International Journal of Information Movement *Vol. 9 Issue XII (April 2025)*
Website: www.ijim.in ISSN: 2456-0553 (online) Pages 51-57

CYBERCRIME IN THE AGE OF ARTIFICIAL INTELLIGENCE: INDIAN LEGAL PERSPECTIVE

Dr. Pooja
Assistant Professor
Vaish College of Law, Rohtak
Email: advocatepoojarao@gmail.com

Abstract: The digital landscape has been completely transformed by the quick development of artificial intelligence (AI), which has brought us both unanticipated benefits and unexpected threats. Malicious actors are increasingly using AI systems to perpetrate complex cybercrimes as these systems are incorporated into communication, economics, healthcare, and governance. AI-enabled cyber threats threaten the fundamental underpinnings of conventional cyber legislation, ranging from automated phishing attacks and AI-generated deep fakes to autonomous malware and bot-driven disinformation campaigns. This study looks at the relationship between AI and cybercrime from a legal standpoint in India, evaluating how well-suited current legal frameworks like the Indian Penal Code and the Information Technology Act of 2000 are to dealing with AI-driven offences. It draws attention to the complexity of jurisdiction, evidence problems, enforcement challenges, and doctrinal gaps that these offences pose.

Drawing upon key judicial pronouncements, expert committee reports, and comparative legal insights from jurisdictions like the United States and the European Union, the study underscores the need for a nuanced, technology-sensitive legal regime. The paper also proposes legal and policy reforms aimed at strengthening India's cybersecurity governance, including the formulation of AI-specific legislation, improved digital forensics infrastructure, cross-border cooperation protocols, and institutional capacity-building. By critically engaging with the ethical, procedural, and regulatory challenges posed by AI-induced cyber offences, this research seeks to contribute to a forward-looking legal framework that balances innovation with accountability and digital growth with human rights.

Keywords: Cybercrime, Cyber Threats, Artificial Intelligence

1.0 Introduction

Artificial Intelligence (AI) technology have advanced and been implemented in every industry at an unprecedented rate in the twenty-first century. These days, AI-powered systems are used in a wide range of industries, including law enforcement, e-commerce, national security, healthcare, education, and finance. Despite the enormous efficiency and transformational potential of these technologies, their abuse has become a major cybersecurity risk on a worldwide scale. In ways that existing legal frameworks were never intended to address, cybercriminals are increasingly using AI to develop, automate, and scale assaults.

A paradigm shift in the environment of digital threats is signalled by the rise of AI-enabled cybercrime. A new class of autonomous, adaptable, and highly intrusive cyberthreats has emerged as a result of the use of AI algorithms to reimagine and reengineer traditional cybercrimes including ransomware, phishing, data theft, hacking, and identity fraud. The distinction between humans and machines in criminal activity has become considerably more hazy due to tools such as deepfake generators, automated social engineering bots, generative AI chatbots, and predictive malware.

India, with over 850 million internet users and one of the world's fastest-growing digital economies, finds itself at the epicenter of both AI innovation and cyber vulnerability. According to CERT-In, the national nodal agency for cyber incidents, India reported over **1.4 million cyber security incidents in 2023** alone, a significant percentage of which showed signs of automation or AI influence.[1] The legal system, however, continues to be governed primarily

[1] Indian Computer Emergency Response Team (CERT-In), *Annual Report 2023*, Ministry of Electronics and

by the **Information Technology Act, 2000 (IT Act)**, and the **Indian Penal Code, 1860 (IPC)**—neither of which explicitly addresses the challenges posed by autonomous or semi-autonomous AI-driven cybercrimes.

Understanding Cybercrime in the AI Era

Hackers working alone in basements are no longer the only ones committing cybercrime. It has developed into an advanced, global sector that uses artificial intelligence (AI) more and more for accuracy, automation, and scalability. While earlier cyberattacks required extensive human input, today's AI-enabled crimes can **self-learn**, **adapt**, and **execute** without human intervention. These systems can analyze vast amounts of data, recognize patterns, and simulate human behavior—making detection and attribution increasingly difficult.

The traditional perimeter of cybercrime—unauthorized access, data breaches, identity theft—has expanded to include **AI-generated misinformation**, **deepfakes**, **AI-enhanced phishing**, and **autonomous decision-making malware**. These developments pose new legal, ethical, and operational dilemmas for regulators, investigators, and courts.

2.0 Categories of AI-Driven Cybercrimes

Based on the type of technology employed and the intended victim, AI-driven cybercrimes can be divided into a number of types. The most prominent types that are now affecting people, companies, and governments are listed below.

2.1 Deepfakes and Synthetic Media Offences: Deepfakes use AI—particularly Generative Adversarial Networks (GANs)—to manipulate audio and video content so convincingly that it appears real. These are often used to:

- Defame individuals by inserting their faces into pornographic content;
- Disseminate misinformation during elections;
- Fabricate evidence in criminal cases.

A notable instance occurred in 2020 when a deepfake of Ukrainian President Volodymyr Zelenskyy was circulated on social media, urging citizens to surrender—a hoax orchestrated using AI tools.[2] Deepfakes have been used to harass women and produce distorted political content in India, however charges are still uncommon because of legal loopholes.

2.2 AI-Enhanced Phishing and Social Engineering: Phishing attacks, once crude and easily detectable, have now evolved. AI is capable of creating context-aware emails, voice spoofing (often known as "vishing"), and modifying tactics in real time in response to user feedback. Data from public platforms is scraped by AI technologies to improve the persuasiveness and targeting of communications.

AI chatbots have also been used in **spear-phishing** to maintain prolonged conversations with targets, making fraud detection by companies and users significantly harder. For example, in 2021, an AI-powered voice clone of a company's CEO was used to trick a UK-based employee into transferring €220,000 to cybercriminals posing as a Hungarian supplier.[3]

2.3 Autonomous Malware and Adaptive Ransomware: AI is increasingly embedded into malware systems to:

- Learn from intrusion detection systems (IDS) and evade them;
- Scan systems for vulnerabilities more efficiently;
- Choose targets based on real-time cost-benefit analysis.

AI-based ransomware can identify high-value files, encrypt them selectively, and adjust ransom demands according to a target's perceived financial capacity.

Ransomware attacks against hospitals and municipal corporations in the sector with outdated systems and lax cybersecurity protocols have increased dramatically in India. In order to get past firewalls and adjust to detection efforts in the middle of an attack, these attackers frequently use AI.[4]

2.4 Botnets and Swarm Attacks: Botnets are networks of compromised devices used to launch **Distributed Denial of Service (DDoS)** attacks. With AI integration, botnets become self-sustaining: they autonomously identify new devices to infect, communicate through encrypted channels, and modify attack vectors.

2.5 AI-Powered Surveillance and Privacy Invasion: AI systems trained in facial recognition, geolocation tracking, and behavioral analysis are being weaponized for:

- Unlawful surveillance by private entities;

Information Technology, Government of India.

[2] BBC News, "Ukraine War: Zelensky Deepfake Video Was a Russian Trick," March 2022.

[3] CNBC, "Criminals Cloned a Company CEO's Voice in a Scam Worth $243,000," August 2021.

[4] CERT-In, *Monthly Cyber Security Bulletin*, October 2023.

- State-sponsored espionage;
- Blackmail and stalking.

The use of tools like **Clearview AI**, which scraped billions of images from social media to create facial recognition profiles, raised global alarm over privacy violations. In India, concerns have been raised about the unregulated use of facial recognition by police without judicial oversight.[5]

3.0 Characteristics of AI-Enabled Cybercrime

AI-driven cybercrimes have unique features that differentiate them from traditional cybercrimes and complicate legal regulation:

1. **Speed and Scalability:** AI can execute thousands of attacks simultaneously, learning and evolving in real-time.
2. **Lack of Human Agency:** These crimes may be initiated or executed without direct human involvement at the operational stage.
3. **Anonymity and Attribution Challenges:** AI systems can obfuscate origins and reroute commands, making it difficult to trace perpetrators.
4. **Cross-Border Complexity:** Data processing and attack execution can span multiple jurisdictions, challenging enforcement.
5. **Evidentiary Complications:** Logs, metadata, and footprints may be tampered with or erased autonomously, weakening prosecutorial evidence.

4.0 India's Legal Framework on Cybercrime and its Interface with AI

India's cyber legal framework continues to rest on two foundational statutes:

- The **Information Technology Act, 2000 (IT Act)** – dealing with digital records, cyber offences, and intermediary liability;
- The **Bhartiya Nyaya Sanhita, 2023 (BNS)** – which replaces the Indian Penal Code, 1860, and governs substantive penal law, including crimes involving cheating, identity fraud, obscenity, and criminal intimidation.

While the IT Act directly targets offences involving computers and information systems, it lacks specificity on **autonomous technologies** like Artificial Intelligence (AI). The BNS, though modernized in structure and language, is similarly **silent on algorithmic or machine-based liability**. These omissions create serious limitations in prosecuting cybercrimes where AI plays an active or central role.

4.1 The Information Technology Act, 2000: Relevant sections of the IT Act invoked in AI-driven cybercrimes include:

- **Section 43** – Deals with unauthorized access, data extraction, virus injection, or disruption of services;
- **Section 66** – Converts acts under Section 43 into criminal offences if done dishonestly or fraudulently;
- **Section 66C** – Pertains to identity theft, especially in digital impersonation and AI-generated fake credentials;
- **Section 66D** – Covers cheating by impersonation using computer resources, which can be used for deepfake-related frauds;
- **Section 66E** – Criminalizes the violation of privacy via electronic means, including AI-enabled surveillance;
- **Section 67** – Addresses publication or transmission of obscene materials, relevant in AI-generated deepfake pornography;
- **Section 70** – Protects "critical information infrastructure," and applies to AI-led cyberattacks on sensitive systems.

These provisions remain **technology-neutral**, failing to explicitly account for **autonomous or machine learning agents** involved in the commission of such offences.

4.2 The Bhartiya Nyaya Sanhita, 2023 (BNS): The **BNS, 2023**, which replaces the **IPC, 1860**, introduces modernized terminology and structure but does not directly address cybercrime or AI. However, the following provisions are often invoked in AI-related cyber offences:

[5] Internet Freedom Foundation (IFF), *Facial Recognition in Indian Policing: A Constitutional and Legal Analysis*, 2022.

- **Section 316** – *Cheating* (corresponds to IPC Section 415): Applied where AI is used to deceive individuals through phishing or impersonation.
- **Section 336** – *Forgery* (IPC Section 463): Invoked when AI tools are used to generate fake documents, signatures, or identity proofs.
- **Section 356** – *Defamation* (IPC Section 499): May be used in cases involving AI-generated defamatory content like deepfakes.
- **Section 351** – *Criminal Intimidation* (IPC Section 503): Covers AI-enabled threats, including voice-generated or chatbot threats.
- **Section 74(2)** – *Sexual Harassment by Use of Technology* (newly introduced): Potentially useful in AI-based stalking or voyeuristic offences.

While the BNS aligns penal language with current societal realities, it **still assumes human agency and intent**, limiting its effectiveness in dealing with AI-generated or AI-automated crimes.

5.0 Gaps and Challenges in the Legal Framework

The increasing integration of Artificial Intelligence into cybercrime operations reveals not only technological advancement among offenders but also **systemic vulnerabilities in the legal and institutional frameworks designed to combat such offences**. While India's **Information Technology Act, 2000**, and the **Bhartiya Nyaya Sanhita, 2023** offer general provisions to address cyber offences, they **fail to account for the autonomous, adaptive, and cross-jurisdictional nature of AI-driven cyber threats**. This chapter discusses the doctrinal, procedural, institutional, and jurisdictional gaps that hinder effective prevention, investigation, and prosecution of AI-enabled cybercrimes in India.

5.1 **Absence of AI-Specific Legal Definitions:** One of the most fundamental legal gaps is the **absence of a definition of "Artificial Intelligence" or "autonomous systems"** under Indian statutes. Without clear statutory language:

- Courts struggle to categorize AI tools as **means, intermediaries, or perpetrators**;
- Investigating agencies lack a standard for **determining criminal liability** when machines perform acts without direct human control.

The **Digital India Act (proposed)** and **Data Protection Act, 2023,** still do not offer concrete legal recognition of **algorithmic autonomy**, **machine learning systems**, or **AI-generated content** as legally significant entities.

5.2 **Reliance on Human-Centric Doctrines:** Traditional criminal law principles are **ill-suited** for AI scenarios:

- **Mens rea** (criminal intent) is a core requirement under BNS for most offences. AI lacks consciousness, thus making this requirement inapplicable.
- **Vicarious liability**—used in corporate contexts—requires a nexus between human direction and machine execution, which AI's autonomous functions can easily disrupt.
- **Actus reus** (guilty act) becomes difficult to attribute when the action is algorithmically generated and **executed without real-time human intervention**.

5.3 **Inadequate Provisions for Autonomous Offences:** While Sections like **66D (IT Act)** or **316 (BNS)** address impersonation or cheating, they assume direct and deliberate acts by identifiable human agents. In cases where:

- A chatbot autonomously **impersonates a bank executive**, or
- A deepfake tool generates content based on automated triggers,

there is **no statutory provision clearly assigning criminal liability** or determining the standard of due diligence required of users, developers, or platforms.

6.0 Procedural Challenges in Investigation and Evidence

6.1 **Attribution and Traceability:** One of the defining challenges of AI-enabled crime is the **difficulty in attribution**:

- AI systems are often hosted on **cloud platforms across borders**, making jurisdiction unclear.
- Offenders may use **proxy servers, anonymizers, or self-deleting bots**, further complicating identification.
- AI tools can be programmed to **replicate or adapt**, raising the question of how long the original creator remains responsible.

6.2 **Admissibility of Machine-Generated Evidence:** Under the **Bhartiya Sakshya Adhiniyam, 2023**, digital evidence must fulfill conditions of:

- Authenticity
- Integrity

- Origin

Machine-generated data such as logs, metadata, or content from self-learning tools is prone to **tampering**, **dynamic alteration**, and **self-erasure**, making admissibility under Section 61 (formerly Section 65B of the Indian Evidence Act) highly problematic.

6.3 Lack of Forensic and Investigative Infrastructure: India's **cyber forensic ecosystem** is still nascent:

- Many police stations lack access to even basic digital evidence retrieval tools;
- Only a handful of states have **AI-trained cyber labs**;
- National bodies like CERT-In are overstretched and **reactive rather than preventive**.

The gap between **technology used by offenders** and **tools available to law enforcement** is growing dangerously wide.

7.0 Enforcement and Institutional Gaps

7.1 Fragmented Jurisdiction and Coordination Failures: Cybercrime, by nature, often spans multiple jurisdictions. AI only amplifies this problem:

- A phishing bot may operate from one country, target victims in another, and store data on servers in a third.
- Indian law enforcement faces obstacles in **mutual legal assistance** and **extradition**, particularly when the crime lacks a clear human agent.

Despite the existence of **inter-agency platforms** like the Indian Cyber Crime Coordination Centre (I4C), there is **no unified database** or **standard protocol** for AI-enabled threats.

7.2 Lack of Platform Accountability: Current Indian laws only impose limited responsibility on platforms. Under **Section 79 of the IT Act**, intermediaries are exempt from liability if they exercise due diligence. However:

- There is **no binding obligation** to detect, prevent, or report AI-generated harmful content;
- **Content hosting platforms** or **AI tool providers** face minimal consequences for misuse unless notified officially.

The **absence of algorithmic transparency mandates** allows platforms to avoid disclosing how their AI tools can or are being misused.

7.3 Inadequate Legal Expertise and Training: Magistrates, prosecutors, and even High Court judges often lack:

- **Technical understanding of how AI functions**;
- Familiarity with **cross-border digital forensics**;
- Training in **interpreting automated logs or data trails**.

This results in **delayed prosecutions**, **frequent acquittals**, or **over-reliance on conventional analogies**.

8.0Legal and Policy Reform Proposals

As Artificial Intelligence continues to be weaponized for cybercrime—through deepfakes, phishing bots, voice cloning, and adaptive malware—India's legal response must move from **retrofitting outdated laws** to **designing forward-looking, AI-sensitive regulatory frameworks**. To close the large legal and enforcement gaps noted in earlier chapters, this chapter offers thorough reform recommendations at the statutory, institutional, procedural, and policy levels. The goals of these reforms are to safeguard due process, empower investigators, protect citizens, and control AI platforms and tools without limiting innovation.

8.1 Enactment of an AI (Regulation and Liability) Act: India must consider enacting a dedicated **Artificial Intelligence (Regulation and Liability) Act**, which may include:

- **Definitions** of AI, autonomous systems, deep synthesis technology, and algorithmic decision-making;
- **Classification of AI systems** by risk levels (e.g., high-risk, low-risk);
- **Mandatory registration** of high-risk AI tools;
- **Developer, deployer, and platform liability** for AI-generated offences;
- **Penalties for misuse** or negligent design of AI algorithms that cause cyber harm.

This statute should draw from models like the **EU AI Act**, **Singapore's Model AI Framework**, and **China's Deep Synthesis Rules**, while being tailored to India's **constitutional and cultural context**.

8.2 Amendment to the Information Technology Act, 2000: Pending the enactment of the **Digital India Act**, urgent amendments to the **IT Act** should include:

- Insertion of a **Chapter on Autonomous Digital Agents**, covering bots, voice clones, and generative tools;
- New sections for:
  - **AI-enabled impersonation**;
  - **Unlawful use of generative content (deepfakes)**;

  - **Unauthorized use of biometric likeness using AI**;
- Clarification of **intermediary obligations** to:
  - Remove harmful AI content on notice;
  - Maintain logs of AI tool usage;
  - Disclose algorithmic decision paths where relevant.

8.3 Integration with the Bhartiya Nyaya Sanhita, 2023: Proposed additions to the **BNS** could include:

- A new **Chapter on Algorithmic Crimes**, defining criminal liability where human intent is absent but harm is caused;
- Presumption of liability (rebuttable) for:
  - Coders who knowingly release high-risk AI tools;
  - Platforms that profit from unregulated use;
- Specific recognition of **AI-based cheating, fraud, and forgery**;
- Creation of an **offence of algorithmic harassment**, for bots or AI-based tools used for stalking or defamation.

9.0 Regulatory and Institutional Reforms

9.1 Establishment of a National AI Accountability Authority (NAIAA): A dedicated statutory body should be formed to:

- **License and audit AI tools** used in high-risk domains;
- **Investigate algorithmic harms** and recommend penalties;
- Serve as a **regulatory interface** between AI developers, platforms, and law enforcement;
- Collaborate with CERT-In, the Data Protection Board, and MeitY.

9.2. Strengthening the Indian Cyber Crime Coordination Centre (I4C): The I4C should be empowered to:

- Maintain an updated **AI Crime Threat Database**;
- Issue **advisories and alerts** on AI tools misused for phishing, fraud, or impersonation;
- Assist in **cross-border enforcement coordination** through INTERPOL and the Budapest Convention (upon India's accession).

9.3.Algorithmic Transparency and Audit Rules: MeitY should notify:

- **Rules mandating periodic algorithm audits** for AI platforms;
- **Disclosure obligations** when AI tools are used in law enforcement or electoral content;
- **Sandbox environments** to test high-risk AI tools before public release.

10.0 Conclusion

This research has demonstrated that the **fusion of Artificial Intelligence and cybercrime** represents one of the most pressing legal and policy challenges of our time. From deepfake harassment and AI-enhanced phishing to autonomous malware and botnet attacks, **cybercrime has evolved beyond conventional paradigms**, increasingly relying on non-human agents to perpetrate harm. India's legal system, which is based on human-centric doctrines and legacy legislation, is finding it increasingly difficult to adjust to this new digital reality as these dangers become more complex and widespread.

India's current cybercrime regime, primarily governed by the **Information Technology Act, 2000**, the **Bhartiya Nyaya Sanhita, 2023**, and the **Bhartiya Sakshya Adhiniyam, 2023**, lacks:

- Recognition of AI systems as autonomous or semi-autonomous agents;
- Doctrinal clarity on intent and liability attribution;
- Procedural tools for handling AI-generated evidence;
- And **institutional infrastructure** for detection, investigation, and prosecution of AI-enabled crimes.

Judicial decisions, while creative in analogy, have been limited by statutory gaps and technological unfamiliarity.

India must not fall behind in terms of legal readiness as it pursues its swift digital transformation. Legal reforms that are AI-sensitive, technology-neutral, and constitutionally compliant are urgently needed. The law must evolve to **identify and mitigate risks**, **assign clear responsibilities**, and **ensure remedies for harm caused by AI tools**—whether human-operated or autonomous. Only then can India's cyber law infrastructure ensure a safe, fair, and accountable digital future.

11.0 References

i. Bhartiya Nyaya Sanhita, 2023, Ministry of Law and Justice, Government of India.

ii. Bhartiya Sakshya Adhiniyam, 2023, Ministry of Law and Justice, Government of India.

iii. Information Technology Act, 2000 (with 2008 amendments), Government of India.

iv. Digital Personal Data Protection Act, 2023, Government of India.

v. Digital India Corporation, *Draft Digital India Act*, 2023, MeitY.

vi. Indian Computer Emergency Response Team (CERT-In), *Annual Report 2023*.

vii. Internet Freedom Foundation, *Facial Recognition and Surveillance in India*, 2023.

viii. Pavan Duggal, "Need for AI-Specific Legislation in India," *Cyber Law India Blog*, 2022.

ix. Sreenidhi Srinivasan, "Artificial Intelligence and Criminal Law in India," *NLS Journal of Legal Studies*, Vol. 33, Issue 2, 2021.

x. Ministry of Home Affairs, *Cyber Crime SOP Guidelines*, I4C, 2022.