International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Artificial Intelligence and Emerging Cyber Crimes: Challenges for the Indian Legal Framework

Aman Kumar[1], Dr. Shova Devi[2]

[1]Student, Amity Law School, Amity University
[2]Assistant Professor, Amity Law School, Amity University

Abstract

The rapid advancement of artificial intelligence (AI) has transformed the digital ecosystem, offering significant benefits in areas such as automation, data analytics, and digital governance. However, the misuse of artificial intelligence technologies has also given rise to a new generation of cybercrimes. AI-driven cyber offences such as deepfake manipulation, automated phishing, biometric spoofing, and identity theft have become increasingly prevalent across the world. These emerging threats raise serious concerns regarding privacy, digital security, and the adequacy of existing legal frameworks.

India has developed a regulatory framework for cybercrime through legislation such as the Information Technology Act, 2000 and various provisions of the Bhartiya Nyaya Sanhita, 2023. However, these laws were enacted during a period when artificial intelligence technologies were still in their early stages of development. As a result, several AI-enabled cyber offences fall within legal grey areas where existing statutory provisions may not adequately address the complexity of these crimes.

This article critically examines the challenges posed by AI-driven cybercrime in India, with particular focus on deepfake technology and identity theft. It analyses the effectiveness of the current legal framework, evaluates relevant judicial decisions, and compares India's regulatory approach with legal developments in jurisdictions such as the United States, the United Kingdom, and the European Union. The article concludes by suggesting legal and policy reforms that may strengthen India's ability to combat emerging cyber threats in the age of artificial intelligence.

Keywords: Artificial Intelligence, Cyber Crime, Deepfake Technology, Identity Theft, Cyber Law, Digital Evidence, Information Technology Act.

INTRODUCTION

The rapid growth of digital technologies has fundamentally transformed modern society. The integration of artificial intelligence into everyday technological systems has created unprecedented opportunities for innovation and economic development. Artificial intelligence systems are now widely used in sectors such as healthcare, finance, transportation, governance, and digital communication. However, alongside

[1] Author
[2] Co-Author

these technological benefits, artificial intelligence has also created new risks and vulnerabilities within the digital environment[3].

Cybercrime has evolved significantly over the past two decades. Earlier forms of cybercrime primarily involved activities such as hacking, unauthorized access to computer systems, and data theft. In recent years, cybercriminals have begun exploiting artificial intelligence technologies to conduct more sophisticated and large-scale attacks. AI-enabled cybercrime includes automated phishing campaigns, deepfake manipulation, biometric identity theft, and algorithmic fraud[4].

Deepfake technology is one of the most concerning developments across this sector. Cybercriminals can use advanced machine learning algorithms to create highly realistic images, audio recordings, or videos that appear authentic but are entirely fabricated. These manipulated media can be used for a variety of malicious purposes, including political misinformation, financial fraud, reputational damage, and sexual exploitation. Identity theft has also become more complex as a result of the integration of artificial intelligence tools. AI-powered systems can copy voices, create realistic visual identities, and mimic digital behavioral patterns. These methods allow scammers to mimic people and get unlawful access to financial accounts, digital platforms, and sensitive data.

In India, cybercrime regulation is primarily governed by the Information Technology Act, 2000 along with various provisions under the Indian Penal Code, 1860 / Bhartiya Nyaya Sanhita, 2023 and Bhartiya Sakshya Adhiniyam, 2023. While these laws provide a legal framework for addressing cyber offences such as hacking, identity theft, and online fraud, they were enacted before the widespread adoption of artificial intelligence technologies. Consequently, several AI-driven cyber offences remain inadequately addressed within the existing legal structure where Indian courts have also played an important role in shaping cyber law jurisprudence. For instance, the Supreme Court in **Shreya Singhal v. Union of India** emphasized the need to balance regulation of online content with the constitutional protection of freedom of speech and expression. Similarly, decisions relating to electronic evidence have established important procedural safeguards for digital investigations[5].

Despite these developments, the Indian legal framework continues to face significant challenges in addressing emerging forms of cybercrime. The absence of specific legislation regulating artificial intelligence misuse creates uncertainty regarding liability, enforcement, and victim protection[6].

This piece of writing will therefore investigate the developing connection between artificial intelligence and cybercrime, with a focus on deepfake technology and AI-driven identity theft. It also analyzes whether the current Indian legal structure is effectively prepared to deal with these rising dangers and examines comparable measures taken in other jurisdictions.

STATEMENT OF PROBLEM

The rapid development of Artificial Intelligence (AI) technology has dramatically altered the web's appearance throughout the world. In India, the growing use of artificial intelligence in fields such as banking, communication, e-commerce, and governance has offered tremendous potential for technological advancement and economic prosperity. However, as technology has advanced, new forms of cybercrime have emerged that take advantage of artificial intelligence techniques. Emerging AI-based

[3] Stuart Russell and Peter Norvig, Artificial Intelligence: A Modern Approach (3rd ed., Pearson Education, 2010).
[4] David S. Wall, Cybercrime: The Transformation of Crime in the Information Age (Polity Press, 2007).
[5] (2015) 5 SCC 1
[6] Pavan Duggal, Cyber Law in India (Universal Law Publishing, New Delhi, 2017).

crimes, like deepfake manipulation, AI-generated identity theft, automated phishing attacks, and synthetic digital fraud, pose severe hazards to individuals, institutions, and national security.

Although India has enacted cyber laws to restrict cybercrime, such as the Information Technology Act of 2000, these rules were drafted at a period when artificial intelligence technologies were not widely used. As a result, various legal issues arise regarding the sufficiency and efficacy of the current legal framework in combating growing AI-driven cybercrime. As a result, the purpose of this study is to determine whether the current Indian cyber law framework is capable of effectively dealing with AI-based cyber offenses, as well as what legislative reforms may be required to deal with these future technical dangers.

LITERATURE REVIEW

Scholars and researchers have increasingly examined the relationship between artificial intelligence and cyber-crime in recent years. Several studies have highlighted the potential misuse of artificial intelligence technologies for criminal activities and the difficulties faced by legal systems in regulating such technologies.

Pavan Duggal in his work *Cyber Law in India* emphasizes that technological innovations often outpace legal regulations, creating regulatory gaps that cyber criminals exploit. He argues that existing cyber laws must be updated to address emerging technological challenges.

Similarly, **Aparna Viswanathan** in *Cyber Law: Indian and International Perspectives* observe that artificial intelligence introduces complex issues regarding legal liability and accountability. When crimes are committed using automated systems, determining responsibility becomes a significant challenge for legal authorities.

International scholars have also examined the role of artificial intelligence in cyber-crime. **Susan W. Brenner** highlights that AI-based cyber-attacks can be highly sophisticated and capable of causing wide spread harm. Automated cyber-attacks can rapidly exploit vulnerabilities in digital networks, making traditional investigative techniques insufficient.

Another important area of scholarly discussion relates to deepfake technologies. Deepfakes are AI-generated synthetic media that can manipulate images, audio and video recordings to create realistic but false representations. These technologies have been used for online harassment, political misinformation and identity fraud.

Legal scholars argue that existing cyber-crime laws may not adequately address the unique challenges posed by artificial intelligence-based offences. Therefore, many researchers advocate the development of specialized regulatory frameworks for artificial intelligence.

HYPOTHESIS

This research is based on the following hypothesis:

- The existing cyber law framework in India, particularly under the Information Technology Act, 2000 and relevant provisions of the Indian Penal Code, 1860, is not fully adequate to address emerging cybercrimes involving artificial intelligence technologies such as deepfakes, AI-generated identity theft, and automated digital fraud.
- Effective regulation of AI-based cybercrime in India requires specific legislative reforms, stronger digital forensic capabilities, and enhanced regulatory mechanisms for online platforms and digital intermediaries.

OBJECTIVE OF THE STUDY

The primary objectives of this research study are as follows:

- To examine the concept and development of artificial intelligence technologies and their impact on the digital ecosystem**.**
- To identify and analyze emerging AI-based cybercrimes**,** including deepfake technology, AI-driven identity theft, and automated online fraud.
- To critically analyze the existing legal framework in India governing cybercrime, particularly the provisions of the Information Technology Act, 2000 and other related laws.
- To study the challenges faced by law enforcement agencies in detecting and investigating AI-based cybercrime.

RESEARCH METHODOLOGY

The present research adopts a doctrinal method of legal research. The study is primarily based on the analysis of statutory provisions, judicial decisions and academic literature relating to cyber crimes and artificial intelligence.

Primary sources used in the research include:

- Statutory provisions contained in the Information Technology Act, 2000.
- Relevant provisions of the Bhartiya Nyaya Sanhita, 2023.
- Judicial decisions of Indian courts concerning cyber crime and electronic evidence.

Secondary sources include:

- Books on cyber law and information technology law.
- Academic journal articles discussing artificial intelligence and cyber security.
- Government reports on cybercrime trends and digital security policies.

The research aims to critically evaluate the adequacy of the existing legal framework in addressing artificial intelligence-enabled cybercrimes in India.

LIMITATIONS

While the study attempts to analyze the emerging challenges posed by artificial intelligence in the field of cybercrime, certain limitations exist.

First, the research primarily relies on secondary sources of information**,** including books, journal articles, government reports, and legal statutes. Due to limited availability of empirical data relating specifically to AI-based cybercrime in India, the study may not include extensive primary data.

Second, artificial intelligence technology is evolving at a rapid pace, and new forms of cybercrime continue to emerge. Consequently, the legal analysis presented in this study may require continuous updating as technological developments progress.

Third, the study focuses primarily on the Indian legal framework governing cybercrime, with limited comparative analysis of selected international legal systems. Therefore, it may not cover all global regulatory approaches to artificial intelligence governance.

Finally, due to the interdisciplinary nature of artificial intelligence and cybersecurity, certain technical aspects of AI technology may not be explored in extensive technical detail within the scope of this legal research.

Concept of Artificial Intelligence and Cyber Crime

Artificial intelligence refers to the capability of machines and computer systems to perform tasks that ty-

pically require human intelligence, such as learning, reasoning, decision-making, and problem solving. AI systems rely on algorithms, large datasets and machine learning techniques to identify patterns and generate outputs without continuous human intervention[7].

Over the past decade, artificial intelligence has been widely integrated into digital platforms including social media networks, financial institutions, e-commerce systems, and biometric authentication technologies. While these developments have improved efficiency and innovation but they have also created new vulnerabilities that may be exploited by cybercriminals.

Cybercrime traditionally refers to unlawful activities carried out using computer systems or digital networks. These offences include hacking, unauthorized access, data theft, online fraud, and cyber harassment. However, with the advancement of artificial intelligence technologies, cybercrime has entered a new phase where criminals use automated tools and intelligent systems to execute complex digital attacks. AI-enabled cybercrime involves the use of machine learning algorithms, automated scripts, and synthetic media technologies to commit illegal activities in cyberspace. Unlike traditional cybercrime, AI-based cyber offences can operate at a much larger scale and often remain difficult to detect[8].

These developments raise serious legal concerns because existing cyber laws were primarily designed to address earlier forms of digital crime rather than highly sophisticated AI-driven attacks[9].

Emerging AI-Based Cyber Crimes

Artificial intelligence has enabled the development of several new forms of cybercrime that pose significant challenges to law enforcement authorities. Some of the most prominent AI-driven cyber offences include automated phishing attacks, deepfake manipulation, biometric identity theft, AI-powered malware, and algorithmic financial fraud[10].

Automated phishing campaigns represent one of the most common applications of artificial intelligence in cybercrime. Using AI algorithms, cybercriminals can generate personalized phishing emails targeting thousands of victims simultaneously. These messages are often designed to appear authentic by analysing the online behaviour and communication patterns of the targeted individual.

AI-powered malware is another emerging threat. Such malware systems can learn from the defensive mechanisms of cybersecurity software and modify their behaviour accordingly in order to evade detection.

However, among the various forms of AI-driven cybercrime, deepfake manipulation and identity theft represent the most serious threats due to their potential to cause reputational, financial, and psychological harm.

Deepfake Technology and Cybercrime

Deepfake technology refers to the use of artificial intelligence, particularly machine learning techniques such as Generative Adversarial Networks (GANs), to create highly realistic synthetic media. These technologies allow users to manipulate images, videos, and audio recordings in a manner that makes them appear authentic.it was initially developed for research and entertainment purposes, but it has increasingly been misused for criminal activities. Cybercriminals can use deepfake tools to impersonate individuals, fabricate compromising videos, or spread misinformation. One of the most alarming

[7] Supra Note 1.
[8] Jonathan Clough, Principles of Cybercrime (2nd ed., Cambridge University Press, 2015).
[9] Supra Note 4.
[10] Shafi Goldwasser et al., "Artificial Intelligence and the Future of Cybersecurity", Harvard Journal of Law & Technology, Vol. 34 (2021).

applications of deepfake technology involves non-consensual synthetic pornography, where the face of an individual is superimposed onto explicit content without their consent. Such activities can lead to severe psychological distress and reputational damage for victims[11]. Deepfakes may also be used for financial fraud. In several international incidents, cybercriminals have successfully used AI-generated voice clones to impersonate corporate executives and authorize fraudulent financial transfers[12].

The growing accessibility of deepfake software has further intensified this threat. Many AI tools capable of generating realistic deepfakes are now available through open-source platforms, making it easier for individuals with limited technical expertise to misuse these technologies.

From a legal perspective, the challenge lies in the fact that deepfake creation does not always involve unauthorized access to computer systems. Instead, the offence arises from the misuse of publicly available images or audio recordings. As a result, existing cyber laws often struggle to address such conduct directly[13].

Identity Theft through Artificial Intelligence

Identity theft has long been recognized as a serious cybercrime. However, artificial intelligence has significantly expanded the methods through which digital identity theft can be carried out. Traditionally, identity theft involved the unauthorized use of personal information such as passwords, bank account numbers, or identification documents. In contrast, AI-enabled identity theft involves the creation of synthetic identities using machine learning technologies[14].

For example, voice cloning technology can copy a person's speech from an extremely short audio sample. Cybercriminals can then utilize the cloned voice to defraud family, friends, financial institutions or corporate personnel. Similarly, facial recognition spoofing enables attackers to bypass biometric security systems by employing AI-generated photos or videos that closely resemble the authorized user. Such methods may contaminate digital payment systems, online banking platforms, and protected government databases.

Another form of AI-driven identity fraud involves the creation of entirely fabricated digital identities known as “synthetic identities.” These identities combine real and artificial data to create new personas capable of passing identity verification systems. These developments indicate that traditional legal definitions of identity theft may no longer adequately capture the complexity of AI-driven impersonation[15].

Legal Provisions Applicable to AI-Based Cyber Crimes in India

In India, cybercrime is primarily governed by the Information Technology Act, 2000. Although the legislation does not specifically mention artificial intelligence, several of its provisions may indirectly apply to AI-enabled cyber offences[16].

For instance, **Section 66C** of the Information Technology Act, 2000 **criminalizes identity theft** involving the fraudulent use of electronic signatures, passwords, or unique identification features. This provision may apply in cases where AI systems are used to create synthetic identities or impersonate

[11] Robert Chesney and Danielle K. Citron, “Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security,” California Law Review, Vol. 107, No. 6 (2019).
[12] Federal Bureau of Investigation, Private Industry Notification: Deepfake Audio Used for Corporate Fraud (2019)
[13] Supra Note 4.
[14] Susan W. Brenner, Cybercrime and the Law: Challenges, Issues, and Outcomes (Northeastern University Press, Boston, 2012).
[15] Information Technology Act, 2000, ss. 66C & 66D (identity theft and cheating by personation using computer resources).
[16] Supra note 4.

individuals in digital environments. Similarly, **Section 66D** of the Information Technology Act, 2000 **penalizes cheating by personation using computer resources.** This provision may apply to cases where AI-generated identities or voice cloning technologies are used to deceive individuals or organizations for financial or fraudulent purposes.

Another relevant provision is **Section 66E** of the Information Technology Act, 2000, **which addresses violations of privacy through the unauthorized capture, publication, or transmission of images of a private area of any person without consent.** Such provisions may become relevant in cases involving AI-generated manipulated images or privacy violations through synthetic media. In cases involving deepfake pornography or manipulated explicit content, authorities may rely on **Section 67** of the Information Technology Act, 2000 **which criminalizes the publication or transmission of obscene material in electronic form.** This provision may be invoked where deepfake videos are used for sexual exploitation or online harassment[17].

Apart from the Information Technology Act, certain provisions of the Indian Penal Code, 1860 and Bhartiya Nyaya Sanhita,2023 may also be applicable to AI-driven cyber offences. For example, offences relating to cheating, impersonation, criminal intimidation, and defamation may be invoked depending on the circumstances of the case[18].

In situations involving online harassment or persistent monitoring through digital platforms, the offence of stalking under **Section 354D of the Indian Penal Code and Section 78(Stalking) of BNS[19], 2023** and **Section 356** (Defamation) of BNS, may also be relevant, particularly where AI-generated content is used to harass or threaten individuals.

From an evidentiary perspective, the admissibility and authenticity of digital evidence in cybercrime cases are governed by the Bharatiya Sakshya Adhiniyam, 2023. The statute recognizes electronic records as admissible evidence and lays down procedural safeguards for their authentication which is provided under **Section 61, 62, 63, 66 of BSA, 2023**.

For example, **Section 61 of the Bharatiya Sakshya Adhiniyam, 2023** recognizes electronic and digital records as documentary evidence, while **Section 63** provides conditions for the admissibility of electronic records. These provisions become particularly significant in cases involving deepfake videos, AI-generated audio recordings, and other forms of digital evidence[20].

Despite these provisions, scholars have argued that the Indian legal framework lacks explicit regulation addressing artificial intelligence misuse. This legislative gap has raised concerns regarding the adequacy of current cyber laws in addressing emerging technological threats.

Judicial Approach and Relevant Case Laws

Indian courts have gradually developed jurisprudence relating to cybercrime and digital evidence over the past two decades. Although the Indian judiciary has addressed several cyber-related offences, specific judicial interpretation concerning artificial intelligence-based cybercrime remains relatively limited. Nevertheless, certain landmark cases provide important guidance regarding online harassment, electronic evidence, and liability in digital environments[21].

[17] Information Technology Act, 2000, s. 66C,66D, 66E and section 67.
[18] K.D. Gaur, Textbook on the Indian Penal Code (6th ed., Universal Law Publishing, New Delhi, 2016).
[19] Section 78 and 356 of BNS, 2023 (45 of 2023)
[20] Section 61, 62, 63, 66 of BSA, 2023, (47 of 2023).
[21] Aparna Viswanathan, Cyber Law: Indian and International Perspectives (LexisNexis Butterworths, New Delhi, 2012).

One of the earliest successful convictions under Indian cyber law occurred in the case of **Suhas Katti v. State of Tamil Nadu[22].** In this case, the accused posted obscene and defamatory messages about a woman on an online forum, leading to harassment and reputational damage. The court convicted the accused under provisions of the Information Technology Act and the Indian Penal Code. This case demonstrated the effectiveness of existing cyber laws in addressing online harassment and marked a significant milestone in the enforcement of cybercrime legislation in India.

Another significant judicial decision relating to internet regulation is the landmark case of **Shreya Singhal v. Union of India[23].** The Supreme Court struck down Section 66A of the Information Technology Act on the ground that it violated the constitutional guarantee of freedom of speech and expression under Article 19(1)(a) of the Constitution of India. While the case primarily addressed freedom of expression, the judgment emphasized the importance of maintaining a balance between regulation of digital spaces and protection of fundamental rights. This principle is particularly relevant in the context of regulating AI-generated content such as deepfakes.

Another important decision concerning cybercrime liability is **Avnish Bajaj v. State (NCT of Delhi)[24],** which involved the sale of obscene material through an online marketplace. The case raised critical questions regarding intermediary liability and the responsibility of digital platforms in preventing illegal content. Although the case did not involve artificial intelligence directly, it highlighted the challenges associated with regulating digital platforms where harmful content may be disseminated rapidly.

Indian courts have also addressed issues relating to cyber harassment and online intimidation. In **Kalandi Charan Lenka v. State of Odisha[25]**, the accused created fake social media profiles of the victim and circulated morphed photographs in order to harass her. The court held that such conduct constituted offences under both the Information Technology Act and the Indian Penal Code. The decision demonstrated that courts are willing to interpret existing cyber laws broadly in order to address technologically facilitated harassment.

In **Facebook Inc. v. Union of India[26]**, the Supreme Court examined the responsibility of social media intermediaries in investigations relating to online content and digital offences. The Court held that social media platforms must cooperate with law enforcement agencies in identifying the originator of harmful online messages.

In Re: Victims of Digital Arrest Related to Forged Documents[27], The Supreme Court initiated suo motu proceedings in response to increasing incidents of "digital arrest" scams**,** where criminals impersonate law enforcement officers through digital platforms and extort money from victims. The Court observed that the fabrication of official documents and impersonation of authorities through digital technologies poses a serious threat to public trust in the justice system and directed authorities to strengthen cybercrime investigation mechanisms. This judgment has direct implications for deepfake videos, misinformation campaigns, and AI-generated harmful content circulating on social media platforms.

[22] Suhas Katti v. State of Tamil Nadu, C.C. No. 4680 of 2004, Additional Chief Metropolitan Magistrate, Egmore, Chennai.
[23] (2015) 5 SCC 1.
[24] (2008) DLT 769 (Delhi High Court).
[25] 2017 SCC OnLine Ori 78.
[26] (2020) 3 SCC 637.
[27] SMW (Crl.) No. 3/2025 (Supreme Court of India).

Although these cases do not specifically involve artificial intelligence, the principles developed through these decisions provide guidance for addressing emerging cyber offences such as deepfake manipulation and AI-based identity fraud[28].

Electronic Evidence and AI-Related Cybercrime

One of the most complex issues associated with AI-driven cybercrime is the collection and admissibility of digital evidence. In cases involving deepfake videos or AI-generated audio recordings, courts must determine whether the evidence presented is authentic and reliable.

The Supreme Court addressed the admissibility of electronic evidence in the landmark case of **Anvar P.V. v. P.K. Basheer[29]**. In this judgment, the Court held that electronic records must be accompanied by a certificate under Section 65B of the Indian Evidence Act in order to be admissible as evidence in court. The Court later reaffirmed this principle in **Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal[30],** where it clarified that the requirement of Section 65B certification is mandatory for the admissibility of electronic evidence.

These decisions are particularly important in cases involving artificial intelligence-generated media. Deepfake videos or manipulated digital content may appear authentic but may actually be fabricated using machine learning technologies. Therefore, digital forensic examination becomes essential in establishing the authenticity of such material.

The increasing use of artificial intelligence in cybercrime investigations may also require the development of advanced digital forensic tools capable of detecting manipulated media and identifying the source of AI-generated content.

Adequacy of the Indian Legal Framework

The emergence of artificial intelligence has significantly altered the nature of cyber threats. While India possesses a statutory framework for addressing cybercrime through the Information Technology Act, 2000 and provisions of the Indian Penal Code, 1860 / Bhartiya Nyaya Sanhita, 2023 and Bhartiya Sakshya Adhiniyam, 2023, remain in question regarding whether these laws are sufficiently equipped to address AI-driven cyber offences[31].

One of the primary limitations of the Information Technology Act is that it was enacted at a time when artificial intelligence technologies were not widely prevalent. Consequently, the legislation focuses primarily on offences such as hacking, unauthorized access to computer systems, and electronic fraud. Although provisions such as **Section 66C** of the Information Technology Act, 2000 and **Section 66D** of the Information Technology Act, 2000 address identity theft and impersonation, they do not explicitly account for AI-generated identities, biometric replication, or synthetic media manipulation. Similarly, while **Section 66E** of the Information Technology Act, 2000 addresses violations of privacy and **Section 67** of the Information Technology Act, 2000 deals with obscene electronic content, these provisions were not specifically designed to regulate deepfake technology[32].

Another limitation arises in relation to jurisdictional challenges. AI-based cybercrime often involves offenders operating across international borders. The territorial jurisdiction of Indian law enforcement agencies may therefore be restricted when cyber offences originate from foreign jurisdictions. Furthermore, law enforcement agencies in India often face technological constraints in investigating

[28] Supra note 4.
[29] (2014) 10 SCC 473.
[30] (2020) 7 SCC 1.
[31] Supra note 4.
[32] Information Technology Act, 2000, s. 66C, 66D, 66E and 67.

sophisticated cyber offences. Detecting deepfake media or tracing AI-generated digital identities requires specialized forensic expertise that may not always be available at the local level[33].

Furthermore, current rules do not impose clear responsibilities on creators or distributors of artificial intelligence systems that may be utilized for unlawful purposes. As a result, regulatory accountability is sometimes placed primarily on those who abuse these technologies, rather than addressing the systemic problems connected with AI development. These reasons highlight that, while the Indian legal framework provides a basic structure for tackling cybercrime, it may not be completely ready to respond effectively to new dangers introduced by artificial intelligence.

Challenges in Enforcement of AI-Based Cybercrime Laws

Despite the existence of legal provisions addressing cybercrime, enforcement remains a significant challenge in many jurisdictions, including India. One of the primary difficulties lies in the rapid pace of technological innovation. Artificial intelligence technologies continue to evolve at a rate that often outpaces legislative reform. As a result, lawmakers frequently struggle to update legal frameworks in response to emerging threats.

Another challenge involves the technical complexity associated with AI-based cybercrime investigations. Detecting deepfake media or identifying AI-generated identities requires advanced digital forensic tools and specialized expertise. Jurisdictional issues also present major obstacles in cybercrime enforcement. Many cyber offences are transnational in nature, with perpetrators operating from different countries. This complicates the process of investigation, evidence collection, and prosecution.

Furthermore, the anonymity provided by digital platforms allows cybercriminals to conceal their identities through encryption technologies, proxy servers, and anonymous networks. These enforcement challenges highlight the need for stronger institutional capacity, specialized training programs, and international cooperation mechanisms to effectively combat AI-driven cybercrime[34].

Suggestions and Policy Recommendations

The increasingly frequent misuse of artificial intelligence in cybercrime needs immediate legal and policy reforms. India has a legal framework to manage cyber-crimes, but new technologies like deepfakes, AI-driven impersonation, and automated fraud necessitate additional specialized regulations.

- **Enactment of Specific Legislation on Artificial Intelligence Misuse**

Existing cyber laws may also be strengthened through targeted amendments. For instance, provisions relating to identity theft under **Section 66C** of the Information Technology Act, 2000 should be expanded to explicitly include biometric identity theft and AI-generated impersonation.

Similarly, provisions dealing with cheating by personation under Section 66D of the Information Technology Act, 2000 may be updated to cover automated phishing attacks and AI-powered digital scams. Amendments may also clarify the applicability of cyber laws to synthetic media manipulation, including deepfake videos used for financial fraud, harassment, or political misinformation.

- **Amendment of Existing Cyber Laws**

Existing cyber laws may also be strengthened through targeted amendments. For instance, provisions relating to identity theft under Section 66C of the Information Technology Act, 2000 should be expanded to explicitly include biometric identity theft and AI-generated impersonation. Similarly,

[33] National Crime Records Bureau, Crime in India Report (2023)
[34] National Crime Records Bureau, Crime in India Report (2023)

provisions dealing with cheating by personation under Section 66D of the Information Technology Act, 2000 may be updated to cover automated phishing attacks and AI-powered digital scams[35].

Amendments may also clarify the applicability of cyber laws to synthetic media manipulation, including deepfake videos used for financial fraud, harassment, or political misinformation.

- **Regulation of Deepfake Technology**

Given the growing threat posed by deepfake manipulation, India should develop specific regulatory guidelines governing the creation and dissemination of synthetic media. These regulations could include requirements for disclosure when AI-generated media is used in public communication.

Criminal penalties should also be introduced for the malicious use of deepfake technology in activities such as identity theft, financial fraud, election interference, and non-consensual explicit content. Such measures may help prevent the misuse of artificial intelligence while preserving its legitimate applications in areas such as entertainment and research.

- **Strengthening Digital Forensic Capabilities**

The investigation of AI-driven cybercrime requires advanced technological expertise and specialized forensic tools. Therefore, India must strengthen the capacity of its cybercrime investigation agencies.

Specialized digital forensic laboratories capable of detecting deepfake media and AI-generated content should be established across the country. Law enforcement officials should also receive training in emerging technologies and cyber investigation techniques.

Furthermore, the collaboration between law enforcement agencies, technology companies, and academic institutions may improve the development of tools capable of identifying manipulated digital media[36].

- **Platform Accountability and Intermediary Responsibility**

Online platforms play a significant role in the dissemination of digital content. Consequently, stronger intermediary responsibility frameworks may be necessary to prevent the spread of harmful AI-generated content.

Digital platforms should be required to implement mechanisms for detecting manipulated media and responding promptly to complaints regarding deepfake harassment or identity fraud. Clear reporting mechanisms and content moderation policies may help reduce the circulation of harmful synthetic media on social networking platforms.

- **Public Awareness and Digital Literacy**

Public awareness plays an important role in preventing cybercrime. Many individuals remain unaware of the risks associated with AI-generated misinformation, voice cloning, and online impersonation. Government agencies, educational institutions, and technology organizations should promote digital literacy programs that educate citizens about emerging cyber threats and safe online practices. Greater awareness may help individuals identify suspicious digital content and reduce the likelihood of falling victim to AI-based cyber fraud.

Conclusion

Artificial intelligence has emerged as one of the most transformative technological innovations of the modern era. While AI technologies have the potential to improve efficiency, innovation, and digital governance, their misuse has also created new opportunities for cybercriminal activity. Emerging threats such as deepfake manipulation, AI-driven identity theft, automated phishing, and algorithmic fraud

[35] Information Technology Act, 2000, s. 66C & s. 66D
[36] Supra note 39.

present significant challenges to existing legal frameworks. These technologies allow cybercriminals to conduct sophisticated attacks that are difficult to detect and investigate.

India's cybercrime legislative system, mainly governed by the Information Technology Act of 2000 and related provisions of the Indian Penal Code of 1860 / Bhartiya Nyaya Sanhita of 2023 and Bhartiya Sakshya Adhiniyam, 2023 which provides a fundamental foundation for dealing with digital offences. However, the rapid evolution of artificial intelligence technologies has exposed certain limitations within these laws.

In addition, the enforcement mechanism faces practical challenges such as lack of technical expertise, difficulties in evidence collection, and issues relating to jurisdiction.[37] The intangible and dynamic nature of AI-based cybercrimes further complicates the process of investigation and prosecution. Therefore, mere reliance on existing statutory provisions is insufficient to address the multifaceted nature of these offences. In light of these challenges, there is an urgent need to strengthen the Indian legal framework through timely legislative reforms, capacity building of enforcement agencies, and greater emphasis on cyber awareness.[38] A proactive and adaptive approach is essential to ensure that the law remains effective in regulating emerging technologies while safeguarding individual rights.

In conclusion, Artificial Intelligence, while being a powerful tool for progress, has also become a catalyst for new forms of cybercrime. The Indian legal system must evolve in a dynamic and responsive manner to address these emerging challenges, ensuring a balance between technological innovation and legal accountability.

BIBLIOGRAPHY

Books

1. Pavan Duggal, Cyber Law in India (Universal Law Publishing).
2. Aparna Viswanathan, Cyber Law: Indian and International Perspectives (LexisNexis).
3. Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace (Praeger Publishers).
4. K.D. Gaur, Textbook on Indian Penal Code (LexisNexis).
5. Stuart Russell & Peter Norvig Artificial Intelligence: A Modern Approach. 3rd ed., Pearson Education, 2010.

Journal Articles

1. David Wall, "Cybercrime and the Internet," International Review of Law, Computers and Technology.
2. Susan Brenner, "Cyberstalking and Online Harassment," Journal of Law and Technology.
3. Chesney, Robert & Danielle Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." California Law Review, Vol. 107, 2019.

Reports

1. Ministry of Electronics and Information Technology, Government of India, Cyber Security Policy Reports.
2. National Crime Records Bureau. Crime in India Report. Ministry of Home Affairs, Government of India, 2023.
3. NITI Aayog National Strategy for Artificial Intelligence. Government of India, 2018.

[37] K.K. Nair, Cyber Law in India (LexisNexis, 2019).
[38] Pavan Duggal, Cyber Law in India (Wolters Kluwer, 2021)

4. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework. United States Department of Commerce, 2023.
5. European Commission. White Paper on Artificial Intelligence. European Union, 2020.