Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

Algorithms of Coercion: Assessing Criminal Liability for Automated Extortion Networks under the Bharatiya Nyaya Sanhita 2023

Subhadarsini Patra[a]

[a]KIIT School of Law, KIIT Deemed to be University, Bhubaneswar, India

Received 29 September 2026; *Accepted* 29 October 2026; *Published* 03 November 2026

Automated extortion networks are increasingly using artificial intelligence (AI), algorithms, and networks used to carry out cyber threats, blackmail, and other kinds of digital concern. These technologies challenge criminal law principles, particularly mens rea and actus reus, by creating a gap between human intent and criminal acts carried out through an automated system. The article analyses criminal responsibility under the Bharatiya Nyaya Sanhita 2023, focusing on Sections 308 (Extortion), Section 61 (Criminal Conspiracy), and Section 45 (Abetment). It examines AI-enabled blackmail, various types of fraud, and ransomware, while considering the possible criminal liability of software developers and various network operators. The article also analyses the role of the Information Technology Act 2000 and the Prevention of Money Laundering Act 2002 in addressing technology-facilitated extortion. Further, it also discusses various challenges of presenting digital evidence under Section 63 of the Bharatiya Sakshya Adhiniyam 2023. The study highlights gaps in existing legal frameworks and also focuses on the importance of coordinated law enforcement, accurate digital forensic methods and a clear legal framework for determining criminal liability in cases of automated extortion.

Keywords: *automated extortion, artificial intelligence, criminal liability, cybercrime.*

INTRODUCTION

Automated extortion networks have changed the nature of cybercrime by using Artificial Intelligence and automated systems to threaten and manipulate victims.[1] Unlike traditional extortion, which generally involves direct interaction between offenders and victims, these networks can identify targets, misuse personal data, and also generate threats on a large scale. This development raises questions about criminal liability under the Bharatiya Nyaya Sanhita 2023[2]. Establishing mens rea (criminal intent) and actus reus (criminal act) can be difficult when automated software carries out various activities. Therefore, the criminal responsibility of developers, operators, and other individuals involved in these networks needs careful legal examination.

Automated extortion also raises concerns about digital evidence, cross-border investigations, and the misuse of digital lending services. Proving criminal liability may require the verification and examination of electronic records under Section 63 of the Bharatiya Sakshya Adhiniyam 2023[3]. This article analyses how the BNS responds to automated extortion and also examines the challenges in determining criminal responsibility. It also explores how the Information Technology Act 2000[4] and the Prevention of Money Laundering Act 2002[5] can support legal action against these offences.

UNDERSTANDING AUTOMATED EXTORTION NETWORKS

Meaning and Mechanisms of Algorithmic Coercion: Algorithmic coercion refers to the use of automated extortion and artificial intelligence to threaten people into meeting demands, usually for financial gain. Unlike traditional technology, where offenders threaten victims directly, automated systems can collect personal data and also send threats to many people at the same time. These systems may misuse personal information, send threatening messages, and also create fake images to pressure victims into making payments. AI tools can also change messages based on the information available about a victim.

---

[1] R Usha, 'CYBER EXTORTION IN INDIA AND ITS LEGISLATIVE MEASURES' (2023) 2(7) International Journal of Legal Research and Analysis <https://www.ijlra.com/public/details/cyber-extortion-in-india-and-its-legislative-measures-by-r-usha> accessed 27 September 2026

[2] Bharatiya Nyaya Sanhita 2023

[3] Bharatiya Sakshya Adhiniyam 2023, s 63

[4] Information Technology Act 2000

[5] Prevention of Money Laundering Act 2002

Role of Bots and Automated Technologies: Bots and Automated tools help extortion networks operate quickly. Data-collection tools gather personal information from online sources. AI technology can create fake images, prepare threatening messages, and also copy voices. Communication bots send these messages through various online platforms. Some systems can change their responses based on how victims react to threats. These technologies allow offenders to target many people with less direct effort. They can also make it difficult to identify the persons responsible. However, using automated systems does not remove human responsibility. Operators, developers, and other individuals may be held liable depending on their actions and involvement. Therefore, the law must examine how these technologies are used and also identify who is responsible for the offence.

LEGAL FRAMEWORK UNDER THE BHARATIYA NYAYA SANHITA (BNS), 2023

Under the Bharatiya Nyaya Sanhita, it provides a legal framework for addressing various criminal activities involving automated extortion. Although the Act does not specifically define automated extortion as a separate offence, its existing provisions may apply when criminals use Artificial Intelligence, automated bots, and other various types of digital tools to threaten victims and also obtain money. The application of these provisions depends on the nature of the offence.

Substantive Liability for Extortion under Section 308 of BNS: Under Section 308[6], it deals with extortion. It applies when a person intentionally puts another person in fear of injury and dishonestly forces them to deliver property. In automated extortion cases, criminals may either use ransomware to demand Cryptocurrency or threaten to release a victim's private data to obtain money. Such an act may fall under Section 308[7] when the required legal elements are established. However, proving criminal liability requires evidence showing the role and also the intention of the individuals involved in creating or using the automated system.

Criminal Conspiracy and Abetment under Sections 61 and 45 BNS[8]: Automated extortion networks may involve several people, including software developers, data collectors, and

[6] Bharatiya Nyaya Sanhita 2023, s 308
[7] *Ibid*
[8] Bharatiya Nyaya Sanhita 2023, ss 45 and 61

also individuals responsible for transferring illegally obtained money. Section 61[9] deals with criminal conspiracy, while Section 45 talks about Abetment.[10] These provisions may apply when individuals agree to commit an offence or intentionally help others carry it out. For example, a person who intentionally supplies harmful software or stolen personal data to help others commit extortion may be held criminally responsible if the legal requirements are fulfilled. However, simply developing software or offering technical services does not make a person guilty of an offence.

Application of Other Relevant Laws: Automated extortion may also involve cheating, impersonation, and the misuse of personal data. Section 318 of the BNS 2023 may apply when the legal requirements of cheating are fulfilled.[11] The Information Technology Act 2000 also provides various relevant legal remedies. For example, under Section 66D[12], it addresses cheating by impersonation using computer resources, while Section 66E provides for specific violations of privacy.[13] These provisions may be applied alongside the BNS, depending on the circumstances of each case. For effective prosecution, investigators must collect reliable electronic evidence, identify the individuals involved, and also establish the legal elements of each case.

ASSESSING CRIMINAL LIABILITY

Establishing criminal liability for automated extortion networks under the Bharatiya Nyaya Sanhita 2023 depends on the actions and intentions of the individuals involved. Although automated systems can send threats and collect information, criminal responsibility depends on the actions of the people who develop, control, and misuse the system. Therefore, identifying each person's role is important for successful prosecution.

Criminal Intention (Mens Rea) and Knowledge in Automated Systems: Criminal intention plays a very important role in determining liability for automated extortion. Section 308[14] deals with extortion, which involves putting a person in fear of injury and dishonestly inducing them to deliver property. In these cases, investigators must examine whether the

[9] Bharatiya Nyaya Sanhita 2023, ss 61
[10] Bharatiya Nyaya Sanhita 2023, ss 45 and 61
[11] Bharatiya Nyaya Sanhita 2023, s 318
[12] Information Technology Act 2000, s 66D
[13] Information Technology Act 2000, s 66E
[14] Bharatiya Nyaya Sanhita 2023, s 308

accused knowingly developed a system to obtain money through threats. For example, a person who creates software to collect personal information and also demands payment by threatening to disclose it may face criminal liability. However, the use of automated technology alone does not prove criminal intent. The person's knowledge, action, and involvement must be established through evidence.

Liability of Developers and Network Operators: Software Developers and Network operators may have different responsibilities in automated extortion cases. Developing general-purpose software does not automatically make a person criminally liable if someone else misuses it. However, a developer who knowingly develops software to assist extortion may face liability if the legal requirements of the relevant offence are satisfied. Network operators may have a different role because they can control automated campaigns, select victims, send threats, and also handle illegal payments. Their liability depends on their actions and involvement. Investigators must examine electronic records, communications, and also financial transactions to establish their role and also establish criminal responsibility.

Abetment and Criminal Conspiracy: Sections 45 and 61 of the BNS, 2023 deal with abetment and criminal conspiracy. Section 45[15] defines abetment as encouraging, conspiring in, and also intentionally helping another person commit an offence. It may apply when someone knowingly provides technical support or personal information to help others in committing extortion.

Section 61[16] deals with criminal conspiracy. For example, people who agree to create extortion software, gather victims' personal information, or handle illegal payments may be held liable if the legal requirements are fulfilled. However, providing technical information or working within a digital network does not automatically make a person criminally liable. The prosecution must prove each accused person's involvement and also establish the required legal requirements. Examining each person's role helps prevent innocent individuals from being held responsible for the misuse of automated technology by others.

[15] Bharatiya Nyaya Sanhita 2023, s 45
[16] Bharatiya Nyaya Sanhita 2023, s 61

CHALLENGES IN ESTABLISHING CRIMINAL LIABILITY

Automated extortion networks create various challenges for criminal investigation and prosecution. These networks use Automated software, digital platforms, and artificial intelligence to identify victims, send threats, and demand money. Under the BNS 2023 and the BSA 2023, establishing criminal liability requires enough evidence of the offence and the involvement of the accused.

Difficulty in Establishing Mens Rea and Causation: Establishing criminal intention (mens rea) and connecting it with the criminal act can be challenging in automated extortion cases. For example, a developer may create software for lawful purposes, but another person may misuse it to create fake images or threaten victims. Investigators must determine whether the developer knowingly contributed to the offence or whether the software was misused without their knowledge. Automated systems may also identify targets and create threatening messages with less human involvement. This creates difficulties in establishing the connection between the accused's intention and the resulting criminal act. Therefore, investigators must carefully examine the evidence to determine individual responsibility and establish criminal liability.

Identification of Offenders in Automated Networks: Identifying offenders in automated extortion networks can be difficult because different individuals may perform different roles in committing the offence. For example, one person may develop the software, another person may collect the victim's personal information, and another person may send threats. Criminals may use anonymous accounts, encrypted communications, and virtual private networks to hide their identities. Investigators must analyse digital records, financial transactions, and communication histories to identify those involved. When Criminals Conspiracy under Section 61[17], is aligned, establishing an agreement between participants who knowingly participate in various criminal activities and those who provide legitimate technical assistance. Therefore, careful investigation is very important to establish individual responsibility and also prevent the wrongful prosecution of innocent people.

Attribution of Criminal Act to Automated Systems: Linking criminal activities with automated systems creates legal challenges because software cannot usually be prosecuted

[17] Bharatiya Nyaya Sanhita 2023, s 61

in the same way as a person. Investigators must identify those who created, operated or deliberately used the system to commit an offence. Electronic evidence, such as digital messages and financial details, can help establish the link between the accused and the crime. Section 63[18] deals with the admissibility of electronic records and also sets out the requirements for their production and certification. Investigators must preserve digital records and ensure that they are properly examined.

REGULATORY GAPS

The BNS 2023 and the BSA 2023 provide various legal frameworks for addressing criminal activities. However, existing laws have certain gaps in addressing automated extortion networks. These gaps make it difficult to identify offenders, prevent unlawful financial transactions, and gather reliable digital evidence.

Lack of Legal Provisions for Autonomous Systems: Indian criminal laws do not particularly address responsibility for crimes committed by autonomous software. When AI tools generate threats or identify victims, investigators must determine which individuals are responsible. This makes it difficult to establish criminal liability.

Challenges under Section 79[19]: Section 79 provides conditional protection to intermediaries against liability for third-party information. Criminals may misuse online platforms and cloud services to carry out unlawful activities. Delays in detecting and removing harmful content can allow illegal activities to continue.

Gaps in Financial Monitoring: Automated extortion networks may transfer money through various bank accounts to conceal illegal earnings. Although existing laws allow authorities to investigate financial crimes, rapid transactions and the misuse of mule accounts make it difficult to trace and freeze the funds.

Challenges in Electronic Evidence: Section 63 provides the requirements for admitting electronic records as evidence. However, collecting and checking digital evidence from different servers can be challenging. Delays and procedural errors in legal procedures may also affect the acceptance of such evidence in court.

[18] Bharatiya Sakshya Adhiniyam 2023, s 63
[19] Information Technology Act 2000, s 79

RECOMMENDATIONS

India needs stronger laws to deal with the increasing cases of automated extortion. Changing existing laws, better financial monitoring, improved monitoring of financial transactions, and better methods of collecting digital evidence can help prevent these types of crimes and identify those who are responsible.

Amendment to the BNS 2023: It is a very important recommendation. The BNS should provide clear provisions to address crime committed through automated extortion. The law should clearly mention the responsibility of the individuals who knowingly create, control or use such systems for criminal purposes. This would help investigators identify those responsible and also prevent offenders from escaping punishment by blaming automated technology.

Strengthening Intermediary Responsibility: It is very important for the online platforms and cloud service providers to act promptly when their services are used for extortion. Section 79[20] provides conditional protection to intermediaries. Clear guidelines should require platforms to identify various types of suspicious activities and also preserve relevant records while maintaining appropriate legal protections.

Improving Financial Monitoring: Banks and Financial institutions should improve their systems to detect suspicious transactions and also identify mule accounts. Faster communication between banks and cybercrime units would help authorities detect illegal payments and also freeze suspicious funds through legal procedures.

Improving Electronic Evidence Collection: Clear guidelines should be introduced to help investigators gather digital evidence from cloud services and automated systems in accordance with Section 63[21].

CONCLUSION

Automated extortion networks have changed the nature of cybercrime through using Artificial Intelligence, automated software, and also various digital platforms to threaten victims and also demand money. These technologies allow criminals to trace various victims

[20] Information Technology Act 2000, s 79
[21] Bharatiya Sakshya Adhiniyam 2023, s 63

easily, making investigation and prosecution more difficult. Traditional criminal law focuses on human intention (mens rea) and criminal act (actus reus), creating challenges in determining responsibility when automated systems are involved. The BNS provides relevant provisions under Sections 45, 61 and 308[22] to identify extortion and criminal conspiracy. However, applying these provisions needs careful examination of the roles and intentions of the person involved.

To eradicate these challenges, India needs stronger legal provisions to address the growing issue of automated extortion. Effective legal provisions and better cooperation between law enforcement agencies and digital platforms can help identify offenders as well as trace unlawful payments. Section 63[23] provides provisions for the admissibility of electronic records, making their proper collection and preservation essential. Investigators should follow appropriate forensic procedures to maintain the validity of electronic evidence. Furthermore, banks and financial institutions should improve their systems for tracing suspicious transactions and also identify mule accounts. These measures can help strengthen investigations and support effective prosecution.

[22] Bharatiya Nyaya Sanhita 2023, ss 45, 61 and 308
[23] Bharatiya Sakshya Adhiniyam 2023, s 63