ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 7| July 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

# AI-ENABLED CYBERCRIME: ADEQUACY OF INDIA'S CRIMINAL LAWS

**Siya**
*Research Scholar, Maharishi Markandeshwar Deemed to be university*

**ABSTRACT**
*Artificial Intelligence (AI) has revolutionised various sectors but has also facilitated sophisticated cybercrimes such as deepfake fraud, AI-powered phishing, identity theft, and automated hacking. These evolving offences challenge the effectiveness of India's existing criminal laws. This paper examines whether the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, the Bharatiya Sakshya Adhiniyam, 2023, and the Digital Personal Data Protection Act, 2023 adequately address AI-enabled cybercrime. It further identifies legal gaps and suggests reforms for an effective regulatory framework that balances technological advancement with public safety and constitutional rights.*
**KEYWORDS***: Artificial Intelligence, Cybercrime, BNS 2023, IT Act 2000, Deepfake, Digital Evidence, Cyber Security.*

## 1. INTRODUCTION

Artificial Intelligence (AI) has transformed communication, finance, healthcare, and governance by enabling automation and data-driven decision-making. However, the same technology is increasingly used to commit cybercrimes, including AI-generated phishing, deepfake scams, identity theft, and ransomware attacks.

Unlike traditional cybercrime, AI-enabled offences are more sophisticated, scalable, and difficult to detect. India's rapid digitalisation has increased vulnerability to such crimes, raising concerns about whether existing criminal laws are sufficient to regulate AI-based offences. This paper critically analyses the adequacy of India's legal framework in addressing AI-enabled cybercrime.

## 2. RESEARCH OBJECTIVES

The study aims to:

- Examine the concept of AI-enabled cybercrime.
- Analyse the adequacy of India's criminal laws.
- Identify legal challenges in prosecuting AI-based offences.
- Suggest reforms for effective AI regulation.

## 3. RESEARCH QUESTIONS

1. What is AI-enabled cybercrime?
2. Are India's existing criminal laws adequate to address AI-driven offences?
3. What legal challenges arise in prosecuting such crimes?
4. What reforms are required to strengthen AI governance?

## 4. RESEARCH METHODOLOGY

The study adopts a **doctrinal research methodology** based on primary and secondary legal sources. Primary sources include the Constitution of India, the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, the Bharatiya Sakshya Adhiniyam, 2023, and the Digital Personal Data Protection Act, 2023. Secondary sources include books, journal articles, reports, and scholarly commentaries.

## 5. AI-ENABLED CYBERCRIME: MEANING

AI-enabled cybercrime refers to offences in which Artificial Intelligence is used to facilitate or execute cybercriminal activities. AI enables criminals to automate attacks, evade security systems, generate realistic fake content, and target victims more efficiently than traditional cybercrime methods.

## 6. EMERGING TRENDS

Major forms of AI-enabled cybercrime include:

- **Deepfake Fraud:** AI-generated fake audio and videos used for financial fraud and misinformation.
- **AI-Based Phishing:** Highly personalised phishing emails and messages.
- **Identity Theft:** AI-assisted biometric spoofing and impersonation.
- **Automated Malware:** Self-learning malware capable of bypassing security systems.
- **Financial Fraud:** AI-driven online investment scams and payment fraud.

## 7. SIGNIFICANCE OF THE STUDY

The rapid growth of AI has created new legal challenges that existing criminal laws were not designed to address. This study evaluates whether India's legal framework effectively regulates AI-enabled cybercrime and highlights the need for specialised legislation and stronger cyber governance.

## 8. SCOPE OF THE STUDY

The research focuses on AI-enabled cybercrime under the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, the Bharatiya Sakshya Adhiniyam, 2023, and the Digital Personal Data Protection Act, 2023. It also briefly considers international developments to suggest reforms for India.

Great. Below is **Part II (Points 9–16)** in the same concise, publication-style format.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 7| July 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

## 9. LEGAL FRAMEWORK IN INDIA

India does not yet have a dedicated law regulating AI-enabled cybercrime. However, several statutes address cyber offences and digital governance:

**(a) Bharatiya Nyaya Sanhita, 2023 (BNS):** Punishes offences such as cheating, forgery, identity theft, criminal intimidation, and publication of false electronic content when committed through AI.

**(b) Information Technology Act, 2000:** Key provisions include Section 43 (unauthorised access and damage to computer systems), Section 66 (computer-related offences), Section 66C (identity theft), Section 66D (cheating by personation using computer resources), and Section 67 (publishing or transmitting obscene material in electronic form).

**(c) Bharatiya Sakshya Adhiniyam, 2023 (BSA):** Recognises electronic records and digital evidence, which are crucial for investigating AI-enabled offences.

**(d) Digital Personal Data Protection Act, 2023:** Provides safeguards for the processing of personal data and imposes obligations on data fiduciaries, thereby reducing the misuse of AI involving personal information.

Although these laws address cyber offences, none specifically regulate autonomous AI systems or assign liability for AI-generated criminal acts.

## 10. CONSTITUTIONAL PERSPECTIVE

AI-enabled cybercrime raises significant constitutional concerns.

- **Article 14** guarantees equality before the law and requires that AI-based decision-making remain free from discrimination and algorithmic bias.
- **Article 19(1)(a)** protects freedom of speech, while reasonable restrictions under **Article 19(2)** may justify regulation of deepfakes and online misinformation.
- **Article 21** protects the right to life and personal liberty, including the **right to privacy**, recognised in *Justice K.S. Puttaswamy v. Union of India* (2017). AI systems processing personal data must therefore comply with constitutional standards of privacy and dignity.

## 11. JUDICIAL DEVELOPMENTS

Although India has limited case law directly on AI, several landmark decisions provide guidance:

- **Justice K.S. Puttaswamy v. Union of India (2017):** Recognised privacy as a fundamental right under Article 21, laying the foundation for AI and data protection regulation.
- **Shreya Singhal v. Union of India (2015):** Struck down Section 66A of the IT Act, reaffirming the balance between free speech and online regulation.
- **Anvar P.V. v. P.K. Basheer (2014):** Clarified the admissibility of electronic evidence, an important principle for AI-generated digital evidence.

These judgments continue to influence the regulation of digital technologies and cybercrime.

## 12. COMPARATIVE ANALYSIS

The **European Union** has adopted the **AI Act**, introducing a risk-based framework for regulating AI systems and imposing strict obligations on high-risk AI applications.

The **United Kingdom** follows a principle-based regulatory approach, relying on existing regulators rather than a single AI statute.

The **United States** regulates AI through sector-specific laws and executive policies, with increasing emphasis on transparency, accountability, and cybersecurity.

Compared to these jurisdictions, India lacks a comprehensive legal framework specifically governing Artificial Intelligence.

## 13. CHALLENGES IN INDIA'S CRIMINAL LAWS

Several challenges limit the effectiveness of India's legal framework:

- Absence of dedicated legislation on Artificial Intelligence.
- Difficulty in fixing criminal liability where AI acts autonomously.
- Rapid technological developments outpacing existing laws.
- Challenges in collecting and authenticating AI-generated digital evidence.
- Cross-border nature of cybercrime leading to jurisdictional issues.
- Shortage of specialised cyber forensic infrastructure and trained investigators.

## 14. RECOMMENDATIONS

To strengthen India's response to AI-enabled cybercrime, the following measures are suggested:

- Enact a comprehensive AI regulatory framework.
- Amend the Information Technology Act, 2000, to specifically address AI-generated offences.
- Establish specialised AI and cybercrime investigation units.
- Develop legal standards for AI accountability and algorithmic transparency.
- Enhance international cooperation for investigating cross-border cybercrime.
- Promote public awareness and digital literacy to reduce cyber risks.

## 15. CONCLUSION

Artificial Intelligence has significantly transformed the nature of cybercrime, creating challenges that traditional criminal laws cannot adequately address. While the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, the Bharatiya Sakshya Adhiniyam, 2023, and the Digital Personal Data Protection Act, 2023 provide a legal foundation for combating cyber offences, they do not comprehensively regulate AI-enabled criminal activities. India must adopt a forward-looking legal framework that promotes innovation while ensuring accountability, cybersecurity, and protection of fundamental rights.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 7| July 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

## 16. REFERENCES AND BIBLIOGRAPHY

**Statutes**

1. *Constitution of India.*
2. *Bharatiya Nyaya Sanhita, 2023.*
3. *Bharatiya Nagarik Suraksha Sanhita, 2023.*
4. *Bharatiya Sakshya Adhiniyam, 2023.*
5. *Information Technology Act, 2000.*
6. *Digital Personal Data Protection Act, 2023.*

**Cases**

1. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
2. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
3. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.

**Books and Articles**

1. *Russell S and Norvig P, Artificial Intelligence: A Modern Approach (4th edn, Pearson 2021).*
2. *Brenner SW, Cybercrime and the Law (Northeastern University Press 2012).*
3. *NITI Aayog, National Strategy for Artificial Intelligence (2018).*
4. *Ministry of Electronics and Information Technology (MeitY), Report on Artificial Intelligence Governance in India.*
5. *World Economic Forum, Global Risks Report (latest edition).*