Page 2326 - 2335 **DOI:** *https://doij.org/10.10000/IJLMH.1110044*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 3

2025

Theft and Extortion in 21st Century India: Evolving Crimes in the Digital Era

MAANIT MAHAJAN[1] AND AKHILENDRA SINGH[2]

ABSTRACT

Theft and extortion are basic crimes in India, but with the arrival of the digital age, their nature, methods, and impact have changed completely. This paper studies how primitive forms of theft and extortion have been transformed into advanced cybercrimes due to technological advancements, globalization, and socio- economic changes. With the rapid growth of internet usage, digital payments, and online services, criminals sought new opportunities through cyber theft, data theft, ransomware, social media blackmail, and Artificial Intelligence exploitation such as deepfake technology. These developments blur legal boundaries within theft, fraud, and extortion making it almost impossible for enforcement and judicial systems built on out-dated legal frameworks to cope. It also highlights the socio-economic factors such as digital under-education and poverty that heighten the exposure of people and institutions to the risks of cybercrimes. The paper advocates to defend vulnerable groups with immediate and extensive legal changes, modernizing law enforcement and increasing international collaboration, and coordinated efforts for digital literacy campaigns. It also emphasizes policies for greater oversight of emerging technologies and the establishment of support systems for victims. Through the integration of these measures, India will create a robust and adaptive system of fighting theft and extortion in the digital age, providing security, justice, and faith for its people and institutions. This research is a call to policymakers, law enforcers, and society to act proactively in meeting the changing reality of crime in the 21st century.

Keywords: *Cybercrime, Theft, Extortion, Digital Transformation, Legal Reform, Digital Literacy.*

I. INTRODUCTION

Theft and Extortion remain the two most common and deeply rooted crimes in India's sociocultural and legal fabric. These acts, historically understood as illegally seizing someone’s property or utilizing violence or threats to gain valuables, have been legislatively addressed for ages within the Indian Penal Code. The turn of the century, along with precocious soci-technological developments, paradigmatic socio-economic transformations,

[1] Author is a Student at Symbiosis Law School, NOIDA, India.

[2] Author is a Student at Symbiosis Law School, NOIDA, India.

and torrents, has multifariously transformed the methods, extent, and severity of robbery and extortion. Crimes that used to be physical in nature have now shifted to a digital setting, creating more difficulties for law enforcement and the legal system, as well as the victims.

Having easy access to the internet, the rise of e-commerce, online banking, and other related technologies have changed technological transactions of a day to day level. This wasn't anything until today, where it poses a new threat to criminals as well. Cybercriminals are able to use the gaps in a digital infrastructure which enables them to carry out thefts such as extraction of financial data, stealing intellectual resources, and even identities. Extortion has now moved online, meaning that it is not only physical coercion. Online blackmail techniques such as ransomware attacks, social media based blackmail, and manipulative fake content threats (known as deepfake technology) have made it easy for anyone to commit what used to be termed as online crimes. These crimes which were previously impossible to commit were limited by borders, however now anyone can commit them anywhere which makes them hard to trace. This alters the way we see crimes, especially with how laws are issued revolve around digital domains, which as of now lack the proper predefined ideas that need to be put one step in front of the other to face crimes through hybrid spaces of virtual existence and the grounding structures of reality.Alongside these realities, the sheer volume of significant, economically disadvantaged populations within India, paired with factors such as digital illiteracy, predispose them to the risks of cyber-enabled crimes. It becomes imperative to reconsider contemporary mechanisms for enforcement and public education in order to construct comprehensive strategies in response to the problem. This research analyzes the phenomenon of theft and extortion in the context of India in the 21st century, evaluates the impact of the available legal and institutional frameworks, and proposes measures for strengthening the country’s capacity to address such crimes that undergo continual change. In doing so, the paper underscores the interdisciplinary nature of the problem and the deep synergy required from law, technology, policy, and education to prop up barriers guarding individuals, institutions, and society from the pitfalls of the digital landscape.

II. Materials and methods

To understand the changing dynamics of theft and extortion in 21st-century India, this paper utilizes a qualitative, doctrinal approach. It draws primarily from secondary sources such as legal texts, research articles, crime reports, case law, and policy reviews. Two comprehensive reports formed the base materials for this research. The two documents explore the historical and virtual forms of these offenses, how they are treated under the Indian Penal Code, and how technology has made it difficult to distinguish among various criminal offenses.

Research aims were the following:

- In order to analyze existing legal frameworks regulating theft and extortion in India and assess their sufficiency in dealing with contemporary crime.
- To research the evolution of theft and extortion from offline crimes to digital and data-facilitated crimes.
- To study the socio-economic and technological conditions driving the proliferation of such crimes.

III. Data analysis

A. The Digital Transformation of Traditional Crimes

The movement from handling items in tangible form to digital form has transformed crimes like theft and extortion in India. While such crimes continue to be based on legal definitions, their current law enforcement avoids historical approaches. Theft, which was framed mostly in relation to having one’s possession, now includes misappropriation of sensitive information, financial assets, intellectual property and one’s identity. Extortion, which used to be exercised though direct intimidation or face-to-face threats, is nowadays increasingly practiced in cyberspace in the form of ransomware, social media bullying or blackmail using sensitive or manipulated footage shot online.

This development has created a gap in many of the older legal frameworks and methods of investigation. The internet not only provides new methods of committing these crimes, but also modern motivations and victims, ranging from individuals and small businesses to huge multinational corporations and even state institutions.

B. Rise of Cyber Theft and Its Mechanisms

The unauthorized capturing of personal documents such as bank details, passwords, customer documents and confidential information ranks among the top law enforcement issues to cyber theft in India. The rise of online financial services has made people more reliant on the internet, sometimes without proper knowledge about cybersecurity techniques; this has made everyone susceptible to phishing emails, counterfeit websites, and fake apps that mimic genuine services. Sensitive information that is shared by users is in most cases using such applications, and criminals tend to use such information for illegitimate financial gains.

Businesses have in recent years ranked among the top victims of cyber theft. Hackers can easily access a corporate databases and steal business intelligence data, trade secrets, customer details alongside confidential business communications. Corporate data breaches can lead to a significant loss of money and at the same time, breach consumer trust towards sustaining the brand. A single breach of stored information can put a company at risk of losing their position in the market and expose them to legal charges.

The most threatening feature of cyber theft is how hard it is to trace criminals. Cyberthieves employ VPNs, proxy servers, and encryption that hide their identities and geographical locations. This anonymity on the internet enables them to conduct transnational operations, which quite often extend beyond the jurisdiction of Indian investigative agencies.

C. Modern Extortion in the Cyber Age

Along with robbery, extortion has similarly become stealthier and more technologically sophisticated. One glaring example is ransomware assaults, which have become all too common. In such attacks, cybercriminals lock up a victim's computer systems, rendering it unusable, and then monetarily extort them. These cybercriminals demand a ransom, usually in some anonymous, non-traceable, digital currency. For complete access to their data again, they often ask for a ransom which is sadly usually in untraceable cryptocurrency. The victim faces great loss because these attacks are not only directed on individuals but entire organizations such as hospitals, banks, and even municipal corporations, or police forces. The consequences, damage may include: interrupted operations, stolen sensitive data, and enormous financial burdens.

One more alarming development is social media driven blackmail with personally identifying and sensitive information. Cybercriminals exploit intimate photographs, compromising videos, or even sensitive messages and make future threats if the victim does not comply with their commands. With the recent increase in the use of artificial intelligence tools, issues like deep fakes are making this even worse. Reasonably indistinguishable from actual content, deepfakes can be used to create compromising material. These tools commonly leave the victim unable to deny the blackmail.

The psychological effect of all such extortion rackets is serious. Most victims, particularly young people or professionals, feel humiliated and powerless into compliance. They might yield to demands in fear of public embarrassment, reputation loss, or losing their jobs. That perpetrators act behind the cloak of cyber-anonymity only encourages their actions and makes the victim's redress even more difficult.

D. Blurring Legal Boundaries Between Theft, Fraud, and Extortion

Cross classification of law is a typical feature of modern cybercrimes and they often overlap various legal categories. These crimes have components of stealing, deceiving and some form of extortion which does not fit within the bounds of current legal frameworks. A phishing attack, for example, is essentially stealing personal information by deceit(breach of trust and theft), then using that information to extort money or further access (extortion). In the same manner, coerced demands are made after trespassing access (coercion combined with theft), as seen in ransomware attacks.

There is no doubt that the Information Technology Act, 2000 was an attempt at regulating the situation. However, the Act is largely responsive in nature and lacks sufficient detailed mechanisms to prosecute more complex cybercrimes. There are no provisions for dealing with advanced crimes within the legal framework resulting in a lot of these offenses existing in what is known as a legal limbo, where the action becomes vaguely defined in its categorization and organizational response.

This lack of clarity impacts not just how cases are charged but also how victims perceive their rights and the remedies that can be accessed. A more mature and cohesive legal system is badly needed, one that recognizes the overlap of criminal activity and provides concrete, enforceable definitions for contemporary cyber crimes.

E. Socio-Economic and Structural Catalysts

The increase in online identity theft and extortion in India cannot be separated from the socio economic situation. One of the factors which enable cybercrime to thrive is the absence of basic computer education. Even though the population in India has access to the internet and smartphones, the majority of users do not have knowledge regarding safe internet practices. Low socio-economic communities who are new to the internet are particularly vulnerable. Their clicking on harmful hyperlinks, poor password choices, and, averting providing private data makes them easy prey. Cyber criminals are capable of these acts of fraud known as phishing, loan frauds, or identity theft.

Financial struggle is a great motivator. Economic recessions and periods of high unemployment are more attendant to societal shocks like during and after COVID-19 pandemic. Despair drives some people to become actively involved in cyber crime or to become unwitting accomplices. Fraudulent job advertisements, fictitious financial institutions, and Ponzi scheme scams were the order of the day during the pandemic. Perpetrator's hands were no doubt helped by under-resourced police forces who developed a culture of impunity that fostered more crime.

Also tell about the particularly acute structural deficit of India in regard to fighting cyber crime. Virtually every police officer lacks basic literacy skills for any form of meaningful investigation. Manpower and funds are lacking for dedicated cyber crime divisions. Long drawn judicial processes pose challenges for victims trying to report crimes or access legal aid. The sluggish pace of this system accentuates the gap between law violators and those tasked with upholding the law.

F. Cross-Sectoral Impacts of Theft and Extortion

The effects of modern day extortion and theft goes beyond personal issues. Both private and public institutions have been heavily affected by the operational disruptions inflicted upon them by cyberattacks. For instance, ransomware attacks on health centers can cripple patient information systems, subsequently prolonging treatments and placing lives at risk. Municipal Corporations have completely lost control over their servers, making basic civic services completely inoperative. Businesses particularly in finance, e-commerce, and education are incessantly under the threat of data breaches, the impact of which can significantly erode consumer trust and severely damage financial health.

Cybercriminals now also target governmental institutions where they can obtain sensitive materials to paralyze services or carryout state humiliation. Aside from the financial ramifications, there geopolitically paying costs when suspicion arises about the involvement of other nations. In this manner, cybercrime has emerged as a new form of asymmetric warfare severely undermining a country’s defense capabilities whilst threatening sovereignty over its economy.

G. Technological Anonymity and Jurisdictional Barriers

Another notable obstacle is the lack of identification provided by digital technologies to criminals. Unlike traditional crimes that require the criminal’s presence at the scene, cybercrimes are committed from remote locations with advanced technologies capable of erasing traces of the perpetrator’s presence online. Criminals use encrypted messaging apps, dark web forums, and cryptocurrency payments to evade surveillance and capture. These methods pose significant jurisdictional gaps. Indian law enforcement institutions find it challenging, especially through weak international treaties, to probe or prosecute foreign nationals who commit cyber crimes due to extraterritorial considerations.

Even when suspects are located within India, the infrastructure and technology to conduct digital forensics trained personnel are lacking, rendered insufficient evidence or unsubstantiated by the court. Such features of the law undermining its execution leave numerous loopholes to be capitalized on, which, in the end, adds to the problem of cybercrime, putting the justice system at risk of being mocked.

IV. Conclusion

The crimes of stealing and extortion have been integrated into society since early history, as they touch on critical areas of human conflict, and in modern times have adapted to technological as well as socio-economic advancements of the 21st century. India, like other countries, has rapidly digitized their economy, governance, and everyday life which has now resulted in dealing with the modern versions of these ancient crimes. In current circumstances, stealing is no longer confined to the physical removal of tangible items from a person; also, the definition of extorting is no longer limited to the use of threats of bodily injury and harm. Both offenses are now committed in the modern sense with the aid of digital tools, platforms, and spaces that have become part of our daily existence.

As demonstrated in this study, the virtual world did not simply provide new opportunities for criminal activities, it also facilitated more complex hybrid crimes that blur or muddle the legal and conceptual distinctions of theft, fraud, and extortion. Cybercriminals who operate internationally and without restraint use a variety of methods, including but not limited to, ransom attacks, phishing emails, deepface blackmail, and social engineering. These crimes are equally novel for the victims and for the enforcement and judicial systems. The crimes tend to be novel for a victim, an enforcement authority, or a judicial system, which all experience unprecedented complexities, multi-jurisdictional involvements, intricate technological frameworks, and unprepared victims who do not have the ability nor the knowledge to report or respond to such abuse.

The context in which these infractions emerge is not in isolation but rather intersects with India's socio-economic condition. The socio-economically vulnerable and took down populations, alongside a rising online user base, succumb to exploitation due to limited digital literacy. This means that cyber exploitation, or cyberFinal, is not merely a technological concern but also one of social law a consequence of inequality in access, information, and protective measures. Economic difficulties, especially during the COVID-19 pandemic, have not only escalated and intensified victimhood but also increased desperation-driven crime. In this context, more sophisticated systemic ailments underlie and produce theft and extortion. The same goes for the Indian jurisprudence, which requires a fundamental change in the technique of construction towards justice in cases where terabytes of evidence and multi-jurisdictional cooperation are pivotal. Also indestructible is the responsibility of the private and social sectors. Financial and social media institutions, as well as technology firms, have a larger obligation to ensure that their monitoring, reporting, and system creation policies are proactive against abuse. Thus, the responsibility to combat such crimes extends beyond the boundaries of law into governance, education, and even corporate accountability.

In the end, the persistence and prevalence of extortion and theft in contemporary India reflect the imperative for an effective and proactive strategy. This has to be founded not just on an awareness of how such crimes have transformed but also on a determination to protect the digital rights and security of all citizens. The fight against these crimes continues and is difficult, with ever-changing strategies and methods. Accordingly, the reply has to be adaptive, collaborative, and forward-looking. Only through an holistic strategy that links law, technology, policy, and public perception can India ever hope to seriously combat the menace of theft and extortion in the age of cyberspace.

V. Recommendation

Integrated approaches, such as changes in law and policy, technological advancements, legal education, and institutional strengthening, are required to deal with commuting robbery and extortion in modern India.

Cyber crime units must be created immediately, provided modern cyber forensic equipment, and staffed by officers with training in information technology and cyber law. Criminal assets should also be regarded as property able to be stolen, and current legislation should be repealed-confined to transformative law in order to redefine digital extortion. The adjustment is bound to assist control computer crimes. Albeit, the prerequisites of proper control over these possessions are lacking, and combating information crime will not be possible without enhancing control over information in general. Therefore, the restructuring of interdisciplinary information, economics, cyber policy, law, and sociology would be required.

Apart from other approaches, awareness and education on the public side are also crucial. Specialized campaigns targeting digital illiteracy should teach citizens, especially the vulnerable like the elderly and those living in rural areas, about secure online practices, privacy, and recognizing phishing attempts and other cyber attacks. Sensitive information companies also need to conduct regular cybersecurity audits and comply with strict data protection policies to mitigate risks.

The introduction of deepfake technologies and other forms of AI will necessitate the formulation of new policies to curb their exploitation for extortion and fraud purposes.

Addressing these emerging challenges will require an investment in detection technologies and collaboration between lawmakers, technology specialists, and law enforcement agencies.

The socio-economic aspects of cybercrime should be addressed as well. Investment, creation of new economic activities and job openings, and enhancement of social welfare will serve to reduce the appeal of committing crimes. Moreover, proactive support for victims of cyber extortion, including counseling and legal aid services, can improve recovery outcomes and encourage reporting.

*****

VI. References

1. James E Clark, Developments in Extortion Cases and Coverages, 10 The Forum (American Bar Association. Section of Insurance, Negligence and Compensation Law) 1341-1353 (1975). https://www.jstor.org/stable/25761073
2. R. Anand, The Changing Nature of Theft in India's Digital Economy, 10 Indian J.L. & Tech. 56 (2019).
3. Law Commission of India, Report on Reforming Cyber Laws Against Extortion, Rep. No. 279, at 45 (2021).
4. K.D. Gaur, Criminal Law: Cases and Materials 234 (9th ed. 2021).
5. Ruchika Gupta & S.P. Agarwal, A Comparative Study of Cyber Threats in Emerging Economies, Int'l J. Mgmt. & IT (2017)
6. Siddharth Luthra & Vidhi Agarwal, White-Collar Crimes in India: The Rise of Financial Fraud and Extortion, 12 Nat'lL. Sch. India Rev. 56 (2021).
7. Aparna Chandra, Cyber Extortion and Legal Challenges in India, 45 Nat'l L. Sch. India Rev. 112 (2022).
8. Kai A Konrad & Stergios Skaperdas, Extortion, 65 Economica 461-477 (1998). https://www.jstor.org/stable/2555183
9. R.V. Kelkar, Criminal Law in India 187 (6th ed. 2018).
10. Pratik Datta, Financial Crimes and Cyber Theft in India: Regulatory Perspectives, 42 Indian Econ. J. 311 (2021).
11. Jerome Hall, Theft, Law and Society—1968, 54 American Bar Association Journal 960-967 (1968). https://www.jstor.org/stable/25724558
12. Nat'l Crime Records Bureau, Ministry of Home Affairs, Crime in India 2022, at 78 (2023).
13. Apar Gupta, Digital Extortion and Ransomware Attacks: Legal Challenges in India, 50 Indian J.L. & Tech. 87 (2023).
14. A Rationale of the Law of Aggravated Theft, 54 Columbia Law Review 84-110 (1954). https://www.jstor.org/stable/1119027

*****