Naveen Shodh Sansar (An International Refereed / Peer Review Multidisciplinary Research Journal)
RNI No.- MPHIN/2013/60638, ISSN 2320-8767, E- ISSN 2394-3793, Scientific Journal Impact Factor (SJIF)- 8.054,
October to December 2025, E-Journal, Vol. I, Issue LII (52), ISO 9001:2015 - E2024049304 (QMS)

Emerging Cybercrimes and Artificial Intelligence: Issues for the Indian Legal System

Dr. Anoop Kailasia*

***Asistant Professor, Govt. Law College, Gwalior (M.P.) INDIA**

Abstract: Numerous industries, including healthcare, banking, entertainment, defence, agriculture, education, and transportation, have been completely transformed by artificial intelligence. In the rapidly evolving digital world of today, artificial intelligence has revolutionized numerous industries and has a big impact on cybersecurity in this information technology age. However, this technological advancement also brings with it a number of new challenges, the most significant of which are related to cybersecurity. With more than 800 million internet users and government initiatives like Aadhaar and Digital India, India's digital environment is rapidly evolving. But along with this growth, there are also more bad actors. Not just India, but the entire world is undergoing a major digital transformation. This wave of change is where artificial intelligence's impact is most apparent, presenting both advantages and risks simultaneously. Therefore, it is more important than ever to develop, deploy, and use AI securely so that future generations can accept these advancements with confidence and without hesitation. The evolution of artificial intelligence, its use in cybersecurity, emerging issues, and possible solutions are all examined in this paper. It highlights the benefits of artificial intelligence as well as the problems with its use. The report also discusses legislative reactions, government initiatives, and the issues of AI in cybersecurity. Using case studies and primary and secondary source analysis,the current study emphasizes the significance of artificial intelligence and cyber security in India.

Introduction - In our digital age, the internet connects our phones, banking, businesses, schools, and even government organizations. Since most activities are now conducted online, security concerns have increased significantly, which has resulted in a rise in cybercrimes, data breaches, hacking, and the spread of false information. Artificial intelligence has become a fresh hope in such a predicament. Computers can now think and learn like humans thanks to this technology. AI is being utilized in cybersecurity to identify threats, stop assaults, and react rapidly to any dangers. Behavioural analytics and machine learning techniques are used by AI in cybersecurity to identify patterns and anomalies in massive datasets. This permits the detection of both known and new threats.By taking a proactive attitude, companies may react rapidly and efficiently, decreasing any threats before they have a chance to inflict major damage. The use of AI in cybersecurity has both benefits and drawbacks. On the one hand, AI can detect threats, automate reactions, analyse massive amounts of data to spot anomalies, and even predict future attacks. However, AI-powered tools can also be used by attackers to create malware automatically, create deepfakes for social engineering, and carry out complex attacks. Cyberattacks have significantly increased in India in recent years, surpassing the global average. This highlights the critical need for robust cybersecurity measures, and AI technology can be very useful in solving these challenges. However, the growing application of AI in cybersecurity raises significant ethical concerns, particularly with regard to privacy. This issue requires careful thought because increasing digitalization will have an impact on both the present and the future. In such a scenario, a lot of personal data—including information, images, videos, files, and documents—will be stored online, so it's crucial to address concerns about data breaches and unauthorized distribution.Legal teams can now automate or expedite tasks. Thanks to technological advancements, legal teams can now automate or expedite tasks that entry-level colleagues previously completed. For example, first-year legal associates at law firms sometimes create legal briefs for supervising attorneys and perform legal research. This process used to take a long time, but these days, machine learning-powered search engines and legal research tools can sort through enormous amounts of documents to discover the relevant information in a fraction of the time it would take a human. Furthermore, given a brief cue, AI-powered text generators can quickly create a preliminary draft of a legal brief.

Over the past 20 years, cybercrime has changed dramatically. In the past, hacking, illegal access to computer

systems, and data theft were the main types of cybercrime. Cybercriminals have started using artificial intelligence technology in recent years to carry out increasingly complex and extensive attacks. Automated phishing campaigns, deepfake manipulation, biometric identity theft, and algorithmic fraud are examples of AI-enabled crimes.

Literature Review

In recent years, researchers and academics have looked more closely at the connection between cybercrime and artificial intelligence. Numerous studies have drawn attention to the potential for artificial intelligence technology to be abused for illegal purposes as well as the challenges legal systems confront in regulating these technologies.

In his book Cyber Law in India, Pavan Duggal highlights how technical advancements frequently surpass legal requirements, leaving regulatory gaps that cybercriminals take advantage of. He contends that in order to handle new technical issues, current cyber laws need to be modified.

Similar to this, Aparna Viswanathan notes in Cyber Law: Indian and International Perspectives that artificial intelligence raises complicated questions about accountability and legal culpability. Determining culpability becomes a major difficulty for law enforcement when crimes are perpetrated via automated methods.

Hypothesis: The following hypothesis serves as the foundation for this study:

1. Emerging cybercrimes involving artificial intelligence technologies, like deepfakes, AI-generated identity theft, and automated digital fraud, cannot be adequately addressed by India's current cyber law framework, especially under the Information Technology Act, 2000, and pertinent provisions of the Indian Penal Code, 1860.
2. Stronger digital forensic capabilities, improved regulatory frameworks for online platforms and digital intermediaries, and specific legislative reforms are necessary for India to effectively regulate AI-based criminality.

Objective Of The Study: This research study's main goals are as follows:

1. To investigate artificial intelligence technology' conception, advancement, and effects on the digital ecosystem.
2. To discover and assess developing AI-based cybercrimes, including deepfake technologies, AI-driven identity theft, and automated online fraud.
3. To critically assess the existing legal framework in India governing cybercrime, particularly the provisions of the Information Technology Act, 2000, and other associated statutes.
4. To explore the issues posed by law enforcement authorities in detecting and investigating AI-based cybercrime.

Research Methodology: In this work, legal research is conducted using a doctrinal approach. Examining legal statutes, court decisions, and academic publications on artificial intelligence and cybercrimes forms the study's primary basis.

Among the primary sources consulted for the study are the following:

1. The Information Technology Act of 2000 contains legal provisions.
2. The relevant sections of the Bhartiya Nyaya Sanhita, 2023.
3. Judicial decisions of Indian courts involving cybercrime and electronic evidence.
4. Secondary sources consist of:
5. Books about information technology and cyber law. Scholarly academic publications on cybersecurity and artificial intelligence.
6. Government reports on digital security regulations and trends in cybercrime.

The study intends to assess critically how well India's current legal system handles cybercrimes enabled by artificial intelligence.

Cybercrimes Based on Emerging AI: Numerous new types of cybercrime have been made possible by artificial intelligence, which presents serious difficulties for law enforcement. Automated phishing campaigns are one of the most prevalent uses of artificial intelligence in cybercrime. Some of the most well-known AI-driven cybercrimes include deepfake manipulation, biometric identity theft, AI-powered malware, and algorithmic financial fraud. Cybercriminals may create customized phishing emails that target thousands of victims at once by using AI algorithms. By examining the targeted person's online behaviour and communication patterns, these communications are frequently crafted to seem genuine.

Another new danger is malware driven by AI. In order to avoid detection, such malware systems are able to learn from cybersecurity software's protective features and alter their behaviour accordingly.

But of all the different types of AI-driven cybercrime, identity theft and deepfake manipulation pose the biggest risks because of the potential for financial, psychological, and reputational damage.

Deepfake Technology and Online Crime: The use of artificial intelligence, especially machine learning methods like Generative Adversarial Networks (GANs), to produce incredibly lifelike synthetic media is known as "deepfake technology." With the help of these technologies, people can alter photos, films, and audio files to make them seem real. Although it was first created for research and amusement, it is rapidly being abused for illegal reasons. Cybercriminals can create compromising movies, disseminate false information, or impersonate people using deepfake techniques. Non-consensual synthetic pornography, in which a person's face is superimposed on explicit content without that person's agreement, is one of the most concerning uses of deepfake technology. Such

actions may cause victims to suffer from serious psychological distress and reputational harm.Financial fraud is another possible use for deepfakes. Cybercriminals have successfully used AI-generated voice clones to pose as business executives and approve fraudulent financial transfers in a number of international incidents.

This threat has increased due to deepfake software becoming more widely available. 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 unauthorised 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.

Technology is changing the legal field: Legal teams can now automate or speed up their work. Technology has made it possible for legal teams to automate or speed up operations. Legal teams can now automate or expedite operations that entry-level colleagues previously handled, thanks to technological advancements. by entry-level colleagues. This work was previously completed by entry-level colleagues due to related technological developments. For instance, first-year legal associates at law firms occasionally conduct legal research and prepare legal briefs for supervisory attorneys. These days, machine learning-driven search engines and legal research tools can quickly find the pertinent information by sifting through massive volumes of documents. Additionally, AI-powered text generators can swiftly produce an initial draft of a legal brief given a brief trigger.

Regretfully, AI may also have detrimental effects on the legal industry. For example, AI's capacity to produce deepfake technology (pictures and videos of fictitious events) might disseminate damaging false information. Attorneys who practice intellectual property (IP) law are particularly concerned about these developments.

Additionally, there is a chance that private information will get into the wrong hands because generative AI—the creation of completely original creative works from straightforward prompts after AI is trained on enormous amounts of old material—relies significantly on big data sets. Indeed, class action lawsuits alleging privacy infringement related to generative AI technologies have already been filed.

Indian Laws Relevant to Cybercrimes Using Artificial Intelligence: The Information Technology Act of 2000 governs cybercrime in India. Although the statute does not specifically include AI, several of its clauses may implicitly cover cyber offenses aided by AI.

For example, the Information Technology Act of 2000's Section 66C makes identity theft—which includes the unauthorized use of passwords, electronic signatures, or distinctive identifiers—illegal. This clause might be applicable in situations where artificial intelligence (AI) systems are utilized to fabricate identities or pose as real people in virtual settings. In a similar vein, the Information Technology Act of 2000's Section 66D forbids utilizing computer resources to cheatThis provision may be relevant when voice cloning or AI-generated identities 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 deals with privacy violations caused by the unlawful capture, publishing, or transfer of images of an individual's private area without that individual's consent. Such regulations may be relevant in cases of manipulated photos produced by artificial intelligence (AI) or invasions of privacy through synthetic media. In cases involving deepfake pornography or modified explicit content, authorities may apply Section 67 of the Information Technology Act, 2000, which prohibits the publication or transmission of pornographic content in electronic form. This rule may be applied when deepfake movies are used for sexual exploitation or internet abuse. Apart from the Information Technology Act, various sections of the Indian Penal Code, 1860, and Bhartiya Nyaya Sanhita, 2023, may also apply to AI-driven cybercrimes. For example, offenses like defamation, criminal intimidation, cheating, and impersonation may be employed, depending on the particulars of the case.

The offenses of stalking under Section 354D of the Indian Penal Code, Section 78 (Stalking) of BNS19, 2023, and Section 356 (Defamation) of BNS may also be pertinent in cases involving online harassment or persistent monitoring through digital platforms, especially when AI-generated content is used to harass or threaten people.

From an evidentiary standpoint, the Bharatiya Sakshya Adhiniyam, 2023, governs the validity and authenticity of digital evidence in cybercrime trials. Sections 61, 62, 63, and 66 of the BSA, 2023, provide procedural safeguards for the authentication of electronic records, which the Act acknowledges as admissible evidence.

For instance, the BharatiyaSakshyaAdhiniyam, 2023's Section 61 acknowledges digital and electronic documents as documentary evidence, and Section 63 lays forth requirements for their inclusion. In situations involving deepfake films, artificial intelligence-generated audio recordings, and other types of digital evidence, these clauses become more important.

Despite these clauses, academics contend that the Indian legal system does not specifically address the abuse of artificial intelligence. Concerns about how well the current cyber laws handle new technology threats have been raised by this legislative gap.

Indian Judiciary: India's socioeconomic structure is rapidly becoming digital, which has raised worries regarding cybersecurity and privacy rights protection. The Supreme

Court's historic ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) gave the right to privacy, which is recognized as a fundamental right under Article 21 of the Constitution, final constitutional significance. This decision not only set the criteria of need, proportionality, and constitutionality for assessing governmental intervention, but it also upheld privacy as fundamental to human dignity and individual freedom.The Digital Personal Data Protection Act of 2023 reinforces the Information Technology Act of 2000, which is the primary law governing cybersecurity in India. The DPDP Act establishes a structured framework for data collection, processing, storage, and consent-based governance, while the IT Act deals with cybercrimes such as hacking, identity theft, and unauthorized access. These laws work together to improve digital security and guarantee the responsibility of data fiduciaries.

The judiciary is still crucial in striking a balance between competing state interests, such as public order and national security, and individual privacy. Courts have strengthened restrictions on arbitrary governmental action and established procedural safeguards on surveillance mechanisms through judicial review and constitutional interpretation. This study critically analyses how legislative actions and judicial supervision have shaped India's digital privacy environment, emphasising the necessity of strict enforcement and rights-oriented governance in the age of growing digital infrastructure.

Conclusion : Artificial intelligence has the potential to fortify and protect India's digital future. Using AI technology in a responsible, ethical, and well-considered approach is the best way to counter the growing cyberthreats. AI-based cybersecurity frameworks require collaboration between the government, business, and academic organizations. India's security and independence will also depend on fostering strategic and security cooperation with other countries on a national and international scale.

AI's increasing importance and utility make it essential for protecting the nation's infrastructure. Therefore, it is now necessary rather than optional to include AI in India's cybersecurity policy. By implementing various solutions and adopting a proactive, collaborative approach, India can significantly reduce cybercrime and offer a safer online environment for its citizens and businesses. By addressing certain challenges and leveraging AI's capabilities, India can ensure its people have a secure and prosperous digital future. Effective regulation is crucial because cyber dangers threaten both national security and individual citizens. Significant control over cybercrime cannot be achieved unless individual citizens continue to be informed, vigilant, and take preventative action, even if the government introduced the National Cyber Security Policy in 2013 and updates pertinent laws over time. No matter how strong the legal system is, responsible behavior and public awareness are necessary to effectively prevent cybercrime.

References:-

1. India Must Invest in AI for Cyber and Border Security: Survey', Hindustan, available at: https://www.live hindustan.com/ncr/new
2. delhi/story-india-must-invest-in-ai-for-cyber-and-border-security-survey-201753106554087.
3. National Crime Records Bureau (NCRB), Ministry of Home Affairs, Government of India, available at:
4. https://www.mha.gov.in/en/national-crime-records-bureau-ncrb.
5. 'India Must Invest in AI for Cyber and Border Security: Survey', Hindustan, available at: https:// www.livehindustan.com/ncr/new
6. delhi/story-india-must-invest-in-ai-for-cyber-and-border-security-survey-201753106554087.
7. Information Technology Act, 2000, s. 66C,66D, 66E and section 67.
8. K.D. Gaur, Textbook on the Indian Penal Code (6th ed., Universal Law Publishing, New Delhi, 2016).
9. Section 78 and 356 of BNS, 2023 (45 of 2023)
10. Section 61, 62, 63, 66 of BSA, 2023, (47 of 2023).
11. Aparna Viswanathan, Cyber Law: Indian and International Perspectives (LexisNexis Butterworths, New Delhi, 2012).
12. 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).
13. Federal Bureau of Investigation, Private Industry Notification: Deepfake Audio Used for Corporate Fraud (2019)
14. Information Technology Act, 2000, ss. 66C & 66D (identity theft and cheating by personation using computer resources).

✻✻✻✻✻✻✻✻✻✻✻✻