International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838, Print ISSN: 2664-682X
Received: 06-06-2025, Accepted: 06-07-2025, Published: 21-07-2025
Volume 7, Issue 3, 2025, Page No. 25-31

Cybercrime investigation in India: An analysis of digital evidence and its role in proving cybercrimes

Dr. Ram Prakash Chaubey
Principal, Department of law, Gyan Ganga Collage of Excellence, Jabalpur, Madhya Pradesh, India

Abstract
The article provides a comprehensive overview of cybercrime investigations in India, emphasizing the impact of recent legislative changes and emerging technologies. It highlights the limitations of traditional methods against sophisticated cyber offenses that transcend borders and involve ephemeral digital evidence, deepfakes, data manipulation, and encryption. The Bharatiya Sakshya Adhiniyam, 2023 (BSA), modernizes evidence law by broadening the definition and admissibility of digital records, while the Bharatiya Nagarik Suraksha Adhiniyam, 2023 (BNSS), introduces procedural updates for electronic reporting, digital statements, jurisdictional clarity, and mandatory forensic investigations. The burgeoning role of Artificial Intelligence (AI) in both perpetrating and investigating cybercrimes is examined. AI offers tools for deepfake detection, anomaly analysis, and malware identification, enhancing investigative capabilities. However, ethical considerations and potential biases in AI deployment are also discussed. Despite these advancements, India faces challenges in combating cybercrime, including the need for capacity building, investment in digital forensics infrastructure, strategic AI integration, inter-agency collaboration, and continuous legal updates. Public awareness and international cooperation are crucial for a comprehensive strategy. The modernization of legal frameworks through the BSA and BNSS is a significant step, but realizing their full potential requires a multi-faceted approach involving technological empowerment, human capital development, collaboration, and global engagement to fortify India's digital frontier and build a more secure cyberspace.

Keywords: Cybercrime investigation, digital evidence, artificial intelligence, bharatiya nagarik suraksha adhiniyam 2023, bharatiya sakshya adhiniyam 2023, india

Introduction

Proving a crime requires proper collection of potential evidence [1] and in the case of cyber crimes it is the digital which should be properly traced, collected and preserved to punish the cyber offenders. Rising cases of cybercrimes in India has made it necessary to properly understand the role of digital evidence in successful investigations of cybercrimes. Emails, call logs, online transactions, social media activity, etc. are crucial footprints to collect digital evidence. The admissibility and relevance of digital evidence in Indian courts are increasingly governed by the Bharatiya Sakshya Adhiniyam, 2023 (BSA), [2] which has now taken place of the Indian Evidence Act, 1872 [3]. Now the modernised law of evidence i.e. the BSA has broadened the definition of "document" & "evidence" to explicitly include electronic and digital records. Earlier various hurdles were faced to prove the admissibility of electronic and digital records but now the BSA's Section 57 [4] treats properly sourced digital records as primary evidence, streamlining their acceptance in the legal proceedings.

The process of leveraging digital evidence involves meticulous steps. Digital forensics experts employ specialized tools and techniques for the identification, preservation, acquisition, examination, and analysis of digital data. Maintaining the chain of custody is paramount to ensure the integrity and admissibility of this evidence. Investigators analyze various digital artifacts, including metadata, network logs, deleted files, and communication records, to reconstruct cybercriminal activities.

The challenges in handling digital evidence are significant. Its volatile nature, potential for alteration, and the complexities of cross-jurisdictional data often require sophisticated forensic capabilities and international cooperation. Encryption further complicates investigations, demanding specialized tools and legal frameworks for lawful access.

Digital evidence is indispensable in proving cybercrimes in India. The modernized legal framework under the BSA, coupled with advancements in digital forensics, is crucial for effectively decoding the digital trails left by cybercriminals and ensuring justice in the increasingly interconnected digital landscape. Continued focus on capacity building and technological upgrades within law enforcement and the judiciary is essential to harness the full potential of digital evidence in combating cyber threats.

Cybercrime and Its Forms

Cybercrime, a growing menace in our digital age, encompasses any illegal activity involving computers, networks, or networked devices, disregarding geographical boundaries. It exploits digital vulnerabilities for illicit gain or malicious intent, differing from traditional physical crimes. Understanding its diverse nature is vital for online safety. At its core, cybercrime uses technology as a tool or target, ranging from individual fraud to attacks on critical infrastructure, driven by financial motives, political agendas, espionage, or disruption. Cyber fraud is a prevalent form, including phishing (deceptive tactics to steal sensitive information), identity theft (unauthorized use of personal data), and online scams (fraudulent schemes exploiting trust). Beyond financial crimes, cybercrime targets data and systems through hacking (unauthorized access for theft or disruption) and malware (viruses, worms, ransomware, spyware causing data theft, encryption, or operational

disruption). Ransomware attacks, demanding payment for data decryption, are increasingly damaging. The digital age has also spawned cyberstalking and online harassment via electronic communication, causing emotional distress. Social media and messaging apps are unfortunately used for such behavior. Furthermore, cybercrime extends to intellectual property through online piracy and unauthorized distribution of copyrighted material, causing financial losses. The impact of cybercrime is far-reaching, causing financial losses, identity theft, reputational damage, and emotional distress for individuals. Businesses face financial losses from fraud and data breaches, along with reputational damage. Governments and critical infrastructure are targeted, risking national security and essential services.

Combating cybercrime requires a multi-faceted approach involving individual awareness (recognizing scams, strong passwords, cautious online behavior, software updates), organizational security measures (firewalls, intrusion detection, anti-malware, encryption, audits, access controls, employee training), and governmental action (enacting laws, specialized agencies, international cooperation). The rapid pace of technological advancement, including AI, IoT, and blockchain, presents new challenges for cybersecurity. Continuous research, innovative security technologies, and adaptive legal frameworks are essential to stay ahead of evolving threats.

Cybercrime Investigations

Cybercrime investigations are complex, transcending borders and leaving vast, often ephemeral digital data trails. These unraveling threads require specialized skills, advanced technology, and meticulous approaches to identify perpetrators and secure justice. The process typically begins with victim reports or proactive intelligence gathering. Initial incident response is crucial for containing damage and preserving evidence, such as isolating infected machines and creating forensic images of hard drives.

The heart of the investigation is digital forensics: identifying, preserving, acquiring, examining, analyzing, and reporting digital evidence. Analysts use specialized tools and techniques to reconstruct digital events. Evidence acquisition follows strict protocols, creating bit-by-bit forensic images of storage and cloud data, with meticulous chain of custody documentation vital for court admissibility.

Evidence examination and analysis involve piecing together the digital puzzle, scrutinizing file systems, logs, network traffic, and browser histories. Techniques include keyword searching, timeline analysis, and hashing. Network forensics and malware analysis are key in intrusion cases.

Attribution is challenging due to obfuscation, but investigators trace IP addresses, analyze domain registrations, and correlate digital evidence with real-world identities, often using Open-Source Intelligence (OSINT). Collaboration is essential for transnational crimes, requiring international cooperation. Investigations culminate in detailed reports, with investigators often testifying to explain technical findings. The evolving digital landscape demands continuous skill updates as new technologies like cloud computing, mobile devices, and IoT present ongoing forensic challenges. AI and machine learning are increasingly explored for large dataset analysis and pattern identification in cybercrime.

Digital evidence and its role in proving Cybercrimes

In our increasingly digital world, cybercrime leaves behind crucial, albeit intangible, digital footprints. This digital evidence—encompassing emails, messages, network logs, and more—is vital for proving cybercrimes and understanding perpetrator actions. Its power lies in its detailed recording of digital interactions and communications.

Digital evidence is crucial at all legal stages. In investigations, it generates leads: network logs trace attacks, email analysis reveals phishing, and recoverable deleted files expose concealment. However, collecting and preserving this evidence is complex. Forensic imaging creates bit-by-bit copies for integrity, while strict chain of custody protocols prevents tampering.

Digital forensic analysis transforms raw data into meaningful evidence. Techniques like timeline analysis reconstruct events, keyword searching identifies relevant terms, and file hashing verifies authenticity. This evidence is powerful for proving various cybercrimes: transaction logs for fraud, compromised data for identity theft, and network logs for hacking.

Despite its value, digital evidence is volatile, easily altered or deleted. Its transnational nature demands international cooperation, and authentication can be challenging. Encryption further hinders investigations. Nevertheless, digital evidence remains invaluable, providing detailed records for uncovering the truth and holding cybercriminals accountable. Its unique characteristics necessitate evolving legal frameworks and forensic techniques to ensure its admissibility and secure justice in the digital age.

Modern Trends and Challenges in Digital Evidence

Cybercrime investigations are rapidly evolving due to our digital world, adopting new technologies while grappling with increasing complexities in digital evidence.

Modern Trends: A key trend is the growing reliance on Artificial Intelligence (AI) and Machine Learning (ML) to analyze vast datasets, identify patterns, and detect malicious activity, such as real-time network traffic analysis for cyberattacks or efficient phishing campaign detection. Proactive threat intelligence is also gaining importance, using OSINT and other sources to anticipate and prevent attacks by understanding threat actor tactics. The rise of cloud computing, mobile devices, and the Internet of Things (IoT) has expanded attack surfaces and introduced new, diverse sources of digital evidence, requiring specialized cloud forensics and tools for data extraction. Furthermore, cross-jurisdictional and public-private collaboration is crucial, with organizations like Interpol and Europol facilitating international cooperation and partnerships with private cybersecurity firms.

Challenges: These trends, however, bring significant challenges for digital evidence. The sheer volume and velocity of digital data make manual analysis impractical. The ephemeral and volatile nature of some digital evidence (e.g., volatile memory, network logs) necessitates rapid incident response. Data encryption remains a persistent obstacle, requiring legal and technical decryption methods. Ensuring integrity and authenticity is paramount, demanding robust chain of custody procedures and cryptographic hashing. Legal and jurisdictional complexities arise from differing international laws on data privacy and cross-border transfers. The rapid pace of technological change constantly

introduces new devices and formats, requiring continuous updates to forensic tools and skills. Finally, privacy implications of digital evidence collection must be carefully balanced with the need to investigate crimes, necessitating clear legal and ethical guidelines.

Cyber Crime Investigations, Forensics and AI

The evolving cybercrime landscape, marked by deepfakes, data manipulation, and pervasive encryption, demands new forensic approaches. Artificial Intelligence (AI) is crucial in solving these complex digital puzzles.

Deepfakes, AI-generated synthetic media, challenge traditional forensics. AI-powered detection tools analyze subtle inconsistencies—like blinking patterns or pixel anomalies—to distinguish them from authentic media. AI also examines digital fingerprints for generative algorithm signs, a field requiring continuous development.

Data manipulation, a growing threat, is detected by AI establishing normal data baselines and flagging anomalies, such as unusual financial transactions or sensor data. This provides real-time detection capabilities.

Widespread encryption hinders investigations. AI can help by analyzing metadata to reveal patterns, assisting in password recovery through sophisticated brute-force attacks, and identifying suspicious communication patterns even within encrypted channels.

Integrating AI into digital forensics automates tasks like file carving and malware analysis, allowing human analysts to focus on complex aspects. However, reliance on AI brings challenges: explainability and transparency of algorithms are crucial for legal acceptance, and addressing bias in training data is vital. The convergence of AI with traditional forensics offers a powerful toolset against sophisticated threats, augmenting human expertise to ensure justice in the digital age.

Bharatiya Sakshya Adhiniyam 2023

The digital revolution has brought forth unprecedented opportunities, but it has also ushered in a new era of criminal activity – cybercrime. Recognizing the unique challenges posed by these technologically driven offenses, the Indian legislature has enacted the Bharatiya Sakshya Adhiniyam, 2023 (BSA), [5] poised to replace the antiquated Indian Evidence Act, 1872. This new legal framework introduces significant provisions aimed at modernizing the admissibility and relevance of digital evidence, thereby bolstering the investigation and prosecution of cybercrimes within the Indian context.

The BSA, came into force on July 1, 2024, fundamentally redefines key concepts to align with the digital age. Section 2(1)(d) [6] expands the definition of a "document" to explicitly include "electronic or digital records on emails, server logs, documents on computers, laptop or smartphone, messages, websites, locational evidence and voice mail messages stored on digital devices." This inclusive definition acknowledges the vast array of digital data that can serve as crucial evidence in cybercrime investigations, moving beyond traditional paper-based documents.

Similarly, Section 2(1)(e) broadens the definition of "evidence" itself to encompass "(i) all statements including statements given electronically which the Court permits or requires to be made before it by witnesses in relation to matters of fact under inquiry and such statements are called oral evidence; (ii) all documents including electronic or digital records produced for the inspection of the Court and such documents are called documentary evidence." This explicitly recognizes the admissibility of electronic statements and digital records as valid forms of evidence, a critical step in addressing cyber offenses where communication and data storage predominantly occur in digital formats.

A cornerstone of the BSA concerning cybercrime investigations lies in its treatment of primary and secondary evidence in the digital realm. Section 57, [7] which defines "primary evidence," now includes explanations specifically addressing electronic records. For instance, where a video recording is simultaneously stored electronically and transmitted, each stored recording is considered primary evidence. Crucially, it states that an electronic or digital record produced from proper custody is primary evidence unless its genuineness is disputed. Furthermore, if an electronic record is stored across multiple storage spaces within a computer resource, each automated storage, including temporary files, is deemed primary evidence. This clarification is vital for establishing the authenticity and reliability of digital evidence collected during cybercrime investigations.

Section 58 [7] outlines "secondary evidence," which can be admitted under specific circumstances, such as when the original is unavailable or its genuineness is questioned. While the BSA retains the concept of secondary evidence for digital records (like printouts or copies), the emphasis on treating properly sourced digital records as primary evidence under Section 57 signifies a move towards recognizing their inherent evidentiary value. This can expedite the legal process in cybercrime cases where obtaining the "original" digital source might be complex or impractical.

To address the technical complexities often involved in digital evidence, Section 39 [8] becomes particularly relevant. It allows the court to form an opinion on electronic evidence by consulting an Examiner of Electronic Evidence. This provision recognizes the specialized knowledge required to interpret and analyze digital data, including aspects related to deepfakes, data manipulation, and encryption. The examiner's report can provide crucial insights into the authenticity, integrity, and relevance of digital evidence presented in cybercrime cases. While the BSA doesn't explicitly detail the procedural aspects of cybercrime investigations (which are primarily governed by the Bharatiya Nagarik Suraksha Sanhita, 2023 – the new Code of Criminal Procedure), its provisions on the admissibility of digital evidence directly impact how these investigations are conducted and how their findings are presented in court. The enhanced recognition of electronic records as primary evidence necessitates that investigating agencies adopt robust protocols for the collection, preservation, and chain of custody of digital evidence. This includes utilizing forensic best practices to ensure data integrity and prevent tampering, which is crucial for the successful prosecution of cybercriminals.

Furthermore, the BSA indirectly addresses the challenges posed by encryption. While it doesn't mandate decryption, the admissibility of metadata and communication patterns as evidence under the broader definition of electronic records can be valuable even when the content remains encrypted. Investigators might rely on traffic analysis, timestamps, and communication logs to establish connections and intent, even without accessing the encrypted data itself. The

provision for expert opinion under Section 39 also allows the court to understand the implications of encryption in the context of the case.

Regarding deepfakes and data manipulation, the BSA's emphasis on the authenticity and integrity of electronic records becomes paramount. The ability of the court to consult an Examiner of Electronic Evidence under Section 39 provides a mechanism to scrutinize digital media for signs of manipulation. AI-powered forensic tools, while not explicitly mentioned in the Act, fall under the purview of expert opinion and can be crucial in analyzing deepfakes for inconsistencies or detecting subtle alterations in data. The burden of proving the genuineness of digital evidence, especially when challenged, rests on the prosecution, and the provisions of the BSA provide the legal framework for this process.

The Bharatiya Sakshya Adhiniyam, 2023 (BSA) significantly modernizes India's legal framework for cybercrime, broadening "document" and "evidence" to include digital records and classifying electronic records as primary evidence. This creates a more robust system for investigating and prosecuting cyber offenses. However, the BSA's effectiveness hinges on capacity building for law enforcement and the judiciary. Understanding electronic records, forensic procedures, and technologies like AI and encryption is crucial for successful implementation, ultimately ensuring a safer digital environment for India.

The CPC, 1908 and Bharatiya Nagarik Suraksha Adhiniyam, 2023 (BNSS)

The escalating tide of cybercrime necessitates a robust legal framework that outlines clear procedures for investigation and prosecution. While the Code of Civil Procedure, 1908 (CPC) [10] primarily governs civil matters, its relevance to cybercrime investigations is limited to aspects like jurisdictional challenges in civil suits arising from online transactions. The primary procedural guidelines for cybercrime investigations in India are laid down in the soon-to-be-enacted Bharatiya Nagarik Suraksha Adhiniyam, 2023 (BNSS), which will replace the Code of Criminal Procedure, 1973 (CrPC). Understanding the interplay and specific provisions within these legal instruments is crucial for navigating the complexities of cyber offenses.

a. The Limited Role of the Code of Civil Procedure, 1908 (CPC) in Cybercrime Investigations

The CPC mainly deals with the procedures followed by civil courts in the adjudication of civil disputes. Its direct application to the investigation of cybercrimes, which are criminal offenses, is minimal. However, certain provisions within the CPC become relevant in the context of civil suits that may arise as a consequence of cybercriminal activities. For instance, issues of jurisdiction in cases where online transactions or interactions lead to civil disputes are often determined based on principles enshrined in Sections 16 to 20 of the CPC. [11] These sections specify where a suit can be instituted based on the place of residence of the defendant, the place where the cause of action arose (which can be online in cyber-related disputes), or the location of the subject matter.

Furthermore, the CPC's provisions on evidence, particularly concerning the production and admissibility of documents, have historically been interpreted to include electronic records, even before specific amendments in other statutes. However, with the enactment of the Information Technology Act, 2000, and now the BSA, 2023, the rules for admissibility of digital evidence in both civil and criminal proceedings are largely governed by these specialized legislations. Thus, while the CPC lays down the general framework for civil procedure, its direct procedural guidelines for the investigation of cybercrimes are absent.

b. The Bharatiya Nagarik Suraksha Adhiniyam, 2023 (BNSS): A New Paradigm for Cybercrime Investigations

The Bharatiya Nagarik Suraksha Adhiniyam, 2023 (BNSS), replaced the CrPC on July 1, 2024, introduces several provisions that are directly relevant to the procedures for investigating cybercrimes in India. While the BNSS does not provide a separate, exhaustive chapter solely dedicated to cybercrime investigation, it incorporates elements and modernizes procedures to address the unique challenges posed by digital offenses.

1. **Reporting of Cybercrimes:** The BNSS, under Section 173, [12] retains the procedure for lodging a First Information Report (FIR) for cognizable offenses. Recognizing the digital nature of cybercrimes, the Act acknowledges the possibility of filing complaints electronically. While the specific mechanisms for online FIR filing may be governed by separate rules and platforms established by state police forces, the BNSS provides a legal basis for the electronic reporting of cyber offenses. Furthermore, Section 173(1) mandates hat if information regarding a cognizable offense is given orally to an officer in charge of a police station, it shall be reduced to writing and signed by the informant. This applies equally to information provided electronically, with a stipulation that such digitally submitted complaints must be signed by the informant within three days to be converted into a formal FIR.

2. **Investigation Powers and Procedures:** The BNSS empowers police officers to investigate cognizable offenses, including cybercrimes, under Chapter XII. While it doesn't prescribe specific digital forensic techniques, the Act's emphasis on the use of technology in investigations is evident. Section 176(3) [13] allows Investigating Officers (IOs) to record statements of witnesses through audio-video electronic means. This can be particularly useful in cybercrime investigations where witnesses might be geographically dispersed or prefer to give their statements remotely. Section 179 [14] of the BNSS (corresponding to Section 179 of the CrPC) deals with jurisdiction in cases where an offense is committed partly in one area and partly in another, or where the consequences of an act occur in a different area. This is highly relevant to cybercrimes, which often have a diffused geographical impact. The section allows for inquiry or trial by a court within whose local jurisdiction either the act was done or the consequence ensued. For cyber offenses like online fraud or data breaches affecting individuals across different locations, this provision provides clarity on jurisdictional matters. Section 182 [15] of the BNSS (corresponding to Section 182 of the CrPC) specifically addresses offenses involving cheating and dishonestly inducing delivery of property through letters or

electronic communication. It allows for inquiry or trial by a court within whose local jurisdiction the letters or electronic communications were sent or received, or where the property was delivered or received by the person deceived. This section directly caters to many forms of online financial fraud and scams. Section 184 [16] of the BNSS (corresponding to Section 184 of the CrPC) provides for the trial of offenses committed beyond India which are triable within India. This is crucial for addressing cybercrimes where perpetrators might be located outside Indian territory but target Indian citizens or systems.

3. **Search and Seizure of Digital Evidence:** Section 94 to 103 [17] of the BNSS (corresponding to Sections 93 to 101 of the CrPC) outline the procedures for search warrants and searches. These provisions are applicable to the search and seizure of digital devices, computer systems, and networks that may contain evidence of cybercrimes. The BNSS, in Section 102, [18] mandates the audio-video recording of search and seizure procedures, enhancing transparency and accountability in the collection of digital evidence. This is particularly important to maintain the integrity and admissibility of sensitive digital data. Section 105 [19] of the BNSS (corresponding to Section 166A of the CrPC) facilitates reciprocal arrangements with foreign countries for assistance in investigations, including cybercrime investigations that often have international dimensions.

4. **Examination of Accused and Witnesses:** The BNSS retains provisions for the examination of the accused (Section 317) and witnesses (Chapter XXV). In the context of cybercrime, this includes the recording of electronic statements and the potential for witnesses to testify through audio-video means as mentioned in Section 275. The admissibility of electronically recorded statements as evidence is further strengthened by the Bharatiya Sakshya Adhiniyam, 2023 (BSA).

5. **Forensic Investigation:** A significant modernization in the BNSS is the mandatory forensic investigation for offenses punishable with imprisonment for seven years or more (Section 176(3). This provision requires forensic experts to visit crime scenes, collect forensic evidence, and record the process using mobile phones or other electronic devices. While "crime scene" traditionally referred to physical locations, its application extends to digital crime scenes in cyber offenses, necessitating the involvement of digital forensic experts in the investigation process. This underscores the importance of proper handling and analysis of digital evidence in serious cybercrimes.

While the Code of Civil Procedure, 1908, has limited direct applicability to the procedures of cybercrime investigations, primarily concerning jurisdictional aspects in related civil suits, the Bharatiya Nagarik Suraksha Adhiniyam, 2023, introduces crucial updates to the criminal procedure to address the unique challenges of cyber offenses. By acknowledging electronic reporting, facilitating the recording of digital statements, clarifying jurisdictional issues in online offenses, mandating the audio-video recording of searches, and emphasizing forensic investigation, the BNSS modernizes the legal framework for tackling cybercrime in India. The effective implementation of these provisions, coupled with capacity building in digital forensics and a clear understanding of the evidentiary rules laid down in the Bharatiya Sakshya Adhiniyam, 2023, will be instrumental in strengthening India's ability to investigate and prosecute cybercriminals in the evolving digital landscape.

Investigations in AI Related Cybercrimes

The rise of Artificial Intelligence (AI) has not only transformed industries but has also introduced a new dimension to cybercrime. Offenses leveraging AI, such as sophisticated phishing attacks, deepfakes used for fraud, and AI-driven malware, pose unique challenges for traditional investigative methods. In the Indian context, the legal framework and investigative procedures are adapting to address these "AI-related cybercrimes," primarily guided by the Bharatiya Nagarik Suraksha Adhiniyam, 2023 (BNSS), set to replace the Code of Criminal Procedure, 1973 (CrPC), and the Information Technology Act, 2000 (IT Act), along with the upcoming Digital Personal Data Protection Act, 2023.

The investigation of AI-related cybercrimes in India necessitates a multi-pronged approach, leveraging both traditional policing methods and specialized digital forensic techniques enhanced by AI itself.

a. **Reporting and Initial Assessment:** Similar to other cybercrimes, the process begins with the reporting of the offense, as per Section 173 of the BNSS. This can be done electronically. When AI is suspected to be involved, the initial assessment involves identifying the nature of the AI's role. Was AI used as a tool to commit the crime (e.g., generating deepfakes), or was the AI system itself the target of the crime (e.g., manipulation of AI algorithms)? This initial categorization is crucial for directing the subsequent investigative steps.

b. **Digital Forensics and AI-Powered Analysis:** Digital forensics forms the backbone of investigating AI-related cybercrimes. Investigators utilize specialized tools to collect and preserve digital evidence from various sources, as outlined implicitly in Chapter XII of the BNSS concerning investigation powers. However, analyzing data related to AI requires advanced techniques. AI is crucial in combating sophisticated cybercrimes. It powers deepfake detection by identifying subtle inconsistencies in synthetic media. AI also performs anomaly detection to spot malicious manipulation of AI systems or data. For malware analysis, AI helps understand propagation and identify infrastructure. Natural Language
Processing (NLP) aids in detecting AI-generated phishing emails by analyzing linguistic cues. AI algorithms can sift through massive datasets of network logs and system activity to identify patterns that might be missed by human analysts, potentially uncovering AI-orchestrated attacks.

c. **Legal Framework and Expert Opinions:** The IT Act, 2000, provides the primary legal framework for cybercrimes in India. Relevant sections, such as Section

43 (damage to computer systems) and Section 66 (computer hacking), can be invoked depending on the nature of the AI-related offense. The upcoming Digital Personal Data Protection Act, 2023, will further strengthen data protection measures relevant in cases where AI is used to compromise personal data.

Section 39 of the Bharatiya Sakshya Adhiniyam, 2023, which allows the court to consult an Examiner of Electronic Evidence, is particularly significant in AI-related cybercrimes. Expert opinions from AI and digital forensics specialists will be crucial in understanding the technical complexities of AI systems, the methods of manipulation, and the interpretation of AI-generated evidence.

d. Jurisdictional Challenges and International Cooperation: Cybercrimes involving AI often transcend geographical boundaries. Section 179 and 182 of the BNSS address jurisdictional issues in cases where the offense has cross-border elements or involves electronic communication across different locations. International cooperation, facilitated under Section 105 of the BNSS, becomes vital in investigating AI-related cybercrimes where perpetrators or infrastructure are located outside India.

Relevant Judgments on Cybercrime Investigation and Digital Evidence

Indian courts have significantly shaped the admissibility of digital evidence, a crucial aspect for emerging technologies like blockchain, cryptocurrency, and AI. The landmark Anvar P.V. vs. P.K. Basheer & Ors. [20] established the mandatory Section 65B (4) certificate (now Section 63 of BSA, 2023) for electronic records presented as secondary evidence. This certificate is vital for authenticating data from blockchain, cryptocurrency, and AI systems. While Shafhi Mohammad vs. State of Himachal Pradesh, [21] offered a slight relaxation when the device isn't with the presenting party, Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantyal & Ors. [22] reaffirmed the certificate's importance for proper procedural compliance. Crucially, State of Karnataka vs. T. Naseer @ Nasir @ Thandiantavida Naseer @ Umarhazi @ Hazi & Ors. [23] clarified that the Section 65B certificate isn't required for primary electronic evidence and can be submitted at any trial stage. This is a significant development for admitting original blockchain records or direct AI system data, provided their integrity is maintained. Earlier, Thana Singh vs. Central Bureau of Narcotics, [24] recognized digital charge sheets as valid electronic records, showing the judiciary's early embrace of digital formats. Beyond specific evidence rules, the Supreme Court's decision to suppress the RBI's crypto trading ban in Internet and Mobile Association of India v. Reserve Bank of India, [25] demonstrates the judiciary's increasing engagement with the legal aspects of cryptocurrencies, which will indirectly influence how related criminal evidence is handled.

Conclusion and Suggestions

India's battle against cybercrime is evolving with the Bharatiya Nagarik Suraksha Adhiniyam, 2023 (BNSS) and Bharatiya Sakshya Adhiniyam, 2023 (BSA), modernizing legal frameworks for the digital age. Cybercrime's transnational nature, volatile digital evidence, and rapid technological shifts, including AI and encryption, pose significant challenges, making traditional investigative methods inadequate.

The BSA is crucial, modernizing digital evidence definitions and admissibility, explicitly recognizing electronic records as primary evidence (Section 57), allowing expert opinions (Section 39), and broadening "document" and "evidence" definitions (Section 2). The BNSS updates procedures for electronic reporting (Section 173), recording digital statements (Section 176), addressing jurisdiction, and mandating forensic investigations for serious offenses (Section 176).

However, legal provisions alone are insufficient. India needs to:

1. Boost capacity building and training for law enforcement, judiciary, and forensic experts.
2. Strengthen digital forensic infrastructure with advanced tools and labs.
3. Strategically leverage AI in investigations for anomaly detection and data analysis.
4. Enhance inter-agency and public-private collaboration for information sharing.
5. Strengthen legal frameworks and enforcement for emerging cyber threats.
6. Raise public awareness and digital literacy to prevent cybercrime.
7. Foster international cooperation for cross-border investigations and intelligence sharing.
8. India's effective navigation of the digital maze requires continuous adaptation, strategic investment, and collaborative efforts to ensure a secure digital future.

Reference

1. Ms. Sadhna Gupta, Ms. Meghali Das, 'Criminal Investigation of Electronic Evidence: Challenges Faced with Digital Forensics' (2023) 2(2) JFJ 1.
2. The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).
3. The Indian Evidence Act, 1872 (Act 1 of 1872).
4. The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 57.
5. The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).
6. The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 2(1)(e).
7. Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 57.
8. The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 58.
9. Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 39.
10. Code of Civil Procedure, 1908 (Act 5 of 1908).
11. The Code of Civil Procedure, 1908 (Act 5 of 1908), ss. 16
12. Bharatiya s. 173.
13. The Bharatiya Nagarik Suraksha Adhiniyam, 2023 (Act 46 of 2023), s. 176(3).
14. The Bharatiya Nagarik Suraksha Adhiniyam, 2023 (Act 46 of 2023), s. 179.
15. The Bharatiya Nagarik Suraksha Adhiniyam, 2023 (Act 46 of 2023), s. 182.
16. The Bharatiya Nagarik Suraksha Adhiniyam, 2023 (Act 46 of 2023), s. 184.
17. The Bharatiya ss. 94-103.

18. The Bharatiya Nagarik Suraksha Adhiniyam, 2023 (Act 46 of 2023), s. 102.
19. The Bharatiya s. 105.
20. (2014) 10 SCC 473.
21. (2018) 2 SCC 801.
22. (2020) 7 SCC 1.
23. 2023 (11) TMI 2011 (SC).
24. (2013) 2 SCC 590.
25. (2020) 10 SCC 693.