

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES
[ISSN 2581-5369]

Volume 9 | Issue 3
2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of any suggestions or complaints, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the International Journal of Law Management & Humanities, kindly email your Manuscript to submission@ijlmh.com.

(De)constructing Consent: An Evaluation of “Sexual Violence” in the Online Sphere

SMRITI SHARMA*

ABSTRACT

The dynamics of human interaction has undergone a significant transformation with the acceleration in development of digital technologies. As social media platforms become ubiquitous, instances of sexual exploitation and abuse seems to pervade the online sphere. The existing Indian statutory framework, while adept in tackling traditional sexual violence, faces substantial obstacles in prosecuting violations in online spaces where there is lack of monitoring of sexual violence cases of cyberstalking, image-based sexual exploitation (deepfakes) and non-consensual sharing of private images as a way of extortion (sextortion).

India's current legal framework, including Bharatiya Nyaya Sanhita (BNS), 2024 and Information Technology Act (IT Act), 2008, offer abysmal protection as the provisions are not equipped to focus on complexities in defining sexual violence in the virtual realm and enumerating the standards of consent. In traditional sexual violence, consent is the verbal or non-verbal unequivocal, voluntary communication between parties before engaging in sexual acts which can also be withdrawn at any time; however, in the digital sphere, there is no specific provision governing the various nuances of consent in relation to its communication, revocation and evidentiary verification.

The evolving technological advancement without corresponding reform in the legislative sphere highlights the urgent need for the Indian criminal law to provide recognition to online sexual violence as a distinct form of violence while re-evaluating the standards of consent in the digital sphere. Hence, this paper is an attempt to understand and measure consent within the context of sexual violence in the digital sphere.

Keywords: *technologically-Facilitated sexual abuse and violence, Image-based sexual violence, Digital Consent, Deepfake, Cyber-Crime*

I. INTRODUCTION

Over the years, there has been a sharp rise in technological advancement and in the use of social media platforms. In fact, the proportion of individuals with access to the internet reached 73.8% of the global population in April 2026, an online presence of 6.12 billion people, with growth

* Author is a Research Scholar at University School of Law & Legal Studies, Guru Gobind Singh Indraprastha University, New Delhi, India.

in internet users over the preceding year of 59 million.¹ This rapid development in technology, namely the internet, has given rise to a new frontier for committing sexual violence.

The United Nations defines sexual violence as an actual or attempted act of a sexual nature against a person without that person's consent, through an abuse of power, vulnerability, or trust.² One form of sexual violence committed through technology is commonly known as technology-facilitated sexual violence and abuse. It encompasses any kind of sexual harassment, exploitation, or violence, and can include image-based sexual abuse, online sexual exploitation, the non-consensual sharing of sexual images, cyberstalking, and sextortion.³ It is an "act of violence perpetrated by one or more individuals, committed, assisted, aggravated and amplified, in part or fully, by the use of information and communication technologies or digital media against a person,"⁴ usually a woman.

The anonymity of the online sphere and the low probability of identification enable perpetrators to commit online sexual violence. These crimes are aggravated because the remnants of the incidents remain online in perpetuity, leading to long-term trauma, harm to reputation, and even continuous threats to the victim.

According to the Internet in India Report, 2025, active internet users in India reached 958 million, of whom 410 million belonged to urban India and 548 million to rural India.⁵ This increase, however, has not been accompanied by digital literacy in online safety, which makes online exploitation easier. This is reflected in an increase of 17.9% in the registration of cybercrime cases, from 86,420 in 2022 to 101,928 in 2024,⁶ of which the cases against women rose from 14,409 in 2022 to 48,475 in 2024.⁷

In the offline world, the criminality of sexual offences against women hinges upon the manifestation of consent, which may be defined as an informed, voluntary agreement, conveyed either by conduct or by words, to engage in a particular act.⁸ It is the essential ingredient

¹ Simon Kemp, *Digital 2026 Mid-Year Global Update Report*, DATAREPORTAL (Apr. 22, 2026), <https://datareportal.com/reports/digital-2026-global-overview-report>.

² UNITED NATIONS, *Glossary on Sexual Exploitation and Abuse* 8 (July 24, 2017).

³ Md Mamunur Rashid Sheikh & Michaela M. Rogers, *Technology-Facilitated Sexual Violence and Abuse in Low and Middle-Income Countries: A Scoping Review*, 25 TRAUMA VIOLENCE & ABUSE 1614 (2024).

⁴ *Technology-Facilitated Gender-Based Violence: A Growing Threat*, UNFPA, <https://www.unfpa.org/TFGBV> (last visited Feb. 18, 2026).

⁵ INTERNET & MOBILE ASS'N OF INDIA & KANTAR, *Internet in India 2025* 4 (2025).

⁶ NAT'L CRIME RECORDS BUREAU, *Crime in India 2024* (Ministry of Home Affairs 2026).

⁷ Anu Maria Francis, *Online Crimes Against Women in India: Deepfakes, Doxxing, and Digital Abuse*, THE NEW INDIAN EXPRESS (Oct. 23, 2025), <https://www.cppr.in/articles/deepfakes-doxxing-and-digital-abuse>.

⁸ The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India), § 63, expl. 2 ("Consent means an unequivocal voluntary agreement when the woman by words, gestures or any form of verbal or non-verbal communication, communicates willingness to participate in the specific sexual act.").

determining whether a sexual act is criminal. In cases of online sexual violence, however, consent becomes significantly more complex. The anonymity of the online sphere hinders any assessment of whether consent is ongoing and clear. For example, the sharing of an intimate image in a private conversation may have been consensual initially, but it can become a crime if one party shares it without the permission of the other. Furthermore, individuals may consent to the use of social media applications under societal pressure, without realising the potential repercussions. This necessitates a definition of consent specific to the online platform, one flexible enough to encompass the range of situations arising on social media. A further issue concerns the revocation of consent and its implications: whether already-shared content must be deleted, or whether revocation relates only to the denial of further sharing.

This intersection of online sexual violence and consent in India therefore poses a number of legal challenges. While emerging technology has provided unique opportunities for interconnection, it has also ushered in exploitation in which the concept of consent is undermined or overlooked. Further, the lack of laws protecting victims in the online sphere deters them from adequately seeking justice.

This paper attempts to understand the laws criminalising online sexual violence in India. It also aims to identify the shortcomings of Indian law in contrast with international standards. It further examines the difficulties in interpreting consent in the online sphere and proposes suggestions to reform the law to protect victims. The scope of this paper is limited to online sexual violence committed against women who are capable of giving valid consent.

II. UNDERSTANDING “SEXUAL VIOLENCE” VIS-À-VIS “CONSENT” IN THE ONLINE SPHERE

Sexual violence against women has been a pervasive part of society and, for the longest time, was limited to physical violence. As the internet expanded, however, sexual violence has migrated to the online sphere as well. A report to the Human Rights Council stated that the internet has become a facilitator of “diverse forms of violence against women, in the form of pornography, sexist games and breaches of privacy.”⁹ Online sexual violence may thus be understood as a form of sexual violence committed using the internet or technology. Owing to

⁹ Human Rights Council, *Report of the Working Group on the Issue of Discrimination Against Women in Law and in Practice*, U.N. Doc. A/HRC/23/50 (Apr. 19, 2013).

growing internet connectivity, the European Union has estimated that 1 in 10 women over the age of 15 have already faced some form of online violence.¹⁰

A. Defining Online Sexual Violence

Great disparity has persisted in the terminology used to refer to the various types of online violence against women and its manifestations, with constant variation among the expressions used by states, international agencies, NGOs, and academia.¹¹ It was the Association for Progressive Communications that first articulated what online violence against women meant, defining it as “acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of information and communication technologies (ICTs), such as mobile phones, the internet, social media platforms, and email.”¹² Globally, it has been accepted that technology is used as a mode for committing such violence. The term that became internationally accepted was “technology-facilitated gender-based violence,”¹³ or technology-facilitated sexual violence and abuse (hereinafter TFSVA). Yet definitional ambiguities relating to TFSVA persist,¹⁴ and different studies use different terms to describe similar forms of abuse falling under its umbrella.

B. Types of Technology-Facilitated Sexual Violence

TFSVA was further exacerbated by the increased digitisation that accompanied the COVID-19 pandemic, prompting research on the pandemic’s impact on TFSVA. One such study examined the experiences of women aged between 18 and 44 who were survivors of online violence during the pandemic.¹⁵ The analysis identified ten modes of online violence, as illustrated in Figure A.

¹⁰ *Cyber violence Against Women and Girls: The Growing Threat of the Digital Age*, UNRIC, <https://unric.org/en/cyber violence-against-women-and-girls-the-growing-threat-of-the-digital-age/> (last visited Feb. 22, 2026).

¹¹ Katya N. Vera Morales, *Online Gender-Based Violence Against Women and Girls: Practical Self-Protection Handbook*, ORG. OF AM. STATES, www.oas.org/en/sms/cicte/docs/Guide-basic-concepts-Online-gender-based-violence-against-women-and-girls.pdf (last visited Mar. 30, 2026).

¹² *Id.*

¹³ *FAQs: Digital Abuse, Trolling, Stalking, and Other Forms of Technology-Facilitated Violence Against Women*, UN WOMEN (2025), <https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women>.

¹⁴ *Supra* note 5.

¹⁵ Inês Amaral et al., *Online Violence Against Women: Reports from the COVID-19 Pandemic Experience*, 42 CRIME, JUSTICE & MEDIA 179 (2022).

Figure A: Modes of Online Violence

Source: Inês Amaral et al. (2022).

Of the ten types identified, only five are of a sexual nature, namely: stalking online, sexual abuse through images, cyber-flashing, sextortion, and image manipulation or deepfakes.¹⁶ These are discussed below.

Stalking online. Stalking online, also known as cyberstalking, is conduct by an individual to stalk a woman using technology. The perpetrator may communicate with the disinterested woman through messages, emails, or her social media accounts.¹⁷ There is often an intersection between online and offline stalking: either physical stalking leads to online stalking, or vice versa. There are also cases of online stalking in which there is no close proximity or prior connection between the perpetrator and the victim.

Sexual abuse through images. The phrase “revenge porn” was initially used but was soon rejected, as it limited the perpetrator’s motive to vengeance and minimised the crime by focusing on the victim’s tainted image.¹⁸ It failed to reflect that the act was a form of sexual abuse, implying instead a scorned lover sharing nudes on pornographic sites. This abuse is now referred to as image-based sexual abuse. It can include, but is not limited to, the consensual

¹⁶ *Id.*

¹⁷ Kushanthi Harasgama et al., *Formulating an Effective Law on Cyberstalking: A Comparative Legal Analysis*, 9 J. NAT’L L. UNIV. DELHI 75 (2023).

¹⁸ *Supra* note 11, at 50.

capturing of photographs or videos followed by their non-consensual dissemination, or the non-consensual capturing and dissemination of such visuals.¹⁹

Cyber-flashing. Cyber-flashing refers to a person sharing an unsolicited intimate image with another through messaging apps, emails, or social media platforms. This act is often treated as a subset of sexual abuse through images.²⁰ With the rampant increase in one-time-watch images and videos, it has become increasingly easy to commit.

Sextortion. Sexual extortion, or sextortion, is a form of coercion that entails threatening to share sexual images in order to pressure the victim into complying with demands. These demands may be financial, such as the payment of a ransom, while others are more insidious, seeking the victim's compliance in engaging in unwanted sexual acts or in sharing further intimate images.²¹

Image manipulation or deepfakes. This act involves using software to seamlessly swap one person's face with another to create pornographic photographs or videos for posting online. Because image manipulation and deepfakes are created using machine-learning techniques, it is significantly difficult to distinguish between real and fake content, given the uncanny similarity to the original.²² It also includes wholly manipulated visual or audio content that may portray a woman saying or doing something she has not said or done, using artificial intelligence.²³ Women are almost exclusively targeted, indicating that the risks associated with deepfakes have gender dimensions,²⁴ and, since most deepfakes involve intimate activity or sexual imagery, they are found on adult-entertainment websites.²⁵

Owing to the overlapping nature of these acts, they are often grouped under the umbrella term TFSVA. The fundamental issue lying at the heart of such online violation is that of consent. In the offline world, the presence of consent provides legitimacy to any sexual interaction between individuals. The online sphere, however, puts forth obstacles to the explanation, establishment, verification, and revocation of consent, potentially increasing the incidence of abuse.

C. Understanding Consent: Traditional v. Digital Context

¹⁹ *Supra* note 16, at 5.6.

²⁰ COUNCIL OF EUROPE, *General Recommendation No. 1 on the Digital Dimension of Violence Against Women*, GREVIO (Oct. 21, 2021).

²¹ Alana Ray & Nicola Henry, *Sextortion: A Scoping Review*, 26 TRAUMA, VIOLENCE, & ABUSE (2024).

²² *Supra* note 13, at 26.

²³ *Cyber Violence Against Women and Girls: Key Terms and Concepts*, EUROPEAN INST. FOR GENDER EQUALITY (2022), https://eige.europa.eu/sites/default/files/cyber_violence_against_women_and_girls_key_terms_and_concepts.pdf.

²⁴ Mariëtte van Huijstee et al., *Tackling Deepfakes in European Policy*, EUROPEAN PARLIAMENTARY RSCH. SERV. (2021).

²⁵ *Supra* note 23, at 50.

Consent is integral to any sexual interaction, online or offline, and so it is important to understand it. As noted above, in the traditional offline setting, consent is present when a person who is capable of consenting voluntarily allows, approves, or agrees either to do something or to abstain from doing something specific.²⁶ This specific nature of consent highlights how a person may consent to one thing but not another, for example, consenting to kissing but not to any subsequent sexual act. Consent is also reversible in nature, meaning it can be revoked for any future act, for example, consenting to a sexual act on one day but not on another.²⁷

In the online sphere, defining consent becomes challenging because of the smokescreen provided by the digital world. It is important to understand who is giving consent, how it is being given, what the person is consenting to, and the moment at which it ends. In the digital space, consent is the express agreement to engage in initiatives involving digital content,²⁸ including “the sharing, creation, and distribution of images, videos, and other forms of digital media.”²⁹ The essentials of consent in the digital sphere, with respect to its informed and voluntary nature and its revocation, may be presumed to be the same as those of consent in the offline world.

Having examined TFSVA and its different modes, and the nuances of consent in the offline and online contexts, it is necessary to examine how the Indian legal framework is designed to combat this emerging threat of online sexual violence.

III. OVERVIEW OF THE INDIAN STATUTORY FRAMEWORK VIS-À-VIS INTERNATIONAL LAW

Despite the clear surge in online sexual violence, India’s statutory framework offers very little recourse to victims. The Information Technology Act, 2000³⁰ (hereinafter IT Act) and the recently implemented Bharatiya Nyaya Sanhita, 2023³¹ (hereinafter BNS) still struggle to keep pace with evolving digital crimes. For instance, there is still no definition of emerging crimes such as image-based sexual abuse, online sexual harassment, or sextortion. Even where provisions exist criminalising the dissemination of private images or stalking, the law remains ill-equipped to handle the complexities of these crimes. Another issue is the lack of

²⁶ *Glossary: Consent*, THOMSON REUTERS PRACTICAL LAW, <https://uk.practicallaw.thomsonreuters.com/w-014-8172> (last visited Mar. 14, 2026).

²⁷ UN WOMEN, *When It Comes to Consent, There Are No Blurred Lines*, MEDIUM (Nov. 15, 2019), <https://un-women.medium.com/when-it-comes-to-consent-there-are-no-blurred-lines-1dfd02cebe10>.

²⁸ *Viewing Consent Through a Digital Lens*, EQUALITY NOW (Aug. 7, 2024), https://equalitynow.org/news_and_insights/viewing-consent-through-a-digital-lens/.

²⁹ *Id.*

³⁰ The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

³¹ The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).

understanding of the meaning of consent in the online sphere. Consent is the integral principle distinguishing acceptable from unacceptable sexual interaction; it is therefore important to begin with how India has viewed consent in relation to the law on sexual offences.

Originally, in India, consent was defined negatively, by laying down the factors that vitiated it, such as fear of injury or misconception of fact.³² This definition applied to all interactions under the Indian Penal Code, 1860, including sexual offences against women. The Criminal Law (Amendment) Act, 2013 then introduced an improved definition of consent, albeit only in cases of rape: consent must be an “unequivocal,” “voluntary” agreement conveying “willingness” to “participate” in a “specific” sexual act.³³ It is further imperative that consent be informed, clear, and communicated verbally or through gestures. In 2023, the BNS repealed and replaced the penal code. Although it carried forward both definitions of consent,³⁴ it remained silent on the role of consent in relation to emerging online sexual crimes against women.

Recently, the Digital Personal Data Protection Act (hereinafter DPDP Act) was introduced to protect individuals’ data and ensure privacy on the basis of the principle of consent.³⁵ The meaning of consent under this Act is quite similar to the traditional understanding of the term: digital consent is freely given and informed, without any conditions, and requires clear and affirmative action; however, it relates solely to the processing of personal data.³⁶ It is clear that, despite defining digital consent, this Act deals specifically with the sharing of personal information³⁷ and does not cover consent in the context of online sexual violence. The BNS, for its part, defines consent only in respect of offline interactions while remaining completely silent on digital consent. The IT Act, finally, was introduced to provide legal validity to transactions facilitated through electronic data interchange and other forms of electronic communication,

³² The Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860 (India), § 90 (“A consent is not such a consent as is intended by any section of this Code, if the consent is given by a person under fear of injury, or under a misconception of fact, and if the person doing the act knows, or has reason to believe, that the consent was given in consequence of such fear or misconception.”).

³³ *Id.* § 375, expl. 2 (“Consent means an unequivocal voluntary agreement when the woman by words, gestures or any form of verbal or non-verbal communication, communicates willingness to participate in the specific sexual act.”).

³⁴ *Union Home Minister Shri Amit Shah Introduces the Bharatiya Nyaya Sanhita Bill 2023, the Bharatiya Nagarik Suraksha Sanhita Bill 2023 and the Bharatiya Sakshya Bill 2023 in the Lok Sabha*, PRESS INFO. BUREAU (2023), <https://pib.gov.in/PressReleaseDetailm.aspx?PRID=1947941>.

³⁵ The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

³⁶ *Id.* § 6(1) (“The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose.”).

³⁷ *Yes Means Yes: Managing Consent Under India’s New Data Protection Law*, SNR LAW, <https://www.snrlaw.in/yes-means-yes-managing-consent-under-indias-new-data-protection-law/> (last visited Mar. 24, 2026).

superseding paper-based methods;³⁸ it merely lays down offences relating to cybercrime without explaining the role of consent. A bare perusal of the existing Indian laws therefore reveals a lack of explicit provisions defining consent in relation to online sexual offences.

Most modes of TFSVA have, directly or indirectly, been made punishable under Indian law, principally through the BNS and the IT Act. The IT Act, after its amendment in 2008, predominantly criminalises cybercrimes of a sexual nature against men and women. Some specific provisions are detailed below.

Section 66C³⁹ punishes identity theft, covering situations where a person dishonestly or fraudulently uses the unique identification features of another.

Section 66D⁴⁰ punishes the use of a communication device or computer resource to cheat by personation. Under the BNS, a person cheats by pretending to be another person, by knowingly substituting one person for another, or by representing himself or another as a different person.⁴¹ A combined reading can punish a perpetrator who gains access to images or video of a person and then manipulates and morphs them into sexually tainted images. A person committing the offence of image manipulation or creating deepfakes can therefore be charged under these sections, even though those explicit terms are not used.

Section 66E⁴² punishes any violation of privacy involving the capturing, publishing, or electronic sharing of images of an intimate nature of a person without their consent.

Sections 67 and 67A⁴³ punish the publication or transmission of obscene or sexually explicit material, which may cover the sharing of pornography online, including instances of “revenge porn” and “cyber-flashing.”

Section 72⁴⁴ penalises the breach of confidentiality and privacy where a perpetrator discloses to another any material gained or accessed without consent. Section 72 can be read together with other sections to bring within its scope the sharing of sexually explicit content procured non-consensually.

Section 79⁴⁵ makes intermediaries liable where they have in any way facilitated the commission of an unlawful act, whether by abetting, aiding, conspiring, or inducing. An intermediary is also

³⁸ *Supra* note 30; the Act is discussed in detail in a later section of this paper.

³⁹ *Supra* note 30, § 66C.

⁴⁰ *Supra* note 30, § 66D.

⁴¹ *Supra* note 31, § 319 (cheating by personation).

⁴² *Supra* note 30, § 66E.

⁴³ *Supra* note 30, §§ 67, 67A.

⁴⁴ *Supra* note 30, § 72.

⁴⁵ *Supra* note 30, § 79.

liable if, upon notification by the appropriate government, it fails swiftly to remove or disable access to material used to commit an unlawful act.

Recently, India took a significant step in its digital-governance framework by updating the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 on 10 February 2026.⁴⁶ These rules aim to bring the dissemination of AI-generated material online under strict control; they reduce takedown timelines, ensure technical traceability, and redefine intermediary obligations.⁴⁷ Some relevant rules are detailed below.

Rule 2(1)(wa) defines “synthetically generated information” as any audio, visual, or audio-visual information created, generated, modified, or altered artificially using a computer resource so as to be perceived as real or authentic.⁴⁸

Rule 3⁴⁹ creates a due-diligence obligation on social media intermediaries (hereinafter SMI). An SMI must ensure that its users do not use its platform to share objectionable information that is obscene, pornographic, or paedophilic. Where a user commits an offence punishable under any law, such as the POCSO Act,⁵⁰ the SMI must report the matter to the appropriate authorities, disable access to or remove the content, and suspend or terminate the user; such removal must occur within three hours of obtaining knowledge.

Rule 4(2)⁵¹ requires an SMI providing messaging services to identify the first originator of content on its computer resource for the purpose of preventing, detecting, investigating, prosecuting, or punishing an offence relating to rape, sexually explicit material, or child sexual abuse material.

The BNS is the principal substantive criminal law complementing the IT Act in protecting women from online sexual violence. Some specific provisions are detailed below.

Section 77⁵² criminalises voyeurism, which includes watching, capturing, or disseminating intimate images of a woman. Intimate images are those captured when the woman had a reasonable expectation of privacy, or when her sexual body parts were exposed or in

⁴⁶ The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India) (as amended Feb. 10, 2026) [hereinafter IT Rules].

⁴⁷ Aayushman Gaikwad & Smruti Mishra, *Three Hours to Comply: India's New Rules for AI-Generated Content and Deepfakes*, LIVE LAW (Feb. 21, 2026), <https://www.livelaw.in/articles/ai-generated-content-deepfakes-524064>.

⁴⁸ IT Rules, *supra* note 46, r. 2(1)(wa).

⁴⁹ *Id.* r. 3.

⁵⁰ The Protection of Children from Sexual Offences Act, 2012, No. 32, Acts of Parliament, 2012 (India).

⁵¹ IT Rules, *supra* note 46, r. 4(2).

⁵² *Supra* note 31, § 77.

undergarments, or when she was using a lavatory. Section 77 covers the consensual capturing but non-consensual dissemination of such images.

Section 78⁵³ criminalises cyberstalking as a subset of traditional stalking. It covers a situation in which a man, without justified reason, persistently follows or monitors the online activity of a woman despite her clear disinterest.

Section 308⁵⁴ criminalises inducing the delivery of property by putting a person in fear of injury. This section may therefore partially cover the offence of sextortion, where a person threatens to release sexual material if financial demands are not met.

It may thus be deduced that the provisions of the IT Act and the BNS show that India has a reasonably established law to combat online sexual violence against women. The concept of digital consent, however, is still missing from the legal framework, which makes it necessary to turn to the international legal frameworks governing online sexual violence to attempt to ascertain digital consent.

Turning to the international instruments, the Budapest Convention⁵⁵ was the first convention⁵⁶ enacted to fight crimes committed online. Although the Convention addresses certain violations committed using the internet or computer resources, it fails to bring online sexual violence within its purview.

The Council of Europe has sought to rectify that gap by adopting a directive on combating violence against women and domestic violence⁵⁷ to tackle violence against women and children. This directive makes it mandatory for member states to criminalise the intentional “non-consensual sharing of intimate or manipulated material,”⁵⁸ “cyber-stalking,”⁵⁹ and “cyber harassment.”⁶⁰ Article 5⁶¹ covers situations of sexual abuse through images, including the sharing of sexually tainted visuals without the person’s consent or the creation of deepfakes, for the purpose of ensuring the victim’s behavioural compliance. Article 6⁶² addresses the offence

⁵³ *Supra* note 31, § 78.

⁵⁴ *Supra* note 31, § 308.

⁵⁵ COUNCIL OF EUROPE, Convention on Cybercrime, E.T.S. No. 185 (opened for signature Nov. 23, 2001, entered into force July 1, 2004) [Budapest Convention].

⁵⁶ *The Budapest Convention and Related Standards*, COUNCIL OF EUROPE, <https://www.coe.int/en/web/cybercrime/the-budapest-convention-old> (last visited Mar. 27, 2026).

⁵⁷ Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on Combating Violence Against Women and Domestic Violence, 2024 O.J. (L 1385) 1.

⁵⁸ *Id.* art. 5.

⁵⁹ *Id.* art. 6.

⁶⁰ *Id.* art. 7.

⁶¹ *Supra* note 57, art. 5.

⁶² *Supra* note 57, art. 6.

of intentionally and repeatedly monitoring a person without their consent or legal authorisation. Article 7⁶³ addresses instances of sextortion and cyber-flashing, without using those specific terms. Throughout the directive, the lack of consent is stressed as an essential ingredient of these offences. Article 35⁶⁴ defines consent in sexual relationships as something voluntarily given as the result of a person's free will, yet it too fails to define consent specific to the digital sphere.

As for the United Nations, it has finalised the “first multi-lateral anti-crime treaty,”⁶⁵ namely the Convention against Cybercrime.⁶⁶ Only in 2024 was it adopted, and it is yet to enter into force. This convention⁶⁷ requires signatory states to criminalise online offences. Article 16 of the Convention⁶⁸ deals with the non-consensual sharing of intimate images, requiring member states to adopt domestic measures criminalising the “selling, distributing, transmitting, publishing or otherwise making available of an intimate image of a person by means of an information and communications technology system, without the consent of the person depicted in the image.”⁶⁹ It makes intention a necessity before criminal liability attaches, but fails to clarify what digital consent would mean. Were consent to be defined for online sexual violence, it could carry the same meaning as traditional consent, the only difference being that it is given electronically for a specific online activity.⁷⁰

It is clear that, despite the recent emergence of sexual violence against women in the online sphere, safeguards do exist to an extent. India has enacted law, through the amendment of the IT Act and the IT Rules, for the protection of women from online sexual violence, and the BNS contains some provisions to ensure their safety online. Internationally, organisations have produced instruments such as the Council of Europe's directive on combating violence against women and domestic violence, and the United Nations' Convention against Cybercrime. Challenges nevertheless remain in effectively addressing the menace of online sexual violence, primarily because of the lack of uniformity in the classification of these crimes.

⁶³ *Supra* note 57, art. 7.

⁶⁴ *Supra* note 57, art. 35 (“Specific measures to prevent rape and to promote the central role of consent in sexual relationships.”).

⁶⁵ *United Nations Convention Against Cybercrime: A Roadmap to Combatting Online Child Sexual Exploitation*, WEPROTECT GLOBAL ALLIANCE, <https://www.weprotect.org/blog/united-nations-convention-against-cybercrime-a-roadmap-to-combatting-online-child-sexual-exploitation/> (last visited Mar. 27, 2026).

⁶⁶ UNITED NATIONS, Convention Against Cybercrime, G.A. Res. 79/243, U.N. Doc. A/RES/79/243 (Dec. 24, 2024).

⁶⁷ *Id.*

⁶⁸ *Id.* art. 16.

⁶⁹ *Id.*

⁷⁰ *Practicing Digital Consent*, NAT'L SEXUAL VIOLENCE RES. CTR. (2022), <https://www.nsvrc.org/saam/2022/learn/practicingdigitalconsent>.

IV. ANALYSIS OF THE LIMITATIONS

After this overview of the domestic laws in contrast with the international instruments, it is clear that the groundwork to combat the menace of TFSVA has been laid. There remains a need to tackle online sexual violence against women more effectively, which makes it important to examine the challenges and to suggest a way forward. A comprehensive framework does exist for tackling many forms of sexual violence against women, but, when it comes to violence in the online sphere, India lacks a robust framework across its existing statutes.

Even though some provisions have been enacted in India, they provide only partial recourse, hinting vaguely at certain forms of online sexual violence. For instance, the recent amendment to the IT Rules defines a deepfake as synthetically generated information, yet does not make its creation a statutory offence; it currently takes a combined reading of Sections 66C⁷¹ and 66D⁷² to criminalise the creation of deepfakes indirectly.

Next, Section 66E⁷³ is very similar to Section 77⁷⁴ (which criminalises voyeurism), despite belonging to different statutes, one criminalising specific cybercrimes and the other a substantive criminal offence; the only distinguishing factor is that the latter also includes simply watching a woman performing a private act.

Sections 67 and 67A⁷⁵ may be used indirectly to include revenge porn or cyber-flashing within their scope, since they punish the transmission of sexually explicit material. Yet revenge porn, in common parlance, involves a scorned lover posting online the intimate images of a partner that were shared consensually, while cyber-flashing entails sharing unsolicited intimate content, whether of the perpetrator or of anyone else. It does not appear that Section 67A was enacted with a view to covering these specific online violations; it may rather have been intended to deter the posting or sharing of pornographic content online.

Section 72⁷⁶ penalises a government official who discloses an electronic record accessed without the consent of the person concerned. Read in the context of online sexual violence, it can criminalise a public officer who, by misuse of office, procures sexually tainted private material of an individual without consent and discloses it to the public. Section 79⁷⁷ revokes the exemption from liability granted to an SMI if it facilitates the hosting of unlawful content or

⁷¹ *Supra* note 39.

⁷² *Supra* note 40.

⁷³ *Supra* note 42.

⁷⁴ *Supra* note 52.

⁷⁵ *Supra* note 43.

⁷⁶ *Supra* note 44.

⁷⁷ *Supra* note 45.

fails to remove such content expeditiously; this section fixes liability without defining its contours. The recent amendments to the IT Rules have helped marginally by giving an expansive definition of synthetically generated images, or deepfakes, and by detailing certain due-diligence obligations of the SMI, but they remain largely silent on deterring a perpetrator from committing a criminal wrong.

Turning to the BNS, Section 78,⁷⁸ which criminalises stalking including cyberstalking, is not a law specific to online sexual violence. It is a subset of traditional stalking, which limits the situations of online stalking falling within its purview. It is also not clearly worded: the terms “repeatedly” and “monitoring the use” are imprecise. The first does not indicate how many instances of contacting the victim it takes to amount to contacting “repeatedly despite clear indication of disinterest by such woman,”⁷⁹ and the second does not delimit its scope, that is, whether it means merely observing the victim’s internet usage or requires active attempts to contact her despite her disinterest.

Section 308,⁸⁰ as worded, is meant solely for the criminalisation of extortion. There is no mention of sextortion in the provision, but, since it is the only provision in Indian law that comes close, there is no option but to fit this online violation partially within its scope under extortion, even though the purpose of sextortion is wider than the receipt of financial favours, which may also be sexual in nature. For instance, a man may capture a woman changing clothes in private and threaten to make the recording public, or to share it with her family, unless she engages in sexual intercourse with him.

This threadbare reading of the provisions reveals that the law in India is in dire need of reform to keep up with evolving online crimes. These crimes require strong deterrence because of their often-irreversible nature, a consequence of the permanence of the internet. Further, the complexity of enforcement is heightened by the fact that a perpetrator may be based anywhere in the world while targeting a victim.

Internationally, it is widely accepted that online sexual violence has increased rapidly and that the risk of facing this kind of violence is high.⁸¹ Yet, when it comes to technology-facilitated violence against women, there is plainly no international consensus on what acts fall under the umbrella of TFSVA. This lack of uniformity in international law breeds ambiguity in the

⁷⁸ *Supra* note 53.

⁷⁹ *Id.* § 78(1)(i).

⁸⁰ *Supra* note 54.

⁸¹ *Facts and Figures: Ending Violence Against Women*, UN WOMEN (2024), <https://www.unwomen.org/en/articles/facts-and-figures/facts-and-figures-ending-violence-against-women>.

domestic sphere as well, and makes a successful comparative analysis with other countries difficult. The issue of cross-border commission of online violence also persists. For instance, a perpetrator in Country A may threaten to leak sexually morphed images of a woman in Country B unless she sends her own intimate images. Prosecuting the perpetrator in this scenario raises multiple problems. First, the lack of uniformity in the laws of different countries may pose a hindrance: Country A may have a strict law on sextortion while Country B, like India, may not. Second, there is no international instrument with a proper definition of sextortion mandating member states to enact protective laws, so states may have no law to address the situation. Third, jurisdictional issues arise as to the place of the offence, that is, whether prosecution will proceed under the laws of Country A or Country B, and why Country A would seek to prosecute its own citizen. This calls for proper provisions criminalising these new offences across jurisdictions.

As to the fundamental issue behind this paper, namely making the digital sphere more accountable, this goal requires a detailed and unambiguous understanding of digital consent. To achieve it, an examination of the definitions of consent was required. The provisions of the BNS⁸² make it clear that they cover only traditional offences, including sexual offences committed against women. The DPDP Act,⁸³ despite defining digital consent, does not extend it to the context of online sexual violence. Even the international instruments fail to give a specific definition of digital consent, although the Council of Europe directive defines consent specifically in relation to rape.⁸⁴ Accordingly, both Indian domestic law and the international instruments have defined consent only in the context of traditional sexual violence, despite the statistics showing that such violence has migrated to the online sphere. What is missing is not only adequate legal safeguards for victims, but also digital literacy.

The statistics show that internet usage and sexual violence in the online sphere are both rising, yet little effort appears to have been made to create educational awareness to ensure the safety of victims. Any person using the internet to share images, whether publicly or with known persons, needs to be informed of the repercussions of such data-sharing. Many users are unaware of online abuse, or of the steps they can take if they fall prey to online sexual violence.⁸⁵

It may therefore be concluded that the legal inadequacies relate to a lack of specific offences criminalising online sexual violence, definitional ambiguities in the existing laws, and the

⁸² *Supra* note 8, §§ 28, 63 expl. 2.

⁸³ *Supra* note 35.

⁸⁴ *Supra* note 57.

⁸⁵ *Technology-Facilitated Sexual Violence*, SHANKAR IAS PARLIAMENT, <https://www.shankariasparliament.com/current-affairs/technology-facilitated-sexual-violence> (last visited Mar. 30, 2026).

absence of any provision detailing the role of consent in the digital sphere. These inadequacies contribute to gaps in the law and to its ineffective implementation.

V. RECOMMENDATIONS: THE WAY FORWARD

Combating online sexual violence requires a holistic approach incorporating legislative reform and awareness programmes. The foundation was laid in India in 2008 with the amendment to the IT Act, but technology and crime have both advanced since then. This section sets out recommendations that India might adopt to address the limitations identified above.

Since India already has the basic framework to tackle some sexually violent acts committed against women, what the country needs is a robust framework defining and punishing specific offences, for example, defining cyberstalking as a separate offence rather than a subset of stalking. The essential elements of the new offences must also be carefully worded so as to identify the *actus reus* that constitutes the perpetrator's conduct, for example, whether, in the case of cyberstalking, repeatedly sending friend requests despite rejection would fall within the offence, or whether the requirement is contacting or attempting to contact a woman by electronic means despite rejection, or whether rejection has no bearing on culpability. Similarly, the *mens rea* should be made wider in scope by extending it beyond intention to include knowledge.

Another key aspect that needs to be explained is digital consent. This can be done in one of two ways: either by adopting the existing definition of consent or by formulating a new one to keep pace with technological change. The standard of consent must also be set, and questions relating to the burden of proving consent should be addressed. Further, the law needs to be stricter where online sexual violence leads to physical sexual violence. Again taking cyberstalking as an example, a perpetrator who has been sending friend requests to a colleague, despite rejection, may threaten her with physical harm and then cause it. The law tackling these offences should be framed after proper deliberation, taking into account the role of intermediaries as well as users.

A recent positive step is the amendment of the IT Rules. SMI are now required to exercise due diligence in trying to identify deepfakes, to disable them expeditiously, and to remove reported content within three hours. These rules should be expanded to control the non-consensual sharing of intimate images of women, including the sharing of unsolicited sexually tainted visuals. After the amendment, SMI must disclose the identity of a user who posts questionable content using its computer resource, but that helps only after a wrongful act has been committed. It would be more conducive to regulate users before a wrongful act occurs. Identification should

therefore be made mandatory before signing up on social media platforms, email services, or other digital platforms, and existing users could be required to furnish identification in order to keep their accounts. In this way, crimes committed under the garb of anonymity would be reduced, as the perpetrator would become traceable.

The Government already operates a National Cyber Crime Reporting Portal⁸⁶ to enable citizens to report cybercrimes, but it can take initiatives to spread awareness about cybercrime and the steps a woman can take if she falls prey to it. Several studies suggest that law enforcement officers are not adequately trained to comprehend and implement these kinds of laws;⁸⁷ the Government can therefore take steps to provide sensitisation training. There is thus a need for legislators not only to incorporate such suggestions and draft amended law to suit the changing times, but also to reach the public through proactive measures.

VI. CONCLUSION

In light of the foregoing, it must be acknowledged that technological advancement has not been limited to positive opportunities for interconnection; it has also resulted in a rise in sexual violence against women in the online sphere. Such acts of violence are referred to as technology-facilitated sexual violence and abuse against women. Among the modes discussed are stalking online, sexual abuse through images, cyber-flashing, sextortion, and image manipulation or deepfakes. The key aspect of consent, which differentiates a positive sexual experience from sexual violence, has so far been defined only in the context of physical sexual violence.

Internationally, the Council of Europe and the United Nations have taken a strong stand against cybercrime by enacting conventions to combat it, but a uniform classification of crimes and a proper definition of digital consent are still missing. An in-depth analysis of the existing provisions in India leads to the conclusion that there is a lack of provisions to combat all kinds of emerging TFSVA, and that only partial recourse is currently available to victims. There is, therefore, a dire need for a comprehensive and robust statutory framework in India to tackle the menace of TFSVA in a targeted manner.

⁸⁶ MINISTRY OF ELECTRONICS & IT, *Taking Measures Against Online Pornography*, Gov't of India, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2113098> (last visited Mar. 31, 2026).

⁸⁷ Shalu Nigam, *Ending Online Violence Against Women in India: Calling for an Inclusive, Comprehensive, and Gender-Sensitive Law and Policy Framework*, IMPRI, <https://www.impriindia.com/insights/ending-online-violence-against-women/> (last visited Mar. 31, 2026).