International Journal of Cyber Warfare and Terrorism (IJCWT)
Volume 3, Issue 1, January–June 2025, pp. 21-25, Article ID: IJCWT_03_01_002
Available online at https://iaeme.com/Home/issue/IJCWT?Volume=3&Issue=1
Impact Factor (2025): 2.10 (Based on Google Scholar Citation)
Journal ID: 2306-9488; DOI: https://doi.org/10.34218/IJCWT_03_01_002

CYBER CRIMES AND LEGAL LOOPHOLES: THE IMPACT OF WEAK JURISDICTION IN INDIA

[1] Asha Thomas,
Assistant Professor.
ORCID ID: https://orcid.org/0009-0002-9993-6812

[2] Neenu K Suresh,
PG Student.

[3] Theja Krishna,
PG Student.

ABSTRACT

The rapid expansion of digital technology in India has led to a significant rise in cyber crimes, exposing critical weaknesses in the country's legal framework. Despite efforts to regulate cyberspace through laws such as the Information Technology Act, 2000, jurisdictional challenges and enforcement gaps persist. This paper analyzes the impact of weak jurisdiction on cyber crime in India, using case studies, statistical data, and expert insights. It compares India's cyber laws with international practices and proposes legal and policy reforms aimed at building a more secure digital environment.

Keywords: Cyber Law, Jurisdiction, Cybercrime, IT Act 2000, Law Enforcement, India, Legal Reforms.

Cite this Article: Asha Thomas, Neenu K Suresh, Theja Krishna. (2025). Cyber Crimes and Legal Loopholes: The Impact of Weak Jurisdiction in India. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 3(1), 21-25.

https://iaeme.com/MasterAdmin/Journal_uploads/IJCWT/VOLUME_3_ISSUE_1/IJCWT_03_01_002.pdf

1. Introduction

1.1 Background

India's digital growth has increased vulnerability to cyber attacks, including data breaches, identity theft, and financial fraud. Existing laws, notably the IT Act, 2000, have not evolved proportionately with emerging threats, resulting in enforcement deficiencies.

1.2 Problem Statement

Ambiguities in cyber law, jurisdictional overlaps, and insufficient law enforcement mechanisms hinder effective prosecution of cyber crimes.

1.3 Objectives

Examine existing cyber laws in India; Identify jurisdictional challenges; Analyze enforcement gaps through case studies; Compare with international standards; Propose legal reforms for better governance.

2. Literature Review

A detailed examination of previous research reveals:

- Surge in cybercrime due to digital adoption (Kumar, 2020)
- Legal frameworks lack provisions for AI and blockchain-related crimes (Bansal et al., 2021)
- Jurisdictional ambiguity is a major enforcement barrier (Singh & Mehta, 2022)

Identified gaps include limited focus on jurisdictional conflicts, lack of empirical victim studies, and insufficient comparisons with global practices.

3. Methodology

3.1 Research Design

A mixed-method approach combining qualitative interviews and quantitative analysis.

3.2 Data Sources

Primary: Interviews (n=30), Victim surveys (n=100)

Secondary: NCRB data, legal documents, CERT-In reports

3.3 Sampling

Purposive sampling of legal professionals, enforcement officers, cybercrime victims, and policy experts.

3.4 Data Analysis

Thematic coding of interviews; Statistical analysis of trends and survey data; Case studies.

3.5 Ethical Considerations

Confidentiality, informed consent, and secure data storage ensured throughout.

4. Results and Discussion

4.1 Statistical Findings

- Conviction rate: 1.6% (2020–2022)
- Pendency rate: >90% in key states
- Victim experience: 45% report legal system distrust

4.2 Thematic Insights

- Legal Loopholes: Outdated laws, vague definitions
- Jurisdictional Barriers: No clarity in cross-state/international cases
- Law Enforcement Challenges: Poor training, weak coordination

4.3 Comparative Analysis

Country | Law | Key Strengths

USA | Computer Fraud and Abuse Act | Strong federal cyber units

EU | GDPR, NIS Directive | Robust data protection

India | IT Act 2000 | Lacks modern provisions

5. Recommendations

5.1 Legal Reforms

- Comprehensive Cybersecurity Act
- Update IT Act
- Revised Section 66A-like provision

5.2 Enforcement Enhancements

- Fast-track cyber courts
- Cyber police units
- Mandatory forensic training

5.3 Public and Institutional Awareness

- Cyber hygiene education
- Awareness campaigns
- Private sector compliance

5.4 International Cooperation

- INTERPOL collaboration
- Threat intelligence sharing

6. Conclusion

Weak jurisdiction and legal loopholes hinder cybercrime enforcement. This paper highlights case studies, data, and comparative practices to advocate for urgent legal reforms and institutional strengthening.

REFERENCES

[1] Bansal, R., Sharma, P., & Gupta, K. (2021). Cyber Law and Digital Crimes in India. Journal of Cybersecurity Studies, 8(2), 45–62.

[2] Kumar, N. (2020). The Rise of Cyber Crimes in India. International Journal of Law and Information Technology, 12(3), 78–95.

[3] Mishra, A. (2018). Jurisdictional Complexities in Cyber Crime Cases. Indian Journal of Legal Studies, 15(1), 34–50.

[4] Singh, R., & Mehta, L. (2022). The Challenge of Enforcing Cyber Laws in India. Cyber Law Review, 10(4), 112–130.

[5] Government of India. (2000). Information Technology Act and Amendments.

[6] NCRB. (2023). Cyber Crime Statistics. Ministry of Home Affairs.

[7] CERT-In. (2023). Cyber Threat Reports. https://www.cert-in.org.in

[8] World Economic Forum. (2022). Global Cybersecurity Outlook.

Citation: Asha Thomas, Neenu K Suresh, Theja Krishna. (2025). Cyber Crimes and Legal Loopholes: The Impact of Weak Jurisdiction in India. International Journal of Cyber Warfare and Terrorism (IJCWT), 3(1), 21-25.

Abstract Link: https://iaeme.com/Home/article_id/IJCWT_03_01_002

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/IJCWT/VOLUME_3_ISSUE_1/IJCWT_03_01_002.pdf

✉ **editor@iaeme.com**