Swami Vivekananda Advanced Journal for Research and Studies
Online Copy of Document Available on: www.svajrs.com

ISSN:2584-105X Pg. 1-10

AI as a Tool to Commit and Prevent Cyber Crime in India: A Critical Legal Analysis

Dr. Priya Gupta
Independent Researcher
Email id: pg.priya90@gmail.com

Accepted: 24/03/2026
Published: 28/03/2026 ***DOI: http://doi.org/10.5281/zenodo.19314275***

Abstract

Artificial Intelligence (AI) has fundamentally transformed the landscape of cyber crime, acting both as an enabler of sophisticated cyber offences and as a powerful tool for their prevention. This paper critically examines the dual role of AI in cyber crime, analyzing its misuse in automated attacsks, deepfakes, and intelligent malware, alongside its role in cybersecurity, fraud detection, and digital forensics. It further evaluates the adequacy of existing legal frameworks in India and globally, identifying regulatory gaps and challenges such as attribution, jurisdiction, and accountability. The paper concludes by proposing legal and policy reforms aimed at ensuring responsible AI governance and effective cyber crime prevention.

Keywords*: Artificial Intelligence, AI, Cyber crime, Deepfakes, IT Act 2000, DPDP Act 2023, Cyber Law, Digital crime*

I. INTRODUCTION

The integration of Artificial Intelligence (AI) into modern technological systems has redefined both opportunities and risks within cyberspace. AI, particularly through machine learning and deep learning algorithms, enables systems to perform tasks that traditionally required human intelligence. However, the same capabilities have been weaponized to commit cyber offences with unprecedented sophistication.

Cybercrime, defined as criminal activities conducted through digital means, has evolved significantly with the advent of AI. The growing reliance on digital infrastructure in countries like India further amplifies vulnerabilities. This necessitates a legal inquiry into whether existing frameworks are sufficient to regulate AI-driven cyber threats.

II. MEANING AND DEFINITION

Meaning:

Artificial Intelligence: AI refers to the capability of machines or computer systems to carry out tasks that usually need human intelligence. These tasks may involve like, gaining knowledge from data, understanding and using language, identifying patterns or objects, solving complex problems, making decisions based on information. In simple terms, AI is the technology that enables machines to imitate human thinking and behavior.

Cyber Crime: Any unlawful activity carried out through computers, digital devices, or the internet.

Definition:

Cyber Crime: Cyber crime is not defined in any Indian law, but it can be understood through a legal dictionary:

According to Justia legal dictionary: An illegal activity, such as theft, fraud, violation of intellectual property rights, or sharing of child pornography, carried out using electronic mediums.[1]

Artificial Intelligence: AI is similarly undefined in Indian law, but it may be interpreted with reference to other authoritative sources:

According to NASA: The definition of Artificial Intelligence (AI) adopted by NASA is based on Executive Order 13960, which refers to Section 238(g) of the National Defence Authorization Act, 2019:

1. Any artificial system capable of operating in changing and uncertain conditions with minimal human intervention, or one that can learn from experience and enhance its performance through data.
2. A system created through software, hardware, or other means that is able to carry out tasks involving human-like abilities such as perception, thinking, planning, learning, communication, or physical actions.
3. An artificial system developed to imitate human thought processes or behavior, including technologies like neural networks and cognitive architectures.
4. A collection of methods and approaches, such as machine learning, that are used to replicate or simulate cognitive functions.
5. An artificial system built to act in a rational manner, such as intelligent agents or robots, which accomplish objectives through perception, reasoning, planning, learning, communication, decision-making, and action.[2]

III. HISTORY OF ARTIFICIAL INTELLIGENCE

In 1950: Alan Turing created the Turing test to determine whether a machine is thought to be intelligent.

1956: The term artificial intelligence was first used to describe simulated machines at a scientific conference.

1966: Saw the creation of the first chatbot, ELIZA.

1972: AI is used in mainstream medicine with MYCIN.

1997: The world chess champion loses against an AI-powered chess system called Deep Blue.

2011: Artificial intelligence is pervasive; cellphones come equipped with voice assistants.

2023: ChatGPT transforms chatbot applications

Till date: We are at present unable to fully imagine what AI will be able to do in the future.

IV. AI AS A TOOL TO COMMIT CYBER CRIME

[1] *available at*: https://dictionary.justia.com/cybercrime (last visited on March 27, 2026).

[2] *available at*: https://www.nasa.gov/what-is-artificial-intelligence/ (last visited on March 26, 2026).

1. Automation of Cyber Attacks

AI enables large-scale automation of cyberattacks, including phishing and Distributed Denial-of-Service (DDoS) attacks. Machine learning algorithms can identify system vulnerabilities and execute attacks without human intervention.

2. Deepfakes and Synthetic Media

Deepfake technology uses generative adversarial networks (GANs) to create realistic but fabricated audio-visual content. Such content is increasingly used in fraud, identity theft, and political misinformation.

3. AI-Driven Malware

Unlike traditional malware, AI-powered malware can adapt to security systems, evade detection, and autonomously modify its behavior.

4. Advanced Social Engineering

AI tools analyze user behavior and personal data to craft highly convincing phishing messages, increasing the success rate of cyber fraud.

V. AI AS A TOOL TO PREVENT CYBER CRIME

1. Threat Detection and Risk Assessment

AI-based cybersecurity systems detect anomalies in network traffic and predict potential threats using predictive analytics.

2. Fraud Detection in Financial Systems

Financial institutions deploy AI to monitor transactions and detect irregular patterns, significantly reducing fraud.

3. Automated Incident Response

AI facilitates rapid identification and containment of cyber threats, minimizing damage and response time.

4. AI in Digital Forensics

AI assists investigators in analyzing large datasets, identifying patterns, and gathering digital evidence efficiently.

VI. LEGAL FRAMEWORK GOVERNING AI AND CYBER CRIME

1 Indian Legal Framework

India regulates cyber crime primarily through the *Information Technology Act, 2000*.

Provisions: Section 43 (damage to computer systems)[3], Section 66 (computer-related offences)[4], Section 66C (identity theft)[5], Section 66D (cheating by personation).[6]

Additionally, the *Digital Personal Data Protection Act, 2023* addresses issues related to data privacy and protection.

However, these laws do not explicitly address AI-specific cyber threats such as deepfakes or autonomous systems.

In *BNS 2023*, Cyber crime has been included under organized crime in section 111, which defines organized crime as a continuing illegal activity by a syndicate.[7] Thus, cyber crime is not treated separately, instead, it is classified as organized crime. However, BNS should include a separate provision for cyber crime or at least define it, because a clear definition helps clarify the nature and scope of the offence and also aids in determining appropriate punishment.

2 International Legal Framework

The *Budapest Convention* on Cyber crime provides a framework for international cooperation in combating cyber crime.

The *European Union's General Data Protection Regulation (GDPR)* also indirectly regulates AI through data protection principles.

VII. CRITICAL LEGAL ANALYSIS OF AI-SPECIFIC LEGISLATION: GLOBAL FRAMEWORKS VS INDIA

The European Union: The EU AI Act, which entered into force in August 2024, is the *world's first comprehensive AI-specific legislation*, which represents the **most advanced and comprehensive AI-specific legislation globally.** Its **Key Features are a risk-based classification** (unacceptable, high,

[3] The Information Technology Act, 2000 (Act 21 of 2000), s. 43.
[4] The Information Technology Act, 2000 (Act 21 of 2000), s. 66.
[5] The Information Technology Act, 2000 (Act 21 of 2000), s. 66 C.
[6] The Information Technology Act, 2000 (Act 21 of 2000), s. 66 D.
[7] Bharatiya Nyaya Sanhita, 2023 (Act of 45 of 2023), s. 111.

limited, minimal risk), **ban on harmful AI practices** (e.g., social scoring), **regulation of generative AI (GPAI), mandatory transparency for deepfakes and Strong enforcement with heavy penalties. Its Approach is** preventive (ex-ante regulation) and rights-based (focus on privacy, dignity, safety). The EU model is **highly structured but *compliance-heavy.***

United States: Sectoral and Market-Driven Approach:

The United States does *not have a single comprehensive AI law* but regulates AI through executive orders, sector-specific laws and federal agency guidelines. A key development is **AI the Executive Order of 2023 (Biden Administration). Its features** focus on **AI safety and security and** Regulation through FTC (consumer protection) and NIST (AI standards). Its **approach is** Innovation-driven and decentralized. The U.S. prioritizes ***flexibility over strict regulation*.**

China: State-Controlled AI Governance:

China has adopted a **strict, state-centric regulatory framework**, including **generative AI Measures (2023) and** Algorithmic recommendation regulations. Its **key features are** mandatory **content moderation,** algorithm registration requirements and state oversight of AI systems. Its **approach is** control-oriented and focus on national security and social stability. China imposes ***strict obligations on AI developers and platforms*.**

United Kingdom: Principles-Based AI Regulation:

The United Kingdom follows a ***soft-law, principles-based approach*** rather than a binding AI Act. Its **features are** AI white paper (2023), regulation through existing regulators and five core principles (safety, transparency, fairness, accountability and contestability). Its **approach is** flexible and pro-innovation. The UK model balances ***innovation with regulatory guidance.***

India: Fragmented and Evolving Framework:

India has not yet enacted a comprehensive AI law. Instead, it regulates AI through the IT Act, 2000, Digital Personal Data Protection Act, 2023, DPDP Rules, 2025, IT Rules, 2021 and Proposed Digital India Act. Its **features are** data-centric regulation, Platform accountability and Judicial intervention in AI harms. Its **approach is** reactive (ex-post) and incremental. India's framework is ***adaptive but lacks clarity and uniformity.***

COMPARATIVE TABLE

Jurisdiction	Nature of Regulation	Approach	AI-Specific Law	Deepfake Regulation	Enforcement
EU	Comprehensive	Preventive	Yes	Strong	Strong
USA	Sectoral	Flexible	No	Limited	Moderate
China	Centralized	Control-based	Yes	Strong	Very Strong
UK	Principles-based	Flexible	No	Emerging	Moderate
India	Fragmented	Reactive	No	Limited	Developing

NEED FOR A HYBRID MODEL IN INDIA

India should adopt a balanced regulatory model that integrates risk-based classification and transparency obligations from the EU, innovation-friendly policies from the USA and UK, and, to a limited extent, platform accountability from China.

VIII. JUDICIAL APPROACH: CASE LAWS ON AI AND CYBER CRIME

1. Indian Case Laws

(i) *Shreya Singhal v. Union of India (2015)*[8]

This landmark judgment addressed the constitutionality of Section 66A of the Information Technology Act, 2000. The Supreme Court struck down the provision on the ground that it violated the fundamental right to freedom of speech and expression under Article 19(1)(a) of the Constitution. The Court held that vague expressions such as annoyance and inconvenience could lead to arbitrary misuse, especially in the context of online communication.

Relevance to AI & Cybercrime: This case is crucial in the age of AI-driven content (such as automated speech and deepfakes), as it sets constitutional limits on regulating online expression and prevents over-criminalization of digital communication.

(ii) *Justice K.S. Puttaswamy v. Union of India (2017)*[9]

In this historic judgment, the Supreme Court declared the Right to Privacy as a Fundamental Right under Article 21 of the Constitution. The Court recognized informational privacy, which includes protection of personal data in the digital ecosystem.

Relevance to AI & Cyber crime: This case forms the constitutional foundation for Data protection laws, Regulation of AI surveillance, Protection against AI-enabled data misuse and profiling.

(iii) *State of Tamil Nadu v. Suhas Katti (2004)*

This was one of India's first cybercrime convictions involving online harassment through defamatory messages posted on a Yahoo group.

Relevance: It established the practical application of the IT Act in prosecuting online offences, which now extend to AI-enabled harassment and trolling.

(iv) *Avnish Bajaj v. State (NCT of Delhi) (2008)*[10]

This case involved the CEO of an online marketplace (Bazee.com) where obscene material was sold online. The Court examined intermediary liability and whether platform providers can be held responsible for user-generated content.

Relevance to AI: With AI-generated content flooding platforms, this case becomes important in determining liability of platforms using AI systems.

(v) *Anvar P.V. v. P.K. Basheer (2014)*

The Supreme Court clarified the admissibility of electronic evidence under Section 65B of the Indian Evidence Act.

Relevance: AI-generated evidence (deepfakes, digital logs, algorithmic outputs) must comply with evidentiary standards established in this case.

2. International Case Laws

(i) *Carpenter v. United States (2018)*[11]

The U.S. Supreme Court held that accessing historical cell phone location data without a warrant violates the Fourth Amendment.

Relevance to AI: AI-driven surveillance and tracking systems must respect privacy rights, reinforcing limits on mass data collection.

(ii) *Google Spain SL v. AEPD (2014)*

The Court of Justice of the European Union (CJEU) recognized the "Right to be Forgotten", allowing individuals to request deletion of personal data.

Relevance to AI: AI systems relying on large datasets must comply with data minimization and erasure rights.

(iii) *R v. Cambridge Analytica (2018)*

This case arose from misuse of Facebook data for political profiling.

Relevance: Highlights risks of AI in Behavioral manipulation, Data analytics misuse and Electoral interference.

(iv) *United States v. Morris (1986)*[12]

This case involved the first conviction under the Computer Fraud and Abuse Act (CFAA) for releasing the Morris Worm.

Relevance: It laid the foundation for prosecuting automated and self-propagating cyberattacks—precursors to AI-driven malware.

[8] *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.
[9] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[10] Avnish Bajaj v. State (NCT of Delhi), 150 (2008) DLT 769.
[11] Carpenter v. United States, 585 U.S. (2018).
[12] United States v. Morris, 928 F.2d 504 (2d Cir. 1991).

(v) *López Ribalda v. Spain (2019)*[13]

The European Court of Human Rights dealt with covert video surveillance of employees.

Held: Surveillance must balance employer interests with employee privacy rights.

Relevance to AI: Important in regulating AI-powered surveillance systems (facial recognition, workplace monitoring).

Analytical Observations: From the above cases, certain legal principles emerge:

1. Privacy as a Core Right: Established in Puttaswamy and reinforced globally, it limits AI surveillance.
2. Freedom of Expression vs Regulation: Shreya Singhal ensures that AI-generated content regulation must not violate free speech.
3. Intermediary Liability: Cases like Avnish Bajaj highlight the responsibility of platforms using AI.
4. Admissibility of Digital Evidence: Anvar P.V. becomes critical in handling AI-generated evidence.
5. Global Convergence: International cases show a shift toward to Data protection, Accountability and Ethical AI governance

Latest Indian AI Jurisprudence (2023–2026):

Deepfake-Specific Case Laws in India

(i) ***Anil Kapoor v. Simply Life India & Ors. (Delhi High Court, 2023)***[14]

This is widely regarded as ***India's first landmark AI-deepfake judgment***.

Observations: Unauthorized use of a person's persona for commercial purposes violates Right to privacy, Right to dignity and Right to livelihood. The Delhi High Court granted a landmark injunction protecting actor Anil Kapoor's personality rights against misuse through AI-generated deepfakes, morphed images, and voice cloning.

Held: The Court restrained unauthorized use of name, voice, image and catchphrases.

Legal Impact: Recognized AI-generated identity misuse as actionable harm, expanded personality rights jurisprudence and became a precedent for all future deepfake litigation in India

Legal Significance: First major Indian ruling explicitly addressing AI-generated identity misuse,

Recognized personality rights in the context of generative AI and established liability for unauthorized commercial exploitation using AI.

(ii) *Arindam Chaudhuri / Ankur Warikoo Deepfake Case (Delhi High Court, 2025)*[15]

The Delhi High Court passed *John Doe injunctions* against unknown persons using AI deepfake technology to impersonate a public figure for financial fraud.

Held: Platforms were directed to remove deepfake content within a fixed time and disclosure of user identities behind such content was ordered.

Legal Significance: Recognized deepfakes as tools of financial cyber fraud, strengthened intermediary liability and due diligence obligations and introduced dynamic injunctions for future AI misuse.

(iii) *Chaitanya Rohilla v. Union of India (Delhi High Court, 2024)*[16]

A Public Interest Litigation (PIL) sought regulation of deepfakes and AI-generated content.

Held: The Court directed the Government to constitute a committee on deepfake regulation, consider global regulatory frameworks and consult stakeholders including victims and intermediaries.

Legal Significance: Judicial recognition of regulatory vacuum in AI law and Shift from reactive to policy-driven AI governance.

(iv) *Aishwarya Rai Bachchan v. YouTube/Google (Delhi High Court, 2024–25)*[17]

The plaintiffs challenged circulation of explicit AI-generated deepfake videos. The court granted an interim injunction and takedown of infringing content. Their legal significance recognizes deepfakes as

[13] López Ribalda v. Spain, App no. 1874/13 (ECHR 2
[14] Anil Kapoor v. Simply Life India & Ors., Delhi High Court (2023).
[15] Ankur Warikoo Deepfake Case, Delhi High Court (2025).
[16] Chaitanya Rohilla v. Union of India, Delhi High Court (2024).
[17] *Aishwarya Rai Bachchan v. YouTube/Google*, Delhi High Court (2024–25).

causing privacy and reputational harm and extends the liability discussions to global tech platforms.

(v) ***Akira Nandan (Pawan Kalyan's Son) Case (Delhi High Court, 2025)***[18]

The Court restrained circulation of an AI-generated film replicating a person's identity without consent. The Court held that AI-generated likeness violates privacy and reputation, Injunction applicable against unknown future offenders. The plaintiffs filed a suit against circulation of explicit AI-generated deepfake videos.

Relief Sought: Removal of content, damages, protection of personality rights.

Legal Significance: Strengthens injunctive relief in AI misuse cases and recognizes irreparable harm caused by synthetic media. Expands liability to global digital platforms and highlights gendered harms of deepfake technology.

(vi) ***Swami Ramdev v. Unknown (John Doe) (Delhi High Court, 2026)***[19]

The Delhi High Court restrained unauthorized use of Swami Ramdev's identity via AI-generated deepfakes and misleading endorsements.

Held: Platforms must remove such content promptly and unauthorized AI use of persona violates publicity rights.

Legal Significance: Reinforces personality rights against AI misuse and recognizes risk of public deception through deepfakes.

(vii) ***Gautam Gambhir v. Unknown (Delhi High Court, 2026)***[20]

A recent suit filed against misuse of identity through AI-generated deepfakes and impersonation.

Key Issue: Unauthorized commercial exploitation and reputational harm.

Legal Significance: Shows rapid rise in celebrity deepfake litigation in India, Emphasizes need for statutory personality rights framework.

(viii) ***Rajat Sharma v. Union of India (PIL, Delhi High Court, ongoing)***[21]

The petitioner sought: Ban or regulation of deepfake creation tools, appointment of nodal officers for complaints and mandatory labeling of AI-generated content.

Legal Significance: Highlights need for platform accountability and Focus on preventive regulation rather than post-harm remedies.

Landmark Judicial Recognition of AI-Generated Harm:

1. Expansion of Personality Rights in AI Era (2024–2025)

Celebrity Deepfake Protection Cases (Delhi & Bombay High Courts, 2024–2025)

Indian courts have increasingly granted **injunctions against AI misuse** involving celebrities such as protection against AI-generated impersonation (e.g., Hrithik Roshan, Salman Khan cases), injunctions against voice cloning, fake endorsements and blocking of infringing links and platforms.

Judicial Trend: Courts are treating voice, facial likeness and Digital persona as **legally protectable intellectual and personality rights.**

2. **Rise of Criminal Liability in Deepfake Misuse**

FIR in Bhagwant Mann Deepfake Case (Punjab, 2024)

A deepfake video of a sitting Chief Minister led to registration of FIR and Invocation of IPC along with IT Act provisions. Its **legal significance is** establishes **criminal liability for AI-generated misinformation and** demonstrates use of existing laws to tackle AI abuse.

3. Strengthening of Injunctive Relief & John Doe Orders (2025–2026)

(i) Akira Nandan v. Unknown (Delhi High Court, 2025)

The Court restrained circulation of an **AI-generated film replicating identity. The court held that the** Deepfake content causes **irreparable reputational**

[18] *Akira Nandan Case*, Delhi High Court (2025).
[19] Swami Ramdev v. Unknown, Delhi High Court (2026).
[20] *Gautam Gambhir v. Unknown*, Delhi High Court (2026).
[21] Rajat Sharma v. Union of India, PIL (Delhi High Court).

harm and granted **dynamic (John Doe) injunctions.** The **significance lies in the** recognition that **AI harm is difficult to quantify and monitor and** courts are moving toward **preventive justice.**

(ii) Deepfake Injunctions by Bombay High Court (2025)

In cases involving actors like Akshay Kumar: The court said that deepfakes are **alarming** and threaten to public order and individual dignity. Its **Legal Impact is that it** strengthens a **strict liability approach for AI misuse and** expands scope of **public interest in deepfake regulation.**

4. Latest 2026 Developments: Recognition of "Weaponisation of Identity"

(i) Gautam Gambhir v. Unknown (Delhi High Court, 2026)[22]

A recent suit has been filed alleging the misuse of identity through AI-generated deepfakes. The key argument is that identity has been weaponised through AI tools. Its legal significance lies in introducing the concept of AI-enabled identity weaponization and strengthening claims for personality and publicity rights protection.

(ii) PILs on AI Regulation (Punjab & Haryana High Court, 2026)

Courts have issued notices to the Central Government and technology companies (Google, Meta, and X), highlighting concerns regarding a 550% increase in deepfake cases, risks of electoral manipulation, and financial fraud. The courts have further called for the enactment of a dedicated AI regulation law and the mandatory labeling of deepfake content.

Significance: Strong judicial push toward **legislative intervention.**

EMERGING DOCTRINAL PRINCIPLES IN INDIAN AI JURISPRUDENCE (2023–2026)

In the analysis of the above cases, the Indian courts have evolved the following principles:

1. Personality Rights as a Core AI Right: It includes voice, face, likeness, and digital identity, which are now protected against AI misuse.

2. Deepfakes is a Constitutional Harm: The Courts links AI misuse with **Article 21 addressing privacy & dignity and Article 19 concerning misuse of speech vs protection.**

3. Preventive & Dynamic Injunctions: The Courts issuing **John Doe /dynamic injunctions** and Covering *future unknown offenders.*

4. Expansion of Intermediary Liability: Platforms now expected to the remove content quickly, prevent re-upload and assist investigation

5. Shift from Reactive to Proactive Regulation: Courts are recognizing legal gaps and directing government to frame **AI-specific laws.**

IX. CRITICAL EVALUATION

Despite progressive judicial intervention as well as courts are actively filling legislative gaps but reliance on defamation on Defamation law, IT Act. But IT Act's provisions is **insufficient for AI-specific harms.** The core problem is that India currently lacks a dedicated AI liability law and a clear framework for deepfakes, algorithmic accountability, and platform liability.

X. CHALLENGES IN REGULATING AI IN CYBER CRIME

1. Attribution and Liability

Determining liability becomes complex when AI systems act autonomously without direct human control.

2. Jurisdictional Issues

Cyber crimes often transcend national boundaries, leading to conflicts of jurisdiction and enforcement difficulties.

3. Absence of AI-Specific Legislation

The existing cyber laws are not sufficient to address emerging AI-driven threats, whether they are BNS, the IT Act or others.

4. No separate provision in BNS

In BNS, cyber crime has not defined separately so that its punishment can also be given separately.

5. Ethical and Privacy Concerns

[22] *Gautam Gambhir v. Unknown*, Delhi High Court (2026).

AI systems may infringe upon privacy rights and exhibit algorithmic bias, raising serious ethical questions.

6. Absence of Mens Rea in AI Actions

Traditional criminal law requires Intention (mens rea) and Knowledge but AI systems has lack of Conscious intent and Legal personality. This creates a doctrinal gap in applying criminal liability.

7. Rapid Technological Evolution vs Slow Legal Response:

The mismatch in pace is one of the biggest challenges as AI evolves rapidly (through monthly or annual innovation cycles), whereas the law evolves slowly (through years of legislation and litigation). Consequently, laws become outdated quickly. For instance, the Information Technology Act, 2000 does not address deepfakes, generative AI, or autonomous systems. Recent developments, such as the EU AI Act, attempt to bridge this gap; however, India remains in a transitional phase.

8. Inadequacy of IT Act, 2000 and Limitations of the Information Technology Act, 2000:

The *Information Technology Act, 2000* was enacted to address conventional cyber offences, such as Unauthorized access (Section 43), Identity theft (Section 66C) and Cheating by impersonation (Section 66D).

However, in the era of Artificial Intelligence, the Act suffers from structural and conceptual limitations**:**

Absence of AI-Specific Definitions*:* The Act does not recognize Artificial Intelligence, machine learning systems and deepfakes or synthetic media. This creates ambiguity in prosecuting AI-generated harms.

No Framework for Algorithmic Liability*:* The Act assumes human intent and direct causation, but AI systems operate autonomously and learn and evolve. This creates a liability gap (developer vs deployer vs platform)

Inadequate Coverage of Deepfakes*:* Deepfake harms (e.g., identity manipulation, misinformation) are currently prosecuted under Defamation law, IT Act provisions. These are indirect and insufficient remedies.

Weak Preventive Mechanisms*:* The IT Act is largely reactive (punishment after offence) and not preventive (no risk classification or pre-deployment checks)

Limited Intermediary Regulation for AI*:* Although IT Rules impose due diligence, they do not specifically regulate AI-generated content and mandate transparency for algorithms.

IT Act, 2000 as a First-Generation Cyber Law*:* This Act requires provisions to be made for the emerging development of second-generation AI regulation at the global level.

9. Inadequacy of DPDP Rules 2025*:*

This does not regulate AI systems directly, nor does it defined deepfakes or algorithmic harms and it lacks of AI-specific liability rules. This Act only regulates the data used by AI.

XI. SUGGESTIONS

1. Enactment of AI-Specific Legislation

India should introduce a comprehensive legal framework specifically regulating AI and its misuse in cyber crime.

2. Strengthening Institutional Mechanisms

Cyber security infrastructure must be enhanced through collaboration between government agencies and private entities.

3. International Cooperation

India should actively participate in global cyber crime conventions and promote cross-border data-sharing mechanisms.

4. Establishing Accountability Frameworks

Clear liability should be defined for AI developers, deployers, and users.

5. Public Awareness and Capacity Building

Educational initiatives are necessary to equip individuals and institutions against AI-driven cyber threats.

6. IT Act **needs a modern AI regulation**

Which can deal with AI-generated cyber crime at the national and international levels.

7. The need for updated legal reform policies

In India, along with creating specific laws to tackle AI-generated cyber crime, there is also a need to develop updated legal reforms policies to prevent it.

XII. CONCLUSION

AI represents both a significant threat and a powerful solution in the domain of cyber crime. While it enhances the capabilities of cyber criminals, it also strengthens cyber security mechanisms. The challenge lies in striking a balance between innovation and regulation. A proactive legal framework, supported by international cooperation and ethical governance is essential to effectively address AI-driven cyber crime.

REFERENCES

1. Debarati Halder, K. Jaishankar, Cyber Crime Against Women in India, 1st Ed., 2017.
2. Debarati Halder and K. Jaishankar, Cyber Crime and Victimization of Women Laws, Rights And Regulations, 2012.
3. Nandan Kamath, Law relating to Computers, Internet and E- commerce: A Guide to Cyber Laws and the Information Technology Act, 2000
4. Dr. Pawan Duggal, Text Book on Cyber Law
5. Dr. Karnika Seth, Cyber Crime Against Women: An Indian Law Perspective, 2018 Edition.
6. The Information Technology Act, 2000 (Act 21 of 2000).
7. Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
8. Council of Europe, *Convention on Cybercrime* (2001).
9. Regulation (EU) 2016/679 (General Data Protection Regulation).
10. *available at*: https://www.nasa.gov/what-is-artificial-intelligence/ (last visited on March 26, 2026).
11. *available at*: https://dictionary.justia.com/cybercrime (last visited on March 27, 2026).

****