INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 2 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

NAVIGATING THE 'FIFTH DOMAIN': THE EFFICACY OF THE INDIAN PENAL CODE IN PROSECUTING CYBERCRIMES AGAINST WOMEN

AUTHOR - AALIYA KHATOON* & DR. JYOTSNA SINGH**

* LLM. (CRIMINAL LAW) STUDENT AT AMITY LAW SCHOOL, AMITY UNIVERSITY UTTAR PRADESH, LUCKNOW CAMPUS

** ASSISTANT PROFESSOR AT AMITY LAW SCHOOL, AMITY UNIVERSITY UTTAR PRADESH, LUCKNOW CAMPUS

BEST CITATION - AALIYA KHATOON & DR. JYOTSNA SINGH, NAVIGATING THE 'FIFTH DOMAIN': THE EFFICACY OF THE INDIAN PENAL CODE IN PROSECUTING CYBERCRIMES AGAINST WOMEN, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (2) OF 2026, PG. 395-402, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

The rapid integration of digital spaces into daily life has precipitated a paradigm shift in gender-based violence, shifting these offenses into the "fifth domain" of cyberspace. Despite the Information Technology Act, 2000 (IT Act) serving as the *lex specialis* for electronic governance, the substantive burden of prosecuting digital crimes against women such as online sexual harassment, cyber stalking, and the non-consensual dissemination of intimate imagery (NCII) continues to fall heavily upon the Indian Penal Code, 1860 (IPC). This research paper critically examines the doctrinal, procedural, and sociological efficacy of specific IPC provisions, namely Sections 354A, 354D, 292, 499, 509, and 366A, in addressing modern digital crimes. Supported by National Crime Records Bureau (NCRB) 2022 data, the analysis explores how the Indian judiciary has progressively re-interpreted Victorian-era concepts of "modesty," "privacy," and physical "presence" to protect the virtual body of the female victim. Furthermore, the paper juxtaposes these IPC sections with complementary IT Act provisions and landmark judgments (such as *Avnish Bajaj* and *X v. Union of India*) to highlight the evolving landscape of intermediary liability and digital defamation. Ultimately, the study concludes that while substantive laws have been judicially adapted to recognize virtual harm, a significant "justice gap" remains. The promise of digital safety is severely stifled by procedural bottlenecks, most notably the extraterritorial acquisition of digital evidence under Section 91 of the CrPC, cross-border jurisdictional disputes, and severe delays in the Mutual Legal Assistance Treaty (MLAT) process.

Keywords: Cybercrimes against Women, Indian Penal Code (IPC), Digital Jurisprudence, Intermediary Liability, Cyber Stalking.

.1 Introduction: The Digital Extension of Penal Jurisprudence

The integration of digital spaces into the fabric of daily life has precipitated a paradigm shift in the nature of gender-based violence, necessitating a rigorous re-evaluation of traditional penal statutes. This Research paper, titled 'Specific Cyber Offences against Women under IPC', constitutes a critical component of the dissertation, aiming to dissect the doctrinal, procedural, and sociological efficacy of the Indian Penal Code, 1860 (IPC) in addressing crimes that occur in the 'fifth domain' of cyberspace. While the Information Technology Act, 2000 (IT Act) serves as the *lex specialis* for electronic commerce and governance, the substantive burden of prosecuting gendered violence ranging from virtual stalking to the non-consensual dissemination of intimate imagery (NCII) continues to fall heavily upon the IPC. This reliance on a Victorian-era statute to

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 2 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

adjudicate modern digital crimes creates a complex jurisprudential landscape where concepts of "modesty," "privacy," and "presence" must be re-interpreted to encompass the virtual body of the female victim.

The analysis within this research paper proceeds through a structured examination of Sections 354A, 354D, 292, 499, 509, and 366A of the IPC, juxtaposed against complementary provisions like Section 67A of the IT Act. It further scrutinizes the procedural bottlenecks inherent in Section 91 of the Code of Criminal Procedure (CrPC), 1973, particularly regarding the extraterritorial acquisition of digital evidence. The discourse is empirically supported by data from the National Crime Records Bureau (NCRB) *Crime in India 2022* report, which highlights a persistent rise in cybercrimes against women, revealing a schism between legislative intent and enforcement reality.[985]

1.2 Sexual Harassment and the Virtual 'Touch': Section 354A IPC

1.2.1 Legislative Genesis and the 'Virtual' *Actus Reus*

The insertion of Section 354A into the IPC via the Criminal Law (Amendment) Act, 2013, was a direct legislative response to the recommendations of the Justice Verma Committee, which sought to expand the definition of sexual offences beyond physical rape. Section 354A(1) criminalizes four distinct acts: (i) physical contact and advances involving unwelcome and explicit sexual overtures; (ii) a demand or request for sexual favors; (iii) showing pornography against the will of a woman; and (iv) making sexually coloured remarks.[986]

In the digital realm, the *actus reus* of "physical contact" is absent, yet the violation of dignity remains profound. Courts have increasingly interpreted the transmission of unsolicited sexual messages, images (cyber-flashing), or videos as satisfying the ingredients of clauses (ii), (iii), and (iv). The "virtual touch" is recognized as an intrusion into the woman's digital personal space, which jurisprudence now treats as an extension of her physical personhood. The offense is cognizable, bailable, and triable by any Magistrate, punishable with imprisonment extending to three years.[987]

1.2.2 The 'Unwelcome' Standard in Social Media

A critical element of Section 354A is that the act must be "unwelcome." In the physical world, rejection can be conveyed through verbal refusal or body language. In the digital sphere, the architecture of social media platforms designed for connectivity complicates this standard. Friend requests, 'likes', and comments can be ambiguous. However, judicial trends indicate that the moment a victim utilizes a "block" feature or leaves a conversation, any subsequent attempt to communicate sexual content fulfils the "unwelcome" criteria.

The interplay with Section 67 of the IT Act is notable here. While Section 354A IPC focuses on the harassment aspect (the effect on the victim), Section 67 IT Act focuses on the obscenity of the material itself.[988] Law enforcement agencies often invoke both sections to ensure a more robust charge sheet, particularly when the harassment involves "sexting" or the transmission of pornography.

1.2.3 Statistical Trends and Reporting Barriers

Despite the broad ambit of Section 354A, NCRB data suggests that online sexual harassment is often under-reported or aggregated under general "harassment" categories unless accompanied by more severe offences like blackmail. The 2022 data indicates a rise in cases where Section 354A is added as a secondary charge in cyber stalking FIRs, reflecting the intersecting nature of digital abuse where harassment serves as a precursor to stalking or defamation.[989]

[985] National Crime Records Bureau, *Crime in India 2022: Statistics Volume I*, Ministry of Home Affairs, Government of India (2023).
[986] The Indian Penal Code, 1860, s. 354A.
[987] *Id.*, s. 354A(1).
[988] The Information Technology Act, 2000, s. 67.
[989] National Crime Records Bureau, *supra* note 1.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 2 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

1.3 The Panopticon of Cyber Stalking: Section 354D IPC

1.3.1 Doctrinal Analysis of Section 354D

Section 354D, also introduced in 2013, represents one of the most significant modernizations of the IPC. It criminalizes stalking in two forms: physical following (Subsection 1(i)) and electronic monitoring (Subsection 1(ii)). The latter is defined as the act of a man who "monitors the use by a woman of the internet, email or any other form of electronic communication."[990]

This provision establishes a lower evidentiary threshold for cyber stalking compared to physical stalking. While physical stalking requires a "clear indication of disinterest" by the woman, the electronic monitoring clause (Subsection 1(ii)) does not explicitly require such a prior rejection in the statutory text, implying that the act of covert surveillance itself is criminal. This reflects the legislative understanding that virtual surveillance spyware, unauthorized access to emails, tracking via GPS violates the fundamental right to privacy and creates an environment of ubiquitous fear.

1.3.2 Judicial Interpretation: *State of Tamil Nadu v. Suhas Katti*

Although *Suhas Katti* (2004) predates Section 354D, it laid the groundwork for cyber stalking jurisprudence under the IT Act. The conviction was based on the harassment of a woman via a Yahoo Message Group. In the post-2013 era, courts have utilized Section 354D to prosecute diverse behaviors, including repeated contact from multiple accounts after being blocked, doxing, and proxy stalking.[991]

The NCRB 2022 data reveals that Section 354D is one of the most frequently invoked sections for cybercrimes against women, reflecting the pervasive nature of this offence.

Table 1.1: High Incidence States for Cyber Stalking (NCRB 2022)

State/City	Stalking Cases (Sec 354D)	Rate (Per Lakh Women)	Sociological Context
Maharashtra	High Registration Volume	4.4	High internet density in Mumbai/Pune correlates with increased reporting.
Telangana	2,341 (Total Cyber Cases)	4.1	Hyderabad reported a rate of 11.1, the highest among metros.[992]
Andhra Pradesh	1,100+ Cases	4.1	Significant rise in stalking complaints linked to social media monitoring.
National Trend	10,495 Total Cases	1.6 (Avg)	A consistent year-on-year increase suggests normalization of digital surveillance.

[990] The Indian Penal Code, 1860, s. 354D(1)(ii).

[991] *State of Tamil Nadu v. Suhas Katti*, CC No. 4680 of 2004 (Addl. CMM, Egmore).

[992] National Crime Records Bureau, *supra* note 1 at Table 9A.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 2 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

1.3.3 The Challenge of Anonymity and Jurisdiction

The primary investigative hurdle in Section 354D cases is the "anonymity" of the perpetrator. Unlike physical stalking where the offender is visible, cyber stalking often involves VPNs, Tor browsers, or fake profiles. This necessitates the invocation of Section 91 CrPC to obtain user details from intermediaries. The "fear of violence" clause in Section 354D(2) is also contentious; defense counsels often argue that "virtual" threats do not constitute "real" violence, although courts are increasingly recognizing psychological trauma as sufficient "harm".

1.4 Obscenity, NCII, and Deepfakes: Section 292 IPC and Section 67A IT Act

1.4.1 The Jurisprudential Conflict: IPC vs. IT Act

The prosecution of Non-Consensual Intimate Imagery (NCII), colloquially termed "revenge porn," involves a complex interplay between Section 292 IPC (Sale/distribution of obscene books, etc.) and Sections 67/67A of the IT Act (Publishing/transmitting obscene/sexually explicit material).

- **Section 292 IPC:** Criminalizes the sale, hire, distribution, or public exhibition of "obscene" objects. It was drafted for tangible media.[993]
- **Section 67A IT Act:** Specifically targets the *act* of transmission in electronic form. It prescribes a harsher punishment (up to 5 years for first conviction) compared to Section 292 (up to 2 years).[994]

In *Sharat Babu Digumarti v. Govt. of NCT of Delhi*, the Supreme Court held that when an offence involves electronic transmission, the IT Act (special law) should prevail over the IPC (general law) to avoid double jeopardy. However, in practice, FIRs for NCII routinely cite Section 292 IPC alongside Section 67A IT Act to preclude the accused from claiming the benefits of the lighter provisions of either statute during bail hearings.

1.4.2 Case Analysis: *Avnish Bajaj v. State (NCT of Delhi)*

The *Avnish Bajaj* case (Bazee.com case) is foundational to understanding intermediary liability in obscenity cases.

- **Facts:** An obscene MMS clip was listed for sale on Baazee.com. The site's CEO, Avnish Bajaj, was charged under Section 292 IPC and Section 67 IT Act.
- **Ratio:** The court held that the strict concept of "automatic criminal liability" does not attach to a Director of a company under the IPC unless there is specific proof of active participation or criminal intent (*mens rea*).[995]
- **Impact:** This judgment necessitated the "Safe Harbour" provisions under Section 79 of the IT Act, protecting intermediaries from liability for third-party content, *provided* they observe due diligence.

1.4.3 Case Analysis: *X v. Union of India* (2021)

If *Avnish Bajaj* protected the intermediary, *X v. Union of India* re-centered the rights of the victim.

- **Facts:** The petitioner's intimate photos were uploaded to a pornographic site. Despite court orders to remove specific URLs, the content reappeared on other links.
- **Judgment:** The Delhi High Court held that intermediaries cannot merely be "passive" recipients of specific URL takedown requests in NCII cases. They must employ automated tools to identify and remove *copies* of the content globally across their platforms.[996]
- **Significance:** The court explicitly stated that failure to remove such content within 24 hours would strip the

[993] The Indian Penal Code, 1860, s. 292.
[994] The Information Technology Act, 2000, s. 67A.
[995] *Avnish Bajaj v. State (NCT of Delhi)*, (2008) 150 DLT 769.
[996] *X v. Union of India*, W.P.(Crl) 1082/2020 (Del. HC 2021).

intermediary of its Section 79 immunity, exposing it to liability under Section 292 IPC and Section 67A IT Act.

1.4.4 Deepfakes and the Lacuna in Law

The rise of Deepfake technology presents a novel challenge to Section 292. A purposive interpretation of Section 67A IT Act ("material containing sexually explicit act") covers deepfakes because the harm lies in the *depiction* and the reputational destruction. Section 66E IT Act (Violation of Privacy) is also pertinent here, as deepfakes violate the privacy of the victim's identity.[997] Yet, the lack of a specific "Deepfake" provision in the IPC often forces police to rely on Section 500 (Defamation) or Section 509 (Insult to Modesty).

1.5 Digital Defamation and Insult to Modesty: Sections 499 & 509 IPC

1.5.1 Section 509: Intruding upon 'Digital Privacy'

Section 509 IPC penalizes words, gestures, or acts intended to "insult the modesty of a woman" or "intrude upon her privacy."[998] Historically used for "eve-teasing," this section has found robust application in cyberspace. Courts have interpreted "privacy" in Section 509 to extend to a woman's virtual spaces her email inbox, her social media timeline, and her direct messages. Sending abusive or sexually suggestive text messages constitutes an intrusion upon her privacy and an insult to her modesty.

1.5.2 Section 499: The Mechanics of Cyber Defamation

Section 499 IPC (Defamation) criminalizes imputations that harm a person's reputation.[999] The "publication" requirement is instantaneously satisfied in cyber defamation due to the global reach of the internet.

- **Fake Profiles:** A prevalent *modus operandi* recorded in NCRB 2022 is the creation of fake profiles to post defamatory content or solicit sexual services in the victim's name.
- **Permanence of Harm:** Unlike spoken defamation (slander), cyber defamation is permanent and searchable. In *S.V. Shekar v. State* (2018), the Madras High Court noted that "forwarding" or "sharing" a defamatory post amounts to a new publication, making the user liable under Section 500/509 IPC.[1000]

Table 1.2: NCRB 2022 Data on Reputational Cyber Crimes

Offence Category	Relevant Sections	Trends
Fake Profiles	Sec 419 IPC / Sec 66D IT Act	High incidence in metropolitan cities; used for social engineering and revenge.
Cyber Blackmailing	Sec 384/503 IPC	Significant increase in cases linked to NCII threats.
Insult to Modesty	Sec 509 IPC	Frequently invoked for online trolling; often coupled with Section 354A.[1001]

1.6 Cyber Grooming and Section 366A IPC: A Doctrinal Stretch?

1.6.1 The Gap in Indian Law regarding 'Grooming'

Unlike Western jurisdictions, India lacks a specific "Cyber Grooming" statute. Grooming involves the methodical process of building trust with a child to facilitate sexual abuse. In the absence of a dedicated law, law enforcement relies on a patchwork of POCSO provisions and Section 366A IPC.

[997] The Information Technology Act, 2000, s. 66E.
[998] The Indian Penal Code, 1860, s. 509.
[999] The Indian Penal Code, 1860, s. 499.
[1000] *S.V. Shekar v. State*, Crl. O.P. No. 13833 of 2018 (Mad. HC).
[1001] National Crime Records Bureau, *supra* note 1.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 2 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

1.6.2 Interpreting Section 366A: 'Procuration of Minor Girl'

Section 366A criminalizes inducing a minor girl to "go from any place" or "do any act" with the intent that she may be forced or seduced to illicit intercourse.[1002]

- **The 'Mobility' Challenge:** The phrase "go from any place" traditionally implied physical movement. However, in cyber grooming, the victim may not leave her house immediately. Legal scholars argue that the "act" of turning on a webcam for sexual purposes or sending nude images constitutes "doing any act" under Section 366A, induced by the perpetrator.
- **The Gender Limitation:** Section 366A applies only to minor *girls*. This leaves a significant lacuna for the grooming of minor boys.

1.6.3 Section 67B IT Act as a Complement

Section 67B of the IT Act is more robust for digital crimes, punishing the "cultivating, enticing or inducing" of children for online sexual acts.[1003] It is gender-neutral and specifically targets the creation of CSAM. Consequently, effective prosecution often requires charging the accused under both Section 366A IPC (for the intent to seduce/procure) and Section 67B IT Act (for the digital act of grooming), creating a cumulative liability that reflects the severity of the crime.

1.7 Evidentiary Challenges and Section 91 CrPC: The Procedural Choke-point

The substantive provisions of the IPC (354D, 292, 509) are rendered toothless without the procedural machinery to harvest evidence from the digital domain. This machinery is primarily Section 91 of the CrPC, which empowers courts and police officers to summon documents or "things" necessary for investigation.[1004]

1.7.1 The Mechanism of Section 91 in Digital Investigations

In a typical cyber harassment or NCII case, the identity of the accused is hidden behind a digital veil (IP address). The Investigating Officer (IO) issues a notice under Section 91 CrPC to the intermediary to produce Basic Subscriber Information (BSI) and Access Logs with timestamps.

1.7.2 The Extraterritoriality and MLAT Bottleneck

A critical impediment is that major intermediaries are incorporated in the United States and store data on foreign servers. When served with a Section 91 notice, these entities often refuse compliance for "content" data (messages, posts), citing the U.S. Electronic Communications Privacy Act (ECPA). They direct Indian agencies to the Mutual Legal Assistance Treaty (MLAT) process. The delay in the MLAT process, often taking 18 to 24 months, acts as a significant barrier to justice for victims of active stalking or ongoing NCII dissemination.

1.7.3 Intermediary Liability and the *WhatsApp v. Union of India* Debate

The IT Rules 2021 attempted to bypass this by mandating the appointment of Chief Compliance Officers in India and requiring the "traceability" of the first originator of mischievous information. This has been challenged in *WhatsApp v. Union of India*, where the platform argues that breaking end-to-end encryption to comply with Section 91/IT Rules violates the fundamental right to privacy.[1005]

1.7.4 Admissibility: The *Arjun Panditrao* Certification

Even if the data is obtained via Section 91, its admissibility is governed by Section 65B of the Indian Evidence Act. The Supreme Court in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* conclusively held that a certificate under Section 65B(4) is mandatory for the

[1002] The Indian Penal Code, 1860, s. 366A.
[1003] The Information Technology Act, 2000, s. 67B.
[1004] The Code of Criminal Procedure, 1973, s. 91.
[1005] *WhatsApp LLC v. Union of India*, W.P.(C) 7281/2021 (Del. HC).

admissibility of electronic records.[1006] Foreign intermediaries often provide the data but fail to provide a certificate that aligns with Indian legal formats, creating a procedural technicality that can lead to acquittals.

1.8 Conclusion

The analysis of Specific Cyber Offences against Women under the IPC reveals a legal system in transition. While Sections 354D, 354A, and 509 have been adapted by the judiciary to criminalize digital violence, the "justice gap" remains significant. The NCRB 2022 statistics paint a picture of rising crime rates, particularly in urban tech-hubs like Telangana and Maharashtra, yet the conviction rates are stifled by procedural archaisms. The *X v. Union of India* judgment offers a beacon of hope, shifting the burden of "digital hygiene" onto intermediaries. However, the efficacy of the IPC provisions is ultimately contingent on the speed of evidence acquisition. As long as Section 91 CrPC remains entangled in cross-border jurisdictional disputes and MLAT delays, the promise of "digital safety" for women will remain elusive.

BIBLIOGRAPHY

Statutes, Acts, and Rules (Primary Sources)

- **Code of Criminal Procedure, 1973 (CrPC)** (Specifically Section 91).
- **Criminal Law (Amendment) Act, 2013**.
- **Indian Evidence Act** (Specifically Section 65B).
- **Indian Penal Code, 1860 (IPC)** (Specifically Sections 292, 354A, 354D, 366A, 384, 419, 499, 500, 503, and 509).
- **Information Technology Act, 2000 (IT Act)** (Specifically Sections 66D, 66E, 67, 67A, 67B, and 79).
- **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**.
- **Protection of Children from Sexual Offences (POCSO) Act**.

Judicial Pronouncements (Cases)

- ***Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*** (Supreme Court of India) – Landmark case on the admissibility of electronic records and Section 65B(4) certification.
- ***Avnish Bajaj v. State (NCT of Delhi)*** (Bazee.com Case) – Foundational case regarding intermediary liability and the requirement of *mens rea* for company directors.
- ***S.V. Shekar v. State* (2018)** (Madras High Court) – Case establishing that forwarding or sharing a defamatory post constitutes a new publication under Section 500/509 IPC.
- ***Sharat Babu Digumarti v. Govt. of NCT of Delhi*** (Supreme Court of India) – Ruling on the prevailing nature of the IT Act (special law) over the IPC (general law) in electronic transmission offenses to avoid double jeopardy.
- ***State of Tamil Nadu v. Suhas Katti* (2004)** – Early case laying the groundwork for cyber stalking jurisprudence under the IT Act via harassment on a Yahoo Message Group.
- ***WhatsApp v. Union of India*** – Challenge regarding the IT Rules 2021, traceability of the first originator, and the fundamental right to privacy.
- ***X v. Union of India* (2021)** (Delhi High Court) – Judgment enforcing proactive intermediary liability to globally remove copies of Non-Consensual Intimate Imagery (NCII) across platforms within 24 hours.

Reports and Committees

- **Justice Verma Committee Report** – Recommended the expansion of the definition of sexual offenses beyond

[1006] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

physical rape, leading to the insertion of Section 354A into the IPC.

- **National Crime Records Bureau (NCRB) *Crime in India 2022* Report** – Provided empirical data on cybercrimes against women, high incidence states for cyber stalking (such as Maharashtra, Telangana, and Andhra Pradesh), and reputational cybercrimes.

International Instruments and Foreign Laws

- **Mutual Legal Assistance Treaty (MLAT)** – Process for the extraterritorial acquisition of digital evidence.
- **U.S. Electronic Communications Privacy Act (ECPA)** – Cited by US-based intermediaries to refuse compliance with Section 91 CrPC notices for "content" data.