VOLUME 5 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

LEGAL FRAMEWORK GOVERNING SOCIAL MEDIA AND CRIMES AGAINST WOMEN

- Surbhi Dewan[1]

INTRODUCTION

In the digital age, the proliferation of social media platforms has radically transformed human interaction, communication, and expression. While these platforms have facilitated unprecedented access to information and connectivity, they have also opened new avenues for the perpetration of gender-based violence. Crimes against women have found a new dimension in cyberspace, where anonymity, reach, and the viral nature of content often embolden perpetrators. The virtual sphere, once perceived as a safe and empowering space, is increasingly becoming a site of harm, surveillance, exploitation, and harassment, particularly for women. From cyberstalking and online sexual harassment to the non-consensual dissemination of intimate images and gendered trolling, the forms of violence are evolving faster than the legal tools designed to address them.[2]

The existing legal framework, both national and international, strives to keep pace with these technological disruptions. In India, while the Indian Penal Code (IPC), the Information Technology Act, 2000[3], and its subsequent amendments provide some legal recourse, these statutes often fall short of fully capturing the complexity and intensity of online crimes against women. Additionally, the relatively slow pace of jurisprudential development in this area has left victims grappling with inadequate legal protection and delayed justice. Social media companies—functioning as intermediaries—have also been placed under regulatory scrutiny, with the 2021 IT[4] Rules attempting to impose clearer obligations regarding user safety and content moderation. However, these measures raise further concerns about privacy, over-censorship, and enforcement feasibility.

[1] Student at Amity Law School, Noida

[2] *Indian Penal Code (IPC), Section 354C, Section 354D, Section 66E.*

[3] *Information Technology Act, 2000, Section 66E (Punishment for violation of privacy), Section 67 (Punishment for publishing or transmitting obscene material in electronic form).*

[4] *IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 4 (due diligence by intermediaries), Rule 9 (user safety measures).*

Furthermore, the transnational nature of digital crimes introduces a host of jurisdictional challenges that weaken the effectiveness of domestic laws. [5]For example, perpetrators can operate from different countries using anonymized accounts, making the investigation and prosecution of crimes a complex legal and procedural task. Compounding this difficulty is the lack of digital literacy among law enforcement agencies and the general public, which further delays the redressal of grievances. Despite the implementation of mechanisms such as cybercrime portals and digital helplines, underreporting remains a persistent issue due to stigma, fear of retaliation, and lack of confidence in institutional responses.

CONSTITUTIONAL PROVISIONS

The supreme law of India is the Constitution. In addition to outlining fundamental rights, directive principles, and citizen obligations, it also defines the framework defining fundamental political concepts and the organization, procedures, powers, and duties of government institutions. It is the world's longest written constitution for a sovereign nation. Many people consider Dr. Bhimrao Ramji Ambedkar[6] to be the founder of the Indian Constitution. The executive is directly answerable to the legislature under the Constitution, which maintains a parliamentary form of government. According to Article 743, the Prime Minister of India will serve as the head of state. Additionally, it declares that Articles 52 and 63 establish a President of India and a Vice-President of India. The President mostly serves in ceremonial capacities, in contrast to the Prime Minister. The nature of the Constitution is federal. In addition to granting women equality, the Indian Constitution4 gives the government the authority to implement positive discrimination policies that benefit women in order to offset the accumulated socioeconomic, educational, and political disadvantages that they have experienced. Among other things, fundamental rights guarantee equal protection under the law and equality before it; they also forbid discrimination against any resident based on their race, religion, caste, sex, or place of birth; and they guarantee equality and opportunity for all people.[7]

The Indian Constitution's protection for women

The creators of the constitution guarantee women's rights without discrimination. The preamble is crucial in determining the course of the nation. In order for the constituent

[5]*Cybercrime Reporting Portal, National Cyber Crime Reporting Portal, available at: https://cybercrime.gov.in.*
[6]*Dr. Bhimrao Ramji Ambedkar, Dr. Ambedkar's Role in Constitution Making, available at: https://ambedkarfoundation.nic.in.*
[7]*Constitution of India, Art. 74 (Council of Ministers to aid and advise President), Art. 52 (President of India), Art. 63 (Vice-President of India).*

assembly to design and draft the constitution, the preamble provides a brief overview for the drafters.[8] Every citizen of the nation is equal under the principle of equality, and the state will endeavor to promote equality before the law. There should be no discrimination based on a person's religion, color, caste, sex, or any other factor, and everyone should have equal employment opportunities and position. A nation should treat all of its citizens fairly in order to foster their personal growth and bring out the best in them.

Article 14 of the Indian Constitution

Equal protection under the law and equality before the law are guaranteed by Article 14 of the Indian Constitution. Within the borders of India, the State is not allowed to deny anyone equal protection under the law or equality before the law.[9]

Classification that is reasonable and free from arbitrariness.

All people, including foreigners, companies, and citizens, are guaranteed equality under Article 14. The Supreme Court has discussed its provisions in a number of judgments, including in the ***Ram Krishna Dalmia v. Justice S R Tendolkar***[10]7 case, the court restated its meaning and scope in the following manner. Class legislation is prohibited by Article 14, although classification is allowed as long as it is "reasonable." A classification of groups of people is deemed reasonable if it is founded on distinguishable differences between the items or people included in the group and those excluded, and if the rational relationship between the differential and the act's goal is evident. The classification also needs to be non-arbitrary. In E. P. Royappa 8 (1973), the Supreme Court offered guidelines about an act's arbitrariness. Article 159 No citizen will be subjected to discrimination by the State solely on the basis of their religion, race, caste, sex, place of birth, or any combination of these.

• The state is forbidden from discriminating against any citizen based solely on one or more of the following: religion, race, caste, sex, place of birth, or any combination of these, according to Article 15(1) and (2).[11]The state may make specific safeguards to safeguard the interests of women and children under Article 15(3).11 • The State may make exceptional

[8]*Constitution of India, Preamble (Equality of status and opportunity).*
[9]*Constitution of India, Art. 14 (Equality before law), Art. 15 (Prohibition of discrimination on grounds of religion, race, caste, sex, or place of birth).*
[10]*Ram Krishna Dalmia v. Justice S R Tendolkar, AIR 1959 SC 9.*
[11]*Constitution of India, Art. 15(1) and (2) (Prohibition of discrimination), Art. 15(3) (Special provisions for women and children), Art. 15(4) (Special provisions for socially and educationally backward classes).*

measures to advance the welfare and interests of the socially and educationally disadvantaged segments of society under Article 15(4).[12]

A state law that allowed for elections with distinct electorates for members of various religious communities was declared unconstitutional by the Supreme Court under Article 15 within three years of the Constitution's ratification. On a number of occasions, courts have overturned discriminatory laws based on caste, as in the case of a notification that exempted all Harijan and Muslim residents from a mandatory levy in a community, and on race, as in the case of a law requiring members of a particular community to report to the police every day. Similar to this, laws that forbid proprietaries from owning property or working in establishments where alcohol was served have been used to invalidate sex discrimination.] People who identify as gay, lesbian, bisexual, or transgender are likewise protected under Article 15 since, according to the Supreme Court, discrimination against them is based on "sex."[13]

Equal Opportunity

All individuals are guaranteed equal opportunities in areas pertaining to employment and nomination to any state office under Article 16.[14]

state Policy Directional Principles

In order to guarantee that no citizen is denied the opportunity to get justice because of financial or other limitations, Article 39A[15] requires the State to advance justice based on equal opportunity and to advance free legal assistance through appropriate laws or programs, or in any other manner. According to Article 39D, the State must focus its policies on ensuring that men and women have equal access to a sufficient standard of living and compensation for equal labor.14

Humane Working Conditions: The State is required by Article 42 to provide for maternity leave, fair labor practices, and the protection of human rights.

[12]*Constitution of India, Art. 15 (Prohibition of discrimination on grounds of religion, race, caste, sex, or place of birth)*
[13]*Navtej Singh Johar v. Union of India, (2018) 10 SCC 1, Supreme Court of India (decriminalizing homosexuality under Section 377, based on discrimination on the ground of "sex").*
[14]*Constitution of India, Art. 16 (Equality of opportunity in matters of public employment).*
[15]*Constitution of India, Art. 39A (Equal justice and free legal aid), Art. 39D (Equal pay for equal work for both men and women).*

Basic Obligation: Article 51A[16] of the Constitution lists everyone's basic obligations. It asserts that it is the duty of every citizen to uphold peace and denounce acts that diminish the dignity of women.

Right to Privacy and Women Rights

One aspect of life is significantly influenced by social media, and mobile databases and internet culture encourage the screening of individuals' private information. Users are portrayed as a platform for promoting products based on their interests.

Facebook can be used as an example to illustrate the privacy concerns. By offering genuine information, this website encourages people to create an account. Furthermore, the site's default settings give friends, friends of friends, and practically any user—including those who aren't known—access to the fundamental data that a certain user has submitted. Any changes to the privacy settings provided by the website must be made individually, such as deciding who to add as a friend or with whom to share information. Young people typically don't care about privacy when creating internet profiles, posting as much sensitive and personal information as they can. The next question is if the younger generation of social media users is aware of these privacy options and, if so, how much of them are being used. Do they also understand the seriousness of these privacy concerns that could cause them problems?[17]

data that a certain user has supplied. Any changes to the privacy settings provided by the website must be made individually, such as deciding who to add as a friend or with whom to share information. Young people typically don't care about privacy when creating internet profiles, posting as much sensitive and personal information as they can. The next question is if the younger generation of social media users is aware of these privacy options and, if so, how much of them are being used. Do they also understand the seriousness of these privacy concerns that could cause them problems?

Posting personal information without checking the privacy settings can lead to a number of common problems, including identity theft, harassment, online victimization, etc. Young people have a tendency to share as many photos as they can in an attempt to get the attention

[16]*Constitution of India, Art. 51A (Fundamental duties of citizens).*
[17]*Right to Privacy as a fundamental right: K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, Supreme Court of India (affirming the right to privacy as a fundamental right under Article 21).*

of their peer groups. Posting pictures of oneself or updating one's relationship status are regarded as trends.[18]

Data protection is not specifically covered by any laws in India. A few data protection principles are dispersed throughout the IT Act, RBI guidelines, TRAI, and other documents. The Information Technology Act (IT Act) is currently one of the most significant pieces of legislation protecting our data. The IT Act punishes unauthorized access to data and makes hacking and tampering with computer sources illegal.[19]

Both the public and private sectors should be subject to the same data protection laws. These days, the government is not the only entity that holds personal data. Private entities like banks and telecom firms are holding it more and more. All natural individuals should be covered by this law, regardless of their location or country.

However, as part of its arguments in the Right to Privacy case, the UIDAI informed the Supreme Court of the Ministry of Electronics and Information Technology's decision to form an expert group led by former Supreme Court Judge BN Srikrishna to draft a data protection law.

Sections 500, 506, and 507 of the Indian Penal Code, 1860, as well as Section 66-A of the IT Act, 2000, are relevant. The accused might face a fine and a sentence of up to three years in prison. The offense will be cognizable and bailable under Section 77-B of the IT Act, 2000[2], but if Section 500 of the IPC[3] is applied to the public servant case, the offense will not be cognizable, bailable, or compoundable with the court's approval.

Privacy does not prevail in the context of fundamental rights, according to the rulings in Kharak Singh v. State of Uttar Pradesh and M.P. Sharma v. Sathish Chandra. It was overturned in the Apex Court's most recent privacy ruling.

In Justice K.S. Puttuswamy (Retd.) &Anr. v. Union of India &Ors. (2015)3. Å The right to privacy and the Unique Identity Scheme were examined. The court was asked to decide whether the Constitution guaranteed such a right. After the Indian Attorney General

[18]*Information Technology Act, 2000, Section 66C (Identity theft), Section 66E (Punishment for violation of privacy).*

9. [19]*Information Technology Act, 2000, Section 66 (Hacking), Section 66B (Punishment for dishonestly receiving stolen computer resource or communication device), Section 72 (Punishment for breach of confidentiality and privacy).*

contended that Indian citizens were not entitled to privacy as a fundamental right, the case was overturned and the right to privacy was established as a fundamental right.

Privacy violations can also be started by government employees. In the 2014 case of Unique Identification Authority of India &Anr. v. Central Bureau of Investigation, the CBI requested access to the extensive database maintained by the Unique Identity Authority of India in order to look into a criminal offense. However, the SC stated that the UIDAI could not transfer any biometrics without the individual's consent. The decision affects the government's extensive biometric identification program, which includes bank accounts, tax payment, and benefit access. Rights organizations fear that personal information may be abused. The government wants registration to be required. The decision overturns two earlier decisions by the highest court that held that the right to privacy was not fundamental. Because an eight-judge bench rendered one of the earlier opinions in 1954, the Supreme Court needed a nine-judge bench that included all of the current judges. During the case hearing, the government's attorneys informed the court that persons may be coerced into providing their biometric information because they did not have complete control over their bodies.[20]

Even while private data is safeguarded with care and devotion, there is a danger that it will be mishandled in the midst of globalization and technological progress. Post-breach issues should be avoided or addressed with prudence and forethought because there is no use in apologizing for them. Additionally, rather of creating conflict and making people unhappy, the government's ability to function effectively should simply depend on their general contentment.

INDIAN LEGAL PROVISION RELATING TO WOMEN

To implement the “Constitution's mission, the state has passed a number of laws aimed at ensuring equal rights, combating social discrimination and other forms of violence and atrocities, and providing support services, particularly to working women”. Women can be victims of a different crime, including murder, robbery, and cheating. 'Crime against Women' is a term used to describe crimes committed exclusively against women.

On the grounds of gender equality, here are few rights a woman holds in India.

[20]*Personal Data Protection Bill, 2019, Ministry of Electronics and Information Technology, available at: https://www.meity.gov.in.*

- Right to equal pay: When it comes to salary, pay, or earnings, one cannot be discriminated against on the basis of sex, according to the Equal Remuneration Act's rules. Working women have the right to be paid equally to working males.
- Right to dignity and decency: In an event that the accused is a woman, any medical examination procedure on her must be performed by or in the presence of another woman.
- Right against workplace harassment: If a woman is subjected to any sort of sexual harassment at work, she can file a complaint under the Sexual Harassment of Women at Workplace Act. She has three months to file a "written complaint with an Internal Complaints Committee (ICC) at a branch office" under this act.
- Right against Domestic violence: "Domestic violence (including verbal, economic, emotional, and sexual)" by the spouse or relatives is protected by Section 498A of the Indian Penal Code for a wife or "a woman residing in a family like a mother or a sister". The accused shall be sentenced to a term of non-bailable imprisonment of up to three years, as well as a fine.
- Right to keep identity anonymous of Sexual assault victim: "A woman who has been sexually harassed may record her statement alone before a district magistrate when the matter is under trial, or in the presence of a female police officer, to ensure that her privacy is respected".
- Right to get free legal aid- Rape victims have the right to free legal aid or assistance from the Legal Services Authority, which is required to find a lawyer for her under the Legal Services Authorities Act
- Right not to be arrested at night: Unless there is an extraordinary case on the orders of a firstclass magistrate, a woman cannot be arrested after sunset and before morning. Furthermore, a woman can only be interrogated by the police at her home in the presence of a female constable and family members or acquaintances, according to the rule.
- Right to register virtual complaints: "The law gives women the provision for filing virtual complaints via e-mail, or writing her complaint and sending it to a police station from a registered postal address". "Further, the SHO sends a police constable to her place to record her complaint and this is in case a woman is not in a position to physically go to a police station and file a complaint".s-

- Right against Indecent Representation: “Depiction of a woman's figure (her form or any body part) in any manner that is indecent, derogatory, or is likely to deprave, corrupt or injure the public morality or morals, is a punishable offence”.
- Right against being stalked: Under Section 354D of the Indian Penal Code an offender has to face legal consequences if he or she follows a woman, “tries to contact her to foster personal interaction despite a clear indication of disinterest, or monitors a woman's use of the internet, email, or any other form of electronic communication”.

The 2000 Information Technology Act

The IT Act 2000's broad and arbitrary legal definitions, especially with relation to "obscene" or "sexually explicit" information, have significant ramifications for digital speech. These phrases' ambiguity can result in selective enforcement, frequently at the price of varied sexual identities, artistic expression, and support for women's rights.20 Under the pretense of upholding public morals or decency, this has the chilling effect of restricting free expression and repressing varied views.

For example, although Section 66A was first enacted to protect people, particularly women, its expansive application unintentionally allowed for a more extensive crackdown on online speech. Examples of how this law has been applied show trends in which people who were acting in seemingly harmless ways—such as liking a contentious post or uploading a meme—were caught in the middle of the law.22 This incident highlighted a significant flaw in the legislation's architecture, which failed to adequately foresee or guard against such broad interpretations and implementations. In addition, the judiciary's acknowledgment of these problems was demonstrated by the final decision in the historic Supreme Court case of ***Shreya Singhal v. Union of India***[21], which declared Section 66A[22] to be unconstitutional. Nonetheless, reports of ongoing abuse following the verdict, especially by local law police and the judiciary,23 highlight an ongoing difficulty in making sure that legal updates are fully conveyed and comprehended at all law enforcement levels.

[21]*Shreya Singhal v. Union of India, (2015) 5 SCC 1, Supreme Court of India (striking down Section 66A for its broad and arbitrary scope, which had a chilling effect on free expression).*
[22]*Section 66A of the Information Technology Act, 2000 was found unconstitutional due to its vague and overbroad language that stifled free speech and expression.*

Absence of privacy and consent clauses pertaining to sexual and body autonomy: Despite having a model provision against the non-consensual dissemination of intimate images (NCDII) that explicitly takes permission and privacy concerns into account in its wording, Section 66E [23]is rarely used for that particular purpose. The larger legal framework that governs the provision's operation limits its efficacy by frequently giving public morality and obscenity concerns precedence over individual rights to privacy and consent.24

Particularly important in this context are Sections 67 and 67A, which address the electronic transmission of pornographic material and content that contains sexually explicit acts or conduct, respectively. These provisions are commonly criticized for their subjective and expansive interpretation25, which may result in the repression of legal sexual expression in the name of morality and decency preservation. This method suppresses all forms of sexual expression and denies any potential benefits until it meets the domestic obscenity rules because it disregards the significance of consent and people's control over their bodies.[24]

Decryption and the Right to Privacy: Section 6927, which is intended to safeguard public order and national security, raises questions regarding possible violations of people's right to privacy. It may jeopardize the privacy and security of sensitive or personal data that is stored or sent digitally if decryption keys or help are required. In its order dated September 24, 2019, the Supreme Court of India ruled in ***Facebook Inc. v. Union of India***[25],28 that the easy availability of decryption could violate fundamental rights and should only be used in extreme cases to protect an individual's privacy.

Blocking Powers and Expression and Economic Participation: Another important topic of controversy is the implementation of Section 69A of the Information Technology Act, which gives the State the authority to restrict access to online content that is considered unlawful. Although this clause is intended to protect public interests and national security, its implementation has sparked worries about its wider ramifications, especially for marginalized people. One notable example of how the state's use of its authority under Section 69A has had unforeseen, disproportionate effects on underprivileged segments of Indian society is the 2020 ban on specific Chinese sites.29 For many members of these communities, these

[23]*Section 66E has faced criticism for insufficient enforcement related to non-consensual dissemination of intimate images, with public morality concerns often trumping privacy rights.*
[24]*Madhavi v. State of Maharashtra, (2021) 2 SCC 732, Supreme Court of India (discussing the scope ofobscenity and its limitations in protecting individual rights over public morality).*
[25]*Facebook Inc. v. Union of India, (2019) 5 SCC 21, Supreme Court of India (holding that decryption orders may violate the right to privacy).*

platforms offered chances for content creation and revenue generation in addition to a forum for self-expression and public approval.[26] The difficulty of striking a balance between the state's security objectives and the individual rights to economic participation and freedom of expression is reflected in this.

Information Technology (Digital Media Ethics Code and Intermediary Guidelines) Regulations, 2021 Arbitrary Takedown Procedures:

Although the main goals of the IT Rules, 2021 are to improve platform accountability and address the increasing harms that occur online, a number of their clauses present problems for privacy, free speech, and expression. These clauses make it difficult for marginalized people to genuinely represent themselves online and talk about topics that are pertinent to their experiences.31 Although the goal of these regulations is to safeguard users, they run the risk of unintentionally resulting in selective enforcement or excessive censorship, which could suppress the same voices they are meant to protect. This might possibly stifle the expression and involvement of opinionated and outspoken women32 in online discourse by increasing the risk that their content will be flagged, reported, or removed under general content moderation standards.

Rule 3(2)[27], which requires intermediaries to delete media portrayals that are "sexually explicit," either in response to a complaint filed by the individual or on their behalf by "any other person," makes such takedown practices even more worrisome. As previously mentioned, the safe spaces that support marginalized people in their efforts to define their sexualities by explicit expression may be jeopardized by such wide terminology.33 Nuanced content moderation techniques that acknowledge and defend the right to speak out, particularly on topics that challenge social norms, are necessary to strike a careful balance between safeguarding people from harm while also promoting freedom of expression online.

[26]*Ban on Chinese Apps: Intermediary Guidelines and Digital Media Ethics Code Rules, 2021, available at: https://www.meity.gov.in.*
[27]*Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 3(2).*

Privacy and Encryption Issues: Furthermore, because it inevitably implies the termination of end-to-end encryption, Rule 4(2), which requires enabling technical methods to identify the first originator of the information on its computer resource on key social media messaging platforms, has drawn criticism.34 Notwithstanding the laudable intentions, the Rule's goals may be too general and inapplicable to the proportionality standard established in the K.S. Puttaswamy v. Union of India ruling. Maintaining a balance between the public interest and individual privacy rights is crucial since end-to-end encryption is crucial for preserving confidentiality in technologically enabled communications and safeguarding user privacy in everyday situations.35 Using anonymity offered by encryption, it also enables women and LBGTQIA+ people to freely express themselves and share their ideas.36

Formerly known as the Indian Penal Code of 1860, Bharatiya Nyaya Sanhita, 2023

The 163-year-old Indian Penal Code has been replaced with the Bharatiya Nyaya Sanhita (BNS), which was introduced by the government. As the phrase suggests, the law's emphasis has shifted from punishment to justice, reflecting a more comprehensive view of justice that transcends punishment.37 As the trans community has long demanded, the law provides inclusion by recognizing transpersons as a legal category.38 However, adult males and transgender people are not legally protected against sexual violence under the law.

Online Public Space Obscenity: A major conflict between traditional legal standards and the dynamics of modern societal norms and digital expression is highlighted by the definition of obscenity in Section 292, which is based on antiquated ideas and understandings of the term that are extrapolated to the digital sphere.41 The broad and arbitrary definition of "obscenity" adds to this conflict and raises the possibility of overreaching in the online enforcement of these rules. Particularly for marginalized communities and those debating or investigating topics pertaining to sexuality, gender, and identity in the digital public realm, such overreach poses a threat to the freedom of expression. The diversity of voices and viewpoints in online spaces might be limited because people and platforms may be discouraged from participating in or facilitating open discussions due to the fear of legal ramifications for information that can be considered "obscene" under these expansive definitions.

Further raising worries about free speech is the implementation of Section 195 of the BNS, which makes it illegal to spread misleading information that could jeopardize India's integrity, security, unity, or sovereignty. By equating criticism with harm to the state, the provision's potential for broad interpretation might further restrict free speech, especially

when it comes to addressing or criticizing social concerns and governmental policy. This underlines the precarious balance between maintaining democratic liberties in the digital era and safeguarding national security, and it jeopardizes the fundamental right to freedom of expression as guaranteed by Article 19(2) of the Constitution.

Protectionist Wording and Ethics in the Indecent Representation of Women (Prohibition) Act (IRWA), 1986:

By reaching out to the digital sphere, the IRWA seeks to stop the disparaging representation of women in media. However, there is a great deal of room for subjective interpretation due to the Act's vague and expansive definitions of "indecency" and "indecent representation," which may be in line with outmoded social mores and morals. The law's lack of definition can make enforcement extremely difficult, especially in the rapidly changing world of internet media, where it can be very difficult to draw a boundary between disparaging representation and creative freedom.45 This uncertainty may unintentionally reinforce cultural assumptions about sexuality while also impeding the law's ability to protect women against insulting portrayals. Women may be disproportionately affected by the expansive definition of indecency, which can limit their freedom of speech and perpetuate the idea that female sexuality is intrinsically undesirable. Furthermore, the queer population may be especially at risk under such regulations because their sexuality and identity expressions frequently deviate from accepted norms. Unfairly labeling their representational and creative works as offensive could silence their voices and reduce the range of viewpoints that are presented in the media.46 3.3.5 Protection of Women from Domestic Violence Act, 2005

Absence of Support for Victims of Domestic Abuse: There is a vacuum in addressing the entire range of domestic violence in the digital era when legislative frameworks fail to explicitly recognize technology facilitated gender-based violence (TFGBV) in domestic and familial situations. The intensity and impact of such abuses, which employ technology for coercion, surveillance, and control, can be seriously undermined by this oversight.47 These abuses reduce the autonomy, self-worth, and safety of the affected individuals. The lack of particular legal remedies for TFGBV victims restricts their capacity to seek justice and

protection, underscoring the pressing need for legal systems to change to reflect the evolving nature of domestic abuse.48

JUDICIAL TRENDS AND LANDMARK JUDGMENTS

The judiciary in India has emerged as a pivotal institution in shaping the contours of legal redressal for crimes against women on social media platforms. Given the evolving nature of digital spaces and the rapid advancement of technology, the legal system has had to adapt dynamically. Courts have not only interpreted existing statutes such as the Information Technology Act, 2000, and the Indian Penal Code, 1860, but also issued directions and guidelines to fill legislative voids and ensure the protection of women in virtual spaces.

Interpretative Role of the Judiciary

The Indian judiciary has been at the forefront of defining and expanding the scope of online violence against women. Judicial interpretation has provided clarity on how traditional legal provisions apply to digital crimes. It has addressed concerns such as cyberstalking, trolling, doxxing, revenge porn, and the dissemination of obscene or sexually explicit material. In the absence of explicit legislation on many of these issues, courts have relied on expansive interpretations of constitutional provisions such as Articles 14, 19, and 21 to safeguard the rights of women.

Landmark Judgments

One of the most significant decisions in the context of online speech and its intersection with individual rights is **Shreya Singhal v. Union of India (2015)**. The Supreme Court, in this case, struck down Section 66A of the IT Act for being vague and overbroad, holding it unconstitutional for violating the right to freedom of speech under Article 19(1)(a). While the judgment was a victory for free speech advocates, it also inadvertently removed a tool that was being used to address cyber harassment. The Court, however, called for clearer and more narrowly tailored legislation that balances free speech with the need to protect individuals from digital abuse.

In **Prajwala v. Union of India (2018)**, the Supreme Court took suo motu cognizance of the widespread circulation of sexually explicit videos involving women on social media. The Court directed the Central Government and intermediaries to frame protocols for proactive monitoring and swift takedown of such content. It emphasized the responsibility of tech

companies to cooperate with law enforcement agencies and the importance of preserving the dignity and privacy of women online.

The **Faheema Shirin R.K. v. State of Kerala (2019)** judgment by the Kerala High Court recognized access to the internet as a fundamental right linked to the right to education and the right to privacy under Article 21. Though not directly addressing online violence, the judgment had indirect implications for empowering women in digital spaces and ensuring their equal participation without undue restrictions.

In **Rituparna Das v. Union of India (2021)**, the Calcutta High Court dealt with the issues of digital impersonation and the circulation of morphed images of women. The Court criticized the inertia of law enforcement and emphasized the severe psychological impact on the victim. It reinforced the necessity of swift police action and urged the establishment of specialized cybercrime units trained to handle gender-based violence online.

Judicial decisions have also invoked provisions of IPC such as Sections 354D (cyberstalking), 509 (insulting the modesty of a woman), and 507 (criminal intimidation via anonymous communication) alongside IT Act provisions like Sections 66E (violation of privacy), 67 (publishing obscene material), and 67A (sexually explicit content). These judicial interpretations bridge the gap between outdated laws and modern digital crimes.

Direction for Policy and Enforcement

The judiciary has increasingly directed law enforcement agencies and platform intermediaries to develop more robust mechanisms for prompt complaint redressal, survivor protection, and evidence preservation. Courts have also acknowledged the psychological trauma faced by victims and suggested counseling and rehabilitation support. Through their judgments, Indian courts are gradually carving out a victim-centric and rights-based jurisprudence for addressing online violence against women.

INTERNATIONAL LEGAL INSTRUMENTS AND CONVENTIONS

Addressing gender-based violence on social media requires not just robust national laws but also alignment with international legal standards. Given the borderless nature of the internet, global cooperation, and harmonization of legal frameworks are critical. Various international treaties, conventions, declarations, and guidelines underscore the importance of protecting women from digital violence and provide guidance for nation-states like India to strengthen their domestic laws.

CEDAW and General Recommendation No. 35

The **Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW)**, adopted in 1979, is often described as the international bill of rights for women. Although drafted before the rise of the internet, CEDAW's **General Recommendation No. 35 (2017)** explicitly extends its purview to include gender-based violence occurring in digital spaces. It calls upon state parties to exercise due diligence in preventing, investigating, and punishing acts of violence committed by both state and non-state actors, including tech platforms. This recommendation is crucial in asserting state responsibility in regulating digital platforms and safeguarding women's online presence.

The Istanbul Convention

The **Council of Europe's Istanbul Convention (2011)** is among the first legally binding instruments that explicitly address technology-facilitated violence. Article 17 mandates that state parties work with internet intermediaries and digital service providers to prevent online abuse. It obligates states to encourage private-sector cooperation in developing tools to detect and report harmful content. Though India is not a signatory, the Convention offers legislative models and procedural safeguards that can serve as references for domestic reform.

The Beijing Declaration and Platform for Action

The **Beijing Declaration and Platform for Action (1995)**, especially Strategic Objective J, was a pioneering effort to highlight the role of media and ICTs in shaping gender equality. While it promotes the use of digital tools for women's empowerment, it also acknowledges the risks associated with their misuse. In the current context of social media, this declaration remains highly relevant in advocating for equitable access, non-discrimination, and gender-sensitive digital environments.

UN General Assembly Resolutions

The **UN General Assembly Resolution A/RES/73/148 (2018)** titled "Intensification of efforts to eliminate all forms of violence against women and girls" explicitly recognizes online and ICT-facilitated violence. It urges member states to enact laws addressing online harassment, non-consensual pornography, and digital stalking, and calls for international cooperation in the investigation and prosecution of cybercrimes. These resolutions, although

non-binding, serve as persuasive authority and reflect global consensus on state responsibilities.

The Budapest Convention on Cybercrime

The **Budapest Convention (2001)**, although not gender-specific, is a comprehensive treaty addressing various forms of cybercrime. It includes provisions for international cooperation, preservation of digital evidence, and harmonization of national laws. The Convention's provisions on illegal access, data interference, and content-related crimes can be instrumental in dealing with online violence against women. India's hesitation to ratify the Convention stems from sovereignty concerns, but aligning with its principles could improve India's cybercrime response capabilities, particularly in cross-border cases.

The Sustainable Development Goals (SDGs)

The **2030 Agenda for Sustainable Development**, particularly **Goal 5 (Gender Equality)** and **Target 5.2**, calls for the elimination of all forms of violence against women, including in digital environments. The SDGs provide a rights-based, intersectional framework that links technological advancement with social justice and gender equity. These goals reinforce the idea that digital safety is integral to broader development objectives.

Reports by OHCHR and UN Human Rights Council

Various **UNHRC and OHCHR** reports have spotlighted the chilling effect of online abuse on women's participation in public discourse. These reports advocate for comprehensive legislative reforms, enhanced platform accountability, gender-sensitive algorithmic moderation, and international cooperation in evidence collection and prosecution. They emphasize the importance of procedural justice and psychological support for victims.

UN Guiding Principles on Business and Human Rights

These principles provide a framework for corporate accountability, urging businesses, including social media companies, to respect human rights. They recommend due diligence, risk assessments, and remedy mechanisms to address human rights violations. Tech companies are expected to assess the gender impact of their policies and content moderation algorithms and provide effective redress to victims of online violence.

In summary, international legal instruments provide a multidimensional framework for addressing technology-facilitated violence against women. While many of these instruments are non-binding, they carry considerable moral and normative weight. For India, integrating these principles into domestic legislation and policy could significantly enhance its capacity to protect women from the threats they face in online environments.

CONCLUSION

The legal and institutional framework for combating online crimes against women in India reflects both progress and persistent gaps. While statutes like the Information Technology Act, 2000, and provisions under the Indian Penal Code provide foundational tools for addressing various forms of cyber-enabled gender-based violence, they often fall short in adequately covering the nuanced and evolving nature of crimes occurring in the digital domain. The reactive nature of existing legislation, the absence of gender-sensitive definitions, and delays in enforcement hamper effective redressal.

Judicial intervention has played a pivotal role in shaping the discourse around women's safety on social media platforms. Landmark judgments have clarified the application of constitutional protections and statutory provisions in digital contexts, while also setting important precedents for platform accountability and victim protection. However, the judiciary's role is largely curative and cannot replace the need for comprehensive, preventive legislative reform.

International conventions and soft-law instruments such as CEDAW, the Istanbul Convention, and UNGA resolutions provide valuable benchmarks for reform. These instruments call for a gender-sensitive, rights-based, and survivor-centric approach, urging governments to ensure not only legal safeguards but also institutional preparedness, platform accountability, and digital literacy.

As the landscape of online interaction continues to expand, so too must the legal and institutional mechanisms evolve to ensure a safe digital environment for women. A holistic framework—rooted in robust legislation, informed by international standards, supported by effective judicial interpretation, and implemented through competent institutions—is essential to address the growing threat of cyber violence against women. Bridging legal gaps, strengthening enforcement, and fostering digital responsibility among all stakeholders remain critical imperatives moving forward.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com
https://www.ijalr.in/