



RESEARCH QUESTION

"What should a person in India do immediately when blackmailed with private images or a recorded video call, what offences under the BNS and IT Act apply to sextortion, how does reporting on the cybercrime portal work, and can content takedown be obtained?"

# Immediate Remedies and Legal Framework Against Online Sextortion and Blackmail in India

TL;DR

The Supreme Court of India in *Sharat Babu Digumarti v. Govt. of NCT of Delhi* (2016) established that the Information Technology Act, 2000, as a special enactment, overrides general penal provisions for offences arising from electronic records, meaning online sextortion must primarily be prosecuted under the IT Act alongside corresponding special provisions of the Bharatiya Nyaya Sanhita (BNS), 2023. Aggrieved individuals must immediately preserve all digital evidence, report the offence on the National Cyber Crime Reporting Portal to trigger local police action, and issue urgent "cease and desist" notices to intermediaries to enforce mandatory content takedown.

| VERIFIED CASES       | STATUTES | LATEST RULING           |
|----------------------|----------|-------------------------|
| 9                    | 5        | 2025                    |
| 7 High Courts · 2 SC |          | High Court of Karnataka |

CONTENTS

|                          |   |
|--------------------------|---|
| I. Detailed Analysis     | 3 |
| II. Statutory Provisions | 5 |
| III. Cases Discussed     | 7 |
| IV. Case Details         | 8 |



## I. Detailed Analysis

### KEY PRINCIPLES ESTABLISHED

#### 01 Violation of privacy through non-consensual electronic transmission

Intentionally or knowingly capturing, publishing, or transmitting the image or video of a person's private areas without consent under circumstances violating their privacy is a severe electronic offence punishable under Section 66E of the IT Act and Section 354C of the IPC (voyeurism), as applied in *Moiz Ahmed v. State of Maharashtra* (2024).

#### 02 Blackmail as a distinct criminal element

Demanding money or compliance by threatening to reveal private images or recordings constitutes blackmail and criminal intimidation, making the perpetrator liable under statutory provisions governing extortion, as observed in *Maridhas v. State* (2021).

#### 03 The compound nature of sextortion (stalking and intimidation)

When a perpetrator repeatedly contacts a victim or monitors them online using threats to disseminate private material to force interaction, they satisfy the ingredients of both stalking and criminal intimidation, as demonstrated in *Abhishek Mishra v. State of Karnataka* (2025).

#### 04 Strict limits on what constitutes electronic obscenity

For a charge of transmitting obscene or sexually explicit material to stand under Sections 67 and 67A of the IT Act, the content must be genuinely lascivious and appeal to prurient interests rather than merely containing vulgar or offensive language, as clarified in *Apoorva Arora & Anr. v. State (Govt. of NCT of Delhi) & Anr.* (2024).

### HOW THE COURTS HAVE APPLIED THIS

#### COORDINATED PERMANENT CONTENT REMOVAL

Courts actively enforce rules requiring intermediaries and search engines to block access and permanently remove non-consensual intimate imagery, directing law enforcement agencies to work dynamically with platforms to prevent re-uploading, as shown in *X v. Union of India* (2021).

**ADMINISTRATIVE  
ENFORCEMENT VIA  
PORTAL REPORTING**

Reporting online cybercrimes through the National Cyber Crime Reporting Portal initiates coordinated enforcement across states, enabling cyber cells to issue urgent directives, such as freezing bank accounts used in blackmail schemes, as illustrated in *Yasmin K.A v. Federal Bank* (2024).

**APPLICATION OF  
BNS STATUTORY  
COUNTERPARTS**

With the active implementation of the Bharatiya Nyaya Sanhita (BNS), 2023, courts have seamlessly transitioned to new equivalents, mapping older IPC modesty and obscenity provisions (such as Sections 294 and 509 IPC) directly to Sections 296 and 79 BNS, as seen in *Dinesh Shetty v. State of Karnataka* (2025).

**UNSETTLED AREAS OR CAVEATS**

### The administrative lag in intermediary takedowns

While victims can issue "cease and desist" notices to intermediaries to prompt content removal, the legal process often suffers from delay. Under the current framework of Section 79 of the IT Act, platforms may express technical or jurisdictional limitations until a formal court order or government block is obtained, as noted in *Rev. Dr. Chegudi Ashok Babu v. Karunakar Sugguna* (2019).

## II. Statutory Provisions 5 PROVISIONS

### SECTION 67A, INFORMATION TECHNOLOGY ACT, 2000 — PUNISHMENT FOR PUBLISHING OR TRANSMITTING OF MATERIAL CONTAINING SEXUALLY EXPLICIT ACT, ETC., IN ELECTRONIC FORM

This section criminalises the electronic publication or transmission of sexually explicit material, prescribing jail terms and heavy fines.

"Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees." *Cited in: Apoorva Arora & Anr. v. State (Govt. of NCT of Delhi) & Anr., Sharat Babu Digumarti v. Govt. of NCT of Delhi*

### SECTION 72A, INFORMATION TECHNOLOGY ACT, 2000 — PENALTY FOR DISCLOSURE OF INFORMATION IN BREACH OF LAWFUL CONTRACT

This section penalises intermediaries or service providers who unlawfully disclose personal information secured through a lawful contract without the consent of the individual concerned.

"Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be liable to penalty which may extend to twenty-five lakh rupees." *Cited in: None*

**SECTION 506, INDIAN PENAL CODE, 1860 — PUNISHMENT FOR CRIMINAL INTIMIDATION**

This section details the punishments for committing criminal intimidation, with enhanced penalties if the threat involves death, grievous hurt, or imputing unchastity to a woman.

"Whoever commits the offence of criminal intimidation shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both; If threat be to cause death or grievous hurt, etc. and if the threat be to cause death or grievous hurt, or to cause the destruction of any property by fire, or to cause an offence punishable with death or imprisonment for life, or with imprisonment for a term which may extend to seven years, or to impute unchastity to a woman, shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine, or with both." *Cited in: Abhishek Mishra v. State of Karnataka*

**SECTION 503, INDIAN PENAL CODE, 1860 — CRIMINAL INTIMIDATION**

This section defines the offence of criminal intimidation as threatening someone with injury to their person, reputation, or property with the intent to cause alarm or force them to act against their legal will.

"Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation." *Cited in: None*

**SECTION 67, INFORMATION TECHNOLOGY ACT, 2000 — PUNISHMENT FOR PUBLISHING OR TRANSMITTING OBSCENE MATERIAL IN ELECTRONIC FORM**

This section imposes penalties, including imprisonment and fines, on anyone who transmits or publishes lascivious or obscene material electronically.

"Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees." *Cited in: Apoorva Arora & Anr. v. State (Govt. of NCT of Delhi) & Anr., Moiz Ahmed v. State of Maharashtra, Sharat Babu Digumarti v. Govt. of NCT of Delhi*

III. Cases Discussed 9 CASES · SUMMARY TABLE

| #  | CASE TITLE                                                                                      | COURT                        | YEAR | KEY HOLDING                                                                                            |
|----|-------------------------------------------------------------------------------------------------|------------------------------|------|--------------------------------------------------------------------------------------------------------|
| 01 | <i>Apoorva Arora &amp; Anr. v. State (Govt. of NCT of Delhi) &amp; Anr.</i><br>ESCR010001992024 | SUPREME COURT OF INDIA       | 2024 | Limits electronic obscenity under Sections 67/67A IT Act to genuinely lascivious acts                  |
| 02 | <i>Moiz Ahmed v. State of Maharashtra</i><br>HCBM030219402020                                   | BOMBAY HIGH COURT            | 2024 | Dissemination of recorded private video constitutes voyeurism and violation of electronic privacy      |
| 03 | <i>Abhishek Mishra v. State of Karnataka</i><br>KAHC010418292024                                | HIGH COURT OF KARNATAKA      | 2025 | Threatening to leak recorded private videos constitutes criminal intimidation, voyeurism, and stalking |
| 04 | <i>Maridhas v. State</i><br>HCMD011005652021                                                    | MADRAS HIGH COURT            | 2021 | Defines blackmail under Section 292A IPC as demanding money using threats of exposure                  |
| 05 | <i>X v. Union of India</i><br>DLHC010200262020                                                  | HIGH COURT OF DELHI          | 2021 | Establishes framework for permanent content takedown and intermediary obligations for intimate images  |
| 06 | <i>Yasmin K.A v. Federal Bank</i><br>KLHC010875212024                                           | HIGH COURT OF KERALA         | 2024 | Highlights how reporting on National Cyber Crime Reporting Portal triggers police action               |
| 07 | <i>Dinesh Shetty v. State of Karnataka</i><br>KAHC010166812025                                  | HIGH COURT OF KARNATAKA      | 2025 | Applies new BNS provisions (Sections 296, 79 BNS) replacing old IPC modesty offences                   |
| 08 | <i>Sharat Babu Digumarti v. Govt. of NCT of Delhi</i><br>ESCR010004882016                       | SUPREME COURT OF INDIA       | 2016 | IT Act is special law overriding general penal code for electronic records                             |
| 09 | <i>Rev. Dr. Chegudi Ashok Babu v. Karunakar Sugguna</i><br>APHC010132892019                     | HIGH COURT OF ANDHRA PRADESH | 2019 | Victim's remedy to issue cease-and-desist notices to intermediaries for content removal                |

## IV. Case Details 9 CASE FILES

### 01 Apoorva Arora & Anr. v. State (Govt. of NCT of Delhi) & Anr.

SUPREME COURT OF INDIA • 2024-03-19 • 2024 INSC 223

The case involved the prosecution of actors, creators, and producers of the web-series 'College Romance' for allegedly publishing obscene and sexually explicit content under sections 67 and 67A of the Information Technology Act, 2000. The complaint stemmed from the use of profanity and vulgar expletives in the series' titles and episodes. The Supreme Court set aside the High Court's decision, ruling that vulgarity and profanity do not inherently constitute obscenity. The Court clarified that to meet the legal threshold, material must be lascivious, appeal to prurient interests, or tend to corrupt the minds of its audience. As the language used was intended to reflect emotions like anger rather than arouse sexual thoughts, the Court quashed the FIR.

**HELD** The Supreme Court ruled that Section 67A strictly criminalises the publication or transmission of material containing "sexually explicit acts or conduct" in electronic form. These terms must be interpreted strictly in the context of "obscenity" under Section 67 and cannot be extended to cover mere profanities, swear words, or expletives.

"s.67A criminalises publication, transmission, causing to publish or transmit in electronic form any material that contains sexually explicit act or conduct – Though the three expressions "explicit", "act", and "conduct" are open-textured and are capable of encompassing wide meaning, the phrase may have to be seen in the context of 'obscenity' as provided in s.67 – Thus, there could be a connect between s.67A and s.67 itself – For example, there could be sexually explicit act or conduct which may not be lascivious – Equally, such act or conduct might not appeal to prurient interests – On the contrary, a sexually explicit act or conduct presented in an artistic or a devotional form may have exactly the opposite effect, rather than tending to deprave and corrupt a person."

SUPREME COURT OF INDIA • 2024

SOURCE ESCR010001992024

### 02 Moiz Ahmed v. State of Maharashtra

BOMBAY HIGH COURT • 2024-12-06 • APPLN/1688/2020

The applicants sought to quash criminal proceedings involving allegations of outraging a woman's modesty and voyeurism after they allegedly displayed a video clip of the complainant and her husband in a private moment. The High Court determined that the charge under Section 354 of the Indian Penal Code was inappropriate as the essential elements of assault or criminal force were not present. However, the Court observed that the dissemination of the private video could constitute offences under Section 354-C of the IPC and potentially under Sections 66-E and 67 of the Information Technology Act.

**HELD** The High Court held that the dissemination of an objectionable, non-consensual video clip of a couple's private moments attracts Section 354C of the IPC (voyeurism) and Section 66E of the IT Act (violation of privacy). The court clarified that while Section 354C applies specifically to offences against women, Section 66E is gender-neutral and applies to any person whose private images are recorded or transmitted without consent.

"Section 354C applies only when the wrong is committed against a woman. Section 66-E of the IT Act applies when wrong is done against a male or female. Section 354C speaks of 'private act' which may expose private parts posterior or breast of a woman exposed or covered in under clothes."

BOMBAY HIGH COURT • 2024

SOURCE HCBM030219402020

### 03 Abhishek Mishra v. State of Karnataka

HIGH COURT OF KARNATAKA • 2025-07-08 • CRL.P/8596/2024

The petitioner sought to quash criminal proceedings involving allegations of voyeurism, stalking, and intimidation under the IPC, the IT Act, and the SC/ST (Prevention of Atrocities) Act. The dispute arose from a soured romantic relationship between the petitioner and the complainant, who had initially met during UPSC coaching. The complainant alleged that the petitioner recorded private videos and threatened to disseminate them. The court examined the complaint and the underlying charges in light of the parties' history and previous interactions.

**HELD** The High Court confirmed that recording private videos without consent and threatening to disseminate them to compromise a person's privacy constitutes voyeurism (Section 354C), stalking (Section 354D), and criminal intimidation (Sections 504 and 506), as well as a direct violation of privacy under Section 66E of the IT Act.

""66-E. Punishment for violation of privacy.— Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both. Explanation .—For the purposes of this section— (a) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons; (b) "capture", with respect to an image, means to videotape, photograph, film or record by any means; (c) "private area" means the naked or undergarment clad genitals, public area, buttocks or female breast; (d) "publishes" means reproduction in the printed or electronic form and making it available for public; (e) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that— (i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or (ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.""

HIGH COURT OF KARNATAKA • 2025

SOURCE KAHC010418292024

## 04 Maridhas v. State

MADRAS HIGH COURT • 2021-12-23 • CRL OP(MD)/20560/2021

The petitioner, a social media commentator, sought to quash an FIR registered against him for remarks made in a YouTube video concerning the Tablighi Jamaat conference held in New Delhi during the 2020 COVID-19 pandemic. The complaint alleged that the video promoted religious hatred and caused public alarm. The court examined the requirements of Sections 292A, 295A, and 505(2) of the Indian Penal Code and concluded that the petitioner's statements did not contain the requisite malicious intent or scurrilous content needed to constitute these offenses. Finding that the content did not target any religion and constituted a critique of a public event, the court quashed the FIR.

**HELD** The High Court outlined that the legal definition of "blackmail" under Indian law specifically refers to the act of demanding money or concessions from an individual by threatening to make private, damaging, or intimate revelations about them.

““Blackmail” refers to the crime of demanding money from a person by threatening to make a revelation about him. I have relied on the meanings assigned to the said expressions in Oxford Advanced Learner's Dictionary.”

MADRAS HIGH COURT • 2021

SOURCE HCMD011005652021

## 05 X v. Union of India

HIGH COURT OF DELHI • 2021-04-20 • W.P.(CRL)/1082/2020

The petitioner sought the removal of her private photographs, which had been unlawfully posted on a pornographic website, from the internet. She raised concerns regarding the failure of authorities to effectively remove the content and the tendency for such material to be re-posted across different platforms, rendering court orders ineffective. The court examined the technological challenges of enforcing removal orders and the legal framework under the Information Technology Act. The case focused on crafting robust and implementable directions for law enforcement and intermediaries to ensure the permanent removal of illegal or offensive content, preventing it from resurfacing.

**HELD** The High Court established a detailed protocol for content takedown, emphasizing that under Section 79 of the IT Act, intermediaries must act with due diligence. Once they are notified of the non-consensual posting of intimate pictures, they must immediately disable access and utilize digital signature matching to ensure permanently removed content is not re-uploaded.

“Ø79. Exemption from liability of intermediary in certain cases.Ñ(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3) , an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him. (2) The provisions of sub-section (1) shall apply ifÑ (a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or (b) the intermediary does notÑ (i) initiate the transmission, (ii) select the receiver of the transmission, and (iii) select or modify the information contained in the transmission; (c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.”

HIGH COURT OF DELHI • 2021

SOURCE DLHC010200262020

## 06 Yasmin K.A v. Federal Bank

HIGH COURT OF KERALA • 2024-03-26 • WP(C)/8321/2024

This case involves several writ petitions filed by various bank account holders whose accounts were frozen or restricted by their respective banks following directions from police authorities across different states through the National Cyber Crime Reporting Portal. The petitioners alleged that these freezes were arbitrary and caused significant financial hardship without providing them with any notice or opportunity to be heard regarding the underlying cybercrime investigations. The Kerala High Court directed the banks to permit the petitioners to operate their accounts, provided they maintained a sufficient balance to cover the disputed amounts specified in the police notifications. The court further ordered the police authorities to expedite their investigations and initiate proceedings under the Code of Criminal Procedure, ensuring the petitioners are given due notice.

**HELD** The High Court illustrated that reporting cybercrimes on the National Cyber Crime Reporting Portal coordinates swift administrative action, allowing nodal cyber officers across different states to issue immediate frozen account notifications to financial institutions to intercept and trace the proceeds of online crime.

“NATIONAL CYBER CRIME REPORTING PORTAL REPRESENTED BY ITS NODAL CYBER CELL OFFICER, KUTCHERY CHOWK, RANCHI, JHARKHAND CYBERPS@JHPOLICE.GOV.IN, PIN - 834001”

HIGH COURT OF KERALA • 2024

SOURCE KLHC010875212024

## 07 Dinesh Shetty v. State of Karnataka

HIGH COURT OF KARNATAKA • 2025-04-28 • CRL.P/3382/2025

The petitioners, owners of bar and restaurant establishments, challenged the registration of FIRs alleging indecent dance performances and violations of various statutes, including the Bharatiya Nyaya Sanhita (BNS) and the Karnataka Police Act. The court found that the essential ingredients for offenses under Section 296 BNS —specifically, proof of annoyance to others—were absent. Furthermore, it noted a failure to record statements required under Section 183(6) of the Bharatiya Nagarik Suraksha Sanhita for offenses related to the modesty of

women. Because the police failed to obtain prior judicial permission for investigating non-cognizable offenses as required by law, the court quashed the FIRs, ruling that their continuation constituted an abuse of legal process.

**HELD** The High Court ruled that the established requirements of demonstrating "annoyance to others" to constitute public obscenity under Section 294 of the IPC continue to apply identically to its direct BNS equivalent, Section 296 BNS. The court quashed the FIRs where these essential ingredients and procedural mandates under the BNSS were not satisfied.

"In the case of N.S. Madhanagopal (supra), the Hon'ble Supreme Court categorically held that mere utterance of obscene words is insufficient to constitute an offence under Section 294(b) of the Indian Penal Code. There must also be evidence that the words or acts caused annoyance to others. In that case, the Court noted the absence of any witness or evidence establishing that the alleged acts caused annoyance, and therefore concluded that the essential ingredients of the offence were not met. The same principle is applicable to Section 296 of the Bharatiya Nyaya Sanhita, which is in pari materia with Section 294 IPC."

HIGH COURT OF KARNATAKA • 2025

SOURCE KAHC010166812025

## 08 Sharat Babu Digumarti v. Govt. of NCT of Delhi

SUPREME COURT OF INDIA • 2016-12-14 • 2016 INSC 1131

This case addressed whether an individual accused of obscenity related to electronic material could be prosecuted under Section 292 of the Indian Penal Code (IPC) after being discharged from charges under Section 67 of the Information Technology (IT) Act. The Supreme Court held that the IT Act is a special law that encompasses the regulation of obscene material in electronic form. Because the IT Act contains specific provisions and overriding clauses that mandate its application in cases involving electronic records, it prevails over the general provisions of the IPC. Consequently, the court quashed the criminal proceedings against the appellant, ruling that he could not be prosecuted under Section 292 IPC for matters governed by the special IT Act.

**HELD** The Supreme Court held that the IT Act, 2000 is a special enactment containing specific provisions. When an offence of obscenity has an undisputed connection or nexus with an electronic record, prosecution under general provisions of the IPC (such as Section 292) is impermissible, as the special provisions and the overriding non-obstante mandate of Section 81 of the IT Act must prevail.

"It has to be borne in mind that IT Act is a special enactment. It has special provisions. Section 292 of the IPC makes offence sale of obscene books, etc. but once the offence has a nexus or connection with the electronic record the protection and effect of Section 79 cannot be ignored and negated. We are inclined to think so as it is a special provision for a specific purpose and the Act has to be given effect to so as to make the protection effective and true to the legislative intent. This is the mandate behind Section 81 of the IT Act."

SUPREME COURT OF INDIA • 2016

SOURCE ESCR010004882016

## 09 Rev. Dr. Chegudi Ashok Babu v. Karunakar Sugguna

HIGH COURT OF ANDHRA PRADESH • 2019-08-02 • WP(PIL)/80/2019

The petitioners, representing a Christian fellowship, filed a Public Interest Litigation seeking to block the release of a short film titled 'Nene Devunni' and its promotional teaser on YouTube. They alleged that the content depicted Jesus Christ in a manner contradictory to the Holy Bible, thereby insulting their religious beliefs and violating their fundamental rights under Article 25 of the Constitution. The petitioners further sought action against the producers and the YouTube platform. The High Court dismissed the petition, observing that the petitioners failed to provide sufficient evidence, such as the actual teaser content, to establish a prima facie case of religious insult. The Court noted that mere screenshots were insufficient to prove constitutional infringement and that any grievances regarding offensive online content should be addressed through appropriate criminal complaints under the Indian Penal Code rather than a writ petition.

**HELD** Relying on the landmark *Shreya Singhal* precedent, the High Court held that the primary and immediate legal remedy for a person aggrieved by sexually explicit or defamatory electronic content is to issue a formal "cease and desist" notice to the intermediary hosting the content. If the intermediary fails to disable access, the victim is entitled to seek urgent judicial intervention for blocking orders.

"In view of the principle laid down by the Apex Court in "*Shreya Singhal v. Union of India* " (referred supra), the remedy open to the petitioner is to issue notice of "cease and desist" to the YouTube, which is subsidiary of Google and Google having control over the postings and in case the said authority did not remove the content and failed to take any action against the respondents, the petitioners are entitled to approach the Court for removal of such offended content or disable the access to certain material."

HIGH COURT OF ANDHRA PRADESH • 2019

SOURCE APHC010132892019

### DISCLAIMER

This memorandum has been generated by Vitark AI on the basis of publicly available judgments and the question posed by the user. It is provided for research assistance only and does not constitute legal advice. All case citations, holdings, and quotations must be independently verified against the source judgment before being relied upon in any filing, opinion, or correspondence.