CRACKING THE CODE OF SILENCE - THE UNDERWORLD OF CYBER EXTORTION IN INDIA

Akshay Kabra* **Dr. Ananya Bibave***

ABSTRACT

A substantial challenge has been presented to people, companies, and law enforcement authorities in India in recent years by an increase in cyber extortion cases. In India's digital ecosystem, cyber extortion has become a prevalent and growing menace, posing serious risks to individuals, organisations, and the country's security. This paper explores the complex topic of cyber extortion with an emphasis on its legal ramifications in the Indian setting. It clarifies the complex nature of cyber extortion, the typical strategies used by hackers, and actual incidents that demonstrate its pervasiveness. The paper also thoroughly examines the Information Technology Act, the Indian Penal Code, and relevant data protection laws that make up India's legal system for dealing with cyber extortion. It also examines the difficulties faced by law enforcement authorities in locating and prosecuting incidents of cyber extortion, and it discusses recent changes in the legislation that have strengthened attempts to reduce cybercrime. The paper also clarifies the essential steps required in examining instances of cyber extortion, the significance of digital evidence, and the need for cyber forensic skills.

Keywords: Cyber Extortion, Data Protection, Cybersecurity, Privacy Laws, Cybercrime Mitigation.

INTRODUCTION

In recent years, India has seen a worrying and quick increase in cyber extortion, with an alarming number of people, companies, and organisations becoming victims of this evil digital threat. Malicious actors use a variety of strategies in the complex ecosystem that has emerged in the virtual underworld of cyber extortion to extract money, confidential information, or other

*ASSISTANT PROFESSOR, PES MODERN LAW COLLEGE, SPPU, PUNE.
*PRINCIPAL, PES MODERN LAW COLLEGE, SPPU, PUNE.

valuable assets from their victims. Examining the complex legal rules that govern cyber extortion in the Indian context is essential to understanding the full scope of this menace.

The global upsurge in cybercrime activities is exemplified by the increase in cyber extortion in India. The population's susceptibility to cyberattacks grows along with the country's unparalleled expansion of its digital footprint. Cyber extortionists target everyone from private individuals to large multinational businesses by taking advantage of the interconnection of the digital world. Their motivations might range from monetary gain and corporate espionage to ideological ambitions, and they frequently leave victims traumatised, broke, and in a murky legal situation.[1]

A wide variety of cyber extortion tactics, such as ransomware attacks, Distributed Denial of Service (DDoS) extortion, data breaches, and the release of private information, define the threat environment in India. To avoid detection by law enforcement, these hackers typically demand ransom payments in cryptocurrency while operating in crafty secrecy. In order to successfully combat this threat, broad legislative measures and law enforcement methods are urgently required, given the rising frequency and sophistication of these assaults.

Law enforcement authorities must understand the legal ramifications of cyber extortion in India, as well as for people, companies, and organisations trying to safeguard themselves from possible dangers. The legal system of India, which is made up of several acts, legislation, and regulations, offers the essential instruments to successfully resist cyber extortion. These legal guidelines specify the obligations of people and organisations in the digital sphere, as well as the consequences of engaging in cyber extortion.

Moreover, for victims seeking justice and compensation, having a thorough awareness of the legal issues is essential. Navigating the judicial system may sometimes be intimidating and difficult, particularly when dealing with cybercrimes that cross regional lines. Knowing their options for legal action can give victims the confidence to report crimes, assist authorities, and seek justice in court. Furthermore, in order to protect their digital assets and sensitive data, firms must create effective cybersecurity plans that follow the law. Legal penalties, reputational harm, and regulatory punishments may occur from failure to abide by these requirements.

[1] Tanu Joshi & Nandini Gaur, *A Study on Cyber Crimes and Cyber Laws in India*, 5 INDIAN J.L. & LEGAL Rsch. 1 (2023).

UNDERSTANDING CYBER EXTORTION AND ITS FACETS

A type of cybercrime called cyber extortion includes threatening people, companies, or organisations with the loss, disclosure, or damage of sensitive data or the disruption of vital systems until a ransom is paid or a set of conditions are satisfied. Cyber extortion is a criminal practice in which perpetrators use technology to influence, threaten, or compel victims into complying with their demands. These requests may involve non-monetary concessions or acts, although they frequently centre on monetary contributions.

The attackers obtain unlawful access to the victim's digital assets, such as databases, confidential papers, or control systems, in a classic cyber extortion scenario. They then threaten to reveal this information, stop crucial services, or cause more harm if the victim doesn't comply with their demands. Various methods of cyber extortion exist, including:[2]

Sextortion: Sextortion is a type of cyber extortion in which the perpetrator obtains access to the victim's private photos or videos before either coercing the victim into having sexual intercourse with him or her or demanding a sizable ransom in exchange for the content's release or even both by threatening to leak the information to the public or the victim's parents. The possession of sexual images or videos which can only be gained through the victim by luring him/her into the trap of false love or affection is a necessary component for this kind of cyber-extortion. The threat to expose the information to the public or send it to the victim's parents or other close family members doesn't come until after the perpetrator has already obtained the data. Sextortion primarily occurs on dating websites and social media platforms like Facebook or Instagram.

Ransomware: One of the most common types of cyber extortion is this. The data of a victim is encrypted by attackers, who then demand a ransom in return for the decryption key. The WannaCry and Ryuk ransomware attacks are notable instances.[3]

Distributed Denial of Service (DDoS) Attacks: The internet services of a victim are overrun by cybercriminals with traffic, making them inaccessible to users until a ransom is paid.

[2] Adam J. Sulkoswki, *Cyber-Extortion: Duties and Liabilities Related to the Elephant in the Server Room*, 2007 U. ILL. J.L. TECH. & POL'y 19 (2007).
[3] R. Thanmayi, *Ransomware: A Cyber Threat to the Business Community*, 5 INT'l J.L. MGMT. & HUMAN. 1263 (2022).

Data Theft and Exposure: Attackers take private material, including customer information or intellectual property, and threaten to sell or publish it unless a ransom is paid.

Threats to Public Reputation: Threats from cybercriminals include everything from revealing private information to interrupting critical services. Although they can include a wider range of behaviours, these threats are typically accompanied by specific demands, which frequently involve paying a ransom.

For recognising and thwarting cyber extortion efforts, it is essential to understand the strategies and methods used by hackers. The following are some typical tactics employed by online extortionists:

Social Engineering: Attackers commonly employ psychological manipulation strategies to take advantage of human shortcomings in social engineering. To deceive victims into performing particular activities or disclosing sensitive information, they may pose as reliable organisations, instil a sense of urgency, or use emotional appeals.

Phishing: Phishing attacks employ misleading emails, texts, or websites that are made to look trustworthy. Attackers get access to victims' systems when they trick them into clicking harmful links or downloading malicious attachments. Moreover, Cybercriminals use targeted assaults to create highly customised phishing messages by doing extensive research on a particular person or group of people. These messages are harder to spot and more persuasive.

Data Exfiltration: Cybercriminals may stealthily exfiltrate critical data over time once they have gained unauthorised access to a victim’s network. They can use this to obtain important information for extortion.

Anonymisation Tools and Cryptocurrencies: Cyber extortionists frequently utilise anonymisation technologies like Tor and demand payments in cryptocurrencies like Bitcoin in order to hide their tracks and make it difficult to track down ransom payments. The pursuit of criminals by law enforcement is made more difficult by their anonymity.

THE LEGAL FRAMEWORK IN INDIA

In India, cyber extortion takes place within a complicated legal framework that mixes already-existing laws and rules with more recent initiatives designed to address the developing nature of cybercrimes.[4]

OVERVIEW OF RELEVANT LAWS AND REGULATIONS

Information Technology Act 2000: In India, the main piece of legislation addressing cybercrimes is the Information Technology Act 2000. Although it was implemented to promote internet commerce, it also handles several cybercrimes, such as cyber extortion. Section 43 of the IT Act of 2000, which deals with illegal access to and damage to computer systems, and Section 66D, which deals with impersonating someone else while using a computer resource, are two important sections that pertain to cyber extortion. Section 66E also addresses invasions of privacy and the unlawful recording of private photographs.

Indian Penal Code 1860: The Indian Penal Code also has various provisions that are pertinent to cyber extortion in addition to the IT Act. In accordance with Section 383's definition of extortion, it is unlawful to threaten someone with physical harm to get their property or valued security. Charges under this provision may result from cyber extortion, which frequently entails threats or coercion through electronic methods. Section 385 targets extortion through inducing fear of harm in the victim.

Data Protection and Privacy Laws: With the adoption of the Digital Personal Data Protection Act of 2023, data protection and privacy regulations in India have undergone substantial changes. The Act establishes strict guidelines for data protection and is intended to control the handling of personal data. Although its primary focus is on data protection, several of its requirements may still have an indirect influence on cyber extortion situations when personal data is stolen. Additionally, the statute increases fines for data breaches.

ROLE OF LAW ENFORCEMENT AGENCIES AND THEIR CHALLENGES

Investigation and prosecution of cyber extortion crimes are vital tasks for law enforcement authorities in India, including the Central Bureau of Investigation (CBI) and the Cyber Crime Cell. These organisations are in charge of managing cases involving cybercrimes and working

[4] Riddhi Kaushik, *Cyber Crimes in India - Trends and Challenges*, 21 Supremo Amicus [224] (2020).

together with other organisations as needed. However, they encounter various difficulties, which are as follows:[5]

Cybercrimes demand particular knowledge and abilities to investigate. Law enforcement organisations frequently have trouble keeping up with the quickly advancing cyber threats and technology. Jurisdictional concerns provide a substantial barrier in the context of cybercrimes, which can be perpetrated anywhere in the world. It's frequently required to coordinate with foreign law enforcement organisations.

It might be difficult to gather digital evidence and make sure it can be used as evidence in court. Legal requirements must be followed for the chain of possession, preservation, and presentation of digital evidence. Law enforcement organisations may lack the personnel and technology resources needed to successfully resist cyber extortion.

RECENT LEGAL DEVELOPMENTS AND AMENDMENTS RELATED TO CYBER EXTORTION

The legal system in India has been actively changed to address the increasing nature of cybercrimes, such as cyber extortion. The legal foundation for investigating, prosecuting, and preventing such crimes while also protecting people's rights and privacy in India is important to understand in order to successfully combat cyber extortion.

To improve its ability to combat cybercrimes, the Indian government has frequently modified the IT Act. These changes sometimes involve the addition of new offences and punishments as well as the extension of definitions and clarification of legal procedures.

An important legal development that will affect how cyber extortion cases involving data breaches are handled is the adoption and enforcement of the Digital Personal Data Protection Act of 2023, which places a strong emphasis on data protection and privacy.

In order to combat cybercrimes on a worldwide level, India has been actively engaging with other nations and international organisations. Mutual legal assistance agreements and treaties that support investigations and prosecutions may result from such partnerships.

[5] Shreya Jetly, *Cyber Crimes*, 1 Nyaayshastra L. REV. 1 (2021).

REAL LIFE FACETS OF THE CYBER EXTORTION

The matter of *State of Tamil Nadu v. Suhas Katti (CC No. 4680 of 2004),* in which the victim and the accused were friends, and he expressed interest in getting married to her after her husband had filed for divorce. The woman refused to let the accused marry her, so the suspect decided to threaten her by sending her emails that were put in a Yahoo chat group using a phoney account to harass, libel, and publish offensive material because the woman was already divorced. The accused also shared the identical emails with the woman who was looking for information about her. After receiving emails from their Yahoo chat group, the victim started getting a lot of obnoxious phone calls from her clients and coworkers. The court sentenced the accused to a fine and imprisonment in accordance with section 67 of the Information Technology Act of 2000, since he was found in possession of a false email.[6]

The Petya/Not Petya Attack (2017): This widespread hack, which was first mistaken for ransomware, was largely intended to inflict disruption and damage rather than to make money. It had an impact on several organisations all around the world, including some in India. It illustrated the pervasive effects of online extortion efforts.

The City Union Bank Cyber Heist (2018): In one instance, hackers broke into the computers of the City Union Bank and started fake SWIFT operations to send $2 million to several accounts in various nations. Even though the main goal was financial gain, it serves as an example of how financial institutions may be the subject of cyber extortion.

The Mira-Bhayandar Municipality Ransomware Attack (2020): Government organisations at the local level, such as the Mira-Bhayandar Municipality in Maharashtra, have also been the target of cyber extortion. In one case, ransomware hampered municipal operations and demanded payment in Bitcoin to restore vital systems. This situation demonstrates how open to cyber-extortion threats are public sector institutions.

These actual instances highlight the necessity of thorough cybersecurity safeguards, knowledge, and readiness to protect against cyber extortion in India. Organisations and people must maintain vigilance and prioritise cybersecurity policies to successfully manage risks as fraudsters continue to develop their strategies.

[6] Apoorva Bhangla & Jahanvi Tuli, *A Study on Cyber Crime and Its Legal Framework in India*, 4 INT'l J.L. MGMT. & HUMAN. 493 (2021).

Targeting home routers and IoT devices, the Mirai Botnet Malware assault gained control of the internet. 2.5 million IoT devices were impacted by this threat. The total includes several Indian computer systems. The unpatched vulnerabilities in this self-replicating malware might be used to gain access to networks and systems.

Uttar Pradesh On March 17, 2021, at 12:17 AM, a ransomware assault targeted Bijli Vitran Nigam, a government-owned corporation in charge of distributing electricity in North Haryana. The hackers obtained the billing information and issued a bitcoin ransom demand. For the recovery of the customer's data, they sought an outrageous price of INR 1 crore, or $10 million.

In another surprising admission, two Indian corporations acknowledged paying $10 million to hackers to keep private data taken from their infiltrated computer networks from being exposed. The assaults, which appear to have started in the Middle East, stayed undetected by the firms even months after payments had been made, and neither company has filed a lawsuit as a result since the stolen material was incriminating in nature. However, the revelation has sparked a hitherto unheard-of level of curiosity about how cyber extortion works and is handled in India. A businessman from Hyderabad recently discovered himself unable to access his company's database because it had been encrypted by a hacker who demanded cash for decryption, in yet another case of cyber extortion.[7]

In 2017, the makers of the well-known program "Orange is the New Black" also fell victim to a lethal cyber extortion attempt when the hacker collective known as the Dark Overload infiltrated its server and managed to gain access to the show's unreleased episodes. The hackers demanded a $50,000 payment from the creators and threatened to release their episodes. Sadly, the episodes were nonetheless published online by the hackers even after Netflix paid the required ransom.

Ashley Madison, a for-profit dating service, was compromised by a group of hackers known as the "Impact Team" in June 2015. In this instance, hackers gained access to the system of the website and obtained personally identifying information as well as the personal data of its users. In contrast to past instances, the hackers demanded that the dating service cease all activities; otherwise, they threatened to reveal the clientele's details to the public. The website kept

[7] Ally Jaffari Ally & Neha Gadgala, *Addressing Cyber Scam as a Threat to Cyber Security in India*, 5 INT'l J.L. MGMT. & HUMAN. 376 (2022).

running as normal. As a result, the hackers exposed a significant amount of the company's data, including the personal data of its customers.

INTERNATIONAL COLLABORATION AND THE GLOBAL PERSPECTIVE

Fighting the worldwide menace of cyber extortion calls for international collaboration more than merely a tactical option. India is committed to establishing a safer online environment for its citizens as well as for the rest of the world, as evidenced by its aggressive engagement in international efforts to combat cybercrime and its participation in bilateral and multilateral accords. These coordinated efforts are crucial for avoiding hackers' advances and safeguarding the digital economy from the plague of cyberextortion. A very sophisticated and international crime, cyber extortion. Its capacity to cross geographical boundaries makes it difficult for individual states to wage an effective war against it. The following are some major factors that emphasise the significance of international collaboration in combating cyber extortion:

Cross-Border Nature of Cyber Extortion: Cyber extortionists sometimes work out of jurisdictions far from those of their victims. They may start assaults from one nation, hit targets in another, and use a sophisticated worldwide network to launder their stolen money. Due to the cross-border nature of cyber extortion, international cooperation is required.

Shared Threat Intelligence: Threats from the internet change quickly. The strategies, methods, and practices that cybercriminals employ are always evolving. Countries may combine their resources and skills through international collaboration to better identify new threats and vulnerabilities. Threat intelligence sharing aids in proactive threat identification and reaction.

Resource Pooling: Resource shortages are a problem for many countries, including India, while tackling cybercrimes. Cybersecurity investigations need a lot of technical, financial, and human resources, especially in complicated situations of cyber extortion. Countries may pool these resources through cooperative initiatives, boosting their ability to successfully tackle cybercrime as a whole.

Deterrence: The sense of anonymity and impunity serves as a common motivator for cybercriminals. International collaboration increases the possible repercussions for hackers and discourages future attempts by sending a clear message that cyber extortion will not be allowed.

Cybercriminals hesitate before launching extortion schemes because they know they may be pursued across international boundaries.

INDIA'S ROLE IN GLOBAL EFFORTS AGAINST CYBERCRIME

India has a thriving cybersecurity industry and a vast pool of qualified workers. By helping with threat detection, analysis, and incident response measures, these professionals play a significant part in international cybersecurity operations. The United Nations Office on Drugs and Crime (UNODC), Europol, and INTERPOL are just a few of the international organisations and agencies with which India actively cooperates. It contributes to a global collective defence against cybercrime by sharing crucial information on cyberthreats, cybercriminals' methods, and bad infrastructure. India is involved in projects aimed at boosting capacity, especially in South Asia. It offers adjacent nations technical support, training, and cybersecurity awareness campaigns to help them improve their ability to combat cybercrime.

India is a leader in the fight for strong international accords and legal frameworks to combat cybercrime. It regularly engages in debates at several international venues, highlighting the necessity for greater global collaboration in preventing cyber extortion. In collaborative operations to capture cybercriminals and take down criminal networks, law enforcement authorities from India and other nations cooperate. These activities make better use of common resources and intelligence to combat cyber extortion.[8]

BILATERAL AND MULTILATERAL AGREEMENTS RELATED TO CYBERCRIME

With a number of nations, India has developed bilateral agreements for reciprocal legal aid in cybercrime investigations. These agreements make it possible to coordinate joint operations, extradite criminals, and share digital evidence. Cooperation between nations makes it easier to find and punish international cyber extortionists.

India's involvement in regional organisations like the Asia-Pacific Group on Money Laundering (APG) and membership in international organisations like INTERPOL allow tighter links and collaboration with other countries. These groups operate as hubs for

[8] Himanshu Morwal, *Cybercrime in India*, 2 INDIAN J.L. & LEGAL Rsch. 1 (2021).

knowledge exchange, resource development, and coordinated operations against online extortionists.

International treaties like the Budapest Convention on Cybercrime have India as a signatory. This agreement offers a thorough framework for nations to unify their cybercrime legislation, strengthen international collaboration in the fight against cyber extortion and other cybercrimes. India regularly engages in regional efforts like the Convention on Mutual Assistance in Criminal Matters of the South Asian Association for Regional Cooperation (SAARC) in the South Asian region. This conference addresses a variety of criminal cooperation topics, including South Asian cooperation on cybercrime.

THE EVOLVING LEGAL LANDSCAPE AND ITS ADAPTATION TO NEW CHALLENGES

The legal environment surrounding cyber extortion confronts several shifting issues as technology continues to improve at a rapid rate, and jurisdictional concerns get more complicated since cyber extortionists sometimes operate from multiple nations. To properly prosecute cybercriminals, future legal frameworks will need to handle international coordination and collaboration.[9]

It is a constant struggle to strike a balance between the demand for privacy and the requirement for efficient criminal investigations. The difficult balancing act that laws and regulations must do is to safeguard people's rights while enabling law enforcement to combat cyber extortion. It has become challenging to track down and retrieve money due to the usage of cryptocurrencies like Bitcoin for ransom payments. The regulation of cryptocurrencies in circumstances of cyber extortion may require consideration in future legal frameworks.

Artificial intelligence and automation are being used by cybercriminals to carry out attacks more effectively. To counteract these advancing tactics, legal institutions will need to adapt and retaliate with their cutting-edge weapons.

[9] Md. Golam Mostofa Hasan, *Laws on Cyber Jurisdiction in International Perspectives*, 29 DHAKA UNIV. Stud. PART F 141 (2018).

THE FUNCTION OF TECHNOLOGY IN PREVENTING AND COMBATING CYBEREXTORTION

In the field of cyber extortion, technology serves as both a tool for prevention and a weapon for criminals. The future of combating cyber extortion in India will be formed by the incorporation of cutting-edge technology in both attack techniques and preventive strategies, as well as the modification of regulatory frameworks to handle new issues. To safeguard people and companies from the changing threat landscape, it will be necessary for legal professionals, law enforcement organisations, cybersecurity specialists, and technological developers to work together.[10]

Emergence of Advanced Attack Vectors: More advanced strategies, like as AI-driven assaults, machine learning algorithms to mimic people, and the use of deepfake technologies to trick victims, are expected to be used by cyber extortionists in the future. As a result, cybersecurity measures must change to recognise and counteract these new dangers.

Big Data Analytics: Big data analytics is being used more and more by law enforcement organisations and cybersecurity professionals to spot patterns and trends in cyber extortion cases. Proactive prevention and early danger identification are made possible by advanced data analysis.

Machine Learning and AI for Prevention: Real-time detection and prevention of cyber extortion attempts are becoming more dependent on AI-driven cybersecurity solutions. Large volumes of data may be analysed by machine learning algorithms to spot abnormalities and potential dangers.

Blockchain for Security: Blockchain technology has the potential to improve data and transaction security. Blockchain technology may be used in future preventative methods to safeguard vital systems and stop data breaches.

CONCLUSION

The threat posed by cyber extortion to people, corporations, and the country's cybersecurity posture is ongoing and dynamic. As technology develops, hackers discover new ways to take

[10] Franklin D. Kramer, *Cyber Security: An Integrated Governmental Strategy for Progress*, 11 GEO. J. INT'l AFF. 136 (2011).

advantage of weaknesses, necessitating the need for India to maintain vigilance in the fight against this threat. Cyber extortion may cause severe financial and reputational harm, which not only has an impact on the targeted individuals but also on the overall economy. Additionally, the digitisation of crucial infrastructure and services emphasises the necessity for robust cyberspace security. Despite the enormous advantages, India's digital revolution also exposes the country to higher cyber hazards. Therefore, combating cyber extortion is not only necessary for national security but also for economic stability.

It is essential to take preventive actions and raise awareness in order to effectively combat cyber extortion. To lessen risks, people and businesses must prioritise cybersecurity education and follow best practices. It is encouraging to see how governments, law enforcement organisations, and cybersecurity specialists are collaborating to improve cybersecurity capabilities and quickly address threats.

Furthermore, to assist law enforcement in locating and prosecuting cyber extortionists, individuals and companies should utilise the available tools and reporting channels. Partnerships between the public and commercial sectors can be crucial in distributing threat intelligence and enhancing collective defence.