INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

VOLUME 3 ISSUE 1

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJLAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

CYBER CRIME IN INDIA: EMERGING LEGAL CHALLENGES AND PREVENTIVE POLICIES

AUTHORED BY - GARIMA[1] & KAMALJEET KAUR[2]

ABSTRACT

Cyber-crime against women in India reflects a continuation of gendered harm that has adapted to digital environments rather than emerging as a wholly new category of offending. The spread of smartphones, social media, and digital payments has expanded opportunities for education, mobility, and participation, yet the same technologies have intensified exposure to harassment, stalking, impersonation, image-based abuse, extortion, and reputational injury. The legal framework spans the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, and the Digital Personal Data Protection Act, 2023. These statutes collectively address obscenity, privacy violations, identity theft, sexual offences, evidentiary standards, and data rights, shaping an evolving doctrinal environment that recognizes electronic communication and digital records as central to contemporary harm. Despite legislative and judicial advances, operational deficits persist; reporting remains partial, investigations face technical and jurisdictional barriers, and intermediaries' responses vary in quality and timeliness. Emerging threats such as deepfake-based abuse and digital-arrest scams show how offenders adapt to new technologies faster than institutional systems respond. The article demonstrates the need for coordinated procedures, survivor-centred mechanisms, platform accountability, and capacity-building in digital forensics to create a coherent framework that protects women's rights and strengthens the pursuit of justice in digital spaces.

[1] Student of LL.M, Student ID: 25072001048, University School of Law, Rayat Bahra University, Punjab, India
[2] Assistant Professor, University School of Law, Rayat Bahra University, Punjab, India.

1. INTRODUCTION

The quick adoption of smartphones, affordable data packages, and state-led digitalization initiatives have transformed daily life in India into a densely networked environment where communication, financial transactions, education, healthcare, and even intimate relationships are increasingly going through apps and platforms. The very processes that make real-time payments through UPI, remote work, and social media interaction possible also increase the area where malicious actors can operate. Cyber offences in India have evolved significantly from the early pictures of isolated hackers to a complex ecosystem of fraudsters, extortionists, organized criminal syndicates, and ordinary individuals who use digital tools to perpetrate harassment, discrimination, and sexualized harm. According to NCRB's "Crime in India 2023" data, 86,420 cases of cyber-crimes were registered, with cyber-crime rates increasing from 4.8 to 6.2 per lakh population. A large share of these crimes are related to fraud, identity theft, and online sexual exploitation, thus pointing to both the extent and the variety of these offences.[3]

Women, children, queer persons, religious and caste minorities are the groups that most probably find digital spaces as the places where their existing inequalities and the patriarchal power relations get reproduced in a new way. Cyber-crime should not be handled as a neutral technological phenomenon; it has to be recognized as being deeply dependent on structural hierarchies that determine which people are most likely to be targeted, whose complaints will be trusted, and how the criminal process will respond in reality.[4]

Against such a background, non-consensual intimate imagery (NCII) has emerged as a deeply disturbing category of cybercrimes in India. It comprises the so-called "revenge porn" scenarios where an ex-partner posts intimate pictures, deepfake pornography where AI tools generate sexualized images, or secret recording and forced sharing of sexual activities, most times, accompanied by threats of exposure, acid attacks, or further violence. In 2025, the Ministry of Electronics and Information Technology released a specialized "Standard Operating Procedure

[3] Electronic Evidence, https://cdnbbsr.s3waas.gov.in/s3ec01a0ba2648acd23dc7a5829968ce53/uploads/2024/12/2024122766.pdf (last visited on December 11, 2025).

[4] Technology-Facilitated Gender-Based Violence in Asia: India, https://www.icrw.org/wp-content/uploads/2021/09/USAID-TFGBV-India.pdf (last visited on December 10, 2025).

to curtail dissemination of Non-Consensual Intimate Imagery (NCII) content" under the "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021", which directs social media intermediaries and other platforms to remove NCII within 24 hours of a complaint and to run multi-channel, victim-centric reporting mechanisms. This paper critically examines the legal challenges in regulating cyber crime in India and evaluates the effectiveness of existing preventive policy mechanisms.

2. RESEARCH PROBLEM AND OBJECTIVES

Research Problem

The central problem addressed in this study is the difference between rapidly evolving online harms and the capacity, coordination, and victim-centered safeguards at the ground level that are required to be able to prevent, remove, investigate, and prosecute these crimes while at the same time granting the basic rights.

Objectives of the Study

The Objectives of the research are:

1. To map emerging patterns of cybercrime in India with a focused lens on gendered harms and non-consensual intimate imagery.
2. To evaluate the real-world effectiveness of platform processes, helplines, portals, and survivor services for prompt relief and long-term removal.
3. To propose practical, rights-respecting policy measures that strengthen investigation, digital forensics, platform cooperation, and survivor-centric procedures.

3. RESEARCH METHODOLOGY

This research implements a doctrinal as well as a policy-analytical approach which is mainly based on desk research. It looks at the government's official reports, the policies that have been notified, the standard operating procedures, the advisories issued by the government, and the credible academic commentary. It also analyses the datasets derived from the National Crime Reporting and Sectoral Helplines, along with the platform transparency disclosures and civil society briefs. The study looks at Indian constitutional jurisprudence, reasoning of the High Court and Supreme

Court on speech, privacy, dignity, electronic evidence, and access. The paper uses comparative references to set the standard for approaches to deepfakes and image- based abuse. Qualitative content analysis and thematic coding helped to identify the link between legal texts and survivor-focused practice. The recommendations have been worked out to the level of clear charging, takedown, evidence, and support routes which are appropriate for the police, prosecutors, platforms, and service providers.

4. CONCEPT AND SCOPE OF CYBER CRIME IN INDIA

The Indian legal system's regulation of cybercrime does not rely on a single penal clause that simply defines a generic offence of "cybercrime." Rather, it is a set of provisions that are scattered in the IT Act, the BNS, and sector-specific statutes which, when read together, constitute a response to offences in which digital technologies are central either as tools, targets, or conduits. The IT Act imparts offences to elements like computer resources, electronic records, and online content, while the BNS and BNSS work as the general codes for substantive criminal law and procedure, thus, dealing with cases of threats, hurt, cheating, sexual offences by deceit, criminal intimidation, and conspiracy that may be carried out through digital means. Moreover, the DPDP Act and related regulations set out the responsibilities concerning data processing and security thus, there is a separate regulatory non-compliance track that intersects with criminal investigations when data breaches or the misuse of personal data is the cause of the harm.[5] The IT Act makes it illegal to commit certain offences such as unauthorized access, causing damage to computer resources, identity theft, cheating by personation, violation of privacy, and sending of obscene or sexually explicit content.

If a bank server is hacked or ransomware is used to disable a hospital system, the computer resource is the direct target; if victims are deceived or coerced through phishing emails, fake loan apps, or sextortion via messaging platforms, the computer is mainly a tool; if a criminal conspiracy happens on an encrypted chat or a sexual assault video is recorded on a phone and later shared, the device is an incidental repository that intensifies the harm. These understanding matters

[5] Ishan Gupta, "Evolving Scope of Intermediary Liability in India", 37 *International Review of Law, Computers & Technology* 1 (2023).

because it determines the manner in which offences are located across the IT Act and the BNS, the way jurisdiction and investigative powers are granted, and how courts interpret mens rea and harm where the loss can be monetary, reputational, psychological, or a mixture of all three.[6]

IT Act 2000 was initially put in place mostly to provide a legal framework for the use of electronic records and digital signatures. The Information Technology (Amendment) Act 2008 has broadened the scope of the offences enumerated under Chapter XI by adding "Section 66C" (identity theft), "Section 66D" (deceiving by a false impersonation using computer resources), "Section 66E" (invasion of privacy by recording and sharing images of the private part), "Section 66F" (cyber terrorism) and refining the obscenity framework by introducing "Sections 67A and 67B" to make the production of sexually explicit material and child sexual abuse material in electronic format a punishable offence. These changes to the law reflect a shift away from simply viewing cyber law as a means to facilitate e-commerce towards acknowledging it as one of the most important regulatory tools for dealing with the dark side of the internet.[7]

The new law specifically in "Section 69 of Bharatiya Nyaya Sanhita" characterizes sexual exploitation by "deceitful means" like false promises of marriage or a job without the intention of fulfilling it, with a penalty of up to ten years in prison and/or a fine thereby changing the judicial trend role of rape provisions in the past. Other provisions, for example, "Section 296" concerning obscene acts, "Section 351" criminal intimidation which can also be done via anonymous communication, and "Section 115" voluntarily causing hurt, have gradually found their way into the first information reports (FIRs) that are related to sextortion, NCII threats, and online blackmail, respectively and mostly in conjunction with the provisions of the IT Act such as "Section 67" and "Section 67B". This multi-layered structure means that a single incident involving intimate images, threats, and monetary extortion may result in the application of both general and special law provisions thus causing a problem of overlapping charges, sentencing

[6] Cyber Crimes "an unlawful act where in the computer is either a tool or a target or both", https://www.mondaq.com/india/technology/28603/cyber-crimes-an-unlawful-act-where-in-the-computer-is-either-a-tool-or-a-target-or-both (last visited on December 6, 2025).
[7] Madhavi Divan, "Tracing the Evolution of India's Cyber Jurisprudence", 59 *Economic & Political Weekly* 16 (2024).

proportionality, and investigative priorities.[89]

5. LEGAL FRAMEWORK OF CYBER CRIME IN INDIA

Cyber-crimes in India do not confine themselves within the frameworks of IT Act and BNS only; they frequently involve laws created for the protection of certain groups of people and specific types of harm. Online child sexual exploitation is the case in point. The "Protection of Children from Sexual Offences Act 2012" (POCSO) defines in "Sections 13 to 15" the use of children for pornographic purposes, storage, and distribution of child sexual abuse material, while "Section 67B of the IT Act" separately penalizes publishing, transmitting, browsing, or collecting electronic material depicting children in sexually explicit acts as well as inducing children into online relationships for sexual purposes or facilitating their online abuse. In reality, the prosecutors in the court frequently use the combination of POCSO and "Section 67B" in cases where the victim is a minor. Hence, the judicial system recognizes the existence of a single aggravated offence with several layers which in turn warrants strict punishments along with special methods for obtaining the evidence and giving anonymity protection to the victim.[10]

Gendered cyber harms have also been connected to the "Indecent Representation of Women (Prohibition) Act 1986", that had been initially conceived with print and visual media in mind, however, it has been understood that the extension of the Act is for the digital content as well. There have been proposals for the sexualized representation forms based on the online and advertising to be clearly recognized. Moreover, the DPDP Act is planting new fault lines by giving a very broad definition of "personal data" as any information about a particular individual and also it provides the lawful grounds for processing under "Section 4", consent requirements under "Section 6", and the series of obligations under "Section 8" that require data fiduciaries to ensure security measures of at least reasonable standard, inform the Data Protection Board as well as the affected individuals when there is a personal data breach and delete personal data when the specified purpose comes to an end or consent is withdrawn, except for cases where there are legal

[8] Section 69 of The Bharatiya Nyaya Sanhita (BNS), https://devgan.in/bns/section/69/ (last visited on December 5, 2025).
[9] Man booked for sharing obscene photos of 16yo girl, https://timesofindia.indiatimes.com/city/bareilly/man- booked-for-sharing-obscene-photos-of-16yo-girl/articleshow/125874324.cms (last visited on December 4, 2025).
[10] Cyber Crimes, https://www.pib.gov.in/PressReleasePage.aspx?PRID=1602398 (last visited on December 3, 2025).

retention obligations. Situations of data breaches and unauthorized data sharing have been the primary causes of phishing schemes, SIM swaps, or doxxing campaigns. As a consequence, they are not only cybercrimes under the IT Act or BNS but also regulatory contraventions that can result in significant monetary penalties under Chapter VIII of the DPDP Act, thus, the attention is being partially shifted from individual offenders to platform governance and organizational accountability.[11]

6. JUDICIAL TRENDS AND CASE LAWS ANALYSIS

Any attempt to regulate cybercrimes through laws in India must take into account the limits imposed by the Supreme Court concerning restrictions on online speech and state surveillance. In the case of *Shreya Singhal v. Union of India*[12], the Court considered the whole of 'Section 66A of the Information Technology Act 2000'to be unconstitutional as it infringed 'Article 19(1)(a)' and was not saved by 'Article 19(2)'. It especially drew the attention to the fact that the indeterminate expressions like "grossly offensive", "annoyance", or "inconvenience" could not be the grounds at the constitutional level for criminalizing online expression.

After two years, in "*Justice K.S. Puttaswamy (Retd.) v. Union of India*[13] the right to privacy was recognized by a nine-judge bench as a fundamental right under "Articles 14, 19, and 21". The court linked informational privacy and data protection explicitly to constitutional guarantees and also laid down a proportionality test for any restriction on privacy.

In "*Kalandi Charan Lenka v. State of Odisha*[14], the Orissa High Court dealt with a fact pattern involving morphed obscene images, fake online profiles, and sustained harassment of a woman student. The prosecution also charged that along with IT Act provisions, Section 354D of the Indian Penal Code, 1860 had been violated. The reasoning in this case has since been used as a reference for interpreting the new provision embodied in the successor law, i.e., "Section 78 of the Bharatiya Nyaya Sanhita, 2023", which is the current law relating to stalking, including monitoring

[11] Punishment for publishing or transmitting obscene material in electronic form, https://blog.ipleaders.in/ obscene-material-electronic-form/ (last visited on December 2, 2025).
[12] (2015) 5 SCC 1.
[13] (2017) 10 SCC 1.
[14] 2017 SCC OnLine Ori 117.

of internet use and unsolicited electronic communication. The Court held that cyberstalking is just one means through which the offender can physically intimidate his victim, rather than the victim being simply annoyed by an online trolling. It acknowledged that, among other things, the digital harassment, the online public humiliation, and the sexually charged language, which were all persistent, thereby led to psychological trauma of the victim

Long time before the concepts of cyberstalking or NCII became well-known terms in the legal and policy fields, Indian trial courts have faced cases of online harassment under the original IT Act provisions. "*State of Tamil Nadu v. Suhas Katti*[15] is referred to by most of the commentaries as the very first lead in the conviction where the posting of obscene and defamatory material about a woman in a Yahoo message group and the sending of email messages to harass her were the acts heavily recognized, which resulted in the filing of the case under "Section 67 of the IT Act 2000" for the publishing of obscene material in electronic form, along with the then general penal code provisions. The case is at a significant moment of change: the court regarded online postings and emails as real means of criminal liability for obscenity and harassment, recognized the serious damage to the reputation and the mental suffering caused by the dissemination of sexualized rumors and images, and agreed to the electronic logs and service provider records as the proof.

7. EMERGING FORMS AND PATTERNS OF CYBER CRIME, WITH FOCUS ON GENDERED HARMS

In India, the pattern of cyber-crimes has been changed substantially over the last ten years. The change is about the move of cyber incidents from hackers, as single cases most of the time, to financially motivated crimes, stealing of credentials, computers infected with viruses, leak of private information, and generally the use of technology for various kinds of abuse - these have become daily affairs for the netizens. Moreover, the internet abuse of women and girls, both online and offline, is increasingly being considered as the most serious problem by policy makers and stakeholders. Therefore, changes in Indian laws and policies regarding cyber- crimes should not only be aimed at improving the security of the technical side or money recovery. They should be about handling gender-related patterns of targeting and hurting which not only constitute the

[15] CC No. 4680 of 2004 (CMM Egmore).

majority of the crimes but also the way of justice that the victims can access.[16]

Contemporary cyber-crimes in India have issues diversity covering financially motivated attacks to political violence and hate. Phishing and UPI related frauds are at one end of the spectrum. In these frauds, victims get fake messages or links that look like banks, e-commerce platforms, or government portals, hence leading to credential compromise and account draining. These frauds mainly victimize those with poor digital literacy and the widespread use of mobile-based payments.

Cyberterrorism "Section 66F" of the IT Act on cyberterrorism recognizes such attacks as those that threaten national security or critical systems. However, law enforcement agencies have so far very few times decided to employ this most serious provision, which is the closest one, in their actions due to its connection with issues of sovereignty and public order.[17]

Technology facilitated violence against women is a discriminatory behavior where digital devices and resources are used to harass, spy on, threaten or violate women and girls, and it is often a patriarchal control that exists offline. In numerous instances, women face online abuse in forms of sexualized trolling, sharing of intimate images without consent, doxxing, cyberstalking, hacking of social media accounts, and threats of rape or acid attack. These are some of the acts that aim to scare and silence women, so that they do not become part of public and political life, and to dominate their sexuality.

The majority of these crimes are fraud-related activities, followed by the sexual exploitation and extortion of persons. The report also identifies "cyber-crimes against women" as a separate category, but the categorization is still very minimal. A large number of crimes against women, such as deepfake dissemination, sextortion in online dating, or NCII along with threats, might be registered under general categories like "fraud", "extortion", or "obscenity" so that it becomes difficult to figure out the victims' gender from the official statistics.

[16] International Day for Elimination of Violence Against Women: Building a Safer, More Inclusive Digital India for Women, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2193644 (last visited on December 8, 2025).
[17] Nandan Kamath, *Law Relating to Computers, Internet and E-Commerce: A Guide to Cyberlaws and the Information Technology Act* 156 (Universal Law Publishing, New Delhi, 5th edn., 2016).

8. JUDICIAL AND DOCTRINAL DEVELOPMENTS IN INDIAN CYBER JURISPRUDENCE

The Indian judiciary has progressively changed its perspective about cybercrimes from regarding them as minor technical problems to understanding them as the main front where constitutional rights, statutory design, and gendered power are challenged. Free speech, privacy, digital dignity, due process, and trustworthiness of evidence are some of the new issues that courts have to deal with in areas which are ruled by platforms, algorithms, and cross border data flows instead of the traditional physical acts.

Judicial engagement with online expression in India has been traced back to the constitutional guarantee of "Article 19(1)(a)" and the set of grounds in "Article 19(2)" that allow reasonable restrictions. However, it is now happening in an environment that is still characterized by persistent trolling, targeted hate, and coordinated misinformation. Courts have been tasked with differentiating between offensive or unpopular speech that should be kept under protection and content that is harmful in a way that can be subjected to criminal sanction or removal. Judicial rulings have moved to require legislative precision, detailed guidelines for blocking and takedown, as well as a nearer relationship between the seriousness of cyber sanctions and the kind of the offending expression.[18]

The reform brought about by the recognition of privacy and dignity in the Indian Constitution has had a profound impact on how Indian courts understand cyber harms. This is true in cases involving the use of personal data, intimate images, or intrusive surveillance. The courts have held that online spaces are the new territories of personhood, reputation, and social participation. Hence privacy which was earlier limited to physical security has now been extended in a way that it covers data trails, metadata, and platform-based profiling. Harms such as the non-consensual dissemination of intimate imagery, cyberstalking, persistent doxxing, and targeted misogynistic campaigns affect bodily integrity as well as the psychological well- being of the victims and thus, are at the core of "Article 21". The courts have evolved the concept of digital dignity to mean not

[18] Aparna Vishwanathan, *Internet Intermediaries And Freedom Of Expression In India* 142 (LexisNexis, New Delhi, 1st edn., 2022).

only the protection against unwanted exposure but also the positive ability to participate in digital life on equal terms.

The former "Indian Evidence Act, 1872" had introduced "Section 65B" as a special provision for electronic records, which mandated a certificate for the admissibility of the secondary copies. Later on, with the enactment of the "Bharatiya Sakshya Adhiniyam, 2023", Parliament has changed the way electronic evidence is presented but has left intact the main idea that digital material requires particular protection. On the one hand, there are cyber forensics labs run by the government and on the other hand, there are accredited private entities, both of which are instrumental in the process of device imaging, deleted data retrieval, and the production of Section 65B style certificates or their BSA equivalents.

9. EMERGING LEGAL CHALLENGES AND PREVENTIVE POLICY MECHANISMS

While changes in law and court decisions have helped shape a legal world less friendly to cyber criminals, everyday enforcement still shows that there are very few abilities, lack of jurisdictional coordination and victim support. The rapid spread of smartphones, cheap data, and AI tools has outpaced the response capacity of traditional police structures to sophisticated fraud, deepfake pornography, and cross border offences. The interaction between the IT Act, BNS, BNSS, POCSO, the DPDP Act, and sectoral regulations creates very complicated compliance requirements for intermediaries as well as investigative agencies. Meanwhile, the experience of the survivors, especially women targeted by NCII and cyberstalking, reveals that there exist serious obstacles in complaint filing, evidence preservation, and long-term content removal.

Preventive policy instruments cover from institutional architectures like I4C and CERT-In to social support programs such as One Stop Centers and NCW helplines; however, fragmentation and uneven awareness weaken their effectiveness. Hence, a future-oriented analysis should determine not only the formal law but also the practical design of reporting portals, training programs, and

regulatory guidance which together determine the results of cyber-crime cases.[19]

Different police forces have realized that a completely different set of skills and a separate infrastructure are needed to deal with cybercrimes which is evident from the creation of specialized cyber police stations, sectoral cyber cells in state crime branches, and national level bodies. However, problems with training, staffing, and forensic resources still exist at district-level police stations, among other places, and this is where oftentimes the first response decides whether digital evidence is preserved or lost. The continuous need for specialized investigators, standard operating procedures, and cross training with prosecutors cannot be overlooked if the promise of these institutions is to lead to an increase in conviction rates and victim-centered outcomes.[20]

Cybercrime is a cross-border problem by nature as it involves data stored on servers located in different countries and perpetrators that use platform based in foreign countries or use anonymizing tools. The BNSS modernizes certain procedural parts, for example, possibilities of e-FIR, summons through electronic means, and search of electronic devices, but its provisions are still interacting with the older MLAT framework and foreign data protection laws. There are conflicts and overlaps between BNS, the IT Act, POCSO, and special statutes such as the DPDP Act, which cause more difficulties in making decisions regarding charges. Prosecutors need to combine cyber-specific offences, sexual offences against children, and data protection breaches to come up with a coherent set of charges.

"Section 79 of the Information Technology Act, 2000" grants a limited safe harbor to intermediaries with respect to third party content, subject to obligations of due diligence and compliance with government issued orders for takedown or blocking. The "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021" elaborate on this framework by prescribing mandatory grievance officers, monthly transparency reporting, 24-hour takedown of certain categories of content upon actual knowledge, and additional obligations

[19] Prashant Prasad, "Cybercrime Governance In India: Capacity, Coordination, Compliance", 12 *Journal of National Security Law & Policy* 5 (2025).
[20] About I4C, https://i4c.mha.gov.in/about.aspx (last visited on December 9, 2025).

for significant social media intermediaries, including traceability of the originator for certain messages. These obligations directly affect the cyber-crime scenarios where victims demand the immediate removal of defamatory, obscene, or non-consensual intimate content, while the accused persons raise free speech rights and privacy concerns regarding traceability. The dispute about traceability essentially pits law enforcement needs for identifying senders of unlawful messages against platform arguments relating to end-to-end encryption and user trust.

The reports from institutions and the empirical research reveal that cyber violence women are still not reported enough, and they blame this situation mainly on stigma, fear of damaging one's reputation, and lack of trust in the criminal justice system. Those who experience the non-consensual intimate image (NCII) and sexualized trolling are often hesitant to take legal action as they fear the further exposure of the imagery in the court or media. The fact that the content still stays online after removal requests makes the victim feel even more powerless as there may be copies, screenshots, or mirror sites that will continue to circulate and thus the criminal proceedings will have no restorative effect.

The system underlines the necessity of victim-centered communication that involves not only the acknowledgment of the complaints but also the periodic status updates and the information about the parallel criminal remedies. The problem is how to deploy the hash bank infrastructure in such a way that privacy is protected, and there is no chance of abuse, particularly in cases where content has been misclassified or where consensual imagery has been mistakenly reported.[21]

Under the IT Rules 2021, significant social media intermediaries and search engines are required to carry out specific actions such as removing unlawful content, appointing compliance personnel in India, and deploying proactive tools for certain categories of material, including child sexual abuse, and possibly NCII and deepfake pornography, depending on future rulemaking. Deepfake technology has made it very easy to create sexually explicit images of real women, which may be public figures or private individuals, without their consent. This puts a lot of pressure on both

[21] Vidushi Sharma, "Understanding Non-Consensual Dissemination Of Intimate Images: Laws In India With Focus On Intermediary Liability", 14 *NUJS Law Review* 2 (2022).

platforms and regulators. Comparative experience from the United Kingdom suggests that the "Online Safety Act 2023" and related amendments to the Sexual Offences Act make it a crime to share intimate deepfakes without the consent of the person depicted. In addition, the government has announced that it will make the creation of sexually explicit deepfakes a criminal offence, and that responsible will be liable to custodial sentences. Several Parliamentary committees and law reform bodies in the UK have proposed different levels of offences and more robust measures to protect victims of image-based abuse, providing a reference point for Indian debates as to whether the IT Act and BNS require explicit deepfake provisions or if existing offences, together with NCII SOP mechanisms, are enough. Social media companies in India will have to create automated systems for detecting deepfakes that will work alongside user reporting and appeals processes. These systems will also need to be able to differentiate between deepfakes as a form of satire, art or political commentary and deepfakes used NCCI-like scenarios. The regulatory balancing act between proactive monitoring and user privacy will probably determine future constitutional challenges as well as gradual changes to intermediary obligations.[22]

10.CONCLUSION

The transformation of Indian cybercrime legislation continues to be a story of effort to harmonize the advantages of the internet like openness and participation with the downside of online abuse, financial fraud, and data misuse. The courts determine both cyber harms and the methods of the investigation. These constitutional norms govern the way judges evaluate surveillance, data retention, and platform regulation when, for instance, women, children, and persons with disabilities, as the most vulnerable groups, suffer from online violence.

The legal regulations have been changed as well. Gender-sensitive offences are retained and elaborated in the transition from the IPC to the "Bharatiya Nyaya Sanhita, 2023", stalking in "Section 78" being one of such offences, which explicitly includes digital monitoring and unwanted electronic contact thus providing a way to deal with cyberstalking cases without resorting to offline conduct. The DPDP Act, 2023, with its consent centric model and the data

[22] Government Crackdown on Explicit Deepfakes, https://www.gov.uk/government/news/government-crackdown-on-explicit-deepfakes (last visited on December 5, 2025).

fiduciaries' duties, is yet another layer that regulates the collection, processing, and sharing of personal data in digital systems which usually are the sources of evidence in cyber-crime investigations. All these legal instruments together constitute a complicated but still gradually unifying legal system where any new cyber offence or investigative practice has to be justified not only in terms of the harm caused but also procedural fairness.

The innovations in the judiciary have, to a great extent, been the consequences of the shortcomings in the system such as the cases of non-consensual intimate imaging and cyber harassment of women. The importance of digital dignity, have given the stalking provisions and IT Act offences a more vigorous role, and have through the executive and intermediaries forced the system to take measures like hash matching and coordinated takedown so that the resurfacing of the intimate material can be effectively prevented. Also, the UK's decision to make the creation and sharing of sexual deepfakes a criminal offence under the Online Safety Act and related reforms can be a source of external reference for the Indian debates on AI- mediated abuse, but it should not be seen as a way that the outcomes are already decided.

Policy mechanisms as well as institutional architectures are still very important for the effective translation of the doctrine into real protection. At the same time, One Stop centers, NCW complaint systems, Mission Shakti, and helplines are the sources of support and the means of accompaniment in the medical, legal, and psychosocial spheres. However, the problem of underreporting, uneven digital literacy, unstandardized forensic infrastructure, and jurisdictional issues in acquiring cross border data still impede the extension of these initiatives to a wider audience. The following path of Indian cybercrime law is going to be heavily influenced by the decision to keep on funding training for investigators and prosecutors. Indian law will be in a better position to deal with the new harms such as fabricated videos, AI- generated scams, and platform-facilitated harassment, thus, ensuring compliance with the constitutional commitments to equality, dignity, and personal liberty if these structural and doctrinal factors come together.