*Page 3499 - 3516* **DOI:** *https://doi.org/10.63108/IJLMH.13151*

# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

**Volume 9 | Issue 5**

**2026**

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: https://www.ijlmh.com/
Under the aegis of VidhiAagaz – Inking Your Brain (https://www.vidhiaagaz.com/)

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

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

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

# Cyber Extortion in India: Emerging Threats and Legal Challenges

SHASHANK TIWARI*

**ABSTRACT**

*The rapid expansion of digital technologies has transformed communication, commerce, and data management while creating new opportunities for cybercriminals to exploit individuals, businesses, and public institutions. Cyber extortion has emerged as a significant cybersecurity and legal concern in India, involving threats to disclose sensitive information, ransomware attacks, unauthorised access to digital systems, and demands for money or other benefits through coercion. This paper examines the evolving nature of cyber extortion in India and evaluates the adequacy of the existing legal framework in addressing emerging threats. The study adopts a doctrinal research methodology, analysing relevant statutory provisions and judicial decisions. Particular attention is given to the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the procedural and evidentiary challenges associated with investigating and prosecuting cyber extortion. The research also considers difficulties arising from offender anonymity, cross-border jurisdiction, digital evidence preservation, technological sophistication, and the underreporting of cybercrime. The study argues that although existing Indian laws provide mechanisms for addressing several forms of cyber extortion, their effective application is complicated by fragmented legal provisions, investigative limitations, and the transnational character of digital offences. It identifies the need for clearer legal coordination, stronger digital forensic capabilities, improved inter-agency cooperation, and enhanced international collaboration. The research concludes that an effective response to cyber extortion requires a coordinated approach combining legal reform, technological preparedness, institutional capacity-building, and victim protection. Such measures are essential to strengthen accountability, safeguard digital rights, and improve confidence in India's evolving digital ecosystem.*

***Keywords:*** *Cyber Extortion, Cybercrime, Information Technology Act, 2000, Ransomware, Criminal Liability, Cybersecurity*

## I. INTRODUCTION

The rapid development of information and communication technologies has transformed commercial transactions, financial services, communication, and the storage of personal

* Author is a Student at Aurora Deemed to be University, Bhongir, Telangana, India.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

information. However, increased dependence on digital infrastructure has also created opportunities for criminal exploitation. Cyber extortion represents one such emerging threat, involving the use of digital systems, electronic communications, or unlawfully obtained information to compel individuals, businesses, or institutions to provide money, property, or other benefits under the threat of harm. Such conduct may include ransomware attacks, threats to disclose confidential information, online blackmail, and demands for payment following unauthorised access to computer systems. The Information Technology Act, 2000, and the general criminal law of India provide legal mechanisms that may apply to different elements of these activities, although their applicability depends upon the facts and ingredients of each offence.[1]

Cyber extortion differs from conventional extortion principally in the means through which threats are communicated, information is obtained, and victims are targeted. Digital anonymity, remote access, encrypted communications, and the potential involvement of offenders operating across national boundaries can complicate the identification and prosecution of perpetrators. Moreover, the consequences extend beyond immediate financial loss to include reputational damage, disruption of essential services, exposure of personal information, and diminished public confidence in digital transactions. These characteristics make cyber extortion a significant concern for India's developing digital economy and require an assessment of whether existing legal and institutional arrangements can respond effectively to its changing forms.

The central problem examined in this paper is whether India's existing legal framework adequately addresses the evolving methods of cyber extortion and the practical difficulties associated with investigation, evidence collection, and prosecution. Although several statutory provisions may apply to conduct associated with cyber extortion, the relevant legal classification depends upon the nature of the threat, the method of obtaining information, the demand made, and the conduct of the accused. Provisions concerning unauthorised access to computer resources, identity-related offences, extortion, and criminal intimidation may therefore become relevant in different circumstances.[2]

The challenge is not limited to the existence of statutory offences. Effective enforcement also depends upon the preservation and authentication of electronic evidence, timely reporting, technical investigative capacity, cooperation between law-enforcement agencies, and access to

[1] Information Technology Act, No. 21 of 2000, INDIA CODE (2000); Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE (2023).
[2] Information Technology Act, No. 21 of 2000, §§ 43, 66, 66C, INDIA CODE (2000); Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 308, 351, INDIA CODE (2023).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

evidence located outside India. The Bharatiya Sakshya Adhiniyam, 2023, establishes provisions governing electronic and digital records, while the Bharatiya Nagarik Suraksha Sanhita, 2023, governs criminal procedure.[3] This paper examines how these legal frameworks operate together and identifies the gaps that may impede an effective response to cyber extortion.

The study is doctrinal. It examines the relevant legislation and judicial decisions, and approaches cyber extortion as both a substantive criminal-law problem and an enforcement challenge, focusing on ransomware-related demands, threats involving confidential information, online blackmail and other forms of digitally facilitated coercion. It does not treat every cybercrime as cyber extortion; instead, it distinguishes conduct that may constitute extortion from related offences that may arise during the same incident.

## II. Concept and Emerging Forms of Cyber Extortion

### A. Meaning and nature of cyber extortion

Cyber extortion refers to the use of digital technologies, electronic communications, or access to computer systems to threaten, intimidate, or coerce a person or organisation into providing money, property, information, or another benefit. Unlike conventional extortion, which may involve physical threats or face-to-face intimidation, cyber extortion can be carried out remotely through digital platforms, compromised accounts, malicious software, and unlawfully obtained information.

The offender may threaten to disclose confidential data, disrupt business operations, damage computer systems, or expose private communications unless the victim complies with a demand. The defining feature is not merely the use of technology, but the use of a threat or coercive demand to obtain an advantage.

Indian criminal law does not treat every incident described as cyber extortion as a single, independent statutory offence. Section 308 of the Bharatiya Nyaya Sanhita, 2023 (BNS), addresses extortion, while section 351 concerns criminal intimidation. Depending on the facts, provisions of the Information Technology Act, 2000, may also apply where the conduct involves unauthorised access, damage to computer resources, or other computer-related offences.[4] Accordingly, cyber extortion must be examined by identifying the conduct involved, the nature of the threat, the demand made, and the statutory ingredients established by the evidence.

[3] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63, INDIA CODE (2023); Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, INDIA CODE (2023).

[4] Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 308, 351, INDIA CODE (2023); Information Technology Act, No. 21 of 2000, §§ 43, 66, INDIA CODE (2000).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

### B. Ransomware and double extortion

Ransomware is one of the most prominent technological methods associated with cyber extortion. It involves malicious software that restricts access to computer systems or data, commonly through encryption, and demands payment in exchange for a decryption key or the restoration of access. Individuals may lose access to personal information, while businesses and public institutions may experience operational disruption, financial loss, and difficulties maintaining essential services.

A further development is double extortion, in which an offender not only encrypts or restricts access to data but also threatens to publish or sell the information if the victim refuses to pay. This technique increases pressure on victims because restoring access to their systems may not eliminate the risk of disclosure. Organisations may consequently face additional concerns involving confidential business information, personal data, contractual obligations, and reputational damage.

From a legal perspective, the use of ransomware may involve several forms of unlawful conduct rather than one isolated offence. Unauthorised access, interference with computer resources, destruction or alteration of data, and coercive demands may require separate legal analysis. The applicability of any particular provision depends on the available evidence and the statutory requirements of the relevant offence.[5]

### C. Data-leak threats and online blackmail

Another form of cyber extortion involves threats to disclose information obtained from personal devices, online accounts, databases, or organisational networks. The threatened material may include financial records, business documents, private photographs, confidential correspondence, or personal information. Offenders may demand money to prevent publication, remove exposed material, or refrain from sharing it with employers, family members, customers, or the public.

Online blackmail can also arise without ransomware or the compromise of an entire computer network. An offender may use information acquired through a personal relationship, deceptive communication, account compromise, or other means to exert pressure on a victim. The coercive effect often depends on the sensitivity of the information and the consequences that disclosure could produce.

[5] Information Technology Act, No. 21 of 2000, §§ 43, 66, INDIA CODE (2000); Bharatiya Nyaya Sanhita, No. 45 of 2023, § 308, INDIA CODE (2023).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Such cases raise questions about the relationship between extortion, criminal intimidation, unauthorised access, and offences involving the misuse of electronic information. The legal classification must depend on the actual conduct rather than the label assigned to the incident. A threat to publish information may be relevant to criminal intimidation, while a demand accompanied by the legally required elements of extortion may attract section 308 of the BNS. Other provisions may apply where the information was obtained through unlawful access or other prohibited conduct.[6]

**D. Emerging techniques and digital anonymity**

Cyber extortion continues to evolve alongside developments in digital communication, cloud computing, remote access technologies, and the storage of personal and commercial data. Offenders may exploit weak passwords, phishing messages, compromised credentials, insecure systems, or vulnerabilities in software to obtain access to information or infrastructure. They may then use that access to threaten disclosure, interrupt services, or demand payment.

Anonymity can make attribution difficult because offenders may operate through compromised accounts, false identities, intermediary systems, or infrastructure located in different jurisdictions. Digital communications can also be created, altered, deleted, or distributed rapidly, complicating the preservation of reliable evidence. Where multiple individuals or groups participate in an attack, investigators may need to distinguish between those who gained access, those who issued threats, and those who received or transferred the proceeds.

These difficulties do not eliminate criminal liability, but they make the collection and interpretation of evidence particularly important. Investigators must establish the connection between the accused, the relevant digital activity, the threat, and the demand. Technical indicators alone may not establish the identity or intention of an offender without corroborating evidence.

**E. Consequences for victims and institutions**

The effects of cyber extortion extend beyond the amount demanded. Individual victims may experience financial hardship, anxiety, reputational injury, or fear of exposure. Businesses may incur recovery costs, lose access to essential records, face interruption of services, and experience reduced customer confidence. Public institutions may encounter operational disruption that affects service delivery and public trust.

[6] Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 308, 351, INDIA CODE (2023); Information Technology Act, No. 21 of 2000, §§ 66C, 66E, INDIA CODE (2000).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Victims may also hesitate to report incidents because of embarrassment, concerns about confidentiality, uncertainty regarding the reporting process, or fear that disclosure will attract further attention. Organisations may face difficult decisions about system recovery, communication with affected persons, regulatory obligations, and engagement with law-enforcement authorities. These circumstances demonstrate why an effective response must combine criminal investigation with prevention, evidence preservation, institutional preparedness, and appropriate victim support.

### F. Analytical conclusion

Cyber extortion is a varied category of digitally facilitated coercive conduct rather than a uniform technological offence. Ransomware, double extortion, threats to disclose confidential information, and online blackmail illustrate how offenders may exploit digital systems and the sensitivity of stored information to obtain unlawful advantages. Although these methods differ technically, they may share the use of threats or coercive demands as a means of securing compliance.

The distinction between cyber extortion and related offences is essential to accurate legal analysis. The applicable provisions of the BNS and the Information Technology Act must be assessed according to the particular facts, evidence, and ingredients of each offence. Understanding the methods and consequences of cyber extortion therefore provides the foundation for examining India's legal framework, the challenges of investigation and prosecution, and the reforms necessary to strengthen accountability and victim protection.

## III. Legal framework governing cyber extortion in India

### A. The Information Technology Act, 2000

The Information Technology Act, 2000 (IT Act), constitutes the principal Indian legislation addressing unauthorised access to computer systems, interference with digital information and specified forms of cybercrime. Although the Act does not establish a single, comprehensive offence called "cyber extortion," several of its provisions may apply where extortion involves hacking, data theft, system disruption, identity misuse or the circulation of unlawful digital content. Its application depends upon the specific conduct, the intention of the accused and the evidence available in each case.[7]

Section 43 addresses unauthorised acts involving computer systems and networks, including unauthorised access, downloading or extraction of data, introduction of computer contaminants,

[7] Information Technology Act, No. 21 of 2000, §§ 43, 66, India Code (2000).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

damage to computer resources and denial of authorised access. These provisions are particularly relevant to ransomware incidents in which attackers infiltrate a network, extract confidential information or prevent legitimate users from accessing their systems. Section 43 principally provides for liability to pay compensation; where the acts specified in that section are committed dishonestly or fraudulently, section 66 may impose criminal punishment. Accordingly, the two provisions must be read together where the facts establish the necessary elements.[8]

Other provisions may become relevant when cyber extortion involves impersonation, stolen credentials or violations of privacy. Section 66C criminalises the fraudulent or dishonest use of another person's electronic signature, password or other unique identification feature. Section 66D addresses cheating by personation through a communication device or computer resource. Section 66E concerns the intentional or knowing capture, publication or transmission of images of a person's private area without consent in circumstances violating privacy. These provisions may apply to particular forms of digital blackmail, but they should not be treated as automatically applicable to every extortion incident.[9]

**B. The Bharatiya Nyaya Sanhita, 2023**

The Bharatiya Nyaya Sanhita, 2023 (BNS), which replaced the Indian Penal Code, 1860, provides the general criminal-law framework for offences involving extortion, threats and related conduct. Section 308(1) defines extortion as intentionally putting a person in fear of injury and thereby dishonestly inducing that person to deliver property, a valuable security or anything signed or sealed that may be converted into a valuable security. Its illustration (a), a threat to publish a defamatory libel unless money is paid, demonstrates its potential relevance to online blackmail and threats to disclose damaging information. The provision may therefore apply where the required elements are established, regardless of whether the threat is communicated physically or through digital means.[10]

Section 351 of the BNS addresses criminal intimidation. It applies where a person threatens another, by any means, with any injury to his or her person, reputation or property, or to the person or reputation of anyone in whom that person is interested, with the intention specified in the provision. Online threats to expose private information, damage a victim's reputation or cause other forms of harm may fall within its scope where the statutory requirements are satisfied. However, the existence of a threatening message alone does not conclusively establish

[8] Information Technology Act, No. 21 of 2000, §§ 43, 66, INDIA CODE (2000).
[9] Information Technology Act, No. 21 of 2000, §§ 66C–66E, INDIA CODE (2000).
[10] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 308(1) & illus. (a), INDIA CODE (2023).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

criminal intimidation; the nature of the threat, the intention behind it and the surrounding circumstances require examination.[11]

The BNS and the Information Technology Act perform complementary functions. The BNS addresses the coercive demand and associated threats, while the IT Act may address the technological conduct used to facilitate the offence. Depending on the facts, the same incident may involve more than one legally distinct offence. Investigators and prosecutors must nevertheless establish the ingredients of each charged offence rather than assume that every cyberattack involving a demand for payment automatically constitutes extortion under section 308.

**C. Procedural law and digital evidence**

The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), establishes the procedural framework governing criminal investigation, inquiry and trial. In cyber extortion cases, effective investigation may require the collection of electronic communications, transaction records, access logs, device data and information obtained from relevant service providers. Investigators must follow applicable legal procedures when obtaining and preserving such material. Delays in securing volatile evidence can make it difficult to reconstruct the attack, identify the person responsible or demonstrate the connection between the threat and the demand for payment.[12]

The Bharatiya Sakshya Adhiniyam, 2023 (BSA), governs the law of evidence, including the admissibility of electronic and digital records. Section 63 addresses the admissibility of electronic records subject to the statutory conditions governing their production. Messages, emails, screenshots, digital files and system records may be important to proving the communication of a threat, the demand for money and the surrounding events. Their evidentiary value, however, depends on compliance with applicable requirements and the ability to establish their authenticity and reliability. A screenshot, considered in isolation, may not adequately establish who created a message, whether it has been altered or how it is connected to the accused.[13]

Maintaining an appropriate chain of custody is also important. Investigators should document the collection, transfer, storage and examination of relevant electronic material, while preserving available metadata and other information that may assist verification. Where the evidence is obtained from overseas service providers or involves foreign-hosted infrastructure, additional cooperation and lawful information-gathering procedures may be necessary. The

[11] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 351(1), INDIA CODE (2023).
[12] Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, INDIA CODE (2023).
[13] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63, INDIA CODE (2023).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

procedural and evidentiary framework is therefore central not merely to prosecuting an offence, but also to ensuring that the evidence relied upon is legally obtained and capable of withstanding judicial scrutiny.

### D. Institutional responsibilities and enforcement limitations

India's cybercrime response also involves specialised institutions and reporting mechanisms. The Indian Computer Emergency Response Team (CERT-In) performs functions relating to cyber incident response, while law-enforcement agencies investigate suspected criminal conduct.[14] CERT-In's technical and incident-response role should be distinguished from the criminal investigation and prosecution functions of the police and other competent authorities. Cooperation among affected organisations, incident-response teams, service providers and investigators can help preserve evidence and reduce the consequences of an attack.

Despite the existence of relevant laws, enforcement remains challenging. Attackers may conceal their identities through compromised accounts, anonymisation services, cryptocurrency transactions and infrastructure located in multiple jurisdictions. Victims may delay reporting because of reputational concerns, fear of further disclosure or uncertainty about the appropriate authority. Small businesses and individuals may also lack the technical resources required to preserve evidence or recover compromised systems.

These limitations reveal that the legal framework is distributed across substantive criminal law, cyber-specific legislation, criminal procedure and evidentiary rules. Although these laws provide important tools for addressing cyber extortion, effective enforcement depends on timely reporting, technically competent investigation, cross-border cooperation and reliable digital evidence. A stronger response therefore requires both consistent application of existing provisions and continuing institutional capacity-building.

## IV. Judicial approach and enforcement challenges

### A. Judicial recognition of cybercrime and electronic evidence

The effectiveness of India's legal response to cyber extortion depends not only on statutory provisions but also on their interpretation and application by courts. Judicial decisions concerning electronic evidence, cybercrime and the misuse of digital technologies provide important principles for investigating and prosecuting offences involving online threats, unauthorised access and digital coercion. Courts must balance the need to address emerging

[14] Information Technology Act, No. 21 of 2000, § 70B(1), (4), India Code (2000) (Indian Computer Emergency Response Team to serve as the national agency for incident response).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

technological threats with the requirement that criminal liability be established through reliable evidence and in accordance with procedural safeguards.

In *Anvar P.V. v. P.K. Basheer*, the Supreme Court emphasised the statutory requirements governing the admissibility of electronic records under section 65B of the former Indian Evidence Act, 1872. The judgment established the importance of complying with the special requirements for admitting secondary electronic evidence. Although the Bharatiya Sakshya Adhiniyam, 2023, now governs the admissibility of electronic records, the decision remains relevant to understanding the historical development of India's electronic-evidence jurisprudence. Its continuing application must, however, be assessed in light of the wording of the current legislation.[15]

Similarly, in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, the Supreme Court reiterated that the certificate required by section 65B(4) of the former Evidence Act is a condition precedent to the admissibility of evidence by way of an electronic record. The decision highlighted that digital material cannot always be admitted merely because it is presented in electronic form. In cyber extortion cases, where prosecution may depend on emails, messaging applications, screenshots or system logs, questions of authenticity and compliance with evidentiary requirements can directly affect the outcome of proceedings. The principles developed under the earlier law must be considered alongside the corresponding provisions of the BSA.[16]

**B. Identification of accused persons and attribution challenges**

A major enforcement difficulty arises from the challenge of connecting an online threat to a particular individual. Cyber extortionists may use false identities, compromised accounts, virtual private networks, proxy servers and infrastructure distributed across several countries. Even when investigators identify an internet protocol address or an account associated with a threat, that information may not independently establish who operated the device or sent the communication. Investigations must therefore consider multiple sources of evidence, including device records, account activity, transaction histories, communication patterns and relevant service-provider information.

Attribution becomes more complicated when attackers operate through intermediaries or exploit compromised systems belonging to innocent users. A computer may be used to send a threat without its registered owner having any knowledge of the activity. Consequently, investigators

[15] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473 (India).
[16] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 (India).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

must distinguish between identifying a device, identifying an account holder and proving the identity and intention of the person responsible. Failure to make these distinctions can weaken prosecution and risk attributing criminal conduct to the wrong person.

### C. Jurisdiction and cross-border cooperation

Cyber extortion frequently involves conduct extending beyond national boundaries. An attacker may operate from one country, use servers located in another, target an Indian victim and demand payment through an international financial or cryptocurrency platform. This creates practical difficulties in obtaining electronic evidence, identifying suspects and coordinating investigative action across jurisdictions. Differences in legal procedures, data-retention practices and cooperation mechanisms may delay the collection of information that is essential to a successful investigation.

Although Indian law provides a basis for addressing specified cyber offences and criminal conduct affecting persons or systems within its jurisdiction,[17] enforcement may depend on cooperation with foreign authorities and service providers. Requests for records can take time, while some digital information may be deleted or become inaccessible before the relevant procedures are completed. International cooperation, timely preservation requests and specialised investigative capacity are therefore important to ensuring that jurisdictional complexity does not undermine accountability.

### D. Reporting, investigation and institutional limitations

Underreporting is another obstacle to effective enforcement. Individuals may avoid reporting cyber extortion because they fear embarrassment, reputational damage, further exposure of private information or retaliation by the offender. Businesses may also be reluctant to disclose ransomware incidents because of concerns about customer confidence, commercial disruption or regulatory consequences. Such delays can deprive investigators of early access to digital evidence and allow offenders to continue targeting additional victims.

The technical complexity of cyber extortion also places demands on law-enforcement agencies. Investigators require training in digital forensics, preservation of electronic records, cryptocurrency tracing and the analysis of malicious software. Coordination among police, technical response organisations, financial institutions and digital service providers is necessary

[17] Information Technology Act, No. 21 of 2000, § 75, INDIA CODE (2000) (applying the Act to an offence or contravention committed outside India by any person, irrespective of nationality, where the conduct involves a computer, computer system or computer network located in India).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

because different entities may hold different parts of the evidentiary record. Inadequate coordination can produce fragmented investigations and delay the identification of offenders.

### E. Critical assessment

The judicial and enforcement challenges surrounding cyber extortion demonstrate that the existence of criminal provisions alone cannot guarantee effective prosecution. The legal framework must be supported by reliable electronic evidence, appropriate investigative procedures and institutional expertise. Judicial decisions concerning electronic records underscore the importance of authenticity and evidentiary compliance, while the practical realities of anonymity and cross-border infrastructure expose the limitations of investigations confined to conventional methods.

A more effective response requires timely reporting, consistent evidence-preservation practices, specialised training and improved coordination between domestic agencies and international counterparts. At the same time, investigative measures must respect privacy, procedural fairness and the presumption of innocence. Strengthening enforcement should therefore involve both greater technical capability and rigorous adherence to legal safeguards. These considerations provide the foundation for assessing the remaining legal gaps and developing targeted recommendations for addressing cyber extortion in India.

## V. Critical analysis of emerging threats and legal gaps

### A. Fragmented legal framework and classification difficulties

India's legal framework provides several provisions that may be applied to cyber extortion, but the absence of a single, comprehensive statutory definition of the offence creates challenges in classification and enforcement. Depending on the circumstances, an incident may involve extortion, criminal intimidation, unauthorised access, identity theft or other offences under the Bharatiya Nyaya Sanhita, 2023 (BNS), and the Information Technology Act, 2000. Although this flexibility enables authorities to address different forms of misconduct, it may also create uncertainty about the appropriate charges, the relationship between overlapping provisions and the evidence required to establish each offence.

The difficulty becomes more significant as cyber extortion evolves beyond conventional threats for money. Ransomware, threats to publish confidential information, impersonation and coercion through compromised digital accounts may involve different forms of criminal conduct within the same incident. The legal framework must therefore be applied according to the specific facts rather than through a general assumption that every digital demand for

payment constitutes the same offence. Clearer guidance on classification and investigation could promote consistency without unnecessarily duplicating existing criminal provisions.

**B. Technological change and the limits of traditional investigation**

The rapid development of cyberattack techniques exposes the limitations of investigative methods designed primarily around identifiable individuals, physical locations and conventional documentary evidence. Cyber extortionists may conceal their identities through anonymisation tools, compromised devices and infrastructure distributed across different jurisdictions. In ransomware incidents, attackers may encrypt information, extract sensitive files and threaten public disclosure, placing victims under pressure to pay before investigators can establish the origin and scope of the attack.

These circumstances create a substantial gap between the speed of digital offending and the time required for lawful investigation. Electronic evidence may be deleted, altered or rendered inaccessible, while the attribution of an attack may depend on records held by several service providers. An internet protocol address, account name or cryptocurrency transaction may provide an investigative lead, but it does not necessarily establish the identity or intention of the offender. Effective enforcement therefore requires technically informed investigation and corroboration from multiple sources.

**C. Evidentiary challenges and procedural safeguards**

The Bharatiya Sakshya Adhiniyam, 2023, establishes the current statutory framework for electronic and digital evidence. Nevertheless, the admissibility and reliability of such evidence remain important practical concerns. Screenshots and forwarded messages may help demonstrate that a threat was communicated, but their evidentiary value depends on questions of authenticity, integrity, context and compliance with applicable legal requirements. Investigators must preserve relevant records and document their handling to reduce the risk of disputes over manipulation or incomplete evidence.

At the same time, strengthening digital investigations must not come at the expense of individual rights. Broad or insufficiently controlled access to private communications and personal data may create risks of disproportionate surveillance or misuse of information. Investigative powers should therefore be exercised within applicable legal limits, with appropriate attention to necessity, proportionality and procedural fairness. A credible response to cyber extortion must protect victims while ensuring that allegations are proved through reliable evidence and that innocent persons are not wrongly implicated.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

### D. Cross-border enforcement and institutional capacity

The transnational character of cyber extortion presents another significant limitation. Offenders may target Indian individuals or businesses while operating from abroad and relying on foreign-hosted servers or international payment channels. Investigators may need assistance from foreign authorities or service providers to obtain information, identify suspects and trace financial transfers. Differences in legal systems and delays in obtaining records can obstruct investigations, particularly where digital evidence is time-sensitive.

Institutional capacity also affects enforcement. Effective investigation requires trained personnel, appropriate forensic facilities and coordination among law-enforcement agencies, technical incident-response bodies and financial institutions. Smaller organisations and individual victims may lack the resources to preserve evidence or respond effectively to attacks. Without accessible reporting mechanisms and timely technical assistance, existing legal protections may remain difficult to use in practice.

### E. Need for a balanced and practical response

The principal weakness in India's response to cyber extortion is not simply the absence of criminal provisions. It is the difficulty of translating those provisions into timely, consistent and evidence-based enforcement. Legislative clarification may be useful, but it should be accompanied by improved investigative capability, reliable evidence-preservation practices, public awareness and stronger domestic and international cooperation.

A balanced response should prioritise rapid reporting, specialised digital-forensic training and clearer coordination between technical responders and criminal investigators. Organisations should also adopt incident-response plans, secure backup systems and procedures for preserving relevant records. Victims require accessible guidance on reporting incidents and protecting compromised accounts, while enforcement authorities must maintain appropriate safeguards for privacy and due process.

Ultimately, cyber extortion is both a legal and a technological challenge. India's existing laws provide a foundation for addressing many of its constituent acts, but their effectiveness depends on coherent application and practical enforcement. Continuous review of emerging methods, combined with proportionate investigative powers and institutional preparedness, offers a more sustainable response than relying exclusively on the creation of additional offences.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

## VI. Findings and recommendations

### A. Principal findings of the study

The analysis of cyber extortion in India demonstrates that digital technologies have expanded the methods through which individuals and organisations can be threatened, coerced and financially exploited. Ransomware, unauthorised access to confidential information, threats to disclose private material and online blackmail illustrate how traditional forms of extortion can operate through digital platforms. These activities can cause financial loss, reputational damage, psychological distress and disruption to essential business operations. The consequences may extend beyond the immediate victim where compromised systems contain the personal or commercial information of others.

The first major finding is that India's existing legal framework provides several avenues for addressing cyber extortion, even though the relevant provisions are distributed across different enactments. The Information Technology Act, 2000, addresses specified computer-related offences, while the Bharatiya Nyaya Sanhita, 2023, contains provisions relating to extortion and criminal intimidation. Their application depends on the facts and the ingredients of the particular offence. The absence of a single comprehensive statutory framework specifically devoted to cyber extortion may complicate classification and consistent enforcement.

The second finding concerns the central importance of electronic evidence. Cyber extortion investigations frequently depend on digital communications, account records, device information, transaction histories and system logs. The Bharatiya Sakshya Adhiniyam, 2023, provides the applicable evidentiary framework for electronic and digital records. However, investigators must establish authenticity, preserve relevant information and comply with applicable admissibility requirements. Technical evidence that cannot reliably be connected to the alleged offender may be insufficient to establish criminal responsibility.

The third finding is that enforcement difficulties are not exclusively legislative. Anonymity, cross-border infrastructure, delays in obtaining information and limited technical capacity can impede investigations. Underreporting further complicates the response because victims may fear reputational harm, exposure of private information or retaliation. Consequently, effective enforcement requires institutional preparedness, cooperation and timely preservation of evidence alongside appropriate criminal provisions.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

### B. Recommendations for legislative and policy improvement

First, the application of existing laws should be clarified through practical guidance for investigators and prosecutors. Such guidance should explain how the relevant provisions of the BNS and the Information Technology Act may apply to different forms of cyber extortion, including ransomware, digital blackmail and threats to disclose confidential information. It should also distinguish between offences involving coercive demands and the separate technological conduct used to facilitate them. This would promote consistency without automatically treating every cyber incident as the same offence.

Second, the government and relevant institutions should periodically assess whether existing legislation adequately addresses emerging methods of digital coercion. Any proposal for a new offence or legislative amendment should be supported by evidence of a genuine legal gap and carefully evaluated against existing provisions. The objective should be to improve clarity and effectiveness rather than create unnecessary duplication or excessive criminal liability.

Third, law-enforcement agencies should receive regular training in digital forensics, electronic-evidence preservation, analysis of malicious software and tracing of digital financial transactions. Investigators should be equipped to document the collection and handling of electronic records and to distinguish technical indicators from proof of an individual's criminal responsibility. Investment in specialised personnel and forensic facilities would strengthen the quality of investigations and reduce avoidable evidentiary weaknesses.

### C. Institutional coordination and victim protection

Coordination between police, technical incident-response organisations, financial institutions and digital service providers should be strengthened. Clear procedures for reporting incidents, preserving relevant records and referring cases to appropriate authorities could reduce delays. Cross-border cases would benefit from timely cooperation with competent foreign authorities and service providers, subject to applicable legal requirements and safeguards.

Accessible reporting and victim-support mechanisms should be improved. Individuals and organisations should receive clear information about reporting cyber extortion, securing compromised accounts, preserving threatening communications and seeking technical assistance. Victims should be encouraged to report incidents promptly, without being discouraged by unnecessary procedural complexity or fear of public embarrassment. Businesses should also establish incident-response plans that identify responsibilities for legal reporting, technical containment and evidence preservation.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Preventive measures should form an essential part of the response. Organisations should adopt regular software updates, multifactor authentication, access controls, secure backups and employee awareness programmes. Individuals should be encouraged to use strong authentication practices, avoid sharing sensitive information with unverified contacts and report suspicious communications. Prevention cannot eliminate cyber extortion, but it can reduce opportunities for attacks and limit their consequences.

### D. Safeguards and implementation

Finally, stronger enforcement must remain consistent with privacy, proportionality and due process. Access to electronic information should comply with applicable law, and investigative conclusions should be supported by reliable evidence. Periodic assessment of reporting trends, investigation outcomes and recurring evidentiary difficulties would help policymakers identify where further reforms are justified.

These recommendations are complementary rather than independent. Legislative clarity without technical capacity may produce limited results, while technical capability without procedural safeguards may undermine public confidence. India's response should therefore combine appropriate legal interpretation, skilled investigation, institutional cooperation, victim support and preventive cybersecurity. Such a coordinated approach offers a practical foundation for addressing the evolving threat of cyber extortion while preserving the principles of fairness and accountability.

## VII. Conclusion

Cyber extortion has emerged as a significant challenge in India's increasingly digital environment, where individuals, businesses and institutions depend on interconnected systems for communication, financial transactions and the storage of sensitive information. The expansion of digital services has created new opportunities for economic and social development, but it has also enabled offenders to use technology to threaten, coerce and exploit victims. Ransomware attacks, unauthorised access to confidential information, threats of public disclosure and online blackmail demonstrate how conventional forms of extortion can be adapted to digital environments. The resulting harm extends beyond financial loss to include reputational damage, psychological distress, disruption of business operations and the erosion of trust in digital services.

This study examined the legal framework governing cyber extortion in India, the challenges associated with its enforcement and the adequacy of existing responses to emerging threats. The analysis establishes that Indian law provides several provisions capable of addressing different

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

aspects of cyber extortion. The Information Technology Act, 2000, addresses specified forms of unauthorised access, computer-related offences and misuse of digital resources, while the Bharatiya Nyaya Sanhita, 2023, contains provisions concerning extortion and criminal intimidation. The Bharatiya Nagarik Suraksha Sanhita, 2023, governs relevant criminal procedures, and the Bharatiya Sakshya Adhiniyam, 2023, establishes the evidentiary framework applicable to electronic and digital records. Together, these enactments provide a legal foundation for investigating and prosecuting cyber extortion, provided that the requirements of the relevant provisions are established in each case.

Nevertheless, the existence of applicable laws does not, by itself, ensure effective enforcement. The study identifies significant practical obstacles, including the difficulty of attributing online conduct to a particular offender, the preservation and authentication of electronic evidence, delays in obtaining information, cross-border jurisdictional complications and insufficient technical capacity. Victims may also hesitate to report incidents because of embarrassment, fear of reputational harm or concern about further exposure of confidential information. These factors may allow offenders to evade accountability and weaken the effectiveness of otherwise applicable legal remedies.

The research therefore indicates that an effective response requires more than the introduction of additional criminal provisions. Clearer guidance on the application of existing laws, specialised training for investigators, improved digital-forensic facilities, stronger coordination among relevant institutions and timely international cooperation are essential. Accessible reporting mechanisms and greater public awareness can encourage early reporting, while preventive measures such as secure backups, multifactor authentication and regular cybersecurity assessments can reduce vulnerability. Any strengthening of investigative powers must also remain consistent with privacy, procedural fairness and the presumption of innocence.

Ultimately, cyber extortion should be understood as both a legal and a technological problem. Its evolving methods require a coordinated response that combines appropriate legislation, reliable evidence, institutional preparedness and effective victim support. India's existing legal framework provides an important starting point, but its practical effectiveness depends on consistent interpretation, timely investigation and the capacity to respond to changing technological conditions. A balanced approach that combines enforcement with prevention and safeguards for individual rights offers the strongest foundation for addressing cyber extortion. Continued assessment of emerging threats and enforcement outcomes will be necessary to ensure that India's legal response remains effective, proportionate and responsive to the realities of digital crime.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]