INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

COMBATING CYBERCRIME IN INDIA: A CRITICAL ANALYSIS OF LEGAL FRAMEWORKS AND ENFORCEMENT MECHANISMS

AUTHORED BY - SINIPRIYA A

Abstract:

The internet, which is an integrated global network structure, is used by numerous individuals worldwide. Even though the number of people using the internet is rapidly increasing, internet access is not evenly distributed between or within countries. Large-scale advancements are promised by increased connectivity and a digital economy, but these developments also expose our digital societies to new threats. With increased cyberattacks and data breaches, cybercrime has become a growing menace in the digital age. Individuals' psychological and financial well-being as well as the economy are significantly impacted by these attacks. As per the reports published by ASSOCHAM, India has witnessed 457% increase in cybercrimes since 2011. To improve social security and national sovereignty, there is a need for raising awareness, reporting cybercrimes, and fortifying cyber laws. In this regard, this paper intends to explore the cyber-attacks on individuals and highlights the measures to be taken to prevent these cyber-crimes. The study also emphasis the role and initiatives of the government towards curbing the cyber-crimes menace in the nation.

***Index Terms*: - Cyber-crimes, Security, Measures, Internet, Government Initiatives.**

INTRODUCTION

Cybercrime is becoming more of an issue as technology advances frequently, yet countermeasures and prevention to safeguard both the technology and its users are not developing as fast. India is poised to become one of the most prominent digital hubs in the world. Large-scale advancements are promised by increased connectivity and a digital economy, but these developments also expose our digital societies to new threats. Since cyberattacks and data breaches have significantly increased in India, cybercrime has become a growing menace in the digital age. The growth of networking and cyberspace has enormously

ISSN: 2582-6433

helped people, however some people exploit this [1]development to get illicit advantages. Cybercrimes, on the other hand, are transnational and have developed at a rate comparable to that of new technologies. Cyber criminals and Scammers are using advanced technologies such as AI and ML tools to create Malwares that break the traditional security firewalls. They take the full advantage of the fact that they are extremely hard to track down. A nation's weak cyber security measures or the deployment of new technologies by cybercriminals are two possible causes of cyberattacks. This study explores the vulnerabilities and difficulties that individuals experience as a result of the current condition of cyber threats in India. It examines how a variety of cybercrimes, including data theft, phishing, online fraud and ransomware that individuals get trapped into. In order to improve social security and national sovereignty, it highlights the significance of raising awareness, reporting cybercrimes, and fortifying cyber laws.

The term *"Cyber Crime"* was first proposed by Sussman and Heuston in the year 1995. According to Saini, H., Rao, Y. S., & Panda, T. C. (2012), Cybercrime is defined as any criminal behavior that is directly connected to the use of computers, including unlawfully entering another person's computer system or database, altering or stealing data that is stored online, or sabotaging hardware and data. The government is aware of the growing prevalence of online fraud and electronic media abuse. Therefore, to monitor cybercrime and Internet fraud, the government established the Information Technology Act, 2000. The Act penalizes individuals who attempt to abuse this channel for their own gain or to scam others with severe penalties.

The number of cyber-crimes reported in India is proliferating each year. This is in line with the increase in the usage of internet and computer, advancement in technology, and digitisation. The table below depicts the no. of cyber-crime cases reported in India taken from National Crime Record Bureau (NCRB), for the years 2012 to 2024.

Table 1: Number of CyberCrimes Reported from the year 2012 to 2024

S.No.	Year	Number of Cyber Crimes Reported
1	2012	3477
2	2013	5693
3	2014	9622

[1] Ms. Sadhna Gupta, Ms. Meghali Das, 'Criminal Investigation of Electronic Evidence: Challenges Faced with Digital Forensics' (2023) 2(2) JFJ 1.

ISSN: 2582-6433

4	2015	11592
5	2016	12317
6	2017	21796
7	2018	27248
8	2019	44546
9	2020	50035
10	2021	52974
11	2022	65893
12	2023	75,656
13	2024	More than 740000

The table 1 reveals that the no. of cases reported each year are not just increasing but they are increasing at an increasing rate. This calls for an immediate action and strict measures to curb this menace. In a recent study by University of Oxford published the World's Cyber-crime Index in its Journal of Plos One which reveals that India stands in the 10th position in terms no. of cyber-crimes reported while Russia and Ukraine stand in the first two positions respectively. This report also states that if timely strategic measures are not taken up, it is not too late for India to be the hotspot.

Important Statistics of Cybercrimes in India in the year 2024 -

- **Average Cases per day: A**lmost 7,000 cases were reported per day as cyber frauds.
- **Cases Cumulatively:** By May 2024, 7,40,000 cases were registered, raised to 12 lakh by September 2024.
- **Amount Lost:** An amount of nearly ₹120 crores is lost in different forms of cybercrime.

From the above information, the Investigations revealed that majority of the scams were operated from other countries like Cambodia, Myanmar, and Laos.[2]

[2] The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).
1. The Indian Evidence Act, 1872 (Act 1 of 1872).
2. The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 57.
3. The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

ISSN: 2582-6433

Review of literature

The complex issues that cybercrime presents to individuals, companies, and society call for coordinated efforts in technology, policy, and research to reduce risks and improve cybersecurity resistance. Several studies investigated the various cyber-crimes and measures to prevent them as highlighted below: -

Kuzior et.al, (2024), analyzed the cybercrimes globally from 2016 to 2023 to present the combating mechanisms to establish a safe and secure cyberspace, shield people from cyber frauds and threats, thereby increasing the potency of the controlling measures in cyberspace. A comparative analysis is made in terms of highest cyber-crime rate and the level of security. It has also suggested several measures to curb the cybercrimes.

Verma, A., & Shri, C. (2022) The COVID-19 epidemic has forced most organisations to undergo digital transformation leading to increased reliance on digital infrastructure increasing its susceptibility to cybercrimes. According to the literature, the most prominent and often used tools by attackers are distributed denial of service (DDoS) assaults, malware attacks, phishing attacks, Internet of Things (IoT) attacks, and SQL injection attacks. An effort has been made in this study to create a framework for defence against these cyberattacks. To do this, this study has chosen to investigate in a methodical, stepby-step manner. A suggested protective framework for the organisations is developed as a result of the synthesis of the information gathered.

Datta et.al. (2020) The paper focuses on the increase in cybercrimes in India, emphasising the unethical use of computers and the internet for illicit purposes. Technical support scams and IRS impersonation scams are common scams that mostly target people between the age groups of 20 and 29, with women and children being especially at risk. It is underlined how important awareness campaigns are to fighting cybercrimes.

Dar and Lone, (2020) expressed that technological advancement has increased the number of cybercrimes in different forms. The rate of cybercrimes in India is increasing day by day. He also focussed on the security measures for the organizations to curb the cyber-attacks and prevention of cybercrimes.

Khan (2020) studied empirically cybercrimes in India from the year 2011 to 2016 and highlighted that India is ranked third globally as a source of malicious activity in the year 2015. He concluded that the government of India refined rules to safeguard interest of individuals and shield them from the harmful experiences online.

Shah (2019) studied the growth in the usage of the Internet and its problems encountered by

ISSN: 2582-6433

the individuals in India. He has examined the types of cyber-crimes and their growing numbers reported under IT Act 2000 and Indian Penal Code (IPC) in India for the period ranging from 2012 to 2016. The actions and policies implemented by the Indian government were also the main focus of this study, which also offers advice on how to prevent the pitfalls.

Mokha (2017) quoted that the use of the internet had increased a lot in daily transactions. He analyzed the cybercrime awareness among the users of the internet with diverse demographics. He found that there is a relationship between the age and the qualifications of the individuals. He expressed that every individual shall be aware of cybercrime and security, and also establish awareness among others.

Iqbal and Beigh (2017) This study focuses on the measures taken by the Indian government towards curbing cyber-crimes. Cybercrime plays a role in the bilateral agreement between Russia and the framework agreement with the United States. Additionally, India has taken another step to improve its cybersecurity with the recent visit of its prime minister to Israel to create the Indo-Israel cyber framework. He recommended that India consider signing the Budapest Cybercrime Convention with Europe to combat cybercrime.

Seema Goel (2016). The IT revolution has greatly benefited the banking industry, which has embraced a number of technologies for online transactions. As technology has advanced, so too have cybercrimes, which now largely target banks and financial organisations to make money. This study investigates the various cybercrime attacks, their effects, and countermeasures with respect to the banking industry.

Karali Y., Panda S., Panda C.S. (2015). This study is based on a quantitative examination of cybercrime cases under the Indian Penal Code and the IT Act in India's most vulnerable states and cities. [3]

Additionally, incidents of cybercrime perpetrated by individuals of various ages have been examined. Important corrective actions that must be performed to reduce the number of cybercrime cases have also been proposed, in addition to the explanation of the many motivations behind cybercrime activities and offences.

Brahme, A. M., & Joshi, S. B. (2013). The paper addresses cybercrime and cyberthreats, stressing the importance of knowledge and preventive measures to address these problems. Along with recommended models for social cyber security, it emphasises the effects of

[3] The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 2(1)(e).
s. Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), 57.
2. The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 58.
s. Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), 39.

ISSN: 2582-6433

cyberthreats on governments, IT industries, and society.

While majority of the studies analysed the technical aspects of cyber-crimes and the technical tools used by the scammers, there are limited studies that highlighted the vulnerabilities and difficulties faced by individuals due to these cyber attackers and criminals. Therefore, this study intends to bring in cyber-crimes against individuals and suggest the measures to prevent themselves.

Objectives of the study

To study about cyber-crimes, in general, and cyber-crimes against individuals in particular.

1. To examine the statistics on cyber-crimes reported in India in the last decade i.e., 2012-2024.
2. To highlight the initiatives taken up by the government of India to prevent cyber-crimes.
3. To suggest some measures of prevention for individuals against cyber-crimes.

Government Initiatives

The **Indian Cyber Crime Coordination Centre** (I4C) was established in 2020 as one of the many steps the Indian government has done to combat the escalating cyberthreats. This program serves as a focal point for managing instances of cybercrime and enhancing law enforcement capabilities.

The **National Cyber Crime Reporting Portal,** initiated in the year 2021**,** also enables individuals to report crimes, with a focus on crimes against women and children. For easy and quick reporting of online cybercrime, a Helpline number, "1930," has been activated.

In 2021, under I4C, the "**Citizen Financial Cyber Fraud Reporting and Management System**" was established to expedite the reporting of financial frauds and prevent the criminals from theft of money. As of today, over 13.36 lakh complaints have resulted in the saving of approximately Rs. 4,386 crore.

Cybercrime Cells: Many states have set up specialized cybercrime cells to investigate and prevent online crimes along with establishing labs and training facilities for cyber forensics to raise awareness and offer instruction in different cities. It also ensures training of all law enforcement and judicial personnel on how to deal with cybercrimes. Various portals and helpline numbers are set up to offer round-the-clock assistance in reporting cybercrime incidents and resolve them at the earliest.

ISSN: 2582-6433

Joint Cyber Coordination Teams (JCCTs) were established at Hyderabad, Vishakhapatnam, Mewat, Guwahati, Ahmedabad, Chandigarh, and Jamtara which were recognized as cybercrime hotspots. **Public Awareness**: There are several programs initiated to educate the public about the risks of cybercrime and online safety. Programs to educate and teach individuals on how to spot phishing scams, dubious emails, and safe online practices. Conducting awareness campaigns on issues like creating secure passwords, avoiding sensitive transactions on public Wi-Fi, and identifying social engineering techniques have been some of the initiatives taken up by the government.

Honourable Prime Minister Shri Narendra Modi addressed the citizens of the India on digital arrest in"**Mann Ki Baat**" programme on 27/10/2024.

Cyber Fraud Mitigation Centre (CFMC) was set up under I4C for mitigation of cybercrimes under the cooperation and collaboration of payment and Telecom service[4] providers, financial and IT intermediaries, bank representatives and officials of Law Enforment agencies.

Measures To Prevent From Cyber Crimes

In order to safeguard the world's second-largest internet population, India has only recently started to build a cybersecurity architecture.

Despite the legal frameworks and efforts to combat cybercrime, there is still much work to be done in terms of enforcement, awareness, and technical capabilities to tackle this evolving issue. However, some of the measures highlighted below enables the individuals to stay aware and cautious in order to lower the risks of cyber-attacks –

- Usage of strong passwords – For every account, create a strong, one-of-a-kind password using a mix of numbers, letters, and symbols.
- Avoid using the same password across the applications and online services.
- Two-step verification or authentication – Implement Multi-factor authentication for additional security.
- One should install and update firewalls, anti-virus, and anti-spyware software on their computers regularly.

[4] The Bharatiya s. 105.
1. (2014) 10 SCC 473.
2. (2018) 2 SCC 801.
3. (2020) 7 SCC 1.
4. 2023 (11) TMI 2011 (SC).
5. (2013) 2 SCC 590.

(2020) 10 SCC 693

ISSN: 2582-6433

- Avoid visiting untrusted websites or clicking on links sent by unidentified or untrusted websites.
- Promote the usage of virtual private networks (VPNs) for public or unprotected networks.
- Avoid clicking pop-ups as they contain malware or other harmful software.
- Do not share personal information such as bank account details, credit or debit card numbers, OTPs, images, address etc.
- Avoid using public wifis

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,"

ISSN: 2582-6433

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[5] 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 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

[5] The Bharatiya Nagarik Suraksha Adhiniyam, 2023 (Act 46 of 2023), s. 182.

1. The Bharatiya Nagarik Suraksha Adhiniyam, 2023 (Act 46 of 2023), s. 184.
2. The Bharatiya ss. 94-103.

The Bharatiya Nagarik Suraksha Adhiniyam, 2023 (Act 46 of 2023), s. 102

ISSN: 2582-6433

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.

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 AIrelated 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.

ISSN: 2582-6433

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[6] 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

1. Bharatiya s. 173.
2. The Bharatiya Nagarik Suraksha Adhiniyam, 2023 (Act 46 of 2023), s. 176(3).
3. The Bharatiya Nagarik Suraksha Adhiniyam, 2023 (Act 46 of 2023), s. 179.

ISSN: 2582-6433

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.

ISSN: 2582-6433

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.