EXTORTION LAWS AND JUDICIAL INTERPRETATION

Vaibhav Singh Payal, Law College Dehradun, Uttaranchal University

Ms. Purnima Tyagi, Law College Dehradun, Uttaranchal University

1. Introduction

This article broadly highlights the offence known as extortion, which has been identified under offences against property as enshrined in Sections 383 to 389 of the Indian Penal Code (IPC). Extortion is that state of affairs whereby a person either instils fear in another or threatens that person in order to compel him to hand over to another person property, valuable security, or a signed or sealed document which may be converted into valuable security. Generally speaking, threats of physical violence, damage to property, loss of money, or abuse of official power are covered by this term. The offence itself is complete by threatening alone; it does not require any actual money or property to be received.

Furthermore, in terms of international law, a very important piece of legislation enacted in December 2023 is the Foreign Extortion Prevention Act, which was signed into law by U.S. President Joe Biden. This federal law criminalizes the collecting or solicitation of bribes by foreign public officials, complementing the Foreign Corrupt Practices Act (FCPA) of 1977. Whereas the FCPA prohibits certain U.S. companies from bribing foreign officials, the FEPA reflects the opposite side of that regulation by penalizing foreign officials who would solicit these bribes. This approach makes the law much more symmetrical and should lead to greater transparency and fairness in the practice of international business[1].

Prevention of Corruption Act, 1988, is the chief legislation on bribery and corruption in India. Its hurdles were initially only up to public servants; subsequently, it has been widened to provide for persons entrusted with public functions. Earlier, the law only penalized a bribe-taker, and the bribe-giver faced no action unless the latter were charged with abetment. But after India's ratification of the United Nations Convention against Corruption (UNCAC), amendments were introduced into the PC Act to bring it into line with international standards. The reform now provides for the prosecution of both taker and giver of the bribe, including

[1] With the amendment to the US domestic bribery statute (Title 18, USC, s. 201)

companies. Thus, India's anti-corruption legislative framework is now better aligned with the global conventions, much like the rest of the legislative measures taken by the United States[2].

2. Extortion (Section 383 IPC) (Section 303 of BNS)

Extortion is defined in law as the use of intimidation, coercion, and threats to illegally get money, property, or valuables from an individual. It has been the practice of intimidation by physical harm or through blackmail, initiated mostly by criminal groups to extort payments from owners of businesses for fear of the worst consequences.

In the digital era, extortion has become modernized in the crime of cyberspace, where threats to a business are made concerning its digital assets or private data. Cyber extortion includes gaining access to an organization’s computer systems, stealing data, and threatening to destroy or release it unless a ransom demand is met. It is this kind of extortion that threatens businesses largely as every other firm becomes more and more data dependent and security conscious.

Extortion is defined, under Section 383 of Indian Penal Code, 1860, as "an act in which a human being induces the other intentionally, under threat of injury to self or another, into discharging property, valuable security, or anything convertible into such valuable asset." In other words, extortion is an induced transfer of property via threats or through fear, causing wrongful sample loss to the victim and unlawful sample gain to the perpetrator.

Illustrations:

1. Suppose X posing danger to Y, states that he would forcibly hold Y's daughter for ransom, and might not give her even a grain of food or a drop of water unless Y gave him a motorbike. Then Y in fright delivered the motorbike-X is guilty of extortion.

2. In another scenario, if M threatens N with the publication of alleged false slander unless the latter parts with property and N succumbs under the duress that is also extortion committed by M.

The act is a violation of personal rights that is furthermore considered a direct threat to public

[2] By way of Prevention of Corruption (Amendment) Act, 2018

safety and stability, rendering the crime much graver under Indian laws[3].

- ***Essential elements of extortion***

a. Intentionally Creating Fear of Injury or Damage - There must exist a dishonest intention, with unlawful gain to the accused and wrongful loss to the victim, for an act to fall under extortion. A vital part of the offence involves actual transfer of property made as a result of fear. In a matter of "R.S. Nayak v. A.R. Antulay (1984)"[4], "A.R. Antulay, the then Chief Minister", was accused of having influenced sugar cooperatives with a tacit suggestion that he would look into all the sugar cooperatives' pending matters if they contributed. However, the Supreme Court held there was no offence committed under extortion, with no evidence to suggest that the alleged act created fear or coercion. Thus, contributions were voluntary; an essential ingredient of threat or fear was absent.

b. Dishonest Consideration - Basically, dishonest consideration was to act as a medium of inducing the other party to part with his property. Prima facie, there has to be wrongful gain to the extortionist or his agent or wrongful loss to the person from whom the property is to be extorted with the intervention of delivery of the property. In this case, Biram Lal and Others v. State (2006)[5], the complainant alleged that the accused and others from their community unlawfully humiliated people and imposed excessive fines. The Court held that extortion means that the victim is dishonestly persuaded to hand over property under the influence of fear. If no property or valuable securities are delivered, it is denoted as "attempted extortion" unless the inducement to do so succeeds in making the victim consent to such a delivery, even if the delivery never occurs.

c. Transfer of Valuable Security- The property extorted could generally be made up of objects of value or any documentation possessing worth, barring unsigned or blank paper. Section 30 of the IPC defines "valuable security." For example, if a minor is coerced into signing any promissory note, as stated in this section, the perpetrator may be liable under extortion. In Anil B. Nadkarni and Others v. Amitesh Kumar (2001)[6], the accused argued that "for extortion, it is a must that the actual transfer of the property should be under pressure." This argument was

[3] Ibrahim, E., Sharif, H., & Aboelazm, K. S. (2025). Legal Confrontation of the Cyber Blackmail: a Comparative Study. Journal of Lifestyle and SDGs Review, 5(2), e04039-e04039.
[4] 1984 AIR 684
[5] RLW2007(1) RAJ713.
[6] (2001) 4 BOMLR402

discarded by the Court and rightly so, as extortion consists, in essence, of obtaining valuable property or documents by deceitful means of creating fear of harm.

- ***Case laws on extortion***

In India, the jurisprudence on extortion has evolved in many important judicial pronounces that reiterated the essential ingredients of the offense. In conscious of harm to the reputation of the victims pertaining to extortion, in Romesh Chandra Arora v. State (1960)[7], while he was habitually blackmailing women for a livelihood, the accused took away a boy and a girl in an area away from the city, took off their clothes, and clicked photographs while putting them in compromising positions, and under threat of publication extorted money out of them. The court convicted him under various provisions of IPC.

Similarly, in State of Karnataka v. Basavegowda alias Chandra (1996)[8], the accused had tricked his first wife into entering the forest under the pretext of going to a wedding, set upon his wife with a stone, and demanded her jewels while threatening her with death. The court convicted him under Section 384, IPC, stating that any threat to life whereby gain wrongfully accruing is sought that is characterized as extortion.

The Supreme Court emphasized that for an act to become extortion, all necessary statutory elements must be fulfilled, especially that property was transferred in fact in Dhananjay Alias Dhananjay Kumar Singh v. State of Bihar and Another (2007)[9]. The ruling in R.S. Nayak v. A.R. Antulay and Another (1986)[10] further emphasized the requirement of proving both fear and dishonest inducement. It was clarified that mere threats without these two ingredients would not constitute extortion.

The distinction between theft and extortion was discussed in Habibul Razak v. King Emperor[11]. The court stated that theft means taking the property away from its owners without their consent, whereas extortion means applying dominant will in the owners' mind through a threat or coercion.

[7] AIR1960SC154
[8] 1997CRILJ4386
[9] 2007 AIR SCW 923
[10] 1986 SCC (2) 716
[11] AIR 1924 All 197

Lastly, the cases of Hemant Dhirajlal Banker v. State of Maharashtra (2023), Mahavir Jain v. State of Rajasthan (2015), and Ravindra Pratap Singh Parihar v. State of Rajasthan (2022) would reiterate the necessity for the prosecution to prove each ingredient of the offense, namely fear, coercion, and resultant delivery of property. These judgments provide an intricate view of the surrounding legal tapestry that has been tortured by scuttles made by the courts, for which the demand of grounds evidencing coercive inducement and property transfer under the apprehension have remained stoutly established for sustaining a conviction.

- ***Punishment for extortion***

a. Extortion as Contained under Section 384 IPC - This section describes the extortion crime. It prescribes punishment for such imprisonment, which may extend to three years, or with fine, or both. Extortion under this provision is cognizable in nature and bailable. It is also non-compoundable as per Section 320 of the Criminal Procedure Code, and can be tried by any magistrate.

b. Section 385 IPC- Under Section 385 IPC, it induces a person intentionally making a threat or creating a situation of fear of loss or injury for another person in order to apply force in committing extortion that may include imprisonment for two years or to pay fine or both. It is cognizable bailable non-compoundable and triable by any magistrate.

c. Section 386 IPC- A person who, under the power of extortion, creates a fear of death or serious injury to another or close to such person can be punished under Section 386 for a period of ten years and with a fine. This is a cognizable but non-bailable and also non-compoundable offence that can be tried at the First Class Magistrate.

d. Section 387 IPC- The extortion under this section shall be treated under situations where there is an extension of the threat of grievous hurt or death. Imprisonment under provision for this offence will extend for a term of seven years and punishment would also require paying a fine. In the case of Gursharan Singh v. State of Punjab (1996)[12], the accused was convicted under Section 387 for demanding money under threats of violence, claiming it was for purchasing arms to be used against terrorists.

e. Section 388 IPC- Section 388 refers to extortion by threatening to falsely charge someone

[12] (1997)116PLR239

with an offence. If a person extorts money by instilling fear of a fabricated criminal charge against a victim or another, he will be punished with imprisonment for a term which may extend to ten years and also pay a fine.

3.Cyber extortion in India

According to the Information Technology Act, 2000, the scope of cyber crimes in India, and more recently as provided under the provisions of "Bharatiya Nyaya Sanhita, 2024". Initially, the IT Act, 2000 dealt largely with computer-related offenses and matters relating to electronic commerce. However, major amendments have been brought in the year 2024 to the definitions of legal terms and to the categories of cyber offenses that are punishable. These statutes also redefined the provisions under the BNS and those under the RBI, as further strengthening the legal framework of cyber crimes and their enforcement[13].

Indian laws also criminalize cyber-blackmail and extortion. Cyber extortion generally involves illegal access to a digital system, where sensitive information is obtained from an individual or group and ransom money demanded for its return. For instance, the CEO may have some confidential business plans—hence, a product development strategy—which were packaged in e-mail that was officially sent. Such emails can be hacked into by a person through hacking the email server and accessing classified information. The hacked information may be exploited to extort money or favours using the weak cybersecurity infrastructure of the organization.

It is still the case that current rapid change in technology poses difficult challenges to the Constitution. The right to privacy was not expressly provided for in the Indian Constitution; nevertheless, it has gained recognition through judicial interpretation especially under Article 21 guaranteeing the right to life and personal liberty as an inherent constitutional right. The interpretation was cemented firmly by the landmark judgment in Justice K. S. Puttaswamy (Retd.) v. Union of India, where the Supreme Court recognized the right to privacy as a fundamental one. The case pertained to the Aadhaar scheme, which is challenged as violating citizens' privacy rights. Besides strengthening individual data's constitutional protection, this verdict is also meant to reshape national discourse on digital rights, surveillance, and bioethical issues regarding the use of biometrics, along with crucial challenges to six core privacy rights

[13] *Available at:* https://indianexpress.com/article/india/rise-cybercrime-2022-economic-offences-ncrb-report-9053882/ (last visited on: Mar 29, 2025)

that the Aadhaar system could likely impact[14].

4. Legal ramifications

As disclosed by the National Crime Records Bureau Year Book 2021, Volume II, published by the "Bureau of Police Research and Development, Ministry of Home Affairs", Delhi accounts for about half of the cyber-extortion cases that arise in India. These cases usually relate to instances where the accused has knowledge of some sensitive or private information of the victim. Between increasing reports and the rise in incidence of such cases, Indian law still fails to provide a clear and unambiguous legal definition or provision pertaining to "cyber-extortion" as a separate offence.

Indian primary legislation covering cyber-related criminal acts, the Information Technology Act, 2000, is fast becoming an act far too outdated in the present context. Cyber-extortion is neither defined nor made punishable as a standalone offence therein. However, presently such acts can be subjected to a multitude of charges under a combination of the provisions of the newly introduced Bharatiya Nyaya Sanhita (BNS), 2024, as well as under the IT Act.

Relevant provisions include:

- Section 303 of the BNS, 2024, which deals with extortion, defined as the forcing or coercing of a person to obtain from another person something he possessed or enjoyed through intimidation of threatened injury to his person, property, or reputation.

- Section 351 of the BNS, 2024, which takes into account criminal intimidation refusing any threat which induces a man to do against his own will act and refrain from exercising any legal right.

- Section 66E of the IT Act states punishment for the infringement of privacy by unauthorized capturing, transmitting, or publishing the private body part images and the punishment up to three years with a monetary penalty, which would probably include it within that range of punishment as well.

Even though those provisions cast a somewhat narrow net with respect to seeking legal

[14] Sari, A. P., Dinata, M. R. K., & Wati, N. (2025). Legal Policy On The Criminal Acts Of Extortion And Threast Via Social Media. *Jurnal Hukum Sehasen*, *11*(1), 245-250.

remedy, they, in no way, adequately cover the peculiar characteristics and ramifications of cyber extortion in contemporary times. As the technological means of extortion become more targeted-increasingly targeting high-profile entities and more vulnerable sections, such as women-an urgent need has arisen for specific and comprehensive legal provision defining and punishing cyber extortion. This provision would not only fortify legal protection for victims but also serve as a deterrent against the misuse of digital platforms for coercive and exploitative purposes.

5. Practical implications and prevention strategies

a. Consistent Data Back-up: Draft a good and exhaustive archiving plan that should include frequent and automatic archives of all sensitive back-up data. Implement a scheduled backup program with multiple versions for data at different time and solve the risk of data loss due to ransomware incidents.

b. Patch Management: Strong patch management policy shall be established so that software updates can be timely identified and applied. Periodic scans of the system enable detection of unpatched software and vulnerabilities suited for exploitation by ransomware threats. Whenever possible, chew through the patching of the critical systems and applications because they are almost always the first targets of this kind of attack. Keep abreast of the latest security advisories and vendor notifications to be informed of emerging vulnerabilities and where new patches become available.

c. Endpoint Security: Advanced Endpoint Protection solutions with real-time capabilities must be utilized to protect against ransom ware the solution should be configured to proactively prevent activities such as unauthorized file encryption, abnormal network behaviour, or suspicious system processes without any user involvement. A multi-layered approach is to be used with respect to antivirus and anti-malware protection, as well as an IDPS through regular updates with the most current threat intelligence to provide protection from evolving forms of ransomware.

6.Moral and Regulatory Aspects

a. Compromise Payment:

- Legal Implications: Dealing with Ransom Demands in exchange for a cyberattack might

infringe laws about money laundering or even terrorism financing. This payment could even pay for the doer, the paying one faces serious liabilities in terms of law and regulations because the paying entity is now exposed to the possibility that it may be supporting a criminal or terrorist organization.

- Ethical and Legal Conundrum: Organizations face pretty serious ethical and legal dilemmas when it comes to paying ransom. The pressure to save imperative data, and resume operations, may tend to make them comply, whereas actually, paying the ransom also empowers the hackers to conduct subsequent strikes. This requires a proper balance between legal risks and moral responsibilities.

- Encourage More Attacks: Giving in to ransom demands may simply mean that certain vulnerability has been signalled, thus leading to future attempts at extortion. In addition, it's possible to escalate not only in this but also in the intensities of attacks against this organization in the future, creating a cycle of cybercrime[15].

b. **Transparency and Disclosure:**

- Striking a Balance: Organizations are supposed to maintain a fine balance between transparency about cyber security incidents and protecting themselves from the potential aftermath. Public notification of breaches could damage the organization's reputation, erode consumer trust, or subject the organization to litigation or regulatory action.

- Regulatory Compliance: Mandatory reporting of data breaches to the regulatory authorities or law enforcement agencies is required in various jurisdictions. Not complying with such legal obligations would give rise to some penalties against the organisation and hurt its credibility in the eyes of regulators and stakeholders.

- Reputational Risk and Stakeholder Trust: The acknowledgment of a cyber incident could damage an organization's public image, as well as relations with its customers, investors, and business partners. Under such circumstances, trust erosion may incur substantial business losses and long-term damage to stakeholder confidence.

[15] Roberts, R. (2025). The United States Supreme Court and the Defederalization of State and Local Public Corruption. Public Integrity, 1-21.

7. Conclusion

Cyber extortion manifests as a serious and increasingly mainstream threat in today's digitally driven world where technology directly affects almost every human activity. In such a scenario, enhanced reliance on digital infrastructure translates into higher chances of cyberattacks, thereby throwing into question the need for strong cybersecurity practices on the part of individuals and organizations. Robust security protocols, timely updates of software, employee awareness on cyber threats, and the institution of effective continuity plans will reduce the impact of these ventures. Equally paramount is a raise in public awareness regarding cyber extortion itself. To appreciate and address it, a joint effort will need to be orchestrated by law enforcement, technologists, and the general public. The time has come for collaborative conduct toward enhancing our collective resilience against the shedding of blackmail by nefarious cybercriminals. Today we need to strengthen all our defenses for tomorrow's persecution of our virtual treasures.