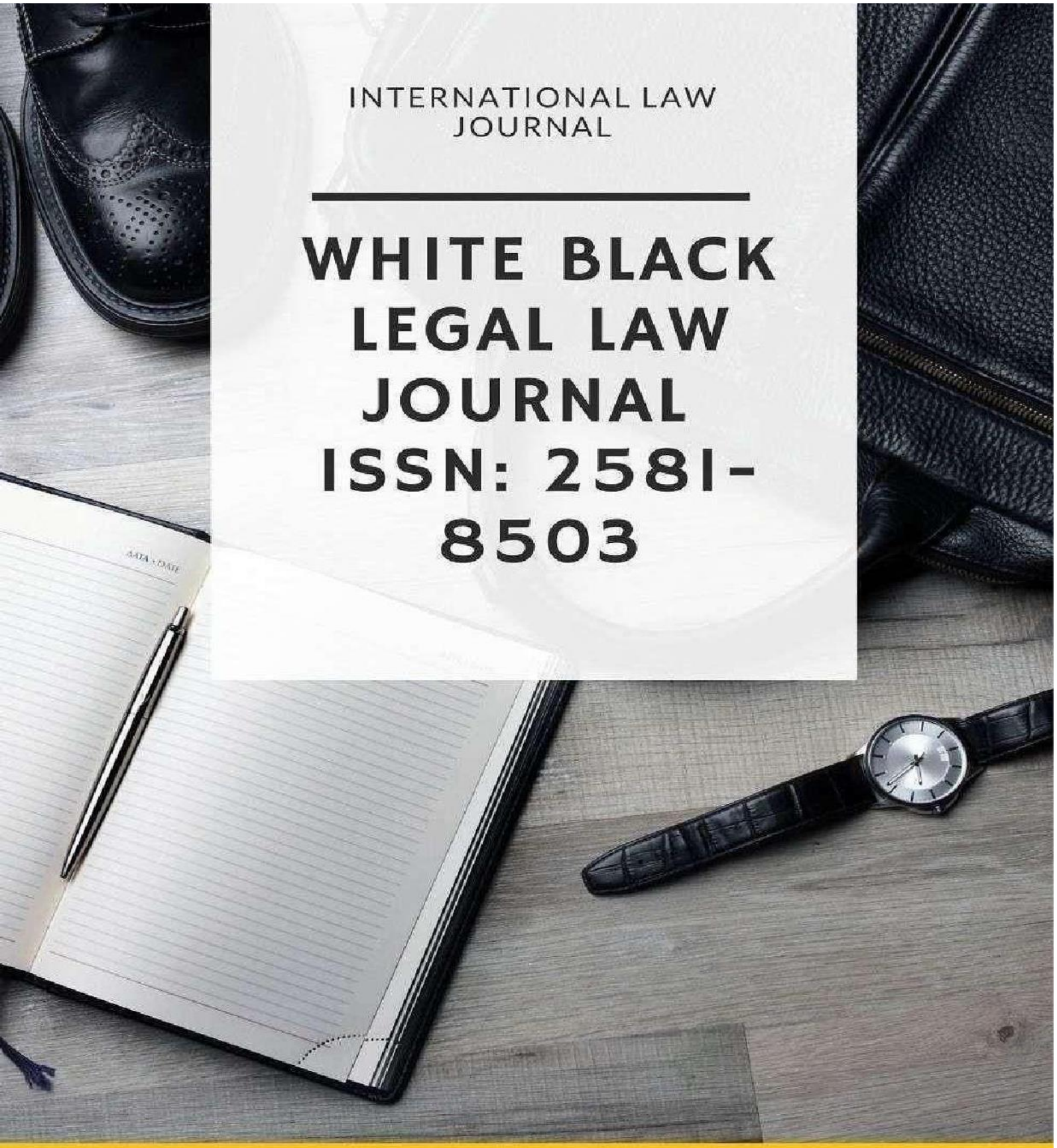


INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

WHITE BLACK LEGAL

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

CYBERCRIME VICTIMISATION IN INDIA: A FORENSIC VICTIMOLOGY STUDY OF DIGITAL EVIDENCE, INVESTIGATIVE CHALLENGES, AND VICTIM PROTECTION

AUTHORED BY - THIRUSHYA R
LLM 1st Year at Tamilnadu
Dr.Ambedkar Law University

ABSTRACT:

The rapid growth of digital technology has increased the occurrence of cybercrimes, creating significant challenges for victim identification, criminal investigation, and victim protection in India. Cybercrime victimisation includes online financial fraud, identity theft, cyberstalking, cyberbullying, phishing, and other forms of digital exploitation. Digital forensics plays a crucial role in collecting, preserving, and analysing electronic evidence to identify offenders and support criminal proceedings. However, investigators and victims face several challenges, including anonymous online identities, deletion of digital evidence, cross-border jurisdictional issues, delayed investigations, and difficulties in reporting cybercrimes. Victims may also experience financial losses, psychological distress, social stigma, privacy violations, and secondary victimisation during the investigation process. The Indian legal framework, including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, and the Bharatiya Sakshya Adhiniyam, 2023, provides relevant provisions for addressing cybercrime, investigation, and electronic evidence. This study adopts a doctrinal and analytical approach to examine the relationship between cybercrime victimisation, digital forensic investigation, and victim protection. It aims to identify existing legal and investigative challenges and suggest measures to strengthen forensic capabilities, improve victim support, safeguard privacy, and promote effective access to justice in India.

Keywords: Cybercrime, Victimology, Digital Forensics, Electronic Evidence, Victim Protection.

1. INTRODUCTION:

With the rapid growth in Information and Communication Technology, it has become easier to communicate, transact and utilise various services. This, however, poses a risk for cyber crimes to occur such as online financial fraud, identity theft, phishing, cyberstalking, cyberbullying and cyber intrusion. These are all illegal actions committed via the use of computers, technology, networks and the internet. With our dependence on technology increasing, risks have increased for individuals to become victims of technology-related crime. Forensic Criminology uses scientific techniques to understand criminal behaviour. Victimology looks at the victim and their experience, vulnerability, impact and how they are treated by the criminal justice system. Combining these disciplines will help provide understanding as to how cybercrimes are committed, the impact on victims and how investigations can be carried out.

Digital Forensics is an important aspect when investigating cybercrime. This identifies, gathers, preserves, examines and analyses digital evidence. This could include mobile phone records, emails, transaction history, digital communication and network logs. This can help identify what has occurred during the incident, and create a link between the suspect and alleged crime. However, this evidence must be properly gathered, preserved and legal requirements must be met. Despite advancements in technology and legal measures there are still challenges faced when investigating cybercrime in India. These include anonymity, international crime, slow forensic processes, lack of reporting and concerns about victim privacy and dignity. The problem of this research is whether digital forensics can effectively investigate cybercrime offenders whilst protecting victims.

This study will look into the relationship between cybercrime victimisation, digital forensic techniques and victim protection in India. A doctrinal and analytical approach will be used to assess relevant legislation, challenges when investigating and current victim support. This research will look at certain types of cybercrime, using digital evidence and legal protections for victims. Ultimately this will provide suggestions on how to improve forensic investigations and create a more effective and victim focused criminal justice system.

2. CONCEPT AND NATURE OF CYBERCRIME VICTIMATION:

Cybercrime victimation refers to individuals or organisations becoming victims of harm, loss or exploitation due to criminal activity conducted using digital devices or computer networks and the internet. It is an important aspect of victimology to understand how individuals can

become victims of cybercrime. Unlike conventional crimes, cybercrimes may be performed from a distance. Offenders are able to target individuals from any geographical location whilst keeping their identity hidden. There are several types of crimes that could be committed online. Financial Fraud refers to the crime of deceiving individuals which results in them sending money online. Phishing is when an individual is sent fraudulent emails or messages or visits a fake website to gain private information including passwords and banking details. Identity Theft involves using someone's personal information to impersonate them. Cyberstalking is when an individual is continuously monitored, threatened or harassed online. Cyberbullying includes harassment, humiliation and intimidation. Sexual Exploitation includes the sharing of explicit images without consent and sexual coercion online.

There are many reasons why individuals may become victims of cybercrime. If individuals do not have knowledge of digital technology they may be unable to identify suspicious links, fake profiles or deceptive messaging. Social Engineering can cause individuals to feel emotions such as fear, trust, urgency and greed to encourage them to give away information or send money. In addition, if individuals share personal information carelessly on social media and do not have secure digital habits they are at risk of being a victim of identity theft. Victims of cybercrime may suffer from anxiety, fear, embarrassment, depression and lose confidence using online services. Socially they may suffer from damage to their reputation, relationship issues and feel stigmatised. Financially they may fall into debt, lose their savings and struggle to recover their stolen money. Individuals and groups may be at greater risk. Children and young people may be the victims of bullying and exploitation online. Older people and those who lack knowledge of digital technology may not be able to spot fraudulent activity. Women may suffer specific types of harassment online and gender based abuse however anyone can be affected by cybercrime. Understanding the nature of cybercrime victimisation is key to develop effective investigation methods. As well as increase digital awareness, protect individuals' rights and provide justice for victims within the Indian criminal justice system.

3. ROLE OF DIGITAL FORENSICS IN CYBERCRIME INVESTIGATION:

3.1 Meaning and Importance of Digital Forensics

Digital forensics is the scientific process of identifying, collecting, preserving, examining, and analysing digital data to obtain evidence relevant to criminal investigations. In cybercrime cases, it helps investigators understand how an offence occurred, identify possible offenders,

establish timelines, and connect digital activities with suspected criminal conduct. From a forensic criminology and victimology perspective, digital forensics is important because it can support the investigation of offences while helping victims establish what happened and seek justice.

3.2 Collection, Preservation, and Analysis of Digital Evidence

Digital forensic investigation generally involves four major stages:

1. **Collection:** Investigators obtain relevant electronic evidence from mobile phones, computers, emails, digital payment records, and other sources through lawful procedures.
2. **Preservation:** Evidence is protected against alteration, deletion, or contamination. Investigators may create forensic copies and use cryptographic hash values to verify that the data remains unchanged.
3. **Examination:** Experts search for relevant files, communications, timestamps, transaction details, and other information connected with the alleged offence.
4. **Analysis and reporting:** The findings are interpreted, correlated with other evidence, and documented in a forensic report for investigation or court proceedings.

3.3 Sources of Digital Evidence

Digital evidence can be obtained from various electronic sources, depending on the nature of the cybercrime. Mobile phones may contain text messages, call records, application data, photographs, and other relevant information. Computers and laptops may provide browsing history, downloaded files, stored documents, and records of user activity. Emails can help investigators examine phishing attempts, fraudulent communications, and suspicious attachments. Digital payment and banking records may assist in tracing fraudulent transactions and identifying beneficiary accounts.

Similarly, network logs and IP address records may provide information about internet connections, access times, and online activities associated with an incident.

For example, in an online banking fraud case, investigators may correlate the victim's messages, transaction records, and relevant account information to reconstruct the movement of money. In a cyberstalking case, preserved messages, timestamps, account details, and lawfully obtained platform records may help establish a pattern of harassment.

However, no single source of digital evidence necessarily proves the identity of an offender. Investigators must correlate multiple sources, verify their authenticity, and consider

alternative explanations before drawing conclusions.

3.4 Integrity and Chain of Custody

The integrity of digital evidence is essential to ensure that it remains reliable and has not been improperly altered. The chain of custody is the documented record of how evidence was collected, transferred, stored, examined, and handled by authorised persons. Investigators should record relevant dates, times, access details, and transfer procedures. Hash values can help verify the integrity of forensic copies.

Failure to maintain proper documentation or preserve evidence may raise questions about its authenticity and reliability. Electronic evidence must also satisfy the applicable requirements of the Bharatiya Sakshya Adhiniyam, 2023.

3.5 Identification of Offenders and Reconstruction of Cyber Incidents

Digital forensic techniques can help reconstruct the sequence of events by correlating timestamps, communications, login records, device information, and financial transactions. However, an IP address or account record alone may not conclusively identify an offender because accounts and devices can be shared, compromised, or accessed by others.

Example 1: Online financial fraud

Suppose a victim loses ₹40,000 after receiving a fraudulent banking message. Investigators may examine the message, relevant device records, transaction details, and beneficiary account information. By correlating these records with other evidence, they may trace the flow of funds and identify potential suspects.

Example 2: Cyberstalking

Suppose a victim receives repeated threatening messages from a fake social media account. Investigators may examine preserved messages, relevant URLs, timestamps, account information, and lawfully obtained platform records. These findings may help establish a pattern of harassment and identify the person potentially responsible.

3.6 Digital Forensics and Victim Protection

Digital forensics must be conducted in a manner that respects victims' privacy and dignity. Sensitive photographs, personal communications, and financial information should be accessed and disclosed only as legally authorised and necessary. Investigators should also avoid unnecessary exposure of victims' identities and preserve relevant evidence promptly.

Thus, digital forensics is an essential component of cybercrime investigation. When combined

with reliable procedures, legal safeguards, and a victim-centered approach, it can strengthen investigations, support accountability, and improve victims' access to justice in India.

4. CHALLENGES IN IDENTIFYING VICTIMS AND OFFENDERS:

The identification of cybercrime victims and offenders presents several challenges for investigators in India. Unlike traditional crimes, cybercrimes can be committed remotely, and offenders may use sophisticated technologies to conceal their identities. These difficulties can delay investigations, affect the recovery of evidence, and prevent victims from obtaining timely justice.

- Anonymous Accounts and Fake Identities

Cybercriminals frequently use fake social media profiles, temporary email addresses, anonymous accounts, and stolen identities to hide their actual identity. They may also use another person's device or account to commit offences. For example, a cyberstalker may create a fake account to threaten a victim, making it difficult to identify the person responsible without further investigation.

- Deletion, Alteration, and Encryption of Digital Evidence

Electronic evidence can be deleted, modified, or concealed using encryption and other technical methods. Messages may disappear, accounts may be deactivated, and important records may become unavailable. Investigators must preserve relevant evidence promptly and use appropriate forensic techniques to recover or examine available data. However, recovery is not always possible, particularly when data has been securely erased or is inaccessible.

- Cross-Border Jurisdictional Difficulties

Cybercrimes may involve offenders, victims, digital platforms, and servers located in different countries. This creates difficulties concerning jurisdiction, applicable laws, and access to electronic records. For example, an offender operating from another country may target an Indian victim through an overseas social media platform. Obtaining evidence may require international cooperation and compliance with the relevant legal procedures, which can delay the investigation.

- Delays in Obtaining Electronic Records and Forensic Reports

Investigations may be delayed when authorities must obtain records from banks, telecommunications companies, or digital service providers. Digital forensic laboratories may also face heavy workloads, resulting in delays in analysing devices and preparing reports. Such delays can affect the timely identification of suspects and may reduce opportunities to trace stolen funds.

- Limited Technical Resources and Expertise

Some investigating agencies may face shortages of trained digital forensic experts, specialised equipment, and adequate infrastructure. The increasing complexity of cybercrime requires continuous training and updated investigative methods. A lack of technical expertise may affect the collection, interpretation, and preservation of digital evidence.

- Underreporting of Cybercrime

Many victims hesitate to report cybercrime because of embarrassment, fear of social stigma, concerns about privacy, or lack of awareness about complaint mechanisms. Victims of cyberstalking and online sexual exploitation may fear blame or further harassment. Underreporting makes it difficult to understand the actual extent of cybercrime and may allow offenders to continue their activities.

- Establishing a Reliable Link Between Evidence and the Offender

The presence of a digital record does not automatically establish who committed the offence. An IP address, phone number, or social media account may be shared, impersonated, or compromised. Investigators must corroborate digital evidence with other reliable information before attributing criminal responsibility to a particular person.

In conclusion, these challenges demonstrate the need for improved forensic infrastructure, trained investigators, timely evidence preservation, stronger inter-agency cooperation, and victim-friendly reporting mechanisms. Addressing these difficulties is essential to ensure reliable cybercrime investigations and effective protection of victims in India.

5. LEGAL FRAMEWORK FOR CYBERCRIME AND VICTIM PROTECTION IN INDIA:

India's legal framework for addressing cybercrime includes legislation defining offences, regulating criminal investigations, recognising electronic evidence, and providing remedies to affected persons. The effectiveness of this framework depends on proper enforcement, reliable digital forensic procedures, and protection of victims' rights.

5.1 Information Technology Act, 2000

The Information Technology Act, 2000 is a principal law addressing various computer-related offences and electronic transactions. Section 43 provides for compensation in specified cases of unauthorised access and damage to computer systems, while Section 66 addresses certain acts under Section 43 when committed dishonestly or fraudulently. Section 66C deals with identity theft, and Section 66D criminalizes cheating by personation using computer resources. Section 67 addresses publishing or transmitting obscene material in electronic form, subject to its statutory requirements. These provisions may apply depending on the facts of the case.

5.2 Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita (BNS), 2023 provides general criminal law provisions that may apply to cybercrime-related conduct. Depending on the circumstances, offences involving cheating, criminal intimidation, stalking, forgery, and related conduct may be prosecuted under applicable provisions. For example, a person who uses online communications to threaten another individual or employs deception to obtain money may attract relevant provisions of the BNS alongside applicable provisions of the Information Technology Act.

5.3 Bharatiya Sakshya Adhiniyam, 2023

The Bharatiya Sakshya Adhiniyam (BSA), 2023 governs the admissibility and proof of evidence in judicial proceedings. Section 61 recognises electronic and digital records as evidence, subject to the Act's requirements, while Section 63 lays down conditions for the admissibility of specified electronic records. These provisions are particularly relevant to cybercrime investigations involving emails, screenshots, digital payment records, and computer data. Proper preservation and authentication of such evidence are essential to establish its reliability in court.

5.4 Bharatiya Nagarik Suraksha Sanhita, 2023

The Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 regulates criminal investigation and procedure. Its provisions concerning reporting of offences, investigation, search, seizure, and procedural safeguards are relevant to cybercrime cases. For example, investigators may need to obtain digital devices and electronic records through lawful procedures while maintaining appropriate documentation and protecting the integrity of evidence. The BNSS operates alongside the substantive criminal laws and applicable rules governing electronic evidence.

5.5 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection (DPDP) Act, 2023 establishes a framework for protecting digital personal data and regulating its processing. It is relevant to cybercrime victimology because misuse or exposure of personal information may increase victims' vulnerability to identity theft, impersonation, and targeted fraud. However, its provisions have a phased commencement schedule notified in November 2025; therefore, the applicability of particular obligations must be assessed according to the provisions in force at the relevant time.

5.6 Cybercrime Reporting Mechanisms

The Government of India provides the National Cyber Crime Reporting Portal [www.cybercrime.gov.in] for reporting cybercrime complaints. Victims of financial cyber fraud can also call 1930 for immediate reporting. Prompt reporting and preservation of transaction receipts, messages, bank statements, screenshots, and other relevant records may assist authorities in investigating the incident and attempting to prevent further financial loss.

5.7 Victims' Remedies and Privacy Protection

Depending on the circumstances, victims may seek criminal action, compensation where legally available, and other appropriate legal remedies. Section 43 of the IT Act provides for compensation in specified cases of unauthorised access or damage, while other provisions may apply to particular offences. Victims should also be protected against unnecessary disclosure of sensitive information during investigation and judicial proceedings. A victim-centered approach requires timely complaint handling, careful treatment of electronic evidence, access to legal assistance, and respect for privacy and dignity.

In conclusion, India's legal framework provides multiple mechanisms to address cybercrime and protect victims. However, effective implementation, timely forensic investigation,

coordination between authorities, and awareness of available remedies remain essential to ensuring access to justice.

6. VICTIM PROTECTION AND SECONDARY VICTIMISATION:

Victim protection is an essential component of cybercrime investigation, as victims may experience not only the direct consequences of an offence but also additional harm during the investigation and judicial process. Secondary victimisation refers to the further psychological, social, or emotional harm experienced by victims due to the insensitive treatment of authorities, institutions, society, or other individuals after the original crime. In cybercrime cases, this may occur when victims are blamed for their online activities, repeatedly questioned in an insensitive manner, or exposed to public humiliation.

Privacy violations are a major concern in cybercrime victimisation. Personal photographs, private messages, financial information, and other sensitive data may be circulated without consent. In cases involving cyberstalking or online sexual exploitation, the further sharing of such information can increase the victim's distress and damage their reputation. Therefore, protecting victims' identities and confidential information is important throughout the investigation and judicial proceedings.

Social stigma and victim-blaming may discourage victims from reporting cybercrimes. For example, a person who experiences online harassment may fear being blamed for sharing personal information or using social media. Similarly, victims of financial fraud may feel embarrassed about being deceived and hesitate to approach the police. These attitudes can increase emotional distress, contribute to underreporting, and make it difficult for victims to obtain timely assistance. Victims may also encounter practical difficulties while reporting offences, providing electronic evidence, communicating with investigators, and following up on complaints. Delays in investigations and uncertainty about legal remedies can further increase their anxiety. To address these concerns, authorities should adopt sensitive and confidential procedures, explain the investigation process clearly, and avoid unnecessary disclosure or repeated handling of sensitive material.

Important measures for victim protection include:

- **Confidentiality:** Safeguarding victims' personal details and sensitive digital evidence against unnecessary disclosure.
- **Timely assistance:** Providing accessible reporting mechanisms, legal guidance, counselling where needed, and appropriate support during investigations.

A victim-centered forensic investigation should balance the collection of reliable digital evidence with respect for victims' dignity, privacy, and emotional well-being. Investigators must handle sensitive material carefully, preserve evidence lawfully, and avoid practices that cause further harm. Effective coordination among law enforcement agencies, forensic experts, legal services, and support organisations can improve victims' access to justice.

In conclusion, preventing secondary victimisation is as important as investigating the original cybercrime. A sensitive, confidential, and victim-centered approach can encourage reporting, strengthen public confidence, and promote a fairer criminal justice system in India.

7. FINDINGS AND SUGGESTIONS:

The study identifies several challenges in addressing cybercrime victimisation in India. Although legal provisions and digital forensic techniques support cybercrime investigation, difficulties such as anonymous identities, deletion of electronic evidence, delays in forensic analysis, and limited technical expertise may obstruct the identification of offenders. Furthermore, fear, social stigma, privacy concerns, and lack of awareness may discourage victims from reporting offences. These issues demonstrate the need for an effective investigative system that combines technological development with victim-centered protection.

The following suggestions may help address these challenges:

- **Strengthening digital forensic infrastructure:** Establish and improve forensic facilities, provide modern investigative tools, and offer regular training to police officers and forensic experts.
- **Improving coordination:** Strengthen cooperation between police authorities, forensic laboratories, banks, telecommunications companies, and digital service providers to facilitate timely access to relevant records through lawful procedures.
- **Timely evidence preservation:** Develop effective procedures for preserving electronic evidence, documenting its chain of custody, and preventing unnecessary loss or alteration of relevant data.
- **Increasing public awareness:** Conduct awareness programmes on phishing, online financial fraud, identity theft, cyberstalking, and safe digital practices. Publicize available reporting mechanisms, including the National Cyber Crime Reporting Portal and helpline 1930 for financial cyber fraud.
- **Protecting victims' confidentiality:** Adopt sensitive reporting and investigation

practices to safeguard victims' identities, personal information, and dignity. Access to legal assistance and counselling should be facilitated where necessary.

- **Strengthening victim support:** Improve access to appropriate legal remedies, complaint follow-up, and compensation where legally available. Support mechanisms should be accessible, timely, and responsive to victims' needs.

In conclusion, effective cybercrime prevention and investigation require coordinated legal, technological, and social measures. Strengthening digital forensic capabilities while prioritizing victims' privacy and welfare can improve investigative outcomes, encourage reporting, and promote access to justice in India.

8. CONCLUSION:

Cybercrime victimisation has become a significant concern in India due to the increasing use of digital technologies and online platforms. This study highlights the relationship between forensic criminology, digital evidence, and victimology in addressing cybercrime. Digital forensics plays a crucial role in collecting, preserving, and analysing electronic evidence to reconstruct criminal incidents and assist in identifying offenders. However, challenges such as anonymous identities, deleted evidence, cross-border jurisdictional issues, and delays in forensic investigations may obstruct the delivery of justice. The study also emphasises that the consequences of cybercrime extend beyond financial loss to include psychological distress, social stigma, privacy violations, and secondary victimisation. Therefore, effective investigation must not focus exclusively on identifying offenders but also ensure the protection of victims' rights, dignity, and confidentiality. Although India's legal framework provides mechanisms to address cybercrime and electronic evidence, effective implementation and accessible victim-support services remain essential. Strengthening forensic infrastructure, improving investigative expertise, ensuring timely evidence preservation, and increasing public awareness can contribute to more effective cybercrime investigations. Furthermore, sensitive handling of victims, access to legal assistance, and appropriate remedies can improve confidence in the criminal justice system. Ultimately, India requires a comprehensive, coordinated, and victim centered approach that combines reliable digital forensic practices with meaningful victim protection to promote accountability, safeguard individual rights, and ensure access to justice in the digital era.

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

1. Casey, Eoghan (ed.), Handbook of Digital Forensics and Investigation (Academic Press, 2009).
2. United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (United Nations, 2013).
3. Council of Europe, Convention on Cybercrime, ETS No. 185 (2001).

Government Reports and Online Sources

1. National Crime Records Bureau, Crime in India 2024, Government of India.
2. Ministry of Home Affairs, Government of India, Cyber Crime Cases and Forensic Capabilities, Press Information Bureau (3 December 2025).
3. Ministry of Home Affairs, Government of India, Indian Cyber Crime Coordination Centre (I4C).
4. Ministry of Electronics and Information Technology, Government of India, Digital Personal Data Protection Rules, 2025.
5. National Cyber Crime Reporting Portal, Government of India, https://cybercrime.gov.in.
6. India Code, Legislative Department and Ministry of Law and Justice, Government of India, https://www.indiacode.nic.in.

WHITE BLACK LEGAL