



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution- Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

Weaponizing Intimacy: Sextortion, Statutory Fragmentation, and the Case for a Dedicated Offence under India's New Criminal Code

~Tanya Kumari

Abstract

Sextortion, the use of real, threatened, or fabricated intimate imagery to coerce a victim into paying money, performing sexual acts, providing further content, or remaining silent, has grown from an occasional interpersonal offence into an industrialised form of transnational cybercrime. In spite of its scale and its documented psychological toll, no jurisdiction, including India, has yet enacted a comprehensive standalone sextortion statute. This article examines the doctrinal architecture that India currently uses to prosecute sextortion, principally section 308 of the Bharatiya Nyaya Sanhita, 2023, together with the Information Technology Act, 2000, and, where minors are involved, the Protection of Children from Sexual Offences Act, 2012 and argues that the retention of a property-based definition of extortion, combined with the gender-specific drafting of related sexual-offence provisions, leaves a structural gap that neither prosecutorial ingenuity nor judicial interpretation can reliably close. Drawing on comparative developments in the United Kingdom, the United States, Canada, Australia, and South Africa, and on recent Indian judicial pronouncements including Soukin v. State, the article intends to argue for a dedicated, gender-neutral sextortion offence, evidentiary reform to accommodate victim-produced digital evidence, and institutional capacity to match the offence's transnational, technology-mediated character.

1. Introduction

Digital connectivity has reorganised both ordinary life and criminal opportunity. Global cybercrime costs were projected to reach roughly USD 10.5 trillion annually by 2025, a threefold rise from 2015 and a sum equivalent to roughly a tenth of global GDP.¹ India's own experience illustrates the pace of change: the country's internet user base grew nearly fourfold in a decade, from about twenty-five crore users in 2014 to over ninety-six crore by late 2024,² while registered cybercrime cases quadrupled over roughly the same period and financial losses attributed to cyber fraud reached tens of thousands of crores of rupees in a single year.³ Within this expanding landscape of digital criminality, sextortion has emerged as one of the most psychologically damaging offence types, precisely because it weaponizes shame and the permanence of digital content rather than merely extracting money.⁴

Cross-national research puts the scale of the problem into sharper relief. A ten-country study of more than 16,000 respondents found that roughly one in seven adolescents and young adults had experienced sextortion, and a 2025 national survey in the United States found that one in five teenagers had been targeted. The introduction of generative artificial intelligence has further widened the pool of potential victims: an offender no longer needs to obtain genuine intimate material, since a convincing fabricated image can now be produced from an ordinary public photograph. In India, the problem is compounded by organized, quasi-industrial criminal networks operating from identifiable domestic hubs and by social norms of honour and shame that both intensify the coercive power of the threat and suppress reporting.

Despite a decade of scholarly and institutional attention, the term "sextortion" appears in no Indian statute of general application, and no jurisdiction anywhere has enacted a fully comprehensive, standalone sextortion law. This article examines why that gap persists in India specifically, notwithstanding the country's most sweeping criminal-law reform since independence the 2023-24 replacement of the Indian Penal Code, the Code of Criminal Procedure, and the Indian Evidence

¹Cybersecurity Ventures, "2024 Official Cybercrime Report" (2024), estimating global cybercrime costs at USD 10.5 trillion annually by 2025.

²Press Information Bureau, "Ten Years of Digital Progress: Building an Inclusive and Future-Ready India" (2025), on the growth of India's internet user base.

³National Crime Records Bureau, Crime in India 2023: Statistics (Ministry of Home Affairs, 2024).

⁴Indian Cyber Crime Coordination Centre, "Annual Report 2024" (Ministry of Home Affairs, 2025).

Act by the Bharatiya Nyaya Sanhita, the Bharatiya Nagarik Suraksha Sanhita, and the Bharatiya Sakshya Adhiniyam and considers what a workable legislative response might look like.

2. What Is Sextortion? Toward a Working Definition

The term "sextortion" was popularised in its cyber enabled form by a 2016 Brookings Institution study, which analysed federal prosecutions to identify the offence's distinctive features-digital communication, the leveraging of intimate imagery, and coercive demands for further content or compliance rather than only money.⁵ The concept nonetheless predates the digital variant: the International Association of Women Judges and, later, Transparency International had already used the term to describe the extraction of sexual favours by persons in positions of institutional power, an authority-based form of corruption distinct from, if related to, the cyber-mediated offence now more commonly encountered.

Sextortion is best understood as a composite offence rather than a single legal wrong. It combines a threat or coercive demand, a sexualised object of that threat whether authentic, obtained without consent, or synthetically generated, a demanded outcome that may be financial, sexual, or simply silence, and an information-technology vector that enables anonymity, scale, and cross-border reach. This composite character is precisely what makes the offence difficult to prosecute under any single existing statutory category it is not simply extortion, because the demand is frequently sexual rather than pecuniary; it is not simply image-based sexual abuse, because dissemination is typically the threat rather than the objective; and it is not simply cyberstalking, because the coercive leverage is tied to a specific piece of content rather than a pattern of surveillance.

3. The Victimological Picture

Sextortion does not distribute its harm evenly. The available evidence suggests a genuinely bidirectional pattern of targeting: adolescent and young adult males are disproportionately targeted for financially motivated sextortion, often by organised networks posing as young women on social media, while women more often face compliance-based coercion involving demands for further sexual content or acts, and LGBTQ+ individuals confront a compounded vulnerability

⁵Benjamin Wittes and others, "Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault" (Brookings Institution, 2016).

across both patterns, frequently intersecting with the additional threat of being outed to family or community.⁶ The Federal Bureau of Investigation documented over 16,000 sextortion complaints in a single year with tens of millions of dollars in direct losses, while acknowledging that the true scale of victimisation is substantially underreported.⁷

The psychological toll documented in the literature is severe and, in several respects, comparable to that produced by contact sexual offences: depression, anxiety, post-traumatic stress disorder, self-harm, and suicidal ideation recur across the available studies, with self-harm rates markedly elevated among LGBTQ+ youth. In India, this harm is compounded by deeply rooted norms of honour and shame around sexual conduct, which both magnify the coercive power of a threat to disseminate intimate material and discourage victims, particularly, though not only, male victims of financially motivated schemes from reporting at all. Underreporting of this magnitude renders official criminal statistics a significant underestimate of the true prevalence of the offence, a problem compounded by the fact that India's National Crime Records Bureau does not maintain any dedicated sextortion category within its annual statistical returns, leaving the offence effectively invisible in the country's principal crime-data infrastructure.

4. India's Patchwork Statute Book

In the absence of a dedicated offence, an Indian prosecutor must assemble a sextortion case from several statutes simultaneously. Section 308 of the Bharatiya Nyaya Sanhita, 2023, the successor to section 384 of the former Indian Penal Code, defines extortion around the "delivery of property or valuable security" language carried over largely unchanged from the colonial-era code.⁸ This creates an immediate and fundamental difficulty in the very cases that dominate the sextortion caseload: where the demand is for sexual compliance, for further intimate content, or simply for the victim's silence, no property changes hands, and the offence may fall outside the section's literal terms altogether. Prosecutors must therefore supplement the extortion charge with provisions of the Information Technology Act, 2000, sections 66C and 66D on identity theft and cheating by personation, section 66E on violation of privacy, and sections 67 and 67A on the publication or

⁶Federal Bureau of Investigation, Internet Crime Complaint Center, Annual Report 2021 (FBI, 2022).

⁸The Bharatiya Nyaya Sanhita 2023, s 308, corresponding to s 384 of the Indian Penal Code 1860; PRS Legislative Research, "Note on the Bharatiya Nyaya Sanhita, 2023" (2023).

transmission of obscene and sexually explicit material.⁹ Where the victim is a minor, sections 11, 13, 14 and 15 of the Protection of Children from Sexual Offences Act, 2012, on sexual harassment and the use of a child for pornographic purposes come into play as well,¹⁰ and where the case involves the misuse of personal data, the Digital Personal Data Protection Act, 2023, offers erasure and grievance-redressal rights that remain largely untested in this context.¹¹

A second doctrinal gap concerns gender. Several of the sexual-offence provisions most relevant to sextortion, sexual harassment, voyeurism, stalking, and insulting the modesty of a woman are drafted to protect only female victims, even though the empirical evidence on financially motivated sextortion consistently shows that adolescent and young adult males make up the larger share of that particular victim pool.¹² A male victim coerced through a fabricated intimate image can generally be protected only through the extortion and information-technology provisions, not through the sexual-offence provisions that would more accurately capture the nature of the violation, and non-binary victims are left with even less textual purchase in the statute book. This patchwork of overlapping, partially applicable provision produces exactly the kind of inconsistency across courts and states that a composite offence, by definition, should not be left to generate.

5. Courts as Reluctant Legislators

In the absence of legislative action, Indian courts have begun to develop a distinctly sextortion-aware jurisprudence, albeit through the comparatively narrow procedural window of bail applications rather than through any authoritative statement on the offence itself. The most significant judicial statement to date comes from the Delhi High Court in *Soukin v State*, which denied anticipatory bail to three men accused of running a sextortion racket that recorded victims on video calls and then extorted money under threat of publication.¹³ The court described sextortion as "a profound violation of privacy" and "a significant social menace," characterising it

⁹The Information Technology Act 2000, ss 66C, 66D, 66E, 67, 67A.

¹⁰The Protection of Children from Sexual Offences Act 2012, ss 11, 13, 14, 15.

¹¹The Digital Personal Data Protection Act 2023; Digital Personal Data Protection Rules 2025 (notified 13 November 2025).

¹²The Bharatiya Nyaya Sanhita 2023, ss 75 (sexual harassment), 77 (voyeurism), 78 (stalking), 79 (word, gesture or act intended to insult the modesty of a woman).

¹³*Soukin v State* (NCT of Delhi) 2024 SCC OnLine Del 2986 (Amit Mahajan J, 24 April 2024).

as a cyber-enabled offence whose clandestine and cross-jurisdictional character poses distinct challenges for law enforcement, and it treated the scale and organisation revealed by the investigation as sufficient reason to deny pre-arrest bail notwithstanding the ordinarily exceptional nature of that remedy.¹⁴ The constitutional scaffolding for this kind of rights-based reasoning was laid several years earlier in *Justice K S Puttaswamy v. Union of India*, which recognised privacy as a fundamental right under Article 21 and thereby gave Indian courts a doctrinal vocabulary for treating the non-consensual circulation, or threatened circulation, of intimate images as a constitutional harm and not merely a property or reputational one.¹⁵

What this body of case law demonstrates is real judicial willingness to name sextortion as a distinct and serious social harm. What it cannot supply, however, is the doctrinal precision that only legislation can provide, no binding Supreme Court judgment yet treats sextortion as a defined offence category, trial-court decisions where the great majority of sextortion prosecutions are actually resolved remain largely unreported, and lower courts are left to navigate the underlying statutory fragmentation described above without authoritative guidance. Judicial creativity has, in short, done real work in this field, but it is not a substitute for coherent statutory design.

6. Comparative Perspectives

No jurisdiction surveyed for this article has yet enacted a fully comprehensive standalone sextortion statute, but several have moved further than India toward closing the doctrinal gap. The United Kingdom's Online Safety Act 2023 inserted new provisions into the Sexual Offences Act 2003 criminalising both the sharing and the threatening to share of intimate images, sidestepping the property-based framing that constrains the Indian extortion provision by locating the wrong in the image-based conduct itself rather than in any pecuniary demand.¹⁶ In the United States, the federal TAKE IT DOWN Act, signed into law in May 2025 with near-unanimous bipartisan support, created the first federal criminal offence targeting the knowing publication or threatened publication of non-consensual intimate imagery expressly including AI-generated deepfakes and required covered platforms to remove reported material within forty-eight hours of a verified

¹⁴*Ibid*, describing sextortion as "a profound violation of privacy" and "a significant social menace" involving the exploitation of intimate images to extort money or favours, and noting its clandestine and cross-jurisdictional character.

¹⁵*Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.

¹⁶Online Safety Act 2023 (UK), ss 66B-66D, inserted into the Sexual Offences Act 2003.

victim request, with enforcement vested in the Federal Trade Commission.¹⁷ Canada has instead relied on a broadly worded non-consensual distribution offence inserted into its Criminal Code in 2014, judicially interpreted to encompass sextortion without a separately named offence,¹⁸ while Australia's regulatory innovation lies less in the criminal law than in the institutional architecture of its eSafety Commissioner, an independent statutory office with complaint-handling, takedown, and systemic-investigation powers that operates alongside, rather than instead of, ordinary criminal prosecution.¹⁹ South Africa's Cybercrimes Act 2020 contains a specific intimate-image disclosure offence,²⁰ and the European Union's AI Act now imposes transparency obligations on deepfake content as part of a broader regulatory response to synthetic media.²¹

At the international level, neither the twenty-year-old Budapest Convention on Cybercrime nor the newly adopted United Nations Convention against Cybercrime contains a sextortion-specific provision, and India remains outside the Budapest framework altogether, relying instead on bilateral mutual legal assistance arrangements that are typically slower and less standardised than multilateral cooperation mechanisms would allow.²² The comparative picture that emerges is one of convergent concern but divergent technique: some jurisdictions have named the offence directly, others have widened existing offences to capture it, and virtually all have supplemented criminal law with a regulatory or platform-accountability layer that Indian law currently lacks entirely.

7. Toward Reform: A Dedicated Offence and Its Limits

The most direct response to the doctrinal gap identified above would be a dedicated, gender-neutral sextortion offence inserted into the Bharatiya Nyaya Sanhita, defined independently of the delivery of property and capable of capturing demands for sexual compliance, further intimate material, or simple silence, whether the underlying image is genuine, obtained without consent, or synthetically

¹⁷Take It Down Act, Public Law 119-2 (US), signed into law 19 May 2025; codified as the Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act.

¹⁸Criminal Code (Canada), s 162.1 (non-consensual distribution of intimate images, enacted 2014).

¹⁹Enhancing Online Safety Act 2015 (Australia), establishing the office of the eSafety Commissioner.

²⁰Cybercrimes Act 19 of 2020 (South Africa).

²¹Regulation (EU) 2024/1689 (EU Artificial Intelligence Act), art 50 (transparency obligations for deepfake content).

²²Convention on Cybercrime (Budapest Convention), ETS No 185 (2001); United Nations Convention against Cybercrime (adopted 24 December 2024, opened for signature October 2025). India has not ratified the Budapest Convention.

generated, with aggravated categories for child victims, organised criminal networks, and offenders in a position of trust, and an explicit link to the abetment-of-suicide provision where the offence has driven a victim to take their own life.²³ Complementary reforms would extend to the Information Technology Act, which currently has no provision specifically addressing deepfake-generated sexual content, and to the evidentiary regime under the Bharatiya Sakshya Adhiniyam, whose certificate requirement for electronic records imposes a formidable, arguably disproportionate, burden on victims attempting to produce screenshots, chat logs, or call recordings as evidence of their own victimisation.²⁴ Institutionally, a dedicated National Crime Records Bureau reporting category for sextortion, and an Indian equivalent of the Australian eSafety Commissioner combining complaints-handling, takedown authority, and platform oversight, would together begin to close the gap between the scale of the problem and the state's present capacity to measure or respond to it.²⁵

None of this, however, should be mistaken for a complete solution. India's cybercrime conviction rate stands at roughly 1.6 per cent, and only around 2.4 per cent of cybercrime complaints are converted into a registered First Information Report at all, figures that reflect an enforcement and forensic capacity deficit no amount of statutory redrafting can, by itself, correct.²⁶ A new offence with a clean definition still depends on police officers trained to recognise it, forensic laboratories equipped to authenticate AI-generated content, and prosecutors and judges familiar with its elements; legislative reform is a necessary but not sufficient condition for a functioning response, and the Digital Personal Data Protection Rules, notified only in November 2025, illustrate how long the gap between a statute's enactment and its practical operation can run in the Indian system.²⁷

8. Conclusion

²³Rawat (n 1), ch 7, proposing a new s 308A of the Bharatiya Nyaya Sanhita defining sextortion independently of the delivery of property, with aggravated categories for child victims, organised networks, abuse of position of trust, and offences resulting in suicide.

²⁴Rawat (n 1), ch 7, proposing amendments to s 63 of the Bharatiya Sakshya Adhiniyam 2023 to relax the certificate requirement for victim-produced electronic evidence in sextortion cases.

²⁵Rawat (n 1), ch 7, proposing a dedicated National Crime Records Bureau reporting category for sextortion and an Indian eSafety Commissioner modelled on the Australian office.

²⁶Rawat (n 1), ch 4 and ch 7, citing India's cybercrime conviction rate of approximately 1.6 per cent and an FIR-conversion rate of approximately 2.43 per cent for cybercrime complaints.

²⁷Digital Personal Data Protection Rules 2025 (notified 13 November 2025).

Sextortion sits at an uncomfortable intersection of extortion, sexual exploitation, privacy violation, and organised cybercrime, and its composite character is precisely what allows it to fall between the cracks of statutes drafted for narrower, more conventional wrongs. India's 2023-24 criminal-law overhaul modernised much of the surrounding procedural architecture, but it did not resolve the property-based definition of extortion or the gender-specific drafting of the sexual-offence provisions most relevant to this crime, leaving courts such as the Delhi High Court in *Soukin v State* to name the harm in the language of privacy and dignity without the benefit of a statute that names it directly. The comparative experience of the United Kingdom, the United States, and other jurisdictions shows that a dedicated legislative response is both technically feasible and increasingly the international norm, even if no jurisdiction has yet perfected it. For India, the more durable lesson may be the familiar one legislative precision matters, but it must be accompanied by the forensic, institutional, and prosecutorial capacity to make a new offence more than a name on the statute book.