GENDER JUSTICE IN CYBERSPACE: THE INDIAN JUDICIARY'S EVOLVING JURISPRUDENCE ON WOMEN'S DIGITAL RIGHTS

Miss Smitarini Chamuah, Research Scholar, Department of Legal Studies, Arunachal University of Studies, Namsai, Arunachal Pradesh

Prof. Stuti Deka, Research Supervisor, Department of Legal Studies, Arunachal University of Studies, Namsai, Arunachal Pradesh

ABSTRACT

In India, the rapid development of digital technology has changed the definition of safety, privacy, and dignity, especially for women using the internet. With an emphasis on how judicial interpretation has extended old constitutional safeguards to confront novel forms of online harassment, the paper critically analyses the development of gender-sensitive cyber jurisprudence in India. This study investigates how courts have incorporated gender perspectives into cyber law enforcement through an examination of seminal rulings and new legal frameworks, such as the Digital Personal Data Protection Act (DPDP), the Bharatiya Nyaya Sanhita (BNS), and pertinent sections of the Information Technology Act. It also examines the shortcomings in victim-centred remedies, procedural justice, and institutional response that still prevent effective reparation. Through a comparative and rights-based approach, the paper examines Indian judicial developments in context and makes it clear that the judiciary is essential to bring constitutional promises reality on the internet and directing India towards a more secure and inclusive cyberspace for women.

Keywords: Cyber Jurisprudence, Gender Justice, Indian Judiciary, Online Harassment, Digital Rights.

INTRODUCTION

In a legal sense, stopping the harassment of women in cyber space requires interpreting the law as it stands in order to address new threats that arise online. Courts emphasize the need for a safe digital environment by applying conventional legal principles to online conduct. Historical precedents emphasize how crucial it is to protect the right to free speech while clearly defining and criminalizing harassment in cyber space. Judges are constantly trying to strike a balance between the right to privacy and the protection against harassment as legal frameworks are adjusted to the ever-changing nature of cyberspace.[1] The goal of evolving jurisprudence is to prevent online abuse and offer victims useful remedies, promoting a safe online environment for women. Law should therefore use the corrective mechanism or the deterrence based on factual matrix while operating the punishment system. The sentencing procedure can be skilfully modulated to be strict where it needs to be and tempered with pity where it is appropriate.[2]

In addressing cyber crimes, the Indian judiciary plays a crucial role in interpreting and enforcing relevant laws, safeguarding the rights of victims, and ensuring the perpetrators are held accountable. The judiciary's interventions aim to create a legal framework that is responsive to the complexities of cyberspace and provides avenues for redressal and justice.[3]

CYBERCRIMES AGAINST WOMEN: A CONCEPTUAL FRAMEWORK

The phenomenon of cybercrime against women reflects how structural gender inequalities in society replicate and intensify in the digital space. While cyber offences are not limited to any one gender, women are disproportionately targeted due to patriarchal attitudes, gender stereotyping, and the objectification of women's bodies and voices online. Understanding the forms, impact, and jurisprudential gaps is critical to framing effective legal and judicial responses.

The legal framework in India includes the Information Technology Act, 2000[4], which has been amended to address cyber crimes, including sexual harassment and online abuse. Landmark

[1] D. Chatur, "Legal Framework Regulating Internet Obscenity: An Indian Perspective" *available at:* https://www.academia.edu/805572/Legal_Framework_Regulating_Internet_Obscenity_An_Indian_Perspective (Last Accessed September 07, 2025).
[2] *Dinesh v State of Rajasthan*, AIR (2006) 3 SCC 771.
[3] Shreyansh Pandey, "Judicial Interpretation of Cyberspace Interpretation"
[4] Information Technology Act, 2000 (Act 21 of 2000).

judgments and legal interpretations by the judiciary have expanded the scope of the law to encompass various forms of cyber crimes and have recognized the need for preventive measures, awareness, and legal remedies. The Supreme Court stated in its most recent decision that while the freedom to engage in any profession or carry on any trade, business, or occupation via the internet is protected by the Constitution under Articles 19(1)(a)[5] and (g)[6], any restrictions on these Fundamental Rights should be made in accordance with Articles 19(2)[7] and (6)[8] of the Constitution, including the proportionality test.[9] According to Articles 21A[10] and 21[11] of the Indian Constitution, respectively, the right to education and the right to privacy both include the right to access the Internet.[12] Access to the internet improves education quality while also increasing students' options to learn.

Much with other categories of crimes, computer-related offences include a variety of motivations. It might involve a variety of things, such as pursuing thrill, seeking retribution, being greedy, wanting personal gain, or even displaying psychopathic traits. In general, it can be seen that almost any type of illegal conduct that can be carried out independently of computers may also be made easier by using computers. These events frequently present intricacies that make them difficult or even impossible to resolve, which makes them major problems for inquiry and prosecution.[13]

However, the Indian judiciary faces several challenges in effectively addressing crime against women in cyber space. These challenges include the anonymity of perpetrators, jurisdictional complexities, technological advancements that outpace legal developments, victim protection concerns, and delays in legal proceedings. Crime against women have emerged as a pressing concern in the digital age, posing significant challenges to their safety, privacy, and well-being. In India, where gender-based violence remains prevalent, the role of the judiciary in addressing and combating cyber crimes is of paramount importance.[14] The advent of technology and the

[5] The Constitution of India, art. 19(1)(a).
[6] The Constitution of India, art. 19(1)(g).
[7] The Constitution of India, art. 19(2).
[8] The Constitution of India, art. 19(6).
[9] *Anuradha Bhasin vs. Union of India and Ors.* (2020)1MLJ574.
[10] The Constitution of India, art. 21A.
[11] The Constitution of India, art. 21.
[12] *Faheema Shirin RK v. State of Kerala and Ors*., AIR 2020 Ker 35.
[13] Lexis Nexis's Cyber Law, "An exhaustive section wise Commentary on The Information Technology Act", 3rd Edition (2023).
[14] J. Singh, "Violence Against Women in Cyber World: A Special Reference to India International Journal of Advanced Research in Management and Social Sciences", available at: https://garph.co.uk/IJARMSS/Jan2015/8.pdf (Last Accessed Jun 5, 2025).

widespread use of the internet have created new avenues for sexual harassment, exploitation, and abuse in cyberspace.[15]Women are increasingly becoming targets of sexual harassment, stalking, non-consensual sharing of intimate images, i.e. revenge porn, and other forms of digital violence. These crimes have severe psychological, emotional, and social consequences, infringing upon the basic rights and dignity of women.[16]

FORMS OF CYBER VIOLENCE AGAINST WOMEN

Cyber violence manifests in multiple forms, often evolving alongside technological innovations. The most prominent include:

a) Cyberstalking

Cyber stalking is one of the most common internet crimes in the present era. 'Stalking' means 'pursuing secretly." Cyber stalking can be synonymous with online harassment and abuse.[17] It is the use of the Internet or other digital tools to stalk or harass another person.[18] The utilization of technology allows stalkers to harass their target from oceans away.[19] It entails compromising a person's privacy by tracking their movements over the Internet by posting posts on bulletin boards, entering chat rooms frequented by the victim, and repeatedly assaulting them with messages and emails containing obscene language. It is believed that more than 75% of the victims are female. In the United States, over a million women and 370,000 men are stalked each year. One in twelve women and one in every forty-five men will be stalked at some point in their lives.[20]

b) Cyber Pornography

Pornography of any kind is an issue for women and children. There are several pornography sites on the internet. These websites rely on internet traffic. Many ladies are unaware that their

[15] D. Singh, "Short Notes on Cyber Law", Allahabad Law Agency, (2013).
[16] N K. Bhatt et al., "A Challenging role of Indian Judiciary at cyberspace to curb cybercrime against women", A Global Journal of Interdisciplinary Studies (2021).
[17] Muthukumaran, "Cyber Crime Scenario in India", available at: http://www.gcl.in/downloads/bm_cybercrime.pdf, (visited on 15th September 2025).
[18] M. Kumar, "Cyber stalking : Online harassment or Online abuses", available on http://www.cyberarmy.in/2010/12/cyber-stalking-onlineharassment-or.html, visited on 17th September 2025.
[19], "Cyber Harassment and Cyber stalking: A growing problem", available on chrome-https://sites.wp.odu.edu/ashields/wp-content/uploads/sites/36136/2024/04/CYSE-200T-Analytical-Paper-Cyber-Harassment-and-Cyberstalking-A-growing-problem-Antonio-Shields.pdf, visited on 17th September 2025.
[20] A. Moore, "Cyberstalking and Women-Facts and Statistics", available on http://womensissues.about.com/od/violenceagainstwomen/a/Cyberstalki ngFS.htm , visited at 18th September 2025.

images are on such websites. A considerable number of cases have been documented in which someone altered and doctored images of women and posted them on pornographic websites. Pornography is a systematic act of exploitation and servitude that dehumanizes women. Cyber pornography is an additional kind of online threat to women's security. It is the vivid, sexually explicit subjection of women through images or words, which also includes Pornography is verbal or visual material that depicts or discusses sexual behaviour that is humiliating or abusive to one or more participants in a way that supports the degradation. The fact that a person decided or consented to be injured, abused, or coerced does not change the demeaning nature of such action. Cyberspace has created a platform for the facilitation of crimes such as pornography. Today, websites display obscene material on the internet. It may be duplicated more cheaply and quickly using modern media such as hard disks, floppy disks, and CD-ROMs. According to Section 67-A of the IT Amendment Act 2008, the crime of pornography is defined as anyone who publishes and transmits or causes to be published and transmitted in electronic form any content that comprises sexually explicit acts or conduct.

c) Morphing

Morphing is the act of an unauthorized user changing the original picture. Morphing occurs when an unauthorized user with a fake identity takes a victim's images and then shares or reloads them after altering them. It has been discovered that female images are obtained from websites by fraudulent users and then re-posted/uploaded on multiple websites by creating phony profiles after editing. This constitutes a breach of the IT Act, 2000. The violator can also be charged with criminal trespass under Section 441, committing a public nuisance under Section 290, printing or publishing grossly immoral or scurrilous materials or matter designed to blackmail under Section 292 A, and defamation under Section 501.[21]

d) Cyber Defamation

Cyber crimes, such as harassment and defamation are another widespread online crime against women. Although this can happen to any gender, women are more vulnerable. This occurs when someone uses computers and/or the Internet to publish defamatory information about someone on a website or sends defamatory e-mails to all of that person's acquaintances. Defamation is

[21] R. Agarwal, "Cyber Crime against women and relations in India", available on http://tmu.ac.in/gallery/viewpointsdcip2013/pdf/track4/T-403.pdf, visited on 16st September 2025.

the harm done to a person's reputation in the eyes of a third party. Cyber defamation is the use of computers or the internet to publish defamatory material about an individual.

e) Cyberbullying

Cyberbullying has become an undesirable side effect of greater online involvement and interactions. Cyberbullying behaviour has both short and long-term effects, with considerable and severe emotional and social consequences. These consequences include, but are not limited to social anxiety, depression, aggression, substance misuse, eating disorders, self-harm, suicidal ideation, and, in some circumstances, suicide. Bullying, whether traditional or cyber, causes severe emotional and psychological pain. Cyberbullying is common on the internet, and most young people will encounter or see it at some point.

Today, people all over the world can interact with one another with the push of a button, and technology introduces new threats. Cyberbullying is the deliberate use of information and communication technology (ICT), mainly mobile phones and the internet, to upset someone else. Globally, India ranks third behind China and Singapore in cyberbullying, additionally referred to as online bullying. The number of suicides due to cyberbullying has increased over the last decade.[22]

f) Fraud on Dating Websites

Men on the lookout seek out vulnerable women yearning for love, since they are an easy target. They begin by befriending the female and extracting all of their personal information. There have been numerous reports of women meeting males on dating services only to be raped or, in the worst-case scenario, murdered. Dating websites are a gift to psychopaths. Women are convenient targets for these psychopaths, who pull them into a cruel web in which they fall for them and reveal all of their personal information. Serial killers also frequent the web because they can hide in anonymity and it is difficult to trace them down.

OBJECTIVES

- To study the forms and impact of cybercrimes against women.

[22] D. Halder et al., "The problem of cyber bullying amongst school students in India: The loopholes in IT Act", available on http://www.careerlauncher.com/lstcontent/plansuppliments/attachment, visited on 17st September 2025.

- To examine the adequacy of existing Indian legal frameworks.
- To evaluate judicial pronouncements shaping women's digital rights.
- To analyse the judiciary's role in bridging legislative gaps.
- To identify challenges faced by courts in cybercrime cases.

RESEARCH PROBLEM

Despite the presence of legal provisions under the **IT Act, BNS, and intermediary guidelines**, women in India continue to face alarming levels of **cyberstalking, online harassment, non-consensual image sharing, deepfake abuse, and other gendered cybercrimes**. Existing laws are largely **gender-neutral** and fail to capture the specific harms women encounter in digital spaces. While the **Indian judiciary has stepped in** through progressive interpretations of privacy, dignity, and accountability, courts still face challenges of **jurisdiction, enforcement, technological expertise, and balancing competing rights**. Despite existing cyber laws, women in India continue to face rising online abuse, and the judiciary struggles with legislative gaps, jurisdictional limits, and enforcement challenges in shaping a gender-sensitive cyber jurisprudence.

METHODOLOGY

This study follows a **doctrinal legal research approach**, analysing statutes, judicial pronouncements, and policies on cybercrimes against women. It uses **primary sources** (laws, judgments, government rules) and **secondary sources** (scholarly works, reports), along with **comparative analysis** of global frameworks. Judicial trends are examined through the lens of **constitutional rights and gender justice**, with the scope limited to gender-specific cybercrimes.

LEGAL AND POLICY FRAMEWORK

a) The Information Technology Act, 2000 (It Act)

IT Act 2000 is an act of the Indian Parliament to deal with cybercrime and e-commerce. This is a law that applies to India as well as persons outside India if the crime involves the usage of

a computer with the internet. It provides a legal framework for e-governance which gives recognition to electronic records and digital signatures. This act also describes the penalties for cybercriminals. As per new amendment, section 66 is substituted by Act 10 of 2009 and thus, subsections 66(1) and 66(2) has been removed from the amendment and has been now merged in section 66 itself.[23]

The Information Technology Amendment Act 2008 (IT Act 2008) is a substantial addition to India's Information Technology Act 2000. The Information Technology Amendment Act was passed by the Indian Parliament in October 2008 and came into force a year later. The act is administered by the Indian Computer Emergency Response Team (CERT-In) and corresponds to the Indian Penal Code. The Information Technology Amendment Act has been widely hailed as a progressive step forward in protecting India's cyber infrastructure and citizens. In recent years, the IT Act has also been updated to include provisions for the regulation of intermediaries, penalties for cybercrime and restrictions on certain types of speech. These changes included expanding the definition of cybercrime and adding new penalties for offenses such as identity theft, publishing private images without consent, cheating by impersonation, and sending offensive messages or those containing sexually explicit acts through electronic means.[24]

The IT Act of 2000 was revised twice, first in 2006 and then in 2008, in response to the rise in Cyber crimes.[10] There are several parts of the Information Technology (Amendment) Act of 2008 that regulate Cyber crimes.

a. **Section 66C**- Identity Theft: This law makes it illegal to steal someone's online identity. If someone fraudulently uses another person's electronic signature, password, or unique identification features, they can be punished with up to three years in prison and a fine of up to one lakh rupees.

b. **Section 66E**- Privacy Violation: This section protects a person's privacy online. If someone captures, publishes, or shares images of a private part of someone without their consent and in a way that invades their privacy, they can face up to three years in prison and a fine.

c. **Section 67**-Obscene Content: This section prohibits the publication, sharing, or

[23] The Information Technology Act, 2000.
[24] The Information Technology (Amendment)Act, 2008

transmission of obscene content online. It's similar to the obscenity law in the Indian Penal Code.

d. **Section 67A** - Sexually Explicit Material: This law deals with sexually explicit content online. Sharing such material can lead to imprisonment for up to five years and a fine for the first conviction.

e. **Section 67B** - Child Sexual Content: This section focuses on the publication or sharing of sexually explicit content involving children. It's a serious offense, and those found guilty can face significant penalties.

b) Bharatiya Sakshya Adhiniyam, 2023

The BSA[25] is to consolidate and to provide for general rules and principles of evidence for fair trial. Section 2 of BSA definitions illustration 2(vi) states that an electronic record; (e) "evidence" and sections in BSA 2023 are related to technological crimes such as ,- Section 39. Opinions of experts. Section 40, Facts bearing upon opinions of experts explore the digital evidence to produce in the court of law. Section 45, Opinions of third persons when relevant. Certain cyber crimes may not be explicitly covered under the Information Technology Act, depending on jurisdiction and circumstances. While some aspects may fall under the Bharatiya Nyaya Sanhita, cyber bullying, online scams, cyber stalking, revenge porn, and cyber extortion lack specific provisions in the Information Technology Act 2000/2008. Therefore, it is essential for law enforcement agencies and policymakers to adapt to emerging cyber threats and continually update legislation to address new forms of cybercrime effectively.[26]

c) Digital Personal Data Protection Act, 2023

Personal data is information that relates to an identified or identifiable individual. Businesses as well as government entities process personal data for delivery of goods and services. The Act shall apply to the processing of Personal Data in India, including both online and digitized offline data, and shall further extend to the processing of such data outside India relating to the offering of goods or services in India. As technologies like Artificial Intelligence advance and

[25] Bharatiya Sakshya Adhiniyam, 2023,
[26] Bharatiya Sakshya Adhiniyam, 2023

permeate various aspects of daily lives, the potential for extensive data collection, analysis, and manipulation grows exponentially.[27]

d) National Cyber Crime Reporting Portal

The Indian government launched the National Cyber Crime Reporting Portal as a way to give people a way to report Cyber crimes online. It enables people to report a variety of Cyber crimes, including phishing schemes, identity theft, financial fraud, and online abuse. The goal of this service is to make it simple for law enforcement to report Cyber crimes and to take the necessary action.

e) Cyber Cells And Cyber Crime Investigation Units

Specialized law enforcement units dedicated to the investigation and prosecution of Cyber crimes are known as cyber cells or cyber crime investigation units. These units are usually formed at different levels, including municipal, state, or federal, inside police departments or other law enforcement organizations. Numerous Cyber crimes, including as hacking, virus assaults, online fraud, identity theft, cyberbullying, and other forms of cyber exploitation, are looked into by cyber cells and cybercrime investigation units. All things considered, Cyber Cells and Cyber Crime Investigation Units are essential to tackling the increasing problems brought about by Cyber crimes and guaranteeing the security and safety of people, companies, and vital infrastructure in the digital age.[28]

Role of Indian Judiciary through Judicial Interpretations

The Indian legal system has been modifying and improving its strategy to successfully tackle cyber offences in response to this changing environment. Online harassment, revenge porn, and other digital sexual misconduct cases are being presented to courts more frequently. The judiciary's role is not limited by conventional legal frameworks; it also requires an understanding of complex technological nuances.

- *Tvf Media Labs Pvt Ltd & Ors v. State Govt. Of Nct of Delhi & Anr*,[29] in response to criticism

[27] Digital Personal Data Protection Act, 2023
[28] S. Barman, "Cybercrime Against Women : How Cybercrime Targets Women's Privacy and Security", East Indian Journal of Social Sciences, Vol-VII.
[29] Live Law (Del) 210 (2023).

of the TVF-produced web series *"College Romance,"* Justice Sharma underlined the explicit language's potential harm to impressionable minds as well as its violation of decency standards. After carefully going over several episodes, including the one in question, the court emphasized how important it is to maintain language decorum in a variety of contexts. Concerns focused on how the series' coarse and morally repugnant content went beyond what was considered appropriate. The Court chastised intermediaries and curators of online content for failing to provide warnings about vulgar language in violation of IT Rules of 2021.

- *Priya Patel v. State of Gujarat*[30] which tackles the serious problem of revenge porn and online sexual harassment, is remembered as a turning point in Indian criminal law. Patel, a resident of Gujarat, suffered great mental distress and harassment when her partner's private video was shared among his acquaintances without her permission. She lodged a thorough complaint under several sections of the Indian Penal Code, including the voyeurism-related Section 354C[31], Section 509 (insulting the modesty of a woman), and Section 292 (publication of obscene material). These provisions now find place under the Bharatiya Nyaya Sanhita (BNS), 2023 as Clause 74 (voyeurism), Clause 77 (acts or gestures intended to insult the modesty of a woman), and Clause 354 (obscene acts and materials). The complaint led to the accused's arrest and charging. In an appeal, the Gujarat High Court upheld the convictions and penalties, acknowledging that Patel's rights to privacy, dignity, and autonomy had been violated. The Indian Constitution protects privacy as a fundamental right, and the court emphasized that sharing private photos without permission is a serious violation of that right and is punishable by law. The ruling emphasized how crucial it is to protect people's rights in the age of easy access to personal information on social media.[32] To sum up, the Priya Patel case was not only successful in getting justice for the victim, but it also had a significant impact on how people talked about the larger issue of defending individual rights in the digital age.[33]

- *State of West Bengal v. Animesh Baxi*[34]*:* In the significant case decided by the District Court of West Bengal, the accused hacked into the victim's mobile phone, accessed her private

[30] *Priya Patel v. State of Gujarat* (2017) AIR 2018 SC 385
[31] Indian Penal Code, 1860 (Act 45 of 2000).
[32] Mandal, Arpita, Digital Sexual Harassment: Perceptions, Laws, and Prevention (Manas Publications, New Delhi, 2017).
[33] Ibid.
[34] GR No. 1587 of 2017.

and offensive images, and used them to extort money by threatening to upload the content online. When the victim did not comply, the accused proceeded to publish her intimate images and videos on a pornographic website. The accused were found guilty by the District Court of West Bengal under sections 66C(identity theft) [35] and 66E(violation of privacy) [36] of the IT Act as well as sections 354A(sexual harassment)[37], 354C(voyeurism)[38], 354D(stalking)[39], and 509(insulting the modesty of a woman)[40] of the IPC. The court notably recognized the repeated online exposure as a form of **"virtual rape",** emphasizing that each viewing of the uploaded content constituted a renewed violation of the victim's dignity. The court highlighted that **Section 354D IPC,** which addresses stalking, was particularly applicable due to the persistent and invasive digital harassment. Under the **BNS, 2023,** these offenses would be punishable under **Clause 66** (identity theft), **Clause 73** (violation of privacy), **Clause 74 (**voyeurism), **Clause 75** (cyberstalking), **Clause 76 (**sexual harassment), and **Clause 77** (insulting the modesty of a woman).

- *K. Srinivas Rao v. D.A. Deepa (2013)*[41]*,* the **Madras High Court** recognized **cyberstalking and online harassment as forms of sexual harassment,** holding that such conduct falls within the ambit of Section 354A of the Indian Penal Code[42] which deals with making sexually coloured remarks and other unwelcome physical, verbal, or non-verbal conduct of a sexual nature. The Court acknowledged the **increasing use of technology to harass, threaten, and invade the privacy of women,** especially through persistent digital communication, impersonation, and defamation. It emphasized that the **psychological and reputational harm** inflicted through online platforms can be as grave as physical stalking and must be treated with equal legal seriousness. Although the case preceded the **BNS 2023,** its reasoning remains highly relevant today, with **Clause 74** of the BNS corresponding to offences of sexual harassment.

- *Manish Kathuria v. Ritu Kohli,*[43] It is recognized as **India's first reported case of cyberstalking and cyber-sex crime.** The accused, Manish Kathuria, created fake online

[35] Information Technology Act, 2000 (Act 21 of 2000) s. 66C.
[36] Information Technology Act, 2000 (Act 21 of 2000) s. 66E.
[37] Indian Penal Code, 1860 (Act 45 of 1860) s. 354A.
[38] Indian Penal Code, 1860 (Act 45 of 1860) s. 354C.
[39] Indian Penal Code, 1860 (Act 45 of 1860) s. 354D.
[40] Indian Penal Code, 1860 (Act 45 of 1860) s. 509.
[41] *K. Srinivas Rao v. D.A. Deepa* (2013) AIR 2013 SC 2176
[42] The Indian Penal Code, 1860 (Act 45 of 1860), S. 354A.
[43] C.C. No. 14616/2014

profiles of the victim, Ritu Kohli, on the website *http://www.mirc.com*, through which he published her private and sensitive information and impersonated her while engaging in vulgar and sexually explicit chats. This led to the real Ritu Kohli receiving repeated harassing phone calls from strangers across India and abroad. The accused's actions constituted a serious violation of the victim's privacy, dignity, and personal safety in the virtual domain. The case was filed under **Section 509 of the Indian Penal Code, 1860,** which punishes words, gestures, or acts intended to insult the modesty of a woman. Though cyber-specific provisions under the **IT Act, 2000** were not invoked at that time due to the novelty of the crime, this case later played a pivotal role in shaping India's cyber laws. Under the **BNS 2023,** such conduct would be addressed under **Clause 77** (insulting the modesty of a woman), **Clause 75** (cyberstalking), and **Clause 73** (violation of privacy, if applicable).

- *State of Tamil Nadu v Suhas Kutti,*[44] is a landmark case and India's **first conviction for cyberpornography,** notable for resulting in the accused's conviction within just seven months of the FIR being filed. The case involved **online defamation and sexual harassment,** where defamatory and obscene remarks and morphed images of a divorced woman were posted in a Yahoo Messenger group. As a result, the victim received numerous harassing calls from strangers soliciting sexual services. A charge sheet was subsequently filed under Section 67[45] of the IT Act, 2000, which outlines the penalties for disseminating or distributing pornographic material in electronic form, as well as Sections 509 (insulting the modesty of a woman) and 469 (forgery for the purpose of harming reputation)[46] of the Indian Penal Code, 1860, the latter of which outlines forgery with the intent to cause reputational harm. These provisions would now correspond to **Clause 198(2)** of **BNS 2023** (publication/transmission of obscene electronic content), **Clause 77** (insulting the modesty of a woman), and **Clause 336** (forgery with intent to harm reputation). This case set a precedent for **swift judicial action in cybercrime matters** and highlighted the growing threat of online sexual exploitation and reputational harm through digital platforms.

- In *Avinash Bajaj v State of Delhi,*[47] arose from the infamous Delhi Public School MMS scandal, in which an obscene video clip involving minors was listed for sale on the e-

[44] C No. 4680 of 2004.
[45] Information Technology Act, 2000 (Act 21 of 2000) s. 67.
[46] Indian Penal Code, 1860 (Act 45 of 1860) s. 469.
[47] (2008) 105 DRJ 721: (2008) 150 DLT 769,

commerce platform **bazee.com.** Although Avinash Bajaj, the CEO of the platform, neither uploaded nor directly facilitated the sale of the clip, he was arrested under **Section 292 of the IPC, 1860** (now replaced by **Section 78 of the BNS, 2023** dealing with obscenity), as well as provisions of the **Information Technology Act, 2000**. His arrest was carried out under the **CrPC**[48] which has now been replaced by the **BNSS, 2023.** The legal issue was whether an **intermediary** a digital platform merely hosting third-party content could be held **criminally liable** in the absence of direct involvement or **mens rea** (guilty mind), which remains a crucial element for criminal liability under both the **BNS** framework. The Delhi High Court held that **criminal intent must be established** before imposing liability, and that platform operators cannot be equated with the content creators. The judgment laid the groundwork for the **2008 amendment** to the IT Act, which introduced **Section 79 (Safe Harbour provision),** shielding intermediaries from liability if they exercised due diligence and acted on takedown requests.

THE CHALLENGES OF INDIAN JUDICIARY IN CYBER CRIME AGAINST WOMEN

The old criminal justice system presented several difficulties for the Indian judiciary in cyberspace. Researcher analysed the main obstacles Indian judges encountered in reducing cybercrime against women, and they are as follows-

- **Digital Evidentiary Challenges**-

Under the previous legal regime, Section 65B of the Indian Evidence Act, 1872, mandated a certificate of authenticity for electronic records to be admissible in court. However, this created significant hurdles, particularly in cases involving foreign service providers like Google or Meta, who often refuse to issue such certificates, resulting in crucial evidence being rejected. Recognizing these challenges, the newly enacted BSA[49] has reformed the evidentiary framework. Section 61 of the BSA, which corresponds to the old Section 65B, allows for the admissibility of electronic records without a certificate in certain circumstances, such as when the party seeking the evidence is not in possession of the device or cannot reasonably procure the certificate. This marks a crucial step forward in addressing digital evidentiary issues.

[48] Code of Criminal Procedure, 1973
[49] Bharatiya Sakshya Adhiniyam, 2023

Further, the BNS[50], which replaces the IPC, incorporates specific provisions for cyber offences. Sections 67 to 69 of the BNS deal with offences such as identity theft, cyber fraud, and electronic transmission of obscene content, underscoring the need for reliable digital evidence in such prosecutions. Procedurally, the BNSS[51] introduces several tech-friendly mechanisms, including provisions for electronic documentation, video recording of search and seizure (Section 176), and digital communication of summons and warrants (Section 356).

- **Decision-making authority**-

The key area of difficulty for the judiciary when dealing with cybercrimes is jurisdiction. Cyber crime is essentially a global crime. The criminal justice system has a particularly difficult decision when deciding jurisdiction for a specific crime of this nature. The United Nations has also cited jurisdiction as a significant concern in cybercrime.[52] Even the Indian government has acknowledged that one of the biggest challenges facing the judiciary is determining jurisdiction in cyber crimes. The government has been ordered by the Supreme Court to establish a common reporting system for cyber crime in this type of situation.

- **Lack of explicit provision**-

There is currently **no explicit legal provision under Indian law that specifically safeguards private rights in the online sphere**, particularly in the context of personal data misuse, privacy violations, and emerging forms of cyber abuse. Women who fall victim to online crimes are primarily protected through the **Information Technology Act, 2000** which though amended in 2008 to address certain cyber offences, still **fails to comprehensively cover the evolving nature of cybercrimes,** such as deepfakes, cyber flashing, doxxing, and AI-generated non-consensual content. This legislative gap poses significant challenges for the judiciary during cybercrime trials, especially when interpreting outdated provisions in the face of rapidly advancing technology.

- **Operational issues**-

[50] Bharatiya Nyaya Sanhita, 2023.
[51] Bharatiya Nagarik Suraksha Sanhita, 2023.
[52] A. Saqf El Hait, "Jurisdiction in Cybercrimes: A Comparative Study", Journal of Law, Policy and Globalization, *available at:* https://core.ac.uk/download/pdf/234649797.pdf. (Last Accessed September 14, 2025).

One of the key **operational challenges in cyber crime investigation** in India stems from **Section 78 of the IT Act**[53]**,** which mandates that only **police officers of the rank of Inspector or above** are authorized to investigate offences under the Act. While intended to maintain investigative integrity, this provision has created **serious practical difficulties,** especially in states and districts with limited availability of qualified officers. This results in **delays in the initiation and progress of cybercrime investigations,** indirectly contributing to the **slow pace of judicial proceedings** and undermining the goal of **timely trials,** as envisioned under Article 21 of the Constitution. Furthermore, **lack of jurisdictional control over the Internet** complicates enforcement.

- **Lack of technical equipment and skilled human resources**-

A critical challenge facing the Indian judiciary in the effective adjudication of cybercrime cases is the **lack of technological infrastructure, skilled personnel, and digital forensic tools.** Courts, especially at the lower levels, often operate without access to advanced **cyber forensic laboratories, case management systems, or trained technical staff,** which significantly delays case processing and weakens evidentiary scrutiny. This shortage of **technologically adept legal professionals and investigators** directly affects the quality and speed of judicial proceedings in cyber-related offences. The Indian Parliament also proposed a nodal agency for cybercrime in 2017 and addressed the issue of training personnel who deal with it.[54]

- **Gap between Technology and Knowledge**-

One of the most pressing challenges in addressing cybercrime in India is the growing disconnect between rapid technological advancements and the conventional framework of the criminal justice system. Although certain cyber offences are now codified under the **BNS**[55] for example, **Section 67** penalizes cyber fraud and identity theft, and **Section 69** deals with publishing or transmitting obscene material electronically many emerging threats such as deepfakes, AI-generated content misuse, and cryptocurrency scams still operate in legal grey areas. Earlier, similar offences were prosecuted under the **IPC**[56] through provisions like **Sections 419 and 420** (cheating and impersonation), but these sections were not designed for

[53] Information Technology Act, 2000.
[54] A.S. Anand, "Judicial Review- Judicial Activism- Need for Caution", Journal of Indian Law Institute, available *at:* https://www.jstor.org/stable/43953808 (Last Accessed September 16, 2025).
[55]Bharatiya Nyaya Sanhita, 2023
[56] Indian Penal Code, 1860

the digital domain. The **IT Act**[57] attempted to address this gap through provisions such as **Section 66C**, **66D**, and **67A** (publishing sexually explicit material), yet it remains limited in scope for handling modern cyber offences like blockchain fraud or AI-enabled crimes. Moreover, procedural enforcement is further weakened by the absence of uniform **SOPs**[58] and the complexities of cross-border data access. The **BNSS**[59] provides updated guidelines on digital evidence handling, yet many judicial officers and investigators struggle with practical implementation during cybercrime trials.

CONCLUSION

The involvement of judiciary in combating crime against women in cyberspace is critical, both in India and overseas. The Indian judiciary is crucial in interpreting and enforcing the legal framework governing cyber harassment. Courts must guarantee that current statutes are enforced properly to meet the complexities of online sexual harassment. The legal system has to guarantee that victims of online sexual harassment receive legal protection. Restraining orders, anonymity protection, and other procedures to protect victims during judicial processes are included. The court may help raise awareness and educate people about cyberbullying by including conversations about it in legal training programmes. This enhances the entire reaction to such instances by assisting legal practitioners in understanding the complexity of internet crimes. Internationally, the courts can help to establish universal guidelines for dealing with sexual harassment on the internet. Precedents set by renowned legal systems can serve as examples for other countries, encouraging a unified approach to the subject. Courts should prioritise human rights protection, ensuring that legal remedies to online assault strike an equilibrium between avoiding abuse and safeguarding fundamental rights like the freedom of speech and confidentiality. International legal bodies and forums can be used to combat cyberbullying on a larger scale. Collaboration through forums such as the United Nations can result in the establishment of global initiatives to tackle sexual harassment on the internet. Finally, the judiciary is critical in defining the legal context for dealing with cyber crime against women in online.

[57] The Information Technology Act, 2000 (amended in 2008)
[58] Standard Operating Procedures
[59] Bharatiya Nagarik Suraksha Sanhita, 2023