DIGITAL VICTIMISATION AND FORENSIC JUSTICE IN INDIA: A CRITICAL STUDY OF CYBERCRIME INVESTIGATION, EVIDENTIARY BARRIERS AND VICTIM RIGHTS

Padma Varshini M, LLM, Tamil Nadu Dr. Ambedkar Law University

ABSTRACT

The increasing integration of digital technologies into everyday life has transformed the nature of criminal activities and created new challenges for the administration of criminal justice in India. Digital victimisation has emerged as a serious legal and social concern, affecting individuals through cyber fraud, online harassment, identity theft, unauthorised surveillance, and misuse of personal information. Unlike conventional crimes, cyber offences often involve complex electronic records that require specialised forensic examination to establish their authenticity and evidentiary value. The effectiveness of cybercrime investigations therefore depends not only on technological expertise but also on compliance with legal procedures governing the collection, preservation, and admissibility of digital evidence. In India, difficulties relating to forensic reliability, inadequate investigative resources, jurisdictional limitations, and procedural delays may obstruct effective prosecution and access to justice. The Information Technology Act, 2000, the Bharatiya Nagarik Suraksha Sanhita, 2023, and the Bharatiya Sakshya Adhiniyam, 2023, provide an important legal framework for examining these concerns. Adopting a doctrinal and analytical research methodology, this study critically evaluates the relationship between digital forensic investigation, evidentiary challenges, and the protection of victim rights. It seeks to identify gaps in the existing legal and investigative framework and recommend reforms that promote reliable forensic practices, institutional accountability, procedural fairness, and effective access to justice for victims of cybercrime in India.

Keywords: Digital Victimisation, Forensic Justice, Cybercrime Investigation, Electronic Evidence, Victims' Rights.

INTRODUCTION

India's growing reliance on digital payments, online communications, cloud storage and networked services has transformed the opportunities for both lawful participation and criminal exploitation. Cybercrime is not a single offence. It encompasses conduct in which a computer or network is the target, the instrument or the environment of the wrongdoing. Victims may lose money through impersonation, experience persistent surveillance, have private images circulated, or discover that their personal information has been used to obtain access to accounts. Such harms may continue even after the original transaction or message has ended because copied information can be redistributed indefinitely.

A conventional criminal investigation often begins with a visible physical event. In contrast, a digital offence may involve a victim in one State, a suspect in another, a payment intermediary elsewhere and data held by a service provider outside India. Electronic traces may be abundant but unstable: logs rotate, accounts disappear, messages are edited and devices are replaced. Consequently, investigators must act promptly without assuming that every screenshot, IP address or device record establishes the identity of a perpetrator.

The central concern of this paper is that evidentiary success and victim justice are related but distinct. A technically competent investigation may still expose intimate information unnecessarily, delay financial recovery or fail to explain procedural developments to the complainant. Equally, a victim-friendly process cannot dispense with reliable proof and the accused's right to a fair trial. A coherent forensic justice 1framework must accommodate both.

This research examines the Indian legal and institutional response through the combined perspectives of cyber law, forensic science and victimology. It places particular emphasis on how electronic evidence is obtained and tested, how investigation practices affect complainants, and whether existing legal remedies respond adequately to the lived consequences of cybercrime.

RESEARCH PROBLEM, OBJECTIVES AND METHODOLOGY

Statement of the Problem

The research problem is whether India's existing cybercrime investigation and electronic evidence framework delivers reliable proof while also securing effective, timely and dignified

justice for victims. The problem is not merely the absence of laws: it concerns the distance between legal recognition, forensic implementation and accessible remedies.

Objectives

The objectives are to examine major forms and consequences of digital victimisation; explain the role and limits of digital forensic methods; analyse admissibility and authentication of electronic evidence under Indian law; identify investigative and institutional obstacles; evaluate constitutional and statutory safeguards for victims; and recommend practical reforms linking forensic reliability with victim-centred justice.

Research Questions

The study asks: How does digital evidence support or obstruct cybercrime prosecution? What procedural failures are most likely to weaken electronic proof? How do investigation and disclosure practices contribute to secondary victimisation? What changes would improve evidence preservation, accountability and victim access to remedies without undermining fairtrial guarantees?

Methodology and Scope

This is a doctrinal and analytical legal study based on statutes, judicial decisions, official institutional materials and established digital forensic principles. Illustrations are hypothetical and are not presented as empirical case findings. The discussion concentrates on India, with limited reference to cross-border evidentiary challenges. It does not claim to measure national prevalence or assess the actual performance of every police unit; those questions require fieldwork and reliable administrative datasets.

DIGITAL VICTIMISATION: NATURE AND CONSEQUENCES

Digital victimisation means harm caused through unlawful or abusive use of digital technologies. The category includes financial fraud, identity theft, cyberstalking, impersonation, unauthorised access, extortion, technology-facilitated sexual abuse and other forms of online harassment. Different offences generate different evidence and call for different protective responses. For example, tracing a fraudulent transfer requires rapid coordination with banks and payment systems; investigating persistent stalking may require an analysis of

account activity, communications and patterns over time.

Cybercrime is sometimes described as a crime without physical boundaries, but its effects are deeply personal. Victims of financial fraud may lose essential savings and struggle to obtain immediate assistance. Victims of online sexual exploitation may experience reputational harm, fear of renewed circulation and pressure to withdraw complaints. Children, older persons and individuals with limited digital literacy can face particular risks, although vulnerability cannot be reduced to age or gender alone. Offenders frequently use social engineering: false urgency, claims of authority, emotional manipulation and carefully crafted impersonation.

A victimological approach examines more than the criminal act. It considers how a person was targeted, what harm followed, whether institutional responses were accessible and whether the justice process generated further injury. Secondary victimisation occurs when insensitive questioning, repeated disclosure of private material, victim-blaming or avoidable delay compounds the original harm. In digital cases the repeated copying of intimate or confidential material can itself become a continuing injury.

Victimology must not be misused to assign responsibility to complainants for clicking a link, trusting a caller or sharing personal information. Such behaviours may help explain an offender's method, but criminal culpability remains with the person committing the offence. The proper research question is how systems can reduce opportunities for exploitation while protecting the agency and dignity of those affected.

Digital victimisation also creates evidentiary asymmetry. Platforms, payment providers and telecommunications entities may hold essential records, whereas the victim may possess only a notification, a screenshot or a partial conversation. This imbalance makes prompt lawful preservation and institutional cooperation crucial. Victims should not be expected to become forensic experts simply to secure a credible investigation.

ROLE AND LIMITATIONS OF DIGITAL FORENSICS

Identification, Acquisition and Preservation

Digital forensics applies documented scientific methods to identify, acquire, preserve, examine, and present electronic material relevant to an incident. Potential sources include smartphones, computers, cloud accounts, transaction logs, emails, messaging applications,

CCTV systems and network records. The first task is to identify which records may be relevant and who lawfully controls them. Investigators must distinguish information voluntarily supplied by a complainant from material that requires legal process to obtain. Forensic preservation aims to minimise changes to source data. Depending on the device and circumstances, specialists may produce forensic images, record acquisition methods and compute cryptographic hash values. A matching hash supports the proposition that two copies are identical at the time tested; it does not by itself prove that the original content was truthful, lawfully obtained or authored by the accused. Those questions require separate evidentiary analysis.

Chain of Custody and Interpretation

Chain of custody records who handled an item, when, why and under what conditions. In digital investigations, documentation should include device identifiers, collection dates, tools and versions used, storage arrangements, transfers and subsequent examination. An unexplained gap may undermine confidence in an exhibit, although its legal consequence depends on the facts and the applicable evidentiary rules. 3Interpretation is especially demanding. An IP address may identify a connection rather than an individual; a user account may have been compromised; metadata can be altered; a screenshot may omit surrounding context. Strong attribution ordinarily requires corroboration from independent sources, such as provider logs, device artefacts, transaction records and witness evidence. Expert reports should state limitations and alternative explanations rather than presenting technical probability as certainty.

Two Illustrative Scenarios

Consider a victim who transfers money after receiving a message impersonating a bank. A forensic inquiry may compare the message header or account identifier, device records, transaction reference numbers and the sequence of transfers. Rapid reporting may assist attempts to freeze or trace funds, but successful recovery is not guaranteed. The complainant should receive clear instructions for preserving messages and transaction details without being told to expose unrelated personal data.

In a second example, a victim receives threatening messages from multiple apparently anonymous accounts. Investigators may preserve URLs, timestamps, message content and

available platform records, then correlate these with lawfully acquired device or network information. The investigation should avoid equating account ownership with authorship and should prevent unnecessary republication of threatening or intimate material.

Emerging Challenges

End-to-end encryption, ephemeral messaging, cloud distribution and artificial intelligencegenerated media complicate acquisition and authentication. Deep fake detection methods can assist scrutiny but are not infallible. A lawful forensic response should combine technical examination, source verification, contextual corroboration and careful expert explanation. The objective is not unrestricted access to private systems it is proportionate collection of relevant material for a legitimate investigation.

INDIAN LEGAL FRAMEWORK AND ELECTRONIC EVIDENCE

Information Technology Act, 2000

The Information Technology Act provides central substantive provisions for specified computer-related misconduct. Section 43 addresses civil liability for certain unauthorised acts involving computer resources section 66 criminalise specified section 43 acts when committed dishonestly or fraudulently. Sections 66C and 66D address identity theft and cheating by personation through computer resources. Depending on the facts, provisions concerning privacy violations and unlawful electronic publication or transmission may also become relevant. The precise ingredients of each offence must be established rather than treating every harmful online act as automatically covered.

Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita may apply to conduct involving cheating, criminal intimidation, stalking, extortion, forgery or related wrongdoing, depending on statutory elements and the facts. Cybercrime can involve overlapping offences under general criminal law and specialised legislation. Investigators and prosecutors should identify the actual act, the required mental element and the evidence supporting each charge, avoiding mechanical multiplication of provisions.

Bharatiya Nagarik Suraksha Sanhita, 2023

The Bharatiya Nagarik Suraksha Sanhita regulates reporting, investigation, search, seizure and criminal procedure. Its procedural rules matter when electronic devices are secured, records are requested and evidence is documented. Section 173 addresses information relating to cognisable offences, including provision for electronic communication subject to statutory requirements. The practical quality of the initial complaint and prompt preservation requests may determine whether time-sensitive records remain available. Section 176(3), concerning forensic expert visits and videography for offences punishable with seven years or more, operates subject to the statutory framework and implementation arrangements; it should not be misdescribed as a universal mandate for every cybercrime.

Bharatiya Sakshya Adhiniyam, 2023

The Bharatiya Sakshya Adhiniyam recognises electronic or digital records within the law of evidence. Sections 61 to 63 are especially significant: they address electronic records and the conditions governing proof of computer output. Section 63 requires attention to statutory conditions and certification in relevant circumstances. A document being digital does not remove the need to establish authenticity, relevance and a trustworthy foundation. Section 39 also concerns opinions of experts, including relevant electronic evidence expertise. The Supreme Court's decisions in Anvar P.V. v. P.K. Basheer (2014) and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020), decided under the earlier Indian Evidence Act, are important for understanding the judicial development of certificate requirements for electronic records. Their application to disputes under the BSA must be assessed with reference to the current statutory text, not assumed without analysis. The core lesson is that electronic evidence requires legally adequate proof, not merely technological confidence.

Constitutional Protection

Article 21 protects life and personal liberty and informs requirements of fair procedure, dignity and privacy. In Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), the Supreme Court recognised privacy as a fundamental right. Cybercrime investigations therefore raise a dual obligation: to investigate offences effectively and to limit unjustified intrusion into personal information. Article 14 reinforces the demand for non-arbitrary and equal treatment. Victims and accused persons alike have legitimate constitutional interests; one set of rights should not

be used to erase the other.

Data Protection and Platform Responsibilities

The Digital Personal Data Protection Act, 2023 and its notified implementation arrangements are relevant to digital personal information, but the commencement and applicability of individual provisions must be checked for the relevant date. Data protection compliance is not a substitute for criminal investigation, nor does it automatically confer a general compensation remedy for every cybercrime victim. Intermediary duties and complaint processes may also arise under the Information Technology Act and applicable rules. These overlapping regimes require careful separation of criminal liability, platform responsibilities, data protection and civil remedies.

INVESTIGATIVE AND EVIDENTIARY CHALLENGES

A major investigative challenge is the speed at which electronic information changes. Service providers may retain different categories of records for different periods, and devices can be reset or discarded. Delayed 5preservation requests can eliminate otherwise useful leads. Standardised first-response protocols should help officers identify urgent evidence sources, document the complainant's account and issue legally appropriate requests promptly.

Anonymity and attribution create a second difficulty. Fake accounts, virtual private networks, stolen credentials and shared devices can obscure the relationship between a digital trace and a human actor. Technical data should therefore be assessed as part of a larger evidentiary narrative. An unsupported assertion that a particular account belongs to an accused person may compromise both the prosecution and the fairness of the trial.

Cross-border data access is a third challenge. A cyber incident may involve an Indian victim, foreign infrastructure and records held by a multinational provider. Obtaining data can require compliance with foreign law and formal cooperation mechanisms. The resulting delay can be especially harmful when victims seek urgent restraint of fraudulent transfers or removal of abusive content. International cooperation should be improved while respecting legality and due process.

Institutional capacity also matters. Investigating officers may have unequal access to forensic tools, training and specialist support. Laboratories may encounter backlogs, while courts

require expert explanations intelligible to non-specialists. The answer is not simply purchasing more software. Quality assurance, validation, continuing education and transparent reporting are necessary to prevent overstatement of forensic conclusions.

Finally, the evidence that victims can preserve is not always the evidence courts need. A screenshot may show a threat but lack metadata; a payment alert may show a debit but not the ultimate recipient; a copied video may not establish its source. Police should guide complainants on safe preservation and promptly pursue corroborating records. A victim should not be blamed for technical deficiencies that only institutional actors have the authority or resources to address.

VICTIM RIGHTS, SECONDARY VICTIMISATION AND REMEDIES

The experience of reporting cybercrime is part of the justice process. Victims need accessible complaint channels, acknowledgement of reports, information about next steps and clear explanations of what can realistically be recovered or proved. India's National Cyber Crime Reporting Portal provides a reporting route, and the 1930 helpline is associated with reporting financial cyber fraud. These mechanisms are valuable points of access, but reporting is not equivalent to registration of a criminal case, successful tracing or guaranteed restitution.

Privacy is central to victim protection. Cyberstalking and image-based abuse investigations may involve intimate photographs, personal messages, location histories and sensitive relationships. Unnecessary copying, casual sharing or repeated display of this material can reproduce the original violation. Investigators should use access controls, secure storage, restricted disclosure and purpose-based collection. Only relevant material should be obtained and circulated, consistently with applicable law and defence rights.

Secondary victimisation may occur when complainants are ridiculed for being deceived, questioned in a humiliating manner or required to repeatedly recount distressing events without a clear investigative purpose. In cases involving sexualised abuse, institutional insensitivity may discourage further cooperation. Training should therefore include trauma-informed interviewing, confidentiality and non-discriminatory treatment, not 6merely technical evidence acquisition.

Victims' rights also include meaningful access to remedies. Criminal prosecution addresses

public wrongdoing but may not restore money, remove harmful material or provide psychological assistance. Depending on the facts, statutory compensation, court-directed remedies, civil proceedings, platform grievance procedures and legal aid may be relevant. No single remedy is available in every cybercrime case. A careful legal assessment must distinguish entitlement, procedural availability and actual enforceability.

A victim-centred model does not mean abandoning safeguards for the accused. Unverified digital accusations can cause serious harm. The rights of complainants to dignity and effective investigation must coexist with the presumption of innocence, lawful searches, disclosure obligations and independent judicial assessment of evidence. Forensic justice is achieved when institutions take victims seriously while maintaining rigorous standards of proof.

CRITICAL FINDINGS AND RECOMMENDATIONS

Findings

First, Indian law contains multiple substantive and procedural mechanisms relevant to cybercrime, but their practical operation depends heavily on timely preservation and competent forensic interpretation. Second, the existence of electronic traces does not necessarily establish attribution; corroboration and transparent expert reporting remain essential. Third, victims can experience additional harm through delays, poor communication and unnecessary exposure of sensitive material. Fourth, criminal prosecution, content-related relief and financial restitution are different objectives and may require coordinated action by different institutions. Finally, the strongest model of justice integrates constitutional safeguards with technical reliability rather than treating privacy as an obstacle to investigation.

Recommendations

A uniform first-response protocol should guide police in documenting complaints, identifying volatile evidence, obtaining lawful preservation and providing complainants with basic evidence-safety instructions. Protocols should distinguish financial fraud, harassment, identity theft and intimate-image abuse because the urgency and types of evidence differ.

Forensic laboratories and police units should adopt auditable chain-of-custody records, validated tools and reporting formats that disclose uncertainty and alternative explanations. Continuing professional education should cover emerging technologies, particularly

AIgenerated media and cloud-based records. Expert testimony should explain what a method can establish and what it cannot.

Victim-facing procedures should provide confidential reporting, clear status communication, referral to legal assistance and counselling when appropriate, and safeguards against needless reproduction of private material. Dedicated assistance should be available for vulnerable complainants without assuming that all members of a demographic group have identical needs.

Coordination among police, banks, payment systems, telecommunications providers, platforms and forensic laboratories should be improved through lawful, time-sensitive procedures. Cross-border evidence requests require predictable cooperation mechanisms and careful attention to jurisdiction. Authorities should publish reliable, appropriately anonymised performance data on complaint handling, investigation delays and 7outcomes to permit evidence-based evaluation.

Legislative and institutional review should examine whether remedies are practically accessible, particularly where financial loss, continuing harassment or persistent circulation of intimate content survives the criminal proceeding. Reforms should be tested against proportionality, privacy, fair-trial guarantees and actual victim needs, rather than measured solely by arrest or conviction counts.

ROLE OF JUDICIARY IN ENSURING FORENSIC JUSTICE AND PROTECTION OF CYBERCRIME VICTIMS

The judiciary plays an important role in ensuring that technological developments in criminal investigation remain consistent with constitutional principles and the protection of individual rights. In cybercrime cases, courts are required to examine the authenticity, admissibility, and reliability of electronic evidence while safeguarding the rights of victims and accused persons. Digital records such as emails, electronic communications, online transaction details, and social media content have become important sources of evidence in criminal proceedings. However, the possibility of manipulation, alteration, or unauthorised access makes judicial scrutiny essential for ensuring fair and effective administration of justice.

The Supreme Court of India has delivered significant judgments concerning electronic evidence and constitutional protection in the digital environment. In Anvar P.V. v. P.K.

Basheer (2014), the Supreme Court emphasised the statutory requirements governing the admissibility of electronic records under the former Indian Evidence Act, 1872. Subsequently, in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020), the Court clarified the requirements relating to electronic evidence certificates under Section 65B of the former Act. These decisions remain important for understanding the development of electronic evidence law, although the Bharatiya Sakshya Adhiniyam, 2023, now governs the corresponding evidentiary requirements under its applicable provisions. lawful procedures without unnecessarily interfering with the privacy and dignity of individuals.

Judicial intervention is essential not only for determining the admissibility of electronic evidence but also for maintaining a balance between effective criminal investigation and constitutional safeguards. Courts must carefully evaluate forensic findings, consider the possibility of technological errors, and ensure that victims receive meaningful opportunities to seek legal remedies.

NEED FOR A VICTIM-CENTRED DIGITAL FORENSIC JUSTICE SYSTEM IN INDIA

The development of an effective cybercrime justice system requires greater emphasis on the experiences, needs, and legal rights of victims. Although digital forensic technologies assist investigating authorities in identifying offenders and reconstructing criminal incidents, the successful administration of justice cannot be measured solely through criminal convictions.

It must also consider whether victims receive timely assistance, protection of personal information, fair treatment, and access to appropriate legal remedies.

One significant concern is the difficulty experienced by victims in understanding technical investigation procedures. Individuals affected by cyber fraud, identity theft, online harassment, or unauthorised disclosure of personal information may lack the technical knowledge required to preserve electronic evidence or communicate effectively with investigating agencies. Providing clear guidance regarding complaint registration, evidence preservation, and available legal remedies is therefore essential.

Another important concern is secondary victimisation. Victims may experience additional psychological distress when they are repeatedly required to disclose sensitive information, face

insensitive questioning, or encounter unnecessary delays in criminal proceedings. In cases involving intimate images, private communications, or online harassment, inadequate confidentiality measures may further expose victims to humiliation and reputational damage. A victim centred forensic approach should therefore ensure that electronic evidence is collected and examined with appropriate safeguards for privacy, dignity, and personal security.

Effective forensic justice also requires institutional coordination among cybercrime police units, forensic laboratories, financial institutions, digital service providers, and legal assistance authorities. Timely preservation of electronic records, specialised training for investigators, and transparent complaint-handling procedures can improve investigative efficiency. Furthermore, victims should receive appropriate information regarding the progress of investigations and the remedies available under law.

CONCLUSION

Digital victimisation exposes the limits of a criminal justice approach concerned only with identifying a suspect and securing a conviction. Electronic evidence can reconstruct transactions, communications and patterns of abuse, but its value depends on lawful acquisition, preservation, reliable interpretation and transparent presentation. A hash value, an account identifier or a screenshot cannot replace contextual corroboration and judicial scrutiny. Equally, a technically successful investigation may fall short of justice when victims face prolonged uncertainty, financial insecurity, stigma or repeated disclosure of intimate information. India's statutory framework under the Information Technology Act, the BNS, the BNSS and the BSA provides important tools for addressing digital wrongdoing. Constitutional principles of dignity, privacy, equality and fair procedure supply a necessary normative foundation. The remaining challenge is institutional: to translate those principles into accessible reporting, rapid preservation, well-supported forensic practice, careful handling of sensitive information and realistic routes to redress. The paper therefore advocates a rightsbased forensic justice model. Such a model does not privilege victims at the expense of accused persons or technology at the expense of legality. It recognises that reliable evidence and humane treatment are mutually reinforcing conditions of public confidence. Strengthening both is essential if cybercrime investigation in India is to deliver meaningful justice in an increasingly networked society.

REFERENCES:

Statutes

1. Information Technology Act, 2000, No. 21 of 2000.

2. Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023.

3. Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023.

4. Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023.

5. Digital Personal Data Protection Act, 2023, No. 22 of 2023.

6. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended.

7. Digital Personal Data Protection Rules, 2025.

Books and International Materials

8. Eoghan Casey (ed.), Handbook of Digital Forensics and Investigation (Academic Press, 2009).

9. Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed., Academic Press, 2011).

10. United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (United Nations, 2013).

11. United Nations General Assembly, Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power, G.A. Res. 40/34 (29 November 1985).

Government Reports and Online Sources

12. National Crime Records Bureau, Crime in India 2023, Ministry of Home Affairs, Government of India.

13. Ministry of Home Affairs, Government of India, Annual Report 2024–2025, available at https://www.mha.gov.in.

14. Ministry of Home Affairs, Government of India, Indian Cyber Crime Coordination Centre (I4C), available at https://www.mha.gov.in.

15. Ministry of Electronics and Information Technology, Government of India, Digital Personal Data Protection Rules, 2025, available at https://www.meity.gov.in.

16. National Cyber Crime Reporting Portal, Government of India, https://cybercrime.gov.in.

17. Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology, Government of India, https://www.cert-in.org.in.

18. India Code, Legislative Department and Ministry of Law and Justice, Government of India, https://www.indiacode.nic.in.