Journal of Contemporary Law and Society, *Volume 2, Issue 2, June 2025, pp. 63-67*

TECHNICAL ARTICLE
Online ISSN: 3139-1079
Doi: 10.18311/JCLS/2025/V2i2/51505

Online ISSN : XXXX-XXXX

Journal of Contemporary Law and Society

Contents available at: *www.informaticsjournals.co.in/index.php/jcls*

JCLS

Legal Aspects of Sextortion: Challenges and Responses in the Digital Age

Debdatta Das[1*] and Ekata Mukherjee[1,2]

[1]Department of Law, University of Burdwan, Bardhaman – 713104, West Bengal, India; d.debdatta@gmail.com

[2]Assistant Professor, Techno India University, Kolkata – 700091, West Bengal, India; ekatamukherjee2@gmail.com

Abstract

Sextortion, a portmanteau of "sex" and "extortion," has emerged as a pervasive cybercrime in the digital age, exploiting vulnerabilities in online interactions to coerce victims into providing sexual favours, explicit content, or money under the threat of public exposure. In India, the absence of a specific legal framework to address sextortion has left victims grappling with inadequate recourse, compounded by societal stigma and patriarchal attitudes. This paper examines sextortion as a modern-day menace, analysing its manifestations in India, the applicable legal provisions, landmark cases, and comparative perspectives from international jurisdictions. It also explores relevant international conventions and advocates for legislative reform to combat this growing threat effectively.

Keywords: *Cybercrime, Cybercrime Victim, Dark Web, Revenge Porn, Sextortion*

1.0 Introduction

Sextortion, a term blending "sex" and "extortion," encapsulates a sinister form of coercion where perpetrators exploit victims by threatening to release intimate images, videos, or information unless demands, often sexual favours, explicit content, or money, are met. This crime has surged in the digital era, fueled by the proliferation of smartphones, social media, and encrypted communication platforms. The Federal Bureau of Investigation (FBI) reported over 26,000 sextortion complaints in 2023, a stark rise from previous years. This has underscored its growing menace. In India, the National Crime Records Bureau (NCRB) noted a significant uptick in cybercrimes against women, with sextortion cases often unreported due to stigma (Manral & Sinha, 2023).

Globally, sextortion manifests in two primary forms: abuse of power by authority figures (*e.g.*, officials demanding sexual favours) and digital blackmail using compromising material (Ray & Henry, 2024). In India, both forms are evident, with cases ranging from workplace exploitation to online scams orchestrated by organised crime syndicates in states like Rajasthan and Haryana (Yadav, 2022). The digital landscape amplifies sextortion's reach, enabling perpetrators to target victims across borders anonymously. Victims, often women and minors, suffer profound psychological trauma, exacerbated by societal judgment, which deters reporting (Beauchere, 2023). In India, the COVID-19 lockdown saw a doubling of sextortion complaints to the National Commission for Women (NCW), highlighting its escalation during periods of heightened online activity (The Swaddle, 2020).

The legal response to sextortion varies widely. While some nations have specific statutes, others, including India, rely on existing laws ill-suited to its gradations. The purpose of this paper is threefold:

(i) to define sextortion's legal scope,

(ii) to analyse prosecution challenges, and

*Author for correspondence

(iii) to propose reforms, with a particular lens on India's position.

India's legal framework, rooted in colonial-era laws such as the Indian Penal Code (IPC) of 1860, has struggled to address this modern crime, despite recent updates like the Bharatiya Nyaya Sanhita (BNS) of 2023. By exploring these dimensions, the paper seeks to advocate for a robust, victim-centric legal approach to combat sextortion in the digital age.

2.0 Sextortion as a Crime: Legal Definitions and Scope

Sextortion is a hybrid offence, merging elements of extortion and sexual exploitation. It typically involves non-consensual acquisition or threatened dissemination of intimate content, often obtained through hacking, coercion, or trust breaches in relationships. Globally, its legal definition varies. In the United States, it is prosecuted under federal statutes like 18 U.S.C. § 2251 (sexual exploitation) or state revenge porn laws. The United Kingdom frames it under the Sexual Offences Act 2003, focusing on coercion and intent. Internationally, the UN's Optional Protocol to the Convention on the Rights of the Child addresses related exploitation. However, it lacks specificity for sextortion (Optional Protocol to the UN Convention on the Rights of the Child, 2000).

In India, sextortion lacks a standalone legal definition, forcing reliance on a patchwork of statutes. The IPC's Section 383 defined extortion as inducing fear to dishonestly obtain property or valuable security, which courts have stretched to include sexual demands. Section 354C (voyeurism) and Section 503 (criminal intimidation) are also invoked, alongside the Information Technology (IT) Act, 2000, Sections 66E and 67A, which penalise privacy violations and transmission of explicit content. The BNS 2023, replacing the IPC, retains these provisions under Sections 77 and 130, respectively, but still does not explicitly name sextortion. A notable Indian case, *State of West Bengal v. Animesh Boxi* (2018), marked the country's first "revenge porn" conviction, where a perpetrator was jailed for sharing a victim's self-recorded videos, illustrating the overlapping nature of sextortion with related crimes (Surawase *et al.*, 2024).

The scope of sextortion is broad, encompassing online scams, where perpetrators pose as romantic partners or authority figures, and offline abuses of power, such as teachers or employers exploiting subordinates. In India, the Delhi High Court in *Soukin v. NCT of Delhi* (2024) labelled sextortion a "significant social menace," noting its exploitation of intimate material and cross-jurisdictional nature (Soukin v. State (NCT of Delhi), 2024). The court's ruling, denying bail to three accused in a Rs. 16 lakh extortion case, underscored the crime's severity. India's position is complicated by its dual prevalence: rural syndicates in Mewat and urban hackers targeting affluent men aged 45-60 (Kulshrestha, 2023). The NCRB reported 686 cybercrime cases linked to sexual exploitation in 2016, a figure likely underrepresenting sextortion due to underreporting (Taskin, 2023).

Globally and in India, the key elements of sextortion are threats, non-consensual acts, and exploitation, which demand a nuanced legal response. India's framework struggles with definitional clarity, leaving victims navigating a fragmented system. This highlights the need for a unified legal identity for sextortion, particularly in India, where cultural stigma and legal gaps exacerbate its impact.

3.0 Existing Legal Frameworks

Legal responses to sextortion vary globally, reflecting diverse legislative priorities. In the United States, federal laws like 18 U.S.C. § 1030 (Computer Fraud and Abuse Act) target hacking-related sextortion, while 18 U.S.C. § 875 addresses interstate threats. The *United States v. Mijangos* (2011) case, where a hacker was sentenced to six years for extorting nude images via malware, exemplifies this approach (U.S. Department of Justice, 2011). State laws, such as California's revenge porn statute, complement federal efforts. In the UK, the Sexual Offences Act 2003 and Malicious Communications Act 1988 cover digital threats, with the Criminal Justice and Courts Act 2015 adding image-based abuse provisions. Internationally, the EU's Directive 2011/93/EU focuses on child exploitation, though adult victims often fall outside its scope.

In India, the legal framework is less cohesive. The IPC's Section 383 (extortion) and Section 354C (voyeurism) are primary tools, supplemented by the IT

Act's Sections 66E (privacy violation) and 67A (explicit content transmission), carrying penalties of up to three and five years, respectively. The Protection of Children from Sexual Offences (POCSO) Act, 2012, addresses child victims, imposing stringent punishments, including life imprisonment for aggravated offences. The BNS, 2023 updates these provisions, with Section 77 mirroring IPC's voyeurism clause and Section 130 enhancing extortion penalties, yet it stops short of defining sextortion explicitly. The *Animesh Boxi* case saw a five-year sentence under IPC and IT Act provisions, a rare successful prosecution.

India's workplace sextortion is tackled by the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013, though it is gender-specific and excludes men. The Delhi High Court's 2024 ruling in *Soukin v. NCT* highlighted the organised nature of sextortion, linking it to syndicates extorting millions. Globally, the Budapest Convention on Cybercrime facilitates cross-border cooperation, which India has not ratified, limiting its international enforcement capacity (Mali, 2024).

Comparatively, the U.S. and UK frameworks offer clearer pathways for prosecution, while India's reliance on broad statutes creates ambiguity. For instance, the *Mijangos* case leveraged specific cybercrime laws, whereas Indian courts stretch IPC provisions, as in *State v. Boxi*. The focus of the POCSO Act on minors leaves adult victims underserved, and the penalties in the IT Act, which are capped at five years, pale against the harm caused by sextortion. India's non-participation in global treaties further isolates its efforts, contrasting with the EU's coordinated approach. This reveals India's legal lag, necessitating targeted reforms to match global standards.

4.0 Challenges in Prosecuting Sextortion

Prosecuting sextortion is a global challenge, magnified in India by technological, jurisdictional, and social barriers. Jurisdictional complexity tops the list: perpetrators often operate across borders, as seen in cases where Indian victims are targeted by Southeast Asian or West African syndicates (Bhaskaran & Gole, 2024). In *Soukin v. NCT* (2024), the Delhi High Court noted the "cross-jurisdictional nature" of sextortion, with the accused using multiple SIM cards across 50 devices, evading local police. India's non-ratification of the Budapest Convention hampers extradition and data-sharing, unlike the U.S., where *United States v. Ogoshi* (2023) saw Nigerian perpetrators extradited (U.S. Department of Justice, 2023).

Evidence collection is another hurdle. Encrypted platforms like Telegram and WhatsApp shield communications, while VPNs and cryptocurrencies obscure identities. In India, the Lucknow cybercrime cell reported 43 sextortion cases in 2023, solving only 15 due to perpetrators' use of untraceable tech from Haryana and Rajasthan (Chakraborty, 2023). The *Mijangos* case required advanced forensics, a resource scarce in India's underfunded police forces. Victim reluctance compounds this: a 2021 study found 60% of sextortion victims avoid reporting due to shame, a trend acute in India's patriarchal society (Fohring, 2024). The suicide of a Bengaluru student, BS Avinash, after paying Rs. 36,000 to sextortionists, underscores this trauma (Johnson, T.A., 2021).

India faces unique challenges. Cultural stigma silences victims, particularly women, as seen in the NCW's doubled complaints during lockdown (The Swaddle, 2020). Legal ambiguity, that is, lacking a sextortion-specific statute, forces reliance on IPC and IT Act provisions, often yielding lenient sentences. In *State v. Boxi*, the five-year term was criticised as inadequate. Technological lag and underreporting further cripple enforcement. These challenges demand a rethink of India's legal and investigative strategies.

5.0 The Dark Web: An Enabler of Sextortion

The dark web is a subset of the deep web, which is internet content not indexed by standard search engines, accessible only through specialised software like Tor (The Onion Router). Unlike the surface web (*e.g.*, Google-accessible sites), the dark web uses encryption and anonymisation to shield user identities, hosting both legitimate and illicit activities. Originating from U.S. Naval Research in the 1990s to protect intelligence communications, it has since become a haven for cybercriminals, including sextortionists.

The dark web operates via overlay networks like Tor, which routes data through multiple encrypted relays worldwide, masking IP addresses. Websites, known as "onion sites," use

"onion" domains, requiring Tor or similar browsers (*e.g.*, I2P) for access. Transactions often occur via cryptocurrencies like Bitcoin, processed through decentralised blockchain systems, ensuring financial anonymity. Communication happens on encrypted forums or messaging platforms, enabling sextortionists to coordinate rackets, share victim data, or sell explicit content without detection.

Tracing dark web activities is arduous due to its layered anonymity. Tor's onion routing bounces data across global nodes, obscuring origins. Self-destructing mailboxes, proxy servers, and VPNs further conceal identities. Cryptocurrency transactions, lacking centralised oversight, resist tracking, while end-to-end encryption (*e.g.*, on Telegram or Signal) thwarts interception. In India, cyber expert Karnika Seth notes that these features make prosecution challenging, as evidence collection lags behind technological sophistication.

Sextortionists leverage the dark web to acquire hacking tools, trade victim material, and orchestrate cross-border rackets. Towns like Mewat and Bharatpur in Rajasthan have emerged as hubs, with gangs using dark web-acquired deepfake software to create fake profiles and extort millions (Yadav, 2022). The anonymity empowers perpetrators to target high-profile individuals like politicians, doctors, and even ministers without fear of immediate reprisal.

6.0 Gaps in Current Legislation

Global and Indian laws reveal significant gaps in addressing sextortion. Internationally, the absence of a unified definition hampers cooperation, as the Budapest Convention omits sextortion-specific provisions. In the U.S., penalties under 18 U.S.C. § 2251 (up to 30 years) dwarf India's IT Act maximum of five years, highlighting sentencing disparities. The UK's laws, while robust, focus on minors, leaving adult victims less protected (Wolak & Finkelhor, 2016).

In India, the lack of a sextortion-specific statute is glaring. The IPC's Section 383 and BNS's Section 130 cover extortion broadly, missing the sexual coercion element. The IT Act's Sections 66E and 67A address digital offences but cap penalties below the crime's gravity. The POCSO Act protects minors effectively, yet adult victims, especially men, lack equivalent safeguards. The *Soukin v. NCT* ruling criticised this gap, noting sextortion's "profound violation of privacy". India's Prevention of Corruption Act (PCA) Amendment, 2018, broadened "undue advantage" to include sexual favours, but its seven-day reporting window deters victims.

Cultural and structural issues widen these gaps. Patriarchal attitudes blame victims, yet, in a recent commendable judgment of the Punjab and Haryana High Court, Justice Sumeet Goel denied anticipatory bail to the accused in a sextortion case, observing that the "grant of anticipatory bail would not be appropriate in cases of sextortion as such crimes severely impact the social fabric" (The Walkers, 2024).

7.0 Proposed Legal Reforms and Solutions

Combating sextortion requires bold reforms. Globally, nations should adopt sextortion-specific laws, as California did by amending its extortion statute (McGlynn & Rackley, 2017). India must follow suit, defining sextortion in the BNS with penalties reflecting its harm, *e.g.*, 10-20 years imprisonment. International cooperation, via ratifying the Budapest Convention, would enhance India's ability to tackle cross-border cases. Cyberforensic training, as in the U.S.'s *Mijangos* prosecution, is critical for India's police.

Victim support is paramount. India's eSafety Commissioner-style anonymous reporting system could reduce stigma. Amending the Prevention of Corruption Act's seven-day reporting rule to a flexible window would protect victims, aligning with global best practices. Public awareness campaigns, like NCMEC's "No Escape Room," could educate India's youth (WeProtect Global Alliance, 2024). Integrating sextortion into the POSH Act to cover all genders would address workplace abuses. These reforms, blending global lessons with India's context, promise a stronger legal shield.

8.0 Conclusion

Sextortion's rise in the digital age tests legal systems worldwide, with India at a critical juncture. Its fragmented laws, such as the IPC, IT Act, and BNS, offer partial recourse, but definitional gaps, lenient penalties, and cultural barriers hinder justice. Globally, clearer frameworks and cooperation set a benchmark India must meet. By enacting specific laws, enhancing enforcement, and supporting victims, India can bridge these gaps, ensuring dignity and justice in a connected world.

9.0 References

Beauchere, J. (2023). Two-thirds of Gen Z targeted for online sextortion: New Snap research. *WeProtect.* https://www.weprotect.org/blog/two-thirds-of-gen-z-targeted-for-online-sextortion-new-snap-research/

Bhaskaran, P., & Gole, Y. (2024). Adjudicating and investigating cross-border cybercrimes: A study of India's jurisdictional framework. *Indian Journal of Integrated Research in Law, 5***(2),** 604-626.

Chakraborty, P. (2023). Beware: Sextortion trap getting wider and dangerous. *The Times of India.* https://timesofindia.indiatimes.com/city/lucknow/sextortion-trap-getting-wider-dangerous/articleshow/104199523.cms

Fohring, S. (2024). #WhyIDidntReport: Exploring victim accounts of non-reporting. *Crime, Media, Culture, 20*(1), 3-22. https://doi.org/10.1177/17488958241283947

Federal Bureau of Investigation. (2023). Sextortion: A growing threat targeting minors. https://www.fbi.gov/news/press-releases/sextortion-a-growing-threat-targeting-minors

Johnson, T. A. (2021). 26-year-old's suicide in Bengaluru points to online 'sextortion' racket. *The Indian Express.* https://indianexpress.com/article/india/online-sextortion-racket-bengaluru-suicide-case-7266977/

Kulshrestha, P. (2023). How Kaithwara became the Jamtara of sextortion. *The Times of India.* https://timesofindia.indiatimes.com/india/how-kaithwara-became-the-jamtara-of-sextortion/articleshow/98274295.cms

Mali, P. (2024). International cybercrime treaties and case laws: An overview (Till December 2024). *Cyber Law Consulting.* https://www.cyberlawconsulting.com/global_cybersecurity_sco_framework.php

Manral, M. S., & Sinha, J. (2023). 24 % rise in cybercrime in 2022, 11 % surge in economic offences: NCRB report. *The Indian Express.* https://indianexpress.com/article/india/rise-cybercrime-2022-economic-offences-ncrb-report-9053882/

McGlynn, C., & Rackley, E. (2017). Image-based sexual abuse. *Oxford Journal of Legal Studies, 37*(3), 534-561. https://doi.org/10.1093/ojls/gqw033

Optional Protocol to the UN Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography. (2000, May 25). *Child Rights International Network (CRIN).* https://archive.crin.org/en/library/legal-database/optional-protocol-un-convention-rights-child-sale-children-child-prostitution6aea.html

Ray, A., & Henry, N. (2024). Sextortion: A scoping review. *Trauma, Violence, and Abuse, 26*(1), 138-155. https://doi.org/10.1177/15248380241277271 PMid:39323232 PMCid:PMC11558931

Soukin v. State (NCT of Delhi), 2024 SCC OnLine Del 2986 (India). https://www.scconline.com/blog/post/2024/05/02/sextortion-represents-profound-violation-of-privacy-is-social-menace-dhc-legal-news/

Surawase, R. H., Bhagat, V. M., & Tripathi, D. (2024). Legal challenges in the digital age: Revenge porn in India. *ANVESAK, 54*(1), 32-43.

State of West Bengal v. Animesh Boxi, C.R.M. No. 11806 of 2017 (2018)

Taskin, B. (2023). 24% spike in cybercrime in India, shows NCRB data. Fraud, extortion and sexual exploitation top motives. *ThePrint.* https://theprint.in/india/24-spike-in-cybercrime-in-india-shows-ncrb-data-fraud-extortion-sexual-exploitation-top-motives/1871498/

The Swaddle. (2020). Cybercrime cases against women spike under COVID-19 lockdown. https://www.theswaddle.com/cybercrime-cases-against-women-spike-under-covid19-lockdown/

The Walkers. (2024). Punjab and Haryana High Court denies anticipatory bail in sextortion case, citing impact on social fabric. https://thewalkers.co.in/judgements/punjab-and-haryana-high-court-denies-anticipatory-bail-in-sextortion-case-citing-impact-on-social-fabric

U.S. Department of Justice. (2011, September 1). Orange County man who admitted hacking into personal computers sentenced to six years in federal prison for 'sextortion' of women and teenage girls. https://www.justice.gov/archive/usao/cac/Pressroom/pr2011/123.html

U.S. Department of Justice. (2023, August 13). Two Nigerian men extradited to the United States after being indicted for international sexual extortion ring. U.S. Attorney's Office, Western District of Michigan. https://www.justice.gov/usao-wdmi/pr/2023_0813_Two_Nigerian_Men_Extradited_To_The_United_States

United States v. Mijangos, No. 8:10-cr-00172 (C.D. Cal. 2011).

WeProtect Global Alliance. (2024). No Escape Room: Building sextortion awareness. https://www.weprotect.org/blog/no-escape-room-building-awareness-of-sextortion/

Wolak, J., & Finkelhor, D. (2016). Sextortion: Findings from an online survey about threats to expose sexual images. Crimes Against Children Research Center and Thorn. https://www.unh.edu/ccrc/sites/default/files/media/2022-02/sextortion-report-final-june-2016.pdf

Yadav, Y. (2022). India becoming 'sextortion' capital of the world? *The Times of India.* https://timesofindia.indiatimes.com/blogs/voices/india-becoming-sextortion-capital-of-the-world/