INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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

CLICK, CRIME, REPEAT: DECODING CYBERCRIME LAWS IN DIGITAL INDIA

AUTHORED BY - HARSHITHA .P. URS

Abstract

The cybercrime is one of the most challenging issues in the present digital world. The reason behind huge rise of cyber offences can be seen from the rapid usage of internet, digital transactions ranging from identity theft to large scale financial frauds. This article judiciously analyzes the legal framework which governs cybercrime investigation in India. It mainly focuses on statutory developments such as Information Technology Act 2000, the Digital personal Data Protection Act, 2023, and the recent enacted criminal laws of 2023. Additionally it also examines investigation procedure, institutional mechanisms, and evidentiary standards. Further this study also underlines judicial pronouncements and emerging challenges like judicial complexities and growth of technological advancements. This article concludes by advising reforms to strengthen cybercrime investigation and ensure effective enforcement in an increasingly digitized society.

Key words:

Introduction:

The rapid advancement of technology has brought unpredictable changes in the society, by this it has changed communication, transact, and interaction of every indivual in the modern society. Conversely, this digital expansion has also given way to cybercrimes. In India due to depending upon internet based services and huge digital platforms has intensified, Hence there is need for effective framework and governance to combat such offences[1]. Effective cybercrime investigation and awareness among indivual can bring control over cybercrime. Further, in the present society, cybercrime investigation has become most challenging with respect to technological complexity, nature and anonymity. This article examines the legal mechanisms governing cybercrime investigation in India, highlighting recent developments, challenges, and the evolving role of law enforcement agencies.

[1] Nat'l Crime Recs. Bureau, *Crime in India 2024* (Ministry of Home Affairs, Govt. of India).

ISSN: 2582-6433

What is Cyber crime?

Cybercrime is one of the most complicated and complex oriented problem in the cyber world. The Indian Law has not given exact meaning and definition for the term 'cybercrime'. In fact, even after amendment by Information Technology (amendment) Act 2008, the Indian Penal Code has not even used the term 'cybercrime'. Cybercrime refers to unlawful acts committed using computers, digital devices, or networks, including hacking, phishing, identity theft, cyber stalking, and online fraud.[2] In India, the increasing penetration of the internet and digital payment systems has significantly contributed to the rise in cybercrime incidents, [3]thereby necessitating a robust legal and investigative framework.

Cyber crimes can be plainly defined as "Crimes directed at a computer or computer system" But the complex nature of cyber crimes cannot be sufficiently expressed in such simple and limited term.

Cybercrime Includes:

1. E mail bombing
2. Hacking
3. Spreading computer virus
4. Identity theft
5. Phishing
6. Internet fraud
7. Cyber warfare
8. Malicious Software
9. SMS spoofing
10. Domain hijacking
11. Voice Phishing
12. Cyber trafficking

Legal Framework:

In present modern society, cybercrime investigation in India is governed through a combination of substantive, procedural, evidentiary and regulatory laws which provides comprehensive and technology oriented legal regime.

[2] Talat Fatima, *Cybercrime* 89 (E. Book Co. 2011).
[3] Id.

ISSN: 2582-6433

1) Information Technology Act, 2000

IT Act, 2000 is the cornerstone legislation India which mainly governs cybercrime. [4]

- Section 65 – Tampering with computer source documents
- Section 66 – Computer-related offences (hacking, data theft, damage)
- Section 66B – Receiving stolen computer resource
- Section 66C – Identity theft
- Section 66D – Cheating by personation (online fraud, phishing)
- Section 66E – Violation of privacy
- Section 66F – Cyber terrorism
- Section 67 – Publishing or transmitting obscene content
- Section 67A – Sexually explicit content
- Section 67B – Child pornography
- Section 67C – Failure to preserve and retain information
- Section 72 – Breach of confidentiality and privacy
- Section 72A – Disclosure of information in breach of lawful contract
- **Section 43** – Damage to computer systems/data (civil offence, often linked with Section 66)

2) Bharatiya Nyaya Sanhita, 2023 (BNS)

BNS does not separately define "cybercrime", but following sections can be applied when offences which are committed through digital/ online means. [5]And under BNS it applies to traditional offences in digital form.

- Section 318 – Cheating
- Section 319 – Cheating by personation
- Section 336 – Forgery
- Section 337 – Forgery of valuable security, will, etc.
- Section 338 – Forgery for purpose of cheating
- Section 340 – Using forged document or electronic record
- **Section 294** – Obscene acts and songs
- **Section 356** – Defamation
- **Section 351** – Criminal intimidation

[4] Information Technology Act, 2000 (India).
[5] Bharatiya Nyaya Sanhita, 2023 (India).

ISSN: 2582-6433

- Section 303 – Theft
- Section 316 – Criminal breach of trust
- Section 111 – Organized crime
- Section 113 – Terrorist acts

3) Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)

Provisions under BNSS with respect to cybercrime is procedural law, such as investigation, search, evidence handling. [6]

- Section 173 – Information in cognizable cases
- Section 176 – Police officer's power to investigate
- Section 179 – Examination of witnesses
- Section 185 – Search by police officer
- Section 186 – Search of place suspected to contain stolen property
- Section 193 – Recording of statements
- **Section 197** – Jurisdiction of courts
- **Section 349** – Use of forensic science

4) **Bharatiya Sakshya Adhiniyam, 2023 (BSA)**

The provisions under BSA provide Electronic Evidence Recognition and Admissibility of digital evidence with respect to cybercrime.[7]

- **Section 61** – Proof of electronic records
- **Section 63** – Admissibility of electronic records
- Section 57 – Primary evidence
- Section 58 – Secondary evidence
- Section 85 – Presumption as to electronic agreements
- Section 86 – Presumption as to electronic records and signatures
- Section 90 – Presumption as to digital signatures

Other various laws relating to cybercrime in India:

- Digital Personal Data Protection Act, 2023
- Digital Personal Data Protection Rules, 2025

[6] Bharatiya Nagarik Suraksha Sanhita, 2023 (India).
[7] Bharatiya Sakshya Adhiniyam, 2023 (India).

ISSN: 2582-6433

- IT (Intermediary Guidelines & Digital Media Ethics Code) Rules, 2021 (amended)
- Reserve Bank of India Act, 1934
- Payment and Settlement Systems Act, 2007
- Banking Regulations + RBI Cybersecurity Guidelines
- Bankers' Books Evidence Act, 1891
- Copyright Act, 1957
- Trade Marks Act, 1999
- Patents Act, 1970

Conclusion

Cybercrime continues to evolve with rapid technological advancements, making investigation and enforcement increasingly complex. While the present legal framework is relatively comprehensive, its effectiveness depends largely on proper implementation and adaptability to emerging threats. There is a need to strengthen investigative capacity through technical training, modern forensic tools, and better coordination among agencies. Additionally, clearer guidelines for cross-border jurisdiction and faster response mechanisms are essential. Enhancing public awareness and promoting responsible digital behaviour can also play a preventive role. Overall, a proactive and continuously updated approach is necessary to effectively combat cybercrime in the digital age.