyber-bullying, sharing of unsolicited images and cyber-stalking. These crimes disproportionately affect women and the perpetrators use digital tools to intimidate and exploit them.

The increase in cybercrime against women is partly due to the patriarchal legal framework, which prioritises economic crimes, national security and the protection of children over gender-specific crimes. Many forms of online harassment, such as cyberbullying and the sharing of unsolicited images, are often dismissed, leaving victims to deal with the trauma in silence. Sextortion offences involving the victim receiving or unknowingly sharing explicit content have increased, especially among young adults.

Due to the lack of adequate law enforcement responses, women are increasingly turning to NGOs and private agencies for help. Support is provided by organisations such as the Internet Watch Foundation (UK, 1996), the World Wide Web Association (US, 1997), the Cyber Angels (US, 1995) and the Cyber Victim Support Centre (India, 2009). But many victims turn to professional hackers to stop online harassment, underlining the failure of law enforcement to deal with cyber threats against women.

Lack of a gender-sensitive legal framework has left cybercrime against women largely unregulated. Unlike victims of financial fraud or child abuse, women receive little emergency government assistance. As cyber threats evolve, new laws need to be drafted in a nonpartisan...

REVIEW OF LITERATURE

VIOLENCE AGAINST WOMEN IN CYBER WORLD: by Jaspreet Singh- The research paper acmes that Violence against women is a violation of human rights and has evolved in India over time. Despite efforts by feminists to combat this, the vulnerability and exploitation of women continues. This paper examines cyber-violence against women in India, its social impact, the causes and the prevention measures. The main challenge in tackling cybercrime is the ability of criminals to exploit the fleeting nature of cyberspace to facilitate their escape. Although many websites offer safety tips, cybercrime against women is on the rise.

MAPPING CYBER CRIMES AGAINST WOMEN IN INDIA by Dr. Shalini Kashmirithe research paper highlights cyber-crimes against women in India which is a completely new phenomenon. To make the paper effective, a comparative

analysis has been done between the cyber laws regulating cyber-crimes in India, United Kingdom and United States of America. The scholar observed in detail the various crimes against women and the legal framework regulating these crimes in India. Finally, the study provides with appropriate suggestions where necessary.

CYBERCRIME: THE TRANSITION OF CRIME IN THE INFORMATION ERA by ShailzaDutt, Dr.Suneyna, Asha Chaudhary the research paper acmes that Cybercrime is increasing in frequency and severity, requiring a review of criminal law. This document examines its types, modes and safeguards. While total elimination is impossible, awareness can reduce its impact considerably. A regulatory system with criminal sanctions is proposed to effectively curb cybercrime.

Cyber-Crimes and their Impacts: by Hemraj Saini, Yerra Shankar,Rao T.C. Panda The research paper highlights In the digital age, most information is now online and is vulnerable to cyber threats. These threats are complex, which makes it difficult to detect them in time. Cyber attacks, deliberate or not, can cause economic disruption, psychological distress and threats to national security. This document analyses cybercrime, its social impact and future trends.

Cybercrime: A threat to Network Security by Ammar Yassir and Smitha Nayak This research paper discusses the study examines cybercrime in detail, including its types, methods and network effects. It also examines the role of network security in mitigating attacks against connected systems. Cyber criminals exploit weaknesses in these systems to gain access to confidential data via viruses and malware. The vast connectivity of the Internet is beneficial, but it also allows criminals to work together and target victims.

CYBERCRIMES: ANOTHER DIMENSION OF WOMEN VICTIMIZATION by Paridhi Saxena & Anisha Malka The research paper highlights various cyber crimes highlighting cyber pornography, cyber bullying, cyber stalking against women. This paper also addresses about various lacunas in IT ACT 2000 and also made some suggestion in regard to these crimes. The scholar observed various crimes against women which are prevailing in India and noted down the suggestions and observations made therein.

CYBER CRIME AGAINST WOMEN IN INDIAby Debarati Halder, K.Jaishankar (2017) It analysed various cybercrimes against women in India, including hate speech, trolling, online grooming, invasion of privacy and sexual assault. Reviewed prevention measures by the police, judicial authorities and victims, as well as the responsibility of websites and service providers. We found that laws are scattered between IPC, the Evidence Act and the Information Technology Act, and offenders use servers outside India.

CYBER CRIME AND VICTIMIZATION OF WOMEN LAWS, RIGHTS AND REGULATIONS, Debarati Halder, K. Jaishankar (2012) this book is to identifies and explain the mostly unexplored crimes of the Internet targeting women in particular. This book is designed to define cyber victimization from women victim's perspective, analyze the trends of victimization, formulation of core rights of women internet users and examine the legal protections towards women victims of cybercrimes in five prime countries. The scholar observed definition, typology and patterns of Victimization Legal Treatment of Cyber Crimes against Women in USA, Canada, U.K. Australia. The scholar he scholar identified the factors associated behind the victimization of women in cyber space. The study revealed that Women victims are near invisible in the eyes of universal cybercrime conventions and domestic internet and cyber communication related laws. The effect of this lawlessness is so huge that government-reporting agencies also sometimes deny any help to the woman in need.

ILE MULTIDISCIPLINARY JOURNAL [IF SCORE – 7.58]
VOLUME 4 AND ISSUE 1 OF 2025
APIS – 3920 – 0007 | ISSN - 2583-7230
Published by
Institute of Legal Education
https://iledu.in

COMPUTERS, INTERNET AND NEW TECHNOLOGY LAWS by Karnika Seth(2016), is a comprehensive work that aptly highlights new laws, policies, cases, concepts, events and studies that have evolved cyber laws in the national and international spheres. The scholar noted that it specially focuses on the development of laws in India including new bills and guidelines that were passed such as Electronic Delivery of Service Bill, 2013, the cabinet approval of the New Consumer Protection Bill 2015 and the new guidelines for the introduction of e-authentication technique using Aadhar-eKYC services. It also discusses land mark cases, including Shreya Singhal vs. UOI, which struck down Section 66A of the IT Act, 2000 as unconstitutional and Anwar vs. P.K Basheer which clarified the law on appreciation of electronic evidence in India. The scholar further noted the emerging crimes such as trolling, sexting, and revenge porn and new developments such as Net Neutrality that have impacted the cyber world. The scholar noted basic concepts of cybercrime and its classifications. It has been observed that with the increase in use of technology the cybercrime is also on rise which is required to be checked.

Objectives of Study: -

• To understand the meaning of cyber-crime against women.

• To find out causation behind the victimization of women.

• To analyse 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 and human rights.

• To find out the steps which should be taken by the government for checking cyber crime against women in India.

Cyber Crime Against Women: Indian Scenario

In India, cyber-crime against women is relatively a new concept. It can be noted that when India started her journey in the field of Information Technology, the immediate need that was felt to protect the electronic commerce and related communications and non-cyber socializing communications. The drafters of the Indian Information Technology Act, 2000, created it on the influence of the Model Law on Electronic Commerce, which was adopted by the resolution of the General Assembly of the United Nations in 1997. The Act turned out to be a half-baked law as the operating area of the law stretched beyond electronic commerce to cover cyberattacks of non-commercial nature on individuals as well. While commercial crimes and economic crimes were moderately managed by this Act, it miserably failed to prevent the growth of cyber-crime against individuals, including women.

Main types of Cyber Crime against women are:

Cyber pornography/ obscenity,

CyberStalking,

CyberBullying,

Cyber Morphing,

Cyber Pornography:

This would include pornographic websites; pornographic magazines produced using computer and the Internet (to down load and transmit pornographic pictures, photos, writings etc.) Predominantly sexually explicit material, lascivious in nature intended primarily for the purpose of arousal of sex desires or erotic activity over the internet and includes pornographic websites, e- magazines containing porn stuff which could be downloaded from the internet, transferrable porn pictures, photos writings etc. Because of the advantage of lack of territorial restrictions, anonymity and fastest means of communication pornographic materials can be reproduced more quickly and cheaply on new media like hard disks, floppy discs and CD-

ROMs. Apart from still pictures and images, full motion video clips and complete movies are also available. Another great disadvantage with a media like this is its easy availability and accessibility to children who can now log on to pornographic web-sites from their own houses in relative anonymity and the social and legal deterrents associated with physically purchasing an adult magazine from the stand are no longer present pornography industry is contributing approximately $ 20 billion annually to the global economy. For example In India Videsh Sanchar Nigam Limited (VSNL) and number of other internet service providers such as Reliance, Vodafone, Airtel , cyber cafes, online portals etc provides for various kinds of internet schemes without restrictions on the nature of persons permitted to avail these services. Moreover the social websites like Facebook, Twitter, Whatsapp, Orkut, free music downloading sites etc do not check the kind of material that is being uploaded and downloaded. They do not have any parameter to differentiate between what we call as an art or pornography. What is more shocking is children (between 8-16 years) indulgence in viewing porn sites. Approximately twenty six popular children's characters such as Pokemon, Action Man, My Little pony reveals thousands of links to porn sites.

The most embarrassing aspect of pornography industry is the child pornography. The Air Force Bal Bharti, Delhi Cyber Pornographic Case (2001) and the Bombay Swiss Couple Case (2003) are the leading examples in this context. It is to be noted that Traditional law of obscenity is contained under sections 292-293 of Indian Penal Code, 1860.Section 292deals with the sale of obscene books and section 293 provides punishment to person dealing in cyber pornography that is accessible to person under twenty years of age with imprisonment up to three years and fine up to two thousand rupees on first conviction and with imprisonment up to seven years and fine up to five thousand rupees on second or subsequent convictions. The IT Act, 2000 was deficient in dealing with obscenity and consist of a single section67 dealing with the crime. IT (Amendment) Act, 2008amended section 67. The combined effect of sections 66-E, 67, 67-A and 67-B obscenity has been brought under the legal regime and child pornography has been separated from mainstream pornography. Section 67 provides that whosoever publishes or transmits obscene material in electronic form shall on first conviction be punished with imprisonment up to three years and fine which may extend up to five lakh rupees and on second or subsequent convictions, imprisonment up to five years and fine up to ten lakh rupees. Section 67A deals with mainstream pornography and provides punishment for publishing or transmitting of material containing sexually explicit act, etc in electronic form with imprisonment up to five years and fine up to ten lakh rupees on first conviction and with imprisonment up to seven years and fine up to ten lakh rupees on second and subsequent convictions. Section 67-B is related to child pornography. This section provides punishment for publishing or transmitting of material depicting children in sexually explicit act, etc, in electronic form or creates text , digital images, collects, seeks , browses, downloads , advertises, promotes, exchanges or distributes material in electronic form depicting children in sexually explicit act or entices or induces children for online relationship with one or more children or facilitates abusing children online with imprisonment up to five years and fine up to ten lakh rupees on first conviction and imprisonment up to seven years and fine upto ten lakh rupees on second or subsequent conviction. Other acts having an impact on cyber pornography are indecent representation of Women's Act, 1986 and Young Persons (Harmful Publication) Act, 1950.

In many countries like India and Malaysia, British law (the Hicklin test for obscenity) left over from a colonial legacy is still used to determine what is obscene. The Hicklin test of obscenity is whether "the tendency of the matter charged as obscenity is to deprave and corrupt those

whose minds are open to such immoral influences and into whose hands a publication of this sort may fall." The test defines 'obscene' as all visual or written material that is "lascivious or appeals to the prurient interest", and has the capacity to corrupt those exposed to it. These standards are relevant in the context of Internet governance as well, since most countries are either extending existing legislation for other media (television and cinema) to the Internet. New laws enacted for the Internet adopt the same definitions regarding obscenity or sexually explicit material, inheriting also the weight of precedents that have determined what is obscene. This definition of obscenity and the penalisation of it under the Indian Penal Code, 1860 (sections 292 and 293) is further extended by other laws that prevent the distribution of such material (Young Persons Harmful Publication Act, 1956, Indecent Representation of Women (Prohibition) Act, 1986). The case that laid down the Hicklin test i.e., was about the mass distribution of inexpensive pamphlets called provocatively "R. vs. Hicklin The Confessional Unmasked" described how priests extracted erotic confessions from female penitents. The publication of the pamphlet was encouraged by the Protestant Electoral Union and used by them to discredit the Catholic Church and specifically to prevent laws that would allow Catholics into the Parliament. A description of the social and political context of this case or even the content of the pamphlet found obscene is rarely found in discussions on obscenity law in the contemporary. In a handbook on pornography law, Thomas C. Mackey discusses this case – "Protestant Electoral Union sought to 'protest against those teachings and practices which are un-English, immoral and blasphemous, to maintain the Protestantism of the Bible and the liberty of England'. Further, the Protestant Electoral Union supported electing as Members of Parliament, men who shared their anti-Catholic sentiments and who wished to 'expose and defeat the deep-laid machinations of the Jesuits'. It is perhaps not so difficult to draw a link between the political and social connotations in this case and the use of obscenity law to control political speech, especially since the birth of print culture and urban spaces, led to the proliferation of explicit sexual writing in early stages of modern Europe that was used to satirise and criticise the church, state and monarchy and was controlled for its defamatory and blasphemous nature, more than its obscenity.

In the legal discourse pornography is missing as a category except as an aggravated form of obscenity (Ranjit Udeshi v. State of Maharashtra). In this case the obscenity of Lady Chatterley's lover was on trial, and it was held that the book as per the Hicklin test is obscene since it has the potential to deprave and corrupt by immoral influences. In essence the judgment deals with slang and colourful language and it was held that there was not enough preponderance of art or social purpose in the text. The judgment does make reference to pornography as "dirt for dirt's sake" further explained as "libidinous writings of high erotic effect unredeemed by anything literary or artistic and intended to arouse sexual feelings". It is this judgment that establishes the Hicklin test as the law to be followed in independent India as well.

In the recent fairly progressive judgment on M.F. Hussain's painting, this definition was reiterated, giving some degree of distinction to the category of pornography apart from it being an aggravated form of obscenity and to say that it is a class of objects, images, paintings, videos designed for sexual arousal, while other material which may or may not be obscene is layered with other meanings (aesthetic, patriotic, narrative). But as such it is not a much more evocative definition than "dirt for dirt's sake". Does this missing descriptive category assist in the rampant circulation of pornography, either online or offline? But perhaps the more interesting question to ask is how the legal discourses side step the question of pornography, while minutely examining material that could be described as obscene.

This intensity of the legal gaze is obvious than in the judgments on obscenity of film, books, magazines (in Indian law) where the material is minutely examined for traces of obscenity.

In the legalistic drive to categorize and label, the court has also drawn fine distinctions between obscenity and vulgarity stating that – "A vulgar writing is not necessarily obscene. Vulgarity arouses a feeling of disgust and revulsion and also boredom but does not have the effect of depraving, debasing and corrupting the morals of any reader of the novel, whereas obscenity has the tendency to deprave and corrupt those whose minds are open to such immoral influences." This case deals with a fiction story published in a relatively popular magazine Prajapati about a character called Sukhen whose slide into the life of decadence and squalor is narrated in first person. Sukhen hates his teachers, hypocritical politicians and is often violent or at least regarded as a goonda by others. This story of all those encountered by the law seems to be indeed the most erotic and fascinating – here is an excerpt of the court's description of the story/novella "Seeing Shikha in that position with the butterfly on her palm and Shikha trying to fix the severed wing in its place in the body of the butterfly, Sukhen is reminded of what happened to Zina, a daughter of one of the officers of the factory at the picnic party of the factory owner and its big executives. Sukhen remembers how at that party Zina, a girl of about 14 years of age was being fondled by the elderly persons holding high posts in the factory and whom Zina would call 'Kaku' (Uncle). Sukhen also recalls that how he thereafter had taken Zina away from those persons to a sugarcane field and had an affair with her there. This part of the affair with Zina in the sugarcane field had been considered to be obscene. Sukhen feels that the butterfly resting in the palms of Shikha resembled Zina in the sugarcane field while she was there with him. After remembering this incident Sukhen turns to Shikha and goes near her. There he notices Shikha's dress and he finds Shikha had only a loose blouse with nothing underneath and a good part of her body was visible and there is some description by Sukhen of what was visible and of his feelings on seeing Shikha in that position. Sukhen's kissing Shikha and going to bed with Manjiro, his friend's sister, are other parts of the book considered obscene. The affairs of Sukhen's 'Mejda' (second elder brother) with the maidservant's daughter and Sukhen's description of the same have also been hold to be obscene."

In the same judgment, pornography was described a little bit more in the words of the High Court judge who held the book to be obscene, and the Supreme Court overruled his decision. The High Court judge stated that the book is in fact pornography – "Pornography it is and with all the gross taste not because it has sacrificed the art of restraint in the description of female body and also because in some part it has indulged in complete description of sexual act of a male with a female and also of lower animal." In the Supreme Court judgment, it was held that the judge must apply his mind dispassionately to the question of whether the book is obscene, and not allow for personal preference or subjective element in the subconscious mind to influence his decision. Eventually while deciding that the book was indeed not obscene, the court justified this by saying that the book would shock readers rather than deprave them, consequently serving as a moral warning for all the sins and vices described. The decision of the court to not ban the book is also buttressed by interventions of scholars from Jadavpur University in support of the book and the moral stand it takes eventually.

It is also perhaps relevant that Sukhen, the main character is on his way to being reformed, from his restlessness, sexual drives and finding solace and peace with himself, especially with the help of his new lover Shikha, when he gets injured in violent clashes between rival political parties and dies. It is from this bleak ending that the court salvages the moral resurrection of this book as not obscene – the dire punishment of

those who succumb to sexual and other vices is most evidently laid out.

The decision in which there was an appeal to the courts to declare that precentorship of cinema in India is unconstitutional is K. A. Abbas v. Union of India and Another. This appeal was not accepted and it was held that pre-censorship in cinema is necessary because of the impact that cinema has on the senses, unlike other mediums such as books, magazines, paintings, etc., – "with trick photography, vista vision and three dimensional representation thrown in has made the cinema picture more true to life than even the theatre or indeed any other form of representative art". The decision relies on Mutual Film Corporation v. Ohio, in spite of an acknowledgement that this decision was no longer relevant to American jurisprudence that does indeed give protection to cinema as well under the First Amendment (freedom of expression).

The description of cinema in Mutual v. Ohio is probably the most indicative of the fear and suspicion with which the image and especially the moving image as perceived in law. Cinema is likened to magic and sorcery – it is said that "indeed (moving pictures, cinema) may be mediums of thoughts, but so are many things, so is the theatre, the circus and all other shows and spectacles. Rather than being organs of public opinions, of ideas and sentiments, published and known, vivid, useful and entertaining no doubt, but as we have said, capable of evil." Echoing this general distrust, it was held in K.A. Abbas that the reason for treating cinema or moving image differently is that "the motion picture is able to stir up emotions more deeply than any other product of art. Its effect particularly on children and adolescents is very great since their immaturity makes them more willingly suspend their disbelief than mature men and women. "The justification of censorship based on the paternalistic role of the State that must protect the infantile public is often repeated in Indian jurisprudence on obscenity, not only as a rationale for classification of material but also for the banning and censorship of different material.

In the introduction to The Public is Watching: Sex, Laws and Videotapes, Lawrence Liang states that rather than giving an account of censorship as incursions into the right of freedom of expression or receiving information, perhaps it is more useful to have a productive account of censorship. This is inspired from Annette Kuhn's work on early British cinema and the linkages she draws between discourse around birth control and censorship paradigms. Annette Kuhn's emphasis on the productive discourse of censorship allows for the shift away from looking only at the content/material that is to be censored to the forces, institutions, notions, ideologies that are pulled into play and are produced for censorship to take place; to move away from a straight forward account of power. Kuhn says – "To question this model is by no means to deny that censorship has anything to do with power. On the contrary, what I want to suggest in fact is that an understanding of power as a purely prohibitive gesture - especially where the object of prohibition is taken to be the representation of some pre-existing reality - does not go far enough, and may actually inhibit our understanding of how, and with what effects, the powers involved in film censorship work. The prohibition model of censorship is usually associated with a further assumption: that censorship is something that takes place within certain organisations, especially in organisations with an explicit institutional remit to censor."

Liang takes this thesis further to state that the prohibitive idea of censorship doesn't allow us to see that the law is building a theory of cinema, of spectatorship and the idea of the public – "The law of instance, is not merely interested in prohibiting a particular kind of 'seeing', but also equally interested in suggesting the proper way of seeing." In other words, the productive project of law is also about a discursive crafting of the ideal viewer of cinema – where he (and this ideal is not inclusive of she) will view cinema, what he will

see and read from it. Hence, each judgment that lays down the meaning of an object – whether Bandit Queen and Prajapati as not erotic but shocking and containing a moral regarding social evils (of vice, alcohol and caste violence) or Hussain's painting Bharat Mata as not erotic/obscene but as patriotic, is also stating that this is what the ideal viewer/spectator would see – this is the meaning that is attached to the image (like a caption) with which it must be read.

The court has a heavy investment in the question of aesthetics and especially narrative as is evident in the decision on Shekhar Kapur's Bandit Queen (Bobby Art International &Ors. v. Om Pal Singh Hoon&Otrs 1996 AIR (SC) 1846). In Bandit Queen, Phoolan Devi is raped and walks through the street of the village, naked. This caused much consternation and led to the case coming up before the court. Aesthetic opinions on the film varied – even as Arundhati Roy described it as the 'great Indian rape trick'the court held that it is a film that attempts to show the reality of a social evil. Consequently, it must show that social evil in the film. The narrative demands that the rape sequence that puts Phoolan Devi on the path to becoming a cruel, vengeful dacoit is essential – "in aid of the theme and intended not to arouse prurient or lascivious thoughts but revulsions against the perpetrators and pity for the victim."

Perhaps the most important decision in this regard, that characterizes the slippage between obscene and pornographic objects, is the case of Pratibha Naithani v. Union of India. The court was called upon to decide whether English movie channels (like HBO and Star Movies) should be pulled off the air for broadcasting adult content, and what controls should be put on the channels (censoring bad language, timings of adult movies, etc.). This case exemplifies the blurry borders of obscenity as a category – whereby innocuous objects are pointed at, as aspects of a sleazy modernity that are separate from Indian culture, and thereby rendered obscene. Indian culture plays an important referent role in most of the judgments on obscenity – to answer the question of what affect is produced in people by allegedly obscene objects and sometimes to emphasize the existence of erotic, sexual texts within Indian culture that are not found objectionable and point to a tradition of eroticism that should be taken into account.

Subsequent judgments have dealt with as varied objects as newspapers and their erotic content, a documentary film by Anand Patwardhan which contains a scene of an aphrodisiac being sold and eventually M. F. Hussain's painting Bharat Mata. This painting depicts India in the shape of a nude woman distressed or grieving and was put up on a website for auctioning for a worthy cause. However, this led to a case about the painting and the court eventually decided that it was not obscene in one of the more progressive judgments about obscenity in India. The purpose of this short account of obscenity jurisprudence in India is perhaps merely to point at how various objects, most of them barely obscene and innocuous, have been examined by the law in much detail. It is this detailed and minute examination that is intriguing. Pornography itself has very blurred boundaries – as various objects slip into this category, whether it is Hollywood films with very minor sexual content, soft porn films often called blue films, BF , films like Choker Bali that are circulated in cinema halls that are meant for blue films21 Soft porn itself points to how there exists various gradations of material – some of them marked only by slang, suggestive language, minimal dressing and references to sexual activity rather than sexual explicitness (nudity, genitalia or sexual activity). Hard core pornography is circulated largely through CDs, DVDs in video parlours and piracy markets and through the Internet; it ranges from material from Europe and America and a smattering of Indian pornography which is mostly heterosexual. Amateur pornography or sexually explicit material which is made and put online either as part of the porn industry, which is not very large especially in comparison to the

global North, or by people themselves, is a relatively new phenomenon assisted by digital technologies and the Internet. In the last decade, the leaking of such material, and consequently the swarm of moral, ethical, social dilemmas that have arisen has led to most of the 'scandals. It is these scandals that are literally pushing the category of pornography out of the grey zones of being a public secret; out of rampant and unexamined illegality into the realm of the law – its imperatives, violence and descriptive plenitude.

Cyber Privacy and Related Problems for Women

The cyber space regulatory laws are partly gender sensitive in the US especially for cases covering stalking, domestic violence, dating violence and the extension of the same in the cyber space. While considering general privacy issues (excluding financial crime), we note that women still remain vulnerable victims. Hacking and stalking are the most sorted crimes that invade the privacy of the victim. Video voyeurism and adult sexting are the two essential component parts of online privacy invading activities.

Legal Treatment of Cyber Crime against Women in UK

This is more evident from the available statistical reports of cyber-crime in the UK. Analysing the 2018-2019 report of "Garlik", "The online experts", it can be seen that among 29.7 million adult internet users in UK, there are approximately 2,374,000 instances of online harassment. By online harassment, the report indicates cases of mental distress of the victim, stalking, sending unwanted abusive mails containing hate messages, racial messages, threatening messages and blackmailing mails etc. This report shows that among other crimes, there were 86,900 instances of identity theft and identity fraud (which includes impersonation, using of other's identity card, identity theft etc mainly for financial gain), 207,700 instances of financial frauds (which includes losses of plastic cards, bank frauds etc), 137,600 instances of computer misuse (the report does not include virus infections) and 609,700 instances of sexual offences which cover victimization of children mainly. Apart from the Garlik report, we did not find any detailed analysis of cyber victimization, especially of women in UK. This could be an indication as how individuals, especially women are conservative about reporting the online crimes that happen to them. A victimization survey to unearth online crimes against women in the UK is the need of the hour. Unauthorized Access and Related Activities.

Hacking and hacking related activities may not always be restricted to crimes committed against the nation or the corporate entities alone. We see it as a crime when done to stored computer data or the computer as a machine of any female victim. To access her personal information including pictures without proper authorization, with intention to misuse it, distribute it in the internet, modify the contents and give a false impression of the victim etc, are also criminal activities like stalking or bullying. Strangely enough, in UK, these sorts of cyber-criminal activities against women have been never given a separate legal treatment on the pretext that these are also one of the hacking related activities which are done to individuals. We feel that the core reason for the growth of internet crimes against women could be lackluster attitude of the law and justice machinery to understand the nature of hacking related activities targeted especially to the women. Such sorts of unauthorized access towards personal data may lead to several other cyber offences including public defamation and humiliation, impersonation, unwanted exposure of the victim in adult entertainment industry etc. Unlike the US, the UK does not have any women – special regulation to cover cyber offences originating from domestic violence or dating violence; rather the offences related to unauthorized access are regulated by a compact legislation called "Computer Misuse Act, 1990". Under this Act, three offences are penalized, namely, unauthorized access to computer material, or

to enable any such access to secure unauthorized access, intention to create further menace with such unauthorized access and unauthorized modification of the computer material. As mentioned earlier, this Act was created to protect both men and women victims. Notably, the drafting of the language could very well suit the needs for preventive actions against harassment of women also when it says that the men's rea must be directed to the 'act' that the offender knows would successfully accomplish his intention to harm his victim. In brief, the offender can be held guilty for unauthorized access if it is proved that he used his technological knowledge to access the computer material or data with intention to harm the victim. The penalties for such offences are on a summary conviction in England and Wales to imprisonment for a term of 12 months or to a monetary fine not exceeding statutory maximum, or both. In case of summary conviction in Scotland, the law prescribes imprisonment for six months or to a fine not exceeding statutory maximum, or both.

Conclusion and Suggestion

Crime in all its forms has a negative impact on society, and in developing economies cybercrime has increased as a result of rapid digitalisation. Technology permeates every aspect of life, from corporate governance to small businesses, and individuals are heavily dependent on digital devices. The fact that the Information Technology Act, 2000, or its 2008 amendment, does not contain a specific definition of cybercrime reflects the evolving nature of these offences. In general, any crime involving a computer - whether as an instrument, a target or a data source - falls within the scope of cybercrime. Even traditional crimes such as theft or fraud may be classified as cyber crimes if they involve the use of digital information.

Cybercrime affects individuals and data security, with women being particularly vulnerable. Women are often victims of cybercrime not only by individuals but also by technological loopholes and inadequate legal frameworks. The exponential growth of cyberspace has outpaced legislative progress, leaving fundamental rights under-protected. Legislators focus mainly on cyber crimes against governments, financial institutions and children, often neglecting cyber crimes specifically targeting women. While laws against child pornography and cyberbullying are being implemented, digital victimisation continues to affect millions of Internet users due to the lack of regulation of the Internet. The online world allows individuals to exercise their freedom without accountability, creating a paradox in which cyberspace can be both a utopia and a prison.

Women are disproportionately affected by online crime, especially when it comes to reputation and privacy. Criminal activities such as cyberstalking, extortion and digital sexual exploitation have increased with technological progress. Cases of recorded attacks, the unauthorised distribution of intimate images and digital harassment highlight the serious consequences of cybercrime. Social norms exacerbate these problems, as women's reputations are often tied to family honour, which makes them the prime targets of cyber-bullying.

The borderless nature of the Internet, combined with anonymity, allows for the digitalisation of traditional crimes such as theft, extortion, libel and counterfeiting. In addition, new cyber-attacks such as hacking, phishing, malware attacks and corporate espionage are emerging. Cybercrime can be classified into three types: computer-based crimes (e.g. hacking, data breaches), computer-based crimes as tools (e.g. fraud, identity theft), and computer-based crimes as accessories (e.g. child pornography, piracy). The rise of the practice of sending a message (voice phishing) further illustrates how cyber criminals are manipulating technology to commit financial fraud.

In India, cybercrime is mainly covered by the Information Technology Act 2000 and BNS 2023.

However, the existing legislation mainly deals with financial crimes and offers unclear definitions and insufficient sanctions. Unlike Canadian, British, and American anti-voyeurism laws, Indian law lacks explicit provisions addressing digital sexual offences. Although Section 67A of the Law on Information Technology prohibits the distribution of sexually explicit material, it is still not sufficient to comprehensively tackle cyber-enabled sexual offences.

Effective legal reforms, strict enforcement and increased cyber awareness are essential to tackle cybercrime. Strengthening data protection legislation, ensuring gender-sensitive legal frameworks and implementing global best practices can improve cyber security. As the digital environment continues to evolve, legal systems need to adapt accordingly to protect individuals against the increasing threats from cybercrime.

References

1. Beza Speaks. (n.d.). *History of cybercrime*. Retrieved from http://www.bezaspeaks.com/cybercrime/history.htm
2. Duggal, P. (n.d.). *Cyber law and cyber crime*. Retrieved from pduggal@vsnl.compavanduggal@hotmail
3. Fatima, T. (2011). *Cyber crime*. Eastern Book Company.
4. United Nations. (n.d.). *International review of criminal policy: United Nations manual on the prevention and control of computer-related crimes.* Retrieved from http://www.uncjin.org/Documents/EighthCongress.html
5. The Indian Express. (2024).
6. Working to Halt Online Abuse. (2000). *WHOA statistics for 2000.* Retrieved from http://www.haltabuse.org/resources/stats/2000stats.pdf
7. Spinderella. (2023, November 22). *Another woman claims Tony Parker was sexting her.* Retrieved from http://thesoulofdfw.com/national/news-gossip/spinderella/another-woman-claims-tony-parker-wassexting-her/
8. Working to Halt Online Abuse. (2001). *WHOA statistics for 2001.* Retrieved from http://www.haltabuse.org/resources/stats/2001stats.pdf
9. MacKinnon, C., & Dworkin, A. (1984). *An act to protect the civil rights of women and children.* Retrieved from http://www.nostatusquo.com/ACLU/dworkin/OrdinanceMassComplete.html
10. WiredSafety. (n.d.). Retrieved from http://www.wiredsafety.org/
11. Cyber Victims. (n.d.). Retrieved from www.cybervictims.org
12. U.S. Congress. (2008). *Megan Meier Cyberbullying Prevention Act.*
13. Fatima, T. (2011). *Cyber crime.* Eastern Book Company.
14. Paranjape, V. (2010). *Cyber crimes and law.* Central Law Agency.
15. Indian Penal Code, § 292 (1860).
16. Indian Penal Code, § 293 (1860).
17. Information Technology (Amendment) Act, § 67 (2008).
18. Information Technology (Amendment) Act, § 32 (2008).
19. Miller v. California, 413 U.S. 15 (1973).
20. K.A. Abbas v. Union of India, (1970) 2 SCC 780.
21. R. v. Hicklin, L.R. 3 Q.B. 360 (1868).

22. Mackey, T. C. (2002). *Pornography on trial: A handbook with cases, laws, and documents.* ABC-CLIO.
23. O'Toole, L. (1999). *Pornocopia: Porn, sex, technology, and desire.* Serpent's Tail.
24. Samaresh Bose v. Amal Mitra, AIR 1986 SC 967.
25. Raj Kapoor v. State, AIR 1980 SC 258.
26. Bobby Art International & Others v. Om Pal Singh Hoon & Others, AIR (SC) 1846 (1996).
27. Annette Kuhn. (1988). *Cinema, censorship, and sexuality.* Routledge.
28. Arundhati Roy. (n.d.). *The Great Indian Rape Trick.* Retrieved from http://www.sawnet.org/books/writing/roy_bq1.html
29. Garlik. (n.d.). *Cybercrime report.* Retrieved from http://www.garlik.com/cybercrime_report.php
30. Computer Misuse Act, § 1 (1990).
31. Police and Justice Act (2006).
32. **Information Technology (Amendment) Act, 2008, § 67A.** Retrieved from http://cybercrime.planetindia.net/ch11_2008