

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 8 | Issue 1

2026

© 2026 International Journal of Legal Science and Innovation

Follow this and additional works at: <https://www.ijlsi.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 Legal Science and Innovation at VidhiAagaz. It has been accepted for inclusion in the International Journal of Legal Science and Innovation 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 Legal Science and Innovation**, kindly email your Manuscript to submission@ijlsi.com.

Sextortion Through Social Media: A Critical Legal Analysis of Women's Protection in India

AKANKSHA* AND DR. POONAM CHOUDHARY**

ABSTRACT

The rapid growth of social media has transformed communication and social interaction, but it has also created new possibilities for technology-enabled sexual violence. One of the newer forms of cyber abuse is sextortion, in which a perpetrator threatens to disclose, distribute or misuse intimate photographs, videos, messages or other sexually explicit content unless the victim meets demands for money, further sexual material, sexual favours or some other form of submission. Women are especially vulnerable, since the threatened leak of personal content may lead to social disapproval, reputational harm, psychological distress and financial loss. Social media aggravates the problem, because offenders can operate through fake accounts, anonymous users, temporary communication channels and rapid dissemination in order to target victims. Indian law does not yet define a single, comprehensive statutory offence of sextortion. Instead, various features of sextortion may be addressed through the provisions of the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 and other legislation. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 also impose due-diligence obligations on intermediaries and provide a means of responding to unlawful online content. This paper critically examines the legal protection available to women against sextortion through social media in India. It considers the constitutional rights to privacy, dignity and personal autonomy, the existing criminal and cyber-law framework, intermediary responsibility, investigation and digital evidence, and the practical realities faced by victims. It argues that the fragmented legal approach fails to capture the continuing, coercive and gendered character of sextortion. The paper recommends clearer statutory recognition of sextortion, greater platform accountability, swift removal of intimate content, specialised cyber investigation and protection of victim confidentiality.

Keywords: Sextortion, Social Media, Women, Cybercrime, Privacy, Digital Sexual Violence, Cyber Law

* Author is a Research Scholar at Department of Law, M.M.H. College, Ghaziabad, Uttar Pradesh, India.

** Author is an Assistant Professor at Department of Law, M.M.H. College, Ghaziabad, Uttar Pradesh, India.

I. INTRODUCTION

Digital technology has become an ordinary part of daily life. Social media has expanded the opportunities for communication, education, employment, entertainment and social interaction. Yet the same platforms have also become arenas in which people are harassed, stalked, sexually exploited, blackmailed and deprived of their privacy. The use of technology to perpetrate violence against women has become a particularly troubling phenomenon, because digital abuse can be carried out at a distance, anonymously and repeatedly.¹

One of the most severe forms of such online misconduct is sextortion. The term is used broadly to describe a situation in which a person threatens to expose or publish intimate content of another person in order to obtain money, further intimate content, sexual favours or compliance with some other demand. The perpetrator may possess genuine intimate photographs or videos, may have obtained them through deception, may have recorded online conversations without permission, may have gained access to an account, or may have taken existing photographs and manipulated them with digital tools. Artificial intelligence and deepfake technology have added a further dimension in recent years, since victims can now be threatened on the basis of fabricated sexual images even where no genuine intimate image exists.²

Social media provides a favourable environment for sextortion. A perpetrator need only approach a woman through Instagram, Facebook, WhatsApp, a dating application or any other messaging service, build a relationship or assume a false identity, and gradually obtain access to personal content. Once the material has been acquired, the threats may begin. The victim may be told that the content will be sent to family members, colleagues or friends, or published on the internet, unless she pays money or complies with the perpetrator's demands. The threats may continue even after the victim has paid.³

Sextortion is, however, different from ordinary financial cyber fraud. Monetary loss is not always its principal weapon; the victim's fear of humiliation, exclusion and loss of dignity is often sufficient. In the case of women, patriarchal social attitudes can heighten this vulnerability. Victims frequently do not report the offence, for fear of being blamed, because of family pressure or because of the reputational consequences. The true incidence of sextortion is therefore likely to be far greater than the reported cases suggest.

¹ PAVAN DUGGAL, CYBERLAW: THE INDIAN PERSPECTIVE 256 (Saakshar Law Publications 2002).

² NATIONAL CRIME AGENCY, *Financially Motivated Sexual Extortion (Sextortion)*, <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/kidnap-and-extortion/sextortion> (last visited Sept. 6, 2026).

³ Duggal, *supra* note 1, at 256.

The law must therefore move beyond a narrow conception of cybercrime. Sextortion combines questions of privacy, bodily autonomy, dignity, sexual exploitation, coercion and criminal intimidation, and, in some instances, extortion and the publication of sexually explicit content.

II. CONCEPT AND NATURE OF SEXTORTION THROUGH SOCIAL MEDIA

Sextortion is a form of coercive digital sexual abuse. Its defining characteristic is the use, or attempted use, of sexually intimate material to obtain something from the victim. The material may take the form of photographs, videos, screenshots, voice recordings, private communications or artificially generated images.

Sextortion on social media takes several forms. First, in relationship-based sextortion the perpetrator forms an online relationship with a woman and persuades her to share intimate material with him. When she attempts to end the relationship, he threatens to expose her.⁴

Second, financial sextortion involves demands for money. The perpetrator may threaten to publish the victim's intimate images, or to send them to her family, unless a sum of money is paid. Repeated demands may turn a single incident into continuing economic exploitation.⁵

Third, sexual sextortion is characterised by demands for further photographs, videos or sexual acts. A victim who gives in to the first demand is likely to be threatened repeatedly, since every new image becomes a further instrument of coercion.

Fourth, social media accounts, cloud storage or personal devices may be accessed without authorisation, giving rise to account-based sextortion. Stolen photographs and conversations then serve as the instrument of blackmail.

Fifth, deepfake sextortion involves sexual content that has been artificially created or altered. With the growing availability of artificial intelligence tools, it is possible to generate convincing images of a person without ever obtaining genuine intimate material. Even where the image is fake, the threat of its distribution can by itself be devastating.⁶

Sextortion carried out online has a particular persistence. Once intimate material has been uploaded or forwarded, it may be impossible to remove entirely. Screenshots, downloads and reposts may survive long after the original account has been deleted. The harm can therefore be perpetual.

⁴ Duggal, *supra* note 1, at 256.

⁵ NATIONAL CRIME AGENCY, *supra* note 2.

⁶ DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 14–16 (Harvard University Press 2014).

III. GENDERED IMPACT OF SEXTORTION ON WOMEN

Sextortion is not gender-neutral in its social consequences. The reputational and social impact may fall more heavily on women because of persisting stereotypes about female sexuality. A victim may fear rejection by her family, loss of employment, the breakdown of relationships or social ostracism.⁷

The psychological effects may also be significant. The victim may experience fear, anxiety, shame, helplessness and insecurity. The continuing threat that intimate material may be shared creates a form of permanent digital vulnerability. Unlike the victim of conventional harassment, she cannot know where the content has travelled or who has seen it.

Economic vulnerability is a further dimension. A victim may pay the offender in the hope that the threats will subside. Payment, however, tends to encourage further demands. Sextortion may thus operate as a chain of blackmail rather than a single offence.⁸

Justification of the offence by reference to the victim's conduct must not be accepted. Consent to the creation or private sharing of an intimate image is not consent to its further distribution. This distinction is especially important in legal proceedings, where victims may be unfairly questioned about their decision to share personal content.

IV. CONSTITUTIONAL DIMENSIONS OF PROTECTION

The Constitution of India supplies the broader normative framework within which women may be protected against digital sexual exploitation. Article 14 guarantees equality before the law and the equal protection of the laws, while Article 15 prohibits discrimination on specified grounds and permits special provision for women and children.⁹

Article 21 is of central importance, since judicial interpretation has developed the right to life and personal liberty to encompass dignity, privacy and personal autonomy. In *K.S. Puttaswamy v. Union of India*,¹⁰ the Supreme Court recognised privacy as a constitutionally protected right. The principle applies directly to sextortion, because the unauthorised sharing of intimate content is a serious intrusion into a person's private sphere.

In the online sphere, privacy cannot be equated with secrecy. It includes the ability to control personal information and the right to decide how intimate aspects of one's life are disclosed.

⁷ FLAVIA AGNES, LAW AND GENDER INEQUALITY: THE POLITICS OF WOMEN'S RIGHTS IN INDIA 1–8 (Oxford University Press 1999).

⁸ NATIONAL CRIME AGENCY, *supra* note 2.

⁹ INDIA CONST. arts. 14–15; M.P. JAIN, INDIAN CONSTITUTIONAL LAW 1057–66 (LexisNexis 8th ed. 2018).

¹⁰ *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).

When a perpetrator turns personal information into a weapon, the victim loses meaningful control over that information.

The dignity promised by the Constitution is equally crucial. Persistent sexual blackmail may diminish the victim's autonomy, since she remains under continuing threat. Sextortion should therefore be understood not merely as an offence concerning electronic content but as conduct capable of infringing dignity, autonomy and personal security.

V. EXISTING LEGAL FRAMEWORK IN INDIA

A. Information Technology Act, 2000

The principal statute dealing with the various forms of misconduct facilitated by technology is the Information Technology Act, 2000. It contains provisions that may apply depending on the facts of a sextortion case.¹¹

Section 66E deals with violation of privacy and punishes the intentional capturing, publishing or transmitting of an image of the private area of a person without his or her consent, in the circumstances set out in the section. Section 67 deals with the publication or transmission of obscene material in electronic form, while Section 67A deals with the publication or transmission of material containing a sexually explicit act in electronic form.¹²

These provisions may be important where the offender threatens to transmit, or actually transmits, intimate material. Nevertheless, they do not comprehensively capture the coercive element of sextortion. Depending on the circumstances, the offence may therefore have to be constructed by combining several provisions.

Sections 66C and 66D may also apply where identity theft or cheating by personation is involved. Section 67C deals with the preservation and retention of information by intermediaries, which may be a crucial source of evidence in a cybercrime investigation.¹³

B. Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023¹⁴ has replaced the Indian Penal Code and contains a series of provisions applicable to the conduct commonly associated with sextortion.

Voyeurism is addressed in Section 77. Notably, the statutory explanation recognises that where a person consents to the capture of an image but not to its dissemination to third parties, the

¹¹ Duggal, *supra* note 1, at 256–57.

¹² The Information Technology Act, No. 21 of 2000, INDIA CODE (2000), §§ 66E, 67, 67A.

¹³ The Information Technology Act, No. 21 of 2000, INDIA CODE (2000), §§ 66C, 66D, 67C.

¹⁴ The Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE (2023).

dissemination itself may constitute an offence. This distinction is directly relevant to the non-consensual sharing of intimate content.¹⁵

Section 78 covers stalking and specifically includes monitoring the use by a woman of the internet, e-mail or any other form of electronic communication. It is particularly relevant where an offender continually tracks or contacts a woman through online means.¹⁶

Section 79 deals with words, gestures or acts intended to insult the modesty of a woman, or with intrusion upon her privacy. This provision may also be applied to online sexual abuse in an appropriate case.¹⁷

Extortion is covered in Section 308. It applies where a person intentionally puts another in fear of injury and thereby dishonestly induces the person so put in fear to deliver property, a valuable security or anything signed or sealed that may be converted into a valuable security. Where intimate material is used to obtain money, the facts may therefore satisfy the requirements of extortion.¹⁸ Where no property is obtained, the threat itself may amount to criminal intimidation.¹⁹

The BNS thus offers a number of legal entry points, yet sextortion as a concept remains dispersed across several offences.

C. Information Technology Rules, 2021

The due-diligence obligations of intermediaries are laid down in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.²⁰ These obligations are significant because social media platforms are usually the first place where malicious intimate content appears.

The framework requires intermediaries to establish grievance redressal mechanisms and to meet specific obligations in respect of unlawful content. Government material also treats the IT Act and the IT Rules as a central element of the framework for regulating online content, including content relating to women.

Speed of response is critical for victims of sextortion. A slow removal process gives time for intimate content to be copied and redistributed. Rule 3(2)(b) accordingly requires an intermediary, on a complaint by the individual concerned, to remove or disable access to content

¹⁵ *Id.* § 77, Explanation 2.

¹⁶ *Id.* § 78(1)(ii).

¹⁷ *Id.* § 79.

¹⁸ *Id.* § 308.

¹⁹ *Id.* § 351 (criminal intimidation).

²⁰ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), r. 3 (India), <https://indiankanoon.org/doc/125230782/>.

that exposes the private area of that individual, shows nudity or a sexual act, or impersonates the individual, including through artificially morphed images, within a fixed time limit.²¹ Eventual removal can therefore be regarded as only one indicator of platform responsibility; the effectiveness and speed of grievance mechanisms matter as much.

VI. ROLE AND RESPONSIBILITY OF SOCIAL MEDIA PLATFORMS

Social media intermediaries play a pivotal role in ensuring that intimate material is not spread further. They possess technical capabilities that may not be available to individual victims or to local police, including the identification of accounts, preservation of metadata, content moderation, hash matching and the removal of reported content.

Significant social media intermediaries are subject to additional compliance requirements under the IT Rules. They must appoint designated officers, publish periodic compliance reports and assist the designated government agencies in the investigation and prevention of offences.²²

Platform responsibility nevertheless involves a difficult balance between privacy, freedom of expression and the capacity for content control. Automated systems cannot always read context or distinguish satire and consensual content from abuse. At the same time, over-reliance on automated systems may fail the victims whose intimate material requires urgent attention.

Automated detection should therefore be combined with human review that is straightforward and victim-centred. Platforms should offer simple reporting tools, preserve relevant evidence once a complaint is made, and ensure that a victim is not required to recount a traumatic experience before several different departments.

VII. INVESTIGATION AND ELECTRONIC EVIDENCE

Sextortion cases are very difficult to investigate. Offenders frequently use fake accounts, virtual numbers, temporary e-mail addresses, VPN services and multiple social media profiles. They may delete messages or accounts once money or sexual content has been obtained.

Electronic evidence may include screenshots, chat histories, e-mail headers, URLs, account details, payment records, device data, metadata and platform records. Victims should preserve relevant evidence rather than deleting threatening messages at the first instance. At the same time, victims cannot be expected to carry out technically complex forensic processes themselves.

²¹ IT Rules, 2021, *supra* note 20, r. 3(2)(b). The Rules as notified prescribed twenty-four hours; the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (Feb. 10, 2026), reduced the period to two hours with effect from Feb. 20, 2026.

²² IT Rules, 2021, *supra* note 20, r. 4(1)(a)–(d), <https://indiankanoon.org/doc/115512526/>.

Law enforcement agencies likewise need specialised cyber-forensic capability. An investigation may involve coordination between the local police, cybercrime units, banks, telecommunications providers and social media companies. Cross-border cases raise further difficulties, since the offender or the platform may be located outside India.

Under the new criminal-law regime, the procedure for investigation and prosecution is laid down in the *Bharatiya Nagarik Suraksha Sanhita*, 2023.²³ Effective enforcement of the substantive cybercrime provisions depends in turn on timely investigation and proper handling of electronic evidence.

VIII. MAJOR LEGAL AND PRACTICAL GAPS

The first significant gap is the absence of a specific statutory offence of sextortion. The provisions currently available penalise various elements of the conduct but fail to reflect the full spectrum of sexual coercion, threats and digital dissemination.

Second, the law does not adequately recognise the different forms of sextortion. Financial sextortion, sexual coercion, relationship-based blackmail and deepfake sextortion may involve different harms and different evidentiary needs.

Third, victims often struggle to have content removed quickly. Once an intimate image has been forwarded, the legal remedy may arrive only after the damage has been done.

Fourth, anonymity creates investigative problems. Fake profiles and platforms based overseas can delay the apprehension of offenders.

Fifth, social stigma discourages reporting. Women may fear that the police, family members or society will condemn them for having shared an intimate photograph. Such victim-blaming undermines the protective purpose of the law.

Sixth, digital evidence is extremely volatile. Messages can be erased, accounts deleted and content edited. Delay in reporting or in the preservation of evidence can therefore undermine prosecution.

Finally, emerging technologies raise new legal issues. AI-generated sexual images can be used to intimidate women without any genuine intimate content ever having been created. Conventional laws focused on the publication of real content may not adequately address the harms caused by fabricated material.

²³ The *Bharatiya Nagarik Suraksha Sanhita*, No. 46 of 2023, INDIA CODE (2023).

IX. SUGGESTIONS FOR LEGAL REFORM

First, Indian law should consider adopting a specific statutory definition of sextortion. It should cover threats to release genuine or fabricated intimate content in order to obtain money, sexual content or sexual acts, or otherwise to coerce the victim.

Second, the legislation must recognise that consent to dissemination is not given merely because consent to the creation or private sharing of intimate material was given. This principle should be clearly integrated into the legal framework and consistently applied in investigation and trial.

Third, specialised cybercrime units should receive gender-sensitive training. Police officers need to understand the psychological dimension of sextortion and must not engage in victim-blaming.

Fourth, platforms need to introduce faster procedures for removing reported intimate content. Victims should be able to report non-consensual intimate material easily, without navigating complex processes.

Fifth, mechanisms for the preservation of evidence must be strengthened. Platforms should retain relevant data once served with a lawful request from investigating authorities, subject to appropriate privacy and procedural safeguards.

Sixth, victims should be afforded confidentiality and legal support. So far as the law allows, the identity and intimate content of the victim must be protected at every stage of investigation and trial.

Seventh, India needs to strengthen cooperation among cybercrime police, social media companies, financial institutions and digital forensic laboratories. Sextortion cases are frequently transnational in character.

Eighth, women and young internet users must be educated about online grooming, privacy settings, safe sharing, fake profiles and reporting mechanisms through awareness programmes. Awareness, however, must never become a substitute for legal accountability. Accountability must rest with the offender alone.

X. CONCLUSION

Sextortion through social media is a pressing contemporary issue in the protection of women's rights in India. It combines sexual exploitation, cyber harassment, violation of privacy, coercion and intimidation, and, in the appropriate case, extortion. The rapid and potentially permanent spread of intimate content makes digital sextortion especially harmful.

Indian law does contain a number of provisions that can be applied to different aspects of sextortion. The Information Technology Act, 2000 covers violation of privacy and the electronic transmission of obscene and sexually explicit material, and the Bharatiya Nyaya Sanhita, 2023 covers stalking, voyeurism, intrusion upon privacy, extortion and related offences. The IT Rules, 2021 also set out the framework for intermediary responsibility and grievance redressal.

The current framework nevertheless remains fragmented. A victim may have to rely on several provisions to address a single continuing course of conduct. Such fragmentation complicates classification, investigation and prosecution. More importantly, it may fail to capture what is distinctive about sextortion, namely its coercive character.

The future legal framework should therefore adopt a victim-centred and technology-sensitive approach. Meaningful protection will require clearer statutory recognition, faster removal of intimate content, effective platform accountability, specialised investigation, preservation of electronic evidence and confidentiality for victims. The development and interpretation of the law should be guided by the constitutional values of privacy, dignity, equality and personal autonomy.

Finally, criminal punishment alone cannot secure effective protection against sextortion. What is needed is a concerted effort by legislatures, courts, police, cyber-forensic agencies, social media platforms and civil society. That effort must be directed towards creating a digital space in which women can exercise their rights to communication and participation online without being sexually coerced, blackmailed or forced to defend their dignity under threat.
