

A STUDY OF LAWS RELATED TO EXTORTION IN INDIA

AUTHORS – YATIN* & SACHIN KUMAR**

* B.A.LL.B. (H), LAW COLLEGE DEHRADUN, FACULTY OF UTTARANCHAL UNIVERSITY. Email –
YATINJAGLAN01@GMAIL.COM

** ASSISTANT PROFESSOR, LAW COLLEGE DEHRADUN, FACULTY OF UTTARANCHAL UNIVERSITY. Email –
SACHINKUMAR@UTTARANCHALUNIVERSITY.AC.IN

BEST CITATION – YATIN & SACHIN KUMAR, A STUDY OF LAWS RELATED TO EXTORTION IN INDIA, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 5 (7) OF 2025, PG. 519-528, APIS – 3920 – 0001 & ISSN – 2583-2344

Abstract

"In this research paper, the legal framework that governs extortion in India is investigated. The article traces the growth of this framework from regulations from the colonial era to present legislation. The purpose of this study is to investigate the difficulties associated with prosecution, various enforcement gaps, and developing trends in extortion cases. This is accomplished via the examination of legislative provisions, major court judgements, and comparative viewpoints. The findings of this study underline the necessity of legislative reforms to address digital extortion and organised crime while maintaining a balance between punitive measures and preventative tactics. The proposals for enhancing the legal framework against extortion in the context of India are presented as the final section of the report after it is finished."

Keywords: Extortion, Indian Penal Code, Criminal Law, Cyber Extortion, Legal Reforms

Introduction

Throughout the course of human history, extortion, which may be defined as the act of gaining something of value via the use of force, threats, or intimidation, has been a persistent criminal activity. There have been many different manifestations of extortion in India, ranging from classic criminal actions to sophisticated cybercrime operations. Particularly via the Indian Penal Code (IPC) of 1860, the Indian legal system has built a comprehensive framework to fight extortion. This framework is reinforced by specialised law that addresses specific circumstances such as organised crime and cybercrime.

The prevalence of extortion in India poses substantial problems to the rule of law, as well as to the growth of the economy and the protection of individual rights. Extortion incidents have been showing a disturbing rising

trend in recent years, according to the National Crime Records Bureau (NCRB), with considerable variances between different states and union territories (NCRB, 2023). This tendency has been seen in recent years. Over the course of history, urban centres like as Mumbai, Delhi, and Bengaluru have been known to have greater rates of extortion, particularly those that are associated with economic activity and real estate transactions. On the other hand, extortion is becoming more prevalent in rural regions as well, with protection rackets and agricultural extortion schemes focussing on local businesses and farmers.

The transition of Indian society into a digital society has also resulted in the creation of new vulnerabilities and opportunities for extortion. In order to get money from individuals and organisations, cybercriminals are now employing methods such as data breaches,

ransomware attacks, and digital blackmail (Bhasin, 2022). The old legal structure that governs extortion in India is facing considerable problems as a result of this growth in criminal behaviour.

In order to give a complete study of the legislative provisions that handle extortion in India, the purpose of this research is to investigate the effectiveness of these laws, identify any gaps in coverage, and investigate the possibility of revisions. The purpose of this research is to provide a contribution to the ongoing discussion on the enhancement of India's legal response to extortion in all of its forms by means of legislative analysis, case study examination, and comparative assessment.

Historical Evolution of Extortion Laws in India

Colonial Origins and the Indian Penal Code

In India, the legal prohibitions that prohibit extortion may be traced back to the colonial legal system that was imposed by the British. The Indian Penal Code (IPC), which was draughted by the First Law Commission and implemented in 1860, continues to be the major legislative instrument that specifically addresses extortion. Lord Macaulay served as the chairperson of the commission. The IPC provides a definition of extortion as follows: "Whoever intentionally puts any person in fear of any injury to that person, or to any other, and thereby dishonestly induces the person so put in fear to deliver to any person any property or valuable security, or anything signed or sealed which may be converted into a valuable security, commits extortion" (Indian Code of Criminal Procedure, 1860).

This definition describes the key components of the crime, which are the instillation of fear, the desire to commit dishonesty, and the acquisition of property or valuable security as a result of the crime. It was recognised by the colonial lawmakers that extortion was a separate crime from theft and robbery. They positioned it as a crime against property, but

one that included compulsion rather than direct physical seizing.

Section 384 provides that the punishment for extortion is a fine, imprisonment for up to three years, or both. The maximum sentence for extortion is three years in jail. With escalating penalties based on circumstances such as putting a person in fear of death or grievous hurt, extortion by threat of accusation of an offence, and extortion by putting a person in fear of accusation of offences affecting reputation, the Indian Penal Code (IPC) also provides for aggravated forms of extortion, which are outlined in Sections 385-389.

Post-Independence Developments

Following the country's attainment of independence in 1947, the legal structure that had been inherited from the colonial era was substantially preserved, including measures that were associated with extortion regulations. However, interpretations changed throughout time as a result of judicial declarations, and new law was enacted in order to handle certain forms of extortion from time to time.

The passage of the Terrorist and Disruptive Activities (Prevention) Act (TADA) in 1985 was a momentous event. This act was subsequently succeeded by the Prevention of Terrorism Act (POTA) in 2002, and then by the Unlawful Activities (Prevention) Act (UAPA) in the years that followed. By providing for increased fines and unique procedural measures, these pieces of law tackled extortion in a roundabout way when it was perpetrated in the context of terrorist activity.

Another significant legislative reaction was the Maharashtra Control of Organised Crime Act (MCOCA) of 1999, which was enacted with the intention of precisely targeting organised crime syndicates that frequently participated in systematic extortion. Other states, like as Karnataka, Gujarat, and Delhi, soon passed legislation that was quite similar to the one that was passed in Delhi (Dhavan, 2021).

The Information Technology Act of 2000, which was revised in 2008, expanded the legal framework to the digital world. It addressed cyber extortion and online threats, despite the fact that it did not use the term "extortion" directly in its provisions.

Current Legal Framework

Extortion under the Bharatiya Nyaya Sanhita (BNS), 2023

The Bharatiya Nyaya Sanhita (BNS), 2023, which replaced the Indian Penal Code (IPC) of 1860, defines and penalizes extortion under Section 308. This provision is similar to the earlier Section 383 of the IPC but with some modifications in the punishment structure.

Definition of Extortion

Under Section 308 of the BNS, extortion is defined as:

"Whoever intentionally puts any person in fear of any injury to that person, or to any other, and thereby dishonestly induces the person so put in fear to deliver to any person any property or valuable security, or anything signed or sealed which may be converted into a valuable security, commits extortion."

Essential Elements of Extortion

1. Putting a person in fear of injury (to themselves or others)
2. Dishonestly inducing the frightened person to deliver:
 - Property
 - Valuable security
 - Documents that can be converted into valuable security

Punishment for Extortion

Section 309 of the BNS prescribes punishment for extortion:

- Imprisonment for up to 3 years, or
- Fine, or
- Both

Aggravated Forms of Extortion

The BNS also recognizes more serious forms of extortion:

1. **Extortion by putting a person in fear of death or grievous hurt** (Section 310)
 - Imprisonment for up to 10 years
 - Fine
2. **Extortion by threat of accusation of an offense** (Section 311)
 - If the offense threatened carries a capital punishment: Imprisonment up to 10 years and fine
 - If the offense threatened carries life imprisonment: Imprisonment up to 7 years and fine
 - In other cases: Imprisonment up to 3 years and fine

Difference from Robbery

It's worth noting that extortion differs from robbery in that:

- In robbery, there is immediate taking of property through force or fear
- In extortion, the property is delivered by the victim under the influence of fear induced by the threat

Special and Local Laws

Several specialized legislations address extortion in specific contexts:

1. **Maharashtra Control of Organised Crime Act (MCOCA), 1999:** Targets specifically organised criminal syndicates that engage in extortion on a systematic basis. Organisational crime, which includes extortion, is subject to severe punishments as outlined in Section 3 of the MCOCA, which includes imprisonment for a period ranging from five years to life. The Karnataka Control of Organised Crime Act, which was passed in the year 2000, and the Gujarat

Control of Terrorism and Organised Crime Act, which was passed in the year 2015, are two examples of laws that are comparable to one another.

2. **Information Technology Act, 2000 (as amended in 2008):** There are many clauses that address conduct that may constitute cyber extortion; however, the term "extortion" is not specifically used within these provisions:

- Section 66E (violation of privacy)
- Section 67 (publishing obscene material)
- Section 66F (cyber terrorism, which may include ransom demands)
- Section 43 (unauthorized access to computer systems, relevant to ransomware attacks)

3. **Prevention of Money Laundering Act (PMLA), 2002:** This approach targets the proceeds of criminal activity in order to address the financial components of extortion. According to the PMLA, extortion is a scheduled offence, which means that the authorities have the authority to investigate and seize any gains that are earned from extortion.

4. **Unlawful Activities (Prevention) Act (UAPA):** The United States Anti-Terrorism Act (UAPA) establishes a legal foundation for prosecution with heightened penalties in situations when extortion is perpetrated in the context of terrorist operations or to support terrorist activities.

Procedural Aspects

The Code of Criminal Procedure (CrPC), 1973, governs the procedural aspects of investigating and prosecuting extortion cases. Key provisions include:

1. **Section 154:** Mandates registration of First Information Report (FIR) for cognizable offenses, including extortion.
2. **Section 161-164:** Regulates the recording of statements from witnesses and confessions.
3. **Section 173:** Governs the filing of police reports upon completion of investigation.
4. **Section 190:** Empowers Magistrates to take cognizance of offenses upon receiving complaints or police reports.

The crime of extortion is considered a cognisable offence, which means that the police are able to make arrests without a warrant and that a judicial order is necessary for the release of the defendant on bail. It is the responsibility of the prosecution to prove all of the components of the offence beyond any reasonable doubt. The burden of proof lies alone with the prosecution.

Judicial Interpretation and Landmark Cases

In the process of interpreting and applying extortion laws, Indian courts have significantly contributed to the process. Legal understanding of extortion has been affected by a number of major judgements, including the following:

Elements of Extortion

The Supreme Court of India made it clear in the case of *State of Maharashtra v. Mohd. Yakub* (1980) that in order for an act to be considered extortion, it is necessary to establish all of the elements that are defined in Section 383. These elements include the instigation of fear, the demonstration of dishonest intention, and the actual delivery of property or valuable security as a consequence of such fear.

It was established in the case of *Romesh Chandra Arora v. State* (1960) that the threat does not have to be explicit; rather, it can be inferred from the circumstances and the behaviour of the accused. Because of this, the definition of "putting a person in fear" under

Section 383 was enlarged to include more circumstances.

Distinction from Other Offenses

The Supreme Court of the United States made a distinction between extortion and robbery in the case of *Gurucharan Singh v. State* (1978). The court pointed out that although both entail the acquisition of property via the use of fear, robbery also requires the use of force or the imminent threat of force.

In the case of *Bhanuprasad Hariprasad Dave v. State of Gujarat* (1968), a distinction was made between extortion and criminal intimidation. The case highlighted the fact that extortion requires the additional element of dishonestly inducing the delivery of property, whereas criminal intimidation merely involves threatening with injury.

Evidence and Proof

In the case of *Ramesh Kumar v. State of Haryana* (2003), it was emphasised that circumstantial evidence might be sufficient to show extortion even in the lack of direct proof, provided that the circumstances create a full chain pointing to the guilt of the accused.

In the case of *Rajiv Kumar v. State* (2011), the Delhi High Court emphasised the significance of corroborative evidence in extortion cases, particularly in situations when the testimony of the complainant serves as the primary basis for prosecution.

Organized Crime and Extortion

The constitutionality of special legislation that targets organised crime was established in the landmark decision of *Kartar Singh v. State of Punjab* (1994). This law included measures that addressed the systematic extortion that is carried out by criminal syndicates.

The case of *Yakub Abdul Razak Memon v. State of Maharashtra* (2013) recognised the connection between extortion and organised crime and confirmed the application of the Maharashtra Criminal Offences Commission

Act (MCOCA) to extortion rackets that were run by organised criminal gangs.

Digital Extortion

There is a growing body of legal precedent that tackles digital forms of extortion. The court acknowledged the extent to which pre-existing legal rules can be used to digital threats and coercion in the case of *CBI v. Arif Azim* (2003), which was one of the first cybercrime trials conducted in India.

In a case that took place more recently, *Shreya Singhal v. Union of India* (2015), the Supreme Court of India held that other sections of the Information Technology Act and the Indian Penal Code continue to be available to address online threats and extortion. This was done while striking down Section 66A of the IT Act.

Challenges in Prosecution and Enforcement

Despite the comprehensive legal framework, several challenges persist in effectively prosecuting extortion cases in India:

→ Evidentiary Challenges

Because extortion frequently takes place in private settings with a small number of witnesses, it can be challenging to collect evidence that supports the allegations. It is common for victims to be threatened with reprisal if they testify, which can result in witnesses becoming hostile or recanting their statements. Significant evidential obstacles are presented by the necessity to demonstrate "dishonest intention" and real inducement of fear (Kumar, 2021).

→ Underreporting

The severe underreporting of extortion is mostly caused by a combination of factors, including fear of reprisal, lack of faith in law enforcement, and societal shame. Extortion in the business world, in particular, is frequently not reported because of worries over the possibility for harm to one's image and interruption to business operations. According to the findings of a survey that was carried out

by the Federation of Indian Chambers of Commerce and Industry (FICCI), roughly 72 percent of companies that were subjected to extortion did not disclose it to the relevant authorities (FICCI, 2022).

→ **Jurisdictional Challenges**

When it comes to investigations and prosecutions, digital extortion frequently contains aspects that span international borders, which presents jurisdictional issues. Extortion operations routinely span numerous states within India, necessitating cooperation between various police units. This is the case even inside India. It is because of the absence of consistent specialised units throughout states that there are differences in the capabilities of law enforcement.

→ **Technological Challenges**

When it comes to investigating complex digital extortion schemes, law enforcement authorities frequently lack the technical skills and resources necessary to do so. This is especially true for schemes that use darknet activities and cryptocurrencies. Additional obstacles are created while attempting to identify those who are responsible for cyber extortion through the use of encryption technology and anonymisation tools.

→ **Political Interference**

It is possible for there to be intervention in the investigation and prosecution of incidents of extortion that involve politically connected persons or that take place in politically sensitive circumstances. This difficulty is more obvious in situations when persons with political ties or those who are operating with political protection are involved in extortion (Shah, 2023).

Comparative Perspectives

Examining how other jurisdictions address extortion offers valuable insights for potential reforms in India:

United Kingdom

Section 21 of the Theft Act of 1968 in the United Kingdom tackles the issue of extortion by defining the crime of "blackmail" as a criminal offence that carries a maximum sentence of fourteen years in prison. Unwarranted requests with threats are the primary emphasis of the legislation, which is a notion that is more expansive than the Indian approach. Both the Computer Misuse Act of 1990 and the Serious Crime Act of 2015 have been enacted in the United Kingdom. These laws especially address cyber extortion and acts that are associated with organised crime.

United States

Legislation at both the federal and state levels in the United States tackles the issue of extortion. Extortion that has an effect on interstate trade is treated as a criminal offence under the Hobbs Act, which imposes penalties of up to twenty years in jail. It is also important to note that the Computer Fraud and Abuse Act has particular sections that target ransomware and digital extortion. The Racketeer Influenced and Corrupt Organisations Act (RICO Act) allows for the prosecution of organised extortion rackets by providing a thorough framework for such prosecutions.

Singapore

Although Singapore's Penal Code has provisions that are comparable to those found in India's, it has been amended more recently to meet contemporary types of extortion. There are particular provisions for cyber extortion that are included in the Computer Misuse Act. These provisions include penalties of up to ten years in jail and hefty fining. Additionally, Singapore has formed specialised cybercrime teams that are equipped with extremely superior technical skills.

Germany

Under Section 253 of the German Criminal Code (Strafgesetzbuch), extortion (also known as Erpressung) is addressed, and Section 255 of the same code tackles more severe versions of

the crime. The German approach places more of an emphasis on the economic harm that is created by extortion as opposed to concentrating exclusively on the strategies that are utilised. In addition, Germany has enacted extensive laws that addresses both organised criminal operations and cybercrime.

Emerging Trends and Challenges

Digital Extortion

Technological advancements have facilitated new forms of extortion:

1. **Ransomware Attacks:** Identity thieves encrypt the data of their victims and then demand money for the decryption keys. The Indian Computer Emergency Response Team (CERT-In) reported that the number of ransomware assaults grew by a factor of 120 percent in 2023 when compared to the previous year (CERT-In, 2023).
2. **Sextortion:** If the demands are not satisfied, the perpetrators threaten to expose photographs or recordings that might compromise the victim's safety. This type of extortion is mainly directed against persons who are weak, and it has shown a considerable increase in frequency as a result of the growth of social media platforms.
3. **Data Breach Extortion:** Unauthorised access is gained by criminals to databases, and they threaten to reveal critical information unless they are paid. This type of extortion is especially dangerous for corporate organisations because of their vulnerability.
4. **Cryptocurrency Facilitation:** However, due to the anonymity that cryptocurrencies offer, they have become the favoured mode of payment for digital extortion, which makes it more difficult to monitor the movement of financial resources.

Organized Criminal Networks

Organized criminal networks continue to evolve their extortion methodologies:

1. **Professionalization:** Extortion operations have been carried out by criminal syndicates that have developed corporate-like organisations with specialised positions for each of the many parts of the operations.
2. **Legitimate Business Infiltration:** A growing number of criminal organisations are using legitimate enterprises as fronts for extortion rackets, which is causing the border between legal and unlawful activity to become increasingly blurry.
3. **Transnational Operations:** Networks that engage in extortion are increasingly operating beyond national lines, taking advantage of globalisation to broaden their scope of influence while also complicating efforts to police laws.

Extortion in Specific Sectors

Certain sectors have become particularly vulnerable to extortion:

1. **Real Estate:** Developers and property owners are subject to systematic extortion, which is especially prevalent in metropolitan areas that are quickly growing.
2. **Entertainment Industry:** Throughout the course of history, both organised crime syndicates and opportunistic criminals have made it their mission to extort money from motion picture producers and actors.
3. **Small and Medium Enterprises:** SMEs frequently lack the resources necessary to implement security measures, which leaves them open to extortion tactics.
4. **Public Officials:** It is possible for government personnel to be subjected to extortion in connection with their

official activities, which can lead to instances of corruption and undermine public administration.

Recommendations for Reform

A number of reforms might increase India's legal response against extortion, according to an examination of existing legal provisions, problems to enforcement, comparative views, and developing trends. These reforms include the following suggestions:

Legislative Reforms

1. **Comprehensive Digital Extortion Provisions:** In order to expressly address the many different types of cyber extortion, such as ransomware attacks, sextortion, and data breach extortion, the Information Technology Act should be amended.
2. **Enhanced Penalties for Organized Extortion:** Implement a national legislation that is standardised and targets organised extortion rackets. This legislation should be comparable to the MCOCA but should have nationwide applicability.
3. **Witness Protection Framework:** In order to offer increased safeguards for witnesses in extortion cases, particularly those involving organised criminal organisations, the Witness Protection Scheme, 2018, should be strengthened.
4. **Harmonization of State Laws:** It is important to develop model legislation that governments might adopt in order to ensure that extortion is addressed in a consistent manner across all jurisdictions.

Procedural Reforms

1. **Specialized Investigation Units:** Dedicated anti-extortion cells should be established in each and every district. These units should be equipped with specialised training and resources to investigate the various types of extortion.

2. **Inter-Agency Coordination:** Formal structures should be established to facilitate cooperation between the many authorities that are engaged in the fight against extortion. These agencies include the police, cybercrime units, financial intelligence units, and overseas partners.

3. **Evidence Collection Protocols:** With regard to extortion cases, particularly those involving electronic communications and cryptocurrency transactions, the development of standardised standards for the collection and preservation of digital evidence is extremely important.

4. **Fast-Track Courts:** In order to expedite the trial of extortion cases, particularly those involving organised criminal organisations or key industries, special courts should be established.

Preventive Measures

1. **Public Awareness Campaigns:** It is important to implement targeted awareness campaigns that educate people about the various types of extortion and reporting systems, with a particular emphasis on vulnerable groups and sectors.

2. **Business Resilience Programs:** In order to strengthen the resistance of enterprises against extortion attempts, it is necessary to develop guidelines and support structures.

3. **Technological Solutions:** It is important to make investments in cutting-edge systems that can monitor, identify, and block efforts at digital extortion.

4. **International Cooperation:** It is important to strengthen international cooperation structures in order to handle the issue of cross-border extortion. These mechanisms should include joint investigative teams and mutual legal aid treaties.

Conclusion

In India, the legal system that addresses extortion has undergone substantial changes from its colonial beginnings. These changes have been made in response to shifting criminal practices and shifting cultural settings. Although the rules of the Indian Penal Code continue to be applicable, they need to be supplemented by specialised laws and procedural changes in order to solve the issues that are present in the modern world.

In addition to giving criminals with improved means for anonymity and reach, the digital revolution of Indian society has resulted in the creation of new vulnerabilities that are susceptible to extortion charges. At the same time, the professionalisation of criminal networks has led to a rise in the level of complexity of extortion operations, which has necessitated legal and police measures that are similarly sophisticated.

An effective response to the issue of extortion calls for a multi-pronged strategy that incorporates aspects of punitive, preventative, and protective measures. The implementation of legislative changes must be accompanied by the implementation of procedural innovations, capacity building, and preventative initiatives. A comprehensive response against extortion in all of its forms requires a number of vital components, including international collaboration and partnerships between the public and commercial sectors.

In light of the fact that extortion continues to exist in Indian culture and has even developed over time, it is imperative that legislative frameworks undergo ongoing evaluation and modification. India is able to improve its legal response to extortion and reduce the socioeconomic effect of the practice by gaining knowledge from other countries' experiences, making use of technology improvements, and addressing structural weaknesses.

References

- ✚ Bhasin, M. L. (2022). Cyber extortion: Trends, challenges and legal responses in the Indian context. *Journal of Financial Crime*, 29(1), 12-31.
- ✚ CERT-In. (2023). *Annual report on cybersecurity incidents in India*. Ministry of Electronics and Information Technology, Government of India.
- ✚ Dhavan, R. (2021). Special criminal legislation in India: Evolution and challenges. *National Law School of India Review*, 33(2), 45-63.
- ✚ Federation of Indian Chambers of Commerce and Industry (FICCI). (2022). *Survey on business security concerns in India*. FICCI Security Department.
- ✚ Indian Penal Code. (1860). Act No. 45 of 1860. Government of India.
- ✚ Information Technology Act. (2000). Act No. 21 of 2000. Government of India.
- ✚ Kumar, A. (2021). Evidentiary challenges in extortion prosecution: An empirical analysis. *Criminal Law Journal*, 127(3), 312-330.
- ✚ Maharashtra Control of Organised Crime Act. (1999). Act No. 30 of 1999. Government of Maharashtra.
- ✚ National Crime Records Bureau (NCRB). (2023). *Crime in India 2022 statistics*. Ministry of Home Affairs, Government of India.
- ✚ Shah, P. (2023). Political economy of organized crime and extortion in India's metropolitan centers. *Economic and Political Weekly*, 58(14), 54-62.
- ✚ Bhanuprasad Hariprasad Dave v. State of Gujarat, AIR 1968 SC 1323.
- ✚ CBI v. Arif Azim, Delhi District Court, 2003.
- ✚ Gurucharan Singh v. State, AIR 1978 SC 179.
- ✚ Kartar Singh v. State of Punjab, (1994) 3 SCC 569.
- ✚ Rajiv Kumar v. State, Delhi High Court, CRLA. 342/2011.
- ✚ Ramesh Kumar v. State of Haryana, (2003) 7 SCC 672.

- ✚ *Romesh Chandra Arora v. State*, AIR 1960 SC 154.
- ✚ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
- ✚ *State of Maharashtra v. Mohd. Yakub*, AIR 1980 SC 1111.
- ✚ *Yakub Abdul Razak Memon v. State of Maharashtra*, (2013) 13 SCC 1.

