Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Volume 2 | Issue 4 | ISSN : 2583-1895
April - June 2025 | DOI: https://doi.org/10.5281/zenodo.15872078

# AI-Driven Cyber Offences: A Rising Menace in India

**Vagisha Kapoor [1], Dr. Mithlesh Malviya[2]**

[1]BBA+LLB Student, School of Legal Studies & Governance, Career Point University, Kota (Raj.)

[2]Assistant Professor, School of Legal Studies & Governance, Career Point University, Kota (Raj.)

## Abstract

The research paper is to examine the swift development of artificial intelligence (AI) has transformed several industries by providing data-driven solutions, efficiency, and creativity. AI has created new opportunities for complex cybercrimes in addition to its advantages. This study examines the growing risk of AI-driven cybercrime in India, emphasising the ways in which criminals are using tools like automated bots, deepfakes, and machine learning to carry out identity theft, phishing, data breaches, and disinformation operations. The use of AI by cybercriminals to increase the scope and accuracy of their attacks is making traditional cybersecurity solutions ineffective. The issues posed by law enforcement in identifying and prosecuting crimes enabled by artificial intelligence are examined, along with noteworthy occurrences and present legal and regulatory frameworks. In order to combat the growing threat of cybercrimes powered by AI, India needs to proactively modify its policies and defences as the technology develops. With its strategic suggestions for a safe cyber future, this report seeks to further the conversation on digital safety in the era of intelligent technologies.

**Keywords:** cybercrime in india, artificial intelligence, cyber law in india, information technology act

## Introduction

The digital revolution in India has greatly increased the possibility for socioeconomic growth, but it has also increased the surface area for targeted cyberattacks. With more than 800 million internet users and a quickly growing ecosystem of mobile-based technological products, such as financial technology, online education, and e-governance, India has entered a phase of historically high cybercrime rates. The number of reported cybercrime occurrences increased by 24% annually from 50,035 in 2020 to 52,974 in 2021 and then to

65,893 in 2022, according to data from the National Crime Records Bureau (NCRB) (Ministry of Home Affairs, 2024).

This increase has been caused by numerous problems. Together with the quick uptake of digital payment methods and the transition to online services, the pandemic caused a significant shift towards remote work that increased national vulnerability. The first legislative foundation for penalising cyber offences is the Information Technology Act of 2000 (as amended in 2008). The POCSO Act, the Indian Penal Code (IPC), and sector-based guidelines also contain additional provisions to address the broader notion of cybercrime. A step towards establishing its own data and privacy legislation is the broader Digital Personal Data Protection Act (2023) (Lawton, 2023). These national efforts also draw upon global standards like the General Data Protection Regulation (GDPR) of the EU and the upcoming EU AI Act (Ministry of Information & Broadcasting, 2023). With regard to financial fraud, cyberbullying and harassment, internet terrorism and disinformation, breach of privacy and hacking, child sexual assault and abuse, and technology theft, this research attempts to categorise the primary forms of cybercrime in India. Using case studies and the use of AI techniques for detection and remediation, it will examine each of their roots. In order to offer general suggestions on policy gaps for ethics, enforcement, and integration with international best practices, the paper will also examine the advantages and disadvantages of India's national legal system. The paper is an attempt to evaluate how government, legislation, and AI interact to create a safe digital future for Indians.

**Review of Literature**

The researcher has made a thoroughly research on these existing literature and the following literature sources are followed. The relationship between cybercrime and artificial intelligence (AI) has drawn more attention as a result of its increasing significance in the current digital environment. Numerous academics, decision-makers, and cybersecurity specialists have examined the pernicious use of AI technologies, especially in developing nations like India.

A report by Kshetri (2021), claims that artificial intelligence (AI) has become a double-edged sword, enabling hackers to launch more accurate and destructive attacks while simultaneously bolstering cybersecurity systems through intrusion detection and predictive

analytics. The study highlights the startling accuracy with which AI-powered techniques like voice cloning, automated phishing, and deepfakes can get past traditional security measures. NITI Aayog's (2018 report), "National Strategy for Artificial Intelligence," acknowledged recognised AI's revolutionary potential in India while simultaneously alerting readers to the serious dangers of its abuse, especially in the field of cybersecurity. In order to lessen the risks posed by AI-powered products, the research recommended the creation of proactive cybersecurity safeguards and ethical AI frameworks.

According to Kumar & Jha (2021), AI-specific cybercrimes are not covered by the Information Technology Act of 2000, there are legal issues in the prosecution and prevention of such offences.

Bradford W. Reyns (2017) "Routine Activity Theory and Cybercrime", stated that various new issues that come up when applying theory to cybercrime are discussed, along with possible remedies and a summary of the field's current status. Routine activity theory is a component of criminology's opportunity perspective, which holds that criminal opportunities are what ultimately lead to criminal incidents. Its main idea emphasises that opportunities for

crime arise when conditions that are favourable to crime exist. Routine activity theory states that a motivated criminal will act when presented with a suitable target who has no effective defence. According to the routine activity idea, in the absence of effective custody, cybercrime uses computer networks to link potential victims with motivated offenders.

**Research Gaps Identified**

There are still a number of important research gaps, especially in the Indian context, despite growing interest in the relationship between artificial intelligence and cybercrime among academics and policymakers. With little in-depth examination of AI as a weapon for cybercrimes, the majority of the material currently in publication concentrates on cybercrime or AI applications. Empirical research explicitly examining the application of AI-driven technologies like deepfake creation, automated phishing, and intelligent malware in actual cyber incidents in India is lacking.

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Volume 2 | Issue 4 | ISSN : 2583-1895
April - June 2025 | DOI: https://doi.org/10.5281/zenodo.15872078

The assessment of India's legal and regulatory systems is another important area of deficiency. Extensive study on how to connect legal systems with AI-enabled dangers is still lacking, despite studies highlighting the shortcomings of current laws. Scientists, legal researchers, sociologists, and politicians must collaborate across disciplines due to the intricacy of AI-driven cybercrimes. The scientific and legal landscape has not kept up with the fast-increasing number of AI-driven cyber offences in India. To create efficient, evidence-based solutions to combat this growing digital danger, it is imperative to close these research gaps. The impact of AI-enabled cybercrimes on various Indian socioeconomic groups, businesses, or geographical areas is not well examined in research. Furthermore, policy integration of AI-based cybersecurity solutions and responsible AI deployment are not discussed.

**Research Methodology**

Secondary sources, including books and articles from different websites, were employed in the examination of how Artificial intelligence related with cybercrime in India.

The growing threat of AI-driven cyber offences in India is examined in this study using a critical and problem-focused methodology. The methodology focusses on the shortcomings, gaps, and restrictions found in the current technological, legal, and digital frameworks. The study uses a qualitative and doctrinal research methodology, critically analysing the topic mainly through secondary sources such news articles, government papers, cybersecurity publications, and scholarly journals. The Ministry of Home Affairs, 2024, CERT-In, 2023; official reports with statistics (NCRB, CERT-In annual reports), government press releases, and reputable media sources (e.g., The Indian Express, Times of India, Reuters) for the most recent incidents and quotes (Manral & Sinha, 2023; Das, 2024; Kalra, 2024) served as our main sources of data. We also looked into technology-focused papers on AI methods, especially those that addressed fraud, intrusion, and deepfake detection. However, our method was analytical rather than experimental. We use both qualitative case studies and quantitative trends whenever possible, such as counts of major crimes [Ministry of Home Affairs, 2024; CERT-In, 2023].

The Information Technology Act, 2000 (Amended 2008), which defines offences like

hacking, data theft, identity theft, unauthorised access, and cyberterrorism (s. 66F), is the main cyber law. Not to be forgotten, in 2015, the Supreme Court ruled that Section 66a, which made "delivering offensive messages" online a crime, was unconstitutional. Similar crimes are examined by other statutes, such as the Protection of Children from Sexual Offences (POCSO) Act, 2012, which addresses online child abuse, and the Indian Penal Code, 1860, which is the source of traditional law offences (murder, defamation, etc.) that can occur offline or online (Das, 2024). Deepfakes and other AI-generated fake content present additional difficulties for India's judicial system. The legitimacy of legal proceedings could be seriously impacted by deepfakes' capacity to sway evidence, damage reputations, and disseminate false information (Helmus, 2022).

This legal vacuum contributes to delayed justice, investigative hurdles, and regulatory loopholes. The study seeks to highlight India's inadequate readiness for cyberthreats driven by artificial intelligence. The research critically examines current institutional and legal systems by concentrating on doctrinal analysis and content assessment. It finds that India is woefully unable to handle the growing threat of AI-driven cyber offences. In order to protect India's digital ecosystem, this necessitates immediate reforms, capacity building, and legislative modernisation.

**Research Findings**

According to the findings, India's capacity to successfully prevent, identify, and punish such acts has a number of serious flaws. AI-powered tools have been shown to increase the scope and severity of conventional cybercrimes. Deepfake technology is being used to fabricate identities, alter films, and disseminate misinformation, while AI-enabled bots are being used to automate major attacks like credential stuffing. In the Information Technology Act of 2000, it has no specific provisions that address crimes involving artificial intelligence. The special characteristics of offences generated by artificial intelligence are not covered by Sections 66 (hacking), 66C (identity theft), and 66D (cheating by personation using computer resources), although they do offer some protection.

Deepfakes, algorithmic bias, and autonomous systems are not mentioned in the law, which makes it challenging and inconsistent to prosecute crimes involving AI. Cyber forensic units that specialise in machine learning, neural networks, or synthetic media detection are scarce.

Consequently, a large number of cyber offences enabled by AI either remain unreported or unresolved. The growing threat of AI-enabled cybercrime is acknowledged in publications from groups like NITI Aayog and the Data Security Council of India, but specific regulatory measures have not yet been put into place. AI governance in India is still in its infancy; unchecked misuse is possible due to the lack of a legislative framework for ethical AI use. In the era of artificial intelligence, India must give top priority to a proactive institutional, technological, and legislative response to guarantee digital safety.

## Conclusion

The study helps in understanding the issue of artificial intelligence (AI)-driven intelligent threats marks a turning point in the development of cybercrime. However, a darker reality of AI-driven cybercrimes has also emerged as a result of its increasing incorporation into digital ecosystems. These crimes provide previously unheard-of risks to national security, digital infrastructure integrity, and individual privacy since they are made possible by automation, deep fakes, voice cloning, machine learning algorithms, and predictive behavioural analytics. India's current cyber laws, which are mostly based on the Information Technology Act of 2000, are not sufficiently prepared to handle the complexity of crimes involving artificial intelligence. Regarding data protection, ethical use, and accountability, there is a substantial legislative and regulatory gap. The prosecution of cybercrime is further hampered by cross-border jurisdictional issues, and law enforcement authorities frequently lack the technological know-how and resources necessary to look into such offences. More focused changes are needed, even while initiatives like the Digital India project, the Indian Cybercrime Coordination Centre, and the Personal Data Protection Bill show that the government is committed to addressing cybersecurity. Digital literacy and public awareness are also important lines of defence. As individuals' reliance on digital platforms grows, they need to be informed about the dangers posed by AI and safe online conduct. The private tech industry also has a significant role to play by incorporating "ethical AI" into their development processes, implementing robust cybersecurity safeguards, and collaborating with law enforcement on compliance and incident response. It is imperative that a strong legal framework be established that explicitly addresses algorithmic transparency, cyber accountability, and AI ethics. The future of India's digital development hinges on how

efficiently it integrates AI as well as how safely and responsibly it handles its hazards.

**Suggestion and Recommendations**

The study helps in understanding the facts in India, a number of measures are required to adequately handle the cybersecurity issues raised by AI. While sophisticated machine learning is crucial for identifying malware, phishing, and undesirable content, criminals utilise AI to develop in an antagonistic manner. It also includes it's critical that technological advancements be accompanied by sensible, robust regulations. Resources and upkeep will be required for new template building laws that strengthen the enforcement of the IT Act and promote legislation pertaining to cybersecurity education. Whether AI can improve security at all will depend on its responsible development and innovation, taking bias and ethics into account. It is now up to lawmakers, the commercial sector, civic society, and academics to take action after we gave them information on recent developments, rich cases and/or programs, and fresh research opportunities.

- Provide Explicit Rules: The Indian government ought to create precise rules that address algorithmic accountability and delineate obligations for both AI developers and consumers.
- Enforce Stronger Data Protection Laws: Businesses will be able to use AI for cyber safety if rules pertaining to data privacy are strengthened.
- International Collaboration: Since cybercrime is a global problem, harmonised legal standards must be established in order for the produced standards to handle AI-based cyberthreats. Such standards require international collaboration.
- Create a Comprehensive Cybersecurity Act: Dedicated legislation that could address all cybersecurity-related issues would improve coherence and clarity in the fight against new dangers brought on by technology advancements like artificial intelligence.

**References**

1. Hemanth Kumar, B. Rx. (2025). The impact of artificial intelligence on cyber laws in India. International Journal on Science and Technology (IJSAT), 16(1), 1–4. https://www.ijsat.org/papers/2025/1/1316.pdf
2. Doe, J., & Smith, R. (2024). Artificial Intelligence in Indian policing and regulatory frameworks. NUJS Journal of Regulatory Studies, 8(4), 1–20. Retrieved from https://www.nujs.edu/wp-content/uploads/2024/01/vol-8-iss-4-1.pdf
3. Karne, R., Dudhipala, A., & Pativada, P. K. (2025). Cybercrime in India: Legal frameworks, emerging threats, and the role of AI in detection and defence. International Journal of Novel Research and Development, 10(4), 786–? Retrieved from https://www.ijnrd.org/papers/IJNRD2504591.pdf
4. Romero-Moreno, F. (2024). Generative AI and deepfakes: A human rights approach to tackling harmful content. International Review of Law, Computers & Technology, 38(3), 297–326. https://doi.org/10.1080/13600869.2024.2324540
5. Treleaven, P., Barnett, J., Brown, D., Bud, A., Fenoglio, E., Kerrigan, C., Koshiyama, A., … Schoernig, M. (2023). The future of cybercrime: AI and emerging technologies are creating a cybercrime tsunami [Working paper]. SSRN. https://doi.org/10.2139/ssrn.4507244