INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 12 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

"AI AND CYBERCRIME: A GLOBAL OVERVIEW WITH FOCUS ON INDIA"

AUTHOR – SONI, PHD SCHOLAR FROM KURUKSHETRA UNIVERSITY, KURUKSHETRA, HARYANA

BEST CITATION – SONI, "AI AND CYBERCRIME: A GLOBAL OVERVIEW WITH FOCUS ON INDIA", *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (12) OF 2026, PG. 52-61, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

AI is now not limited to laboratories or any industries. Now, it is a part of everyday life and digital life, in areas such as banking, communication, education, health, and online commerce. This technology has created new opportunities for criminals to commit cybercrimes because AI can be used to make fraudulent messages, imitate voices, manipulate videos, and assist criminals in committing cybercrimes. Although AI is a development that has arisen in India, this development raises important legal questions for India. The country has already made laws that apply in several forms to curb these crimes, such as the Information Technology Act, the Bharatiya Nyaya Sanhita, the Digital Personal Data Protection Act, etc. But these rules are not developed so that they can address the challenges that are created by AI.This paper presents and examines the relationship between AI and cybercrime in India. It considers the various ways, or tells us the various ways, through which criminals may exploit AI, and evaluates the Indian legal system. It identifies the legal and institutional responses. This paper argues that India does not need an entirely separate criminal law to tackle AI. But India needs technology friendly laws that can tackle the modern ongoing cybercrimes.

Keywords: AI (Artificial intelligence) ; Cyber-crime ; Online Safety ; Legal-Reform ; Deepfakes crime ; Digital Law

INTRODUCTION-

In today's world, the internet is a basic need of every individual. It means that the internet has changed the livelihood of people because everyone communicates, works, studies, and does everything with the help of the internet nowadays. The internet provides various services that, traditionally, people needed to access physically to perform those activities. Now, those activities can be done by sitting at home with the help of the internet in just seconds using smartphones. For example, financial transactions. All these can be done through UPI by sitting at home with the help of a smartphone. Therefore, the internet provides us with various services that we enjoy by sitting at home, such as digital payments, online banking, government services, and everyday activities, etc.

With the progress of the digital environment, no doubt it provides more opportunities to people, but it also creates opportunities for criminal activities because cybercriminals have now moved from simple forms of online fraud to specialised or sophisticated methods used to commit cybercrimes. Now, AI also adds a layer to these cybercrimes because AI is quick, cheap, and convincing, and with the development of AI, cybercrimes are becoming easier to commit.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 12 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

From a broader perspective, we cannot say that AI is a criminal technology. It is a tool, like other technologies; it is just a tool that we can use, and it is made to perform or simplify work easily. But its misuse is going on. For example, AI can be used by a person to write or translate a document from one language to another. But that can be used by the same person to prepare deceptive messages or to commit cybercrime against another person. Therefore, AI is highly misused by people.

So now, it creates problems in criminal law because cybercrimes are increasing day by day. AI does not create entirely new offences, but it changes the way of committing them. A fraudulent transaction remains fraudulent, but with the help of an AI-generated voice, it can be used to persuade the victim. And AI makes investigations complicated because it is difficult to find out who is controlling the system, who is giving the relevant instructions to commit that crime, who is benefiting from committing that crime, and who is responsible for committing that crime by using the technology. So, it makes investigations very complicated.

So, AI is creating problems in the criminal system. It creates evidentiary problems as well. How? It creates evidentiary problems in voice recordings, photographs, and videos because they can now be artificially generated with the use of AI. So, how can we rely on them?

India already possesses various cyber bodies and criminal laws, such as the Information Technology Act, the Bharatiya Nyaya Sanhita, 2023, and the Digital Personal Data Protection Act, 2023. All these govern the digital environment, or we can say cybercrimes in India. But the real issue is whether India has a law that mentions AI. The more important question is whether the existing legal system is flexible enough to govern, tackle, or provide speedy resolution for such cybercrimes.

This paper will examine or consider all such issues, including how AI is used to commit various cybercrimes, what the major gaps are in the enforcement and evidence of the Indian legal system, and how we can reform them in comparison with other countries.

Literature review –

In this article the author examine the judicial precedents, literature, and reports in order to identify the central issue. Thus, the author uses Indian laws, including the Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023, and international treaties and conventions, to analyze the gaps in the legislation concerning AI-related crimes.

The review of academic journals, legal literature, and reports published by government of India .In, the National Cyber Crime Reporting Portal, and other organizations was conducted to support the author's arguments and identify the extent of the issue. The findings of the study were compared to similar research conducted by foreign analysts in order to come to a conclusion regarding the legislative changes required to address crimes committed with the help of artificial intelligence.

Research Methodology –

The article is based on a doctrinal research method applying legal research techniques in it.

There is a need for more stringent laws that can adequately tackle AI-driven changes in cybercrime and effectively deal with cybercrimes through Indian laws and institutions, so that cybercrimes can be curbed and there can be further development in Indian laws and institutions.

At present, studies on AI and cybercrimes show that AI is both a useful tool for cybersecurity and a technology that can strengthen criminal cyber activities. In this article, I highlight the use of AI for committing cybercrimes such as phishing, social engineering, deepfakes, identity fraud, etc. The literature also indicates that crimes can be more difficult to detect because criminals may use technology to hide evidence.

This study mainly focuses on legal challenges such as the authenticity of digital evidence, harms related to deepfakes, misuse of seized data, and misuse of payment platforms in the name of or for the purpose of providing services. It tries to identify the limitations present in the existing legal framework and suggests changes to the legal framework of the Indian system so that cybercrimes committed through the use of AI can be addressed effectively.

HOW AI IS CHANGING CYBERCRIME

One of the important characteristics of AI-driven cybercrimes is that, in very little time and with technical support, AI-related cybercrimes require little effort but can target a large number of victims by using AI.

There are the following cybercrimes which are done because of AI.

- **AI-Enhanced Phishing and Social Engineering**

In this, phishing is not a new crime. It is one of the oldest ones. And it is also one of the common forms of cyber fraud. But criminals generally try to attempt or create a conversation with the victim in a way that they can trust them. They behave like a trusted person, such as a bank, government department, or online service provider. By gaining the trust, they persuade the victim. Their objective may vary in different situations, such as they can do it to obtain the password, to obtain their financial information, to get their authentication codes, or any other sensitive information so that they can misuse it.

Earlier, there were phishing messages which were easy to recognize because there was no use of AI earlier in those messages, and because of that, those messages were easy to understand because of their poor grammar, generic language, and obvious inconsistent use of words. But by using AI, now phishing messages are also created like actual messages, because of which now it is not easy to understand or recognize whether those messages are genuine or not.

Now, on the other hand, when criminals use AI tools, they produce messages which are so accurate that the recipient always fails to recognize them. Information available on social media and public platforms is used to show them or to gain their trust so that the communication appears to be more personal, because they have all the information gathered from social media accounts or any other public platforms.

From a legal perspective, if we see, the main difficulty is not the creation of the message or recognizing it. But the main difficult task is connecting the message or finding the message in a way that connects the message with the person who is responsible for committing that fraud. Or it is difficult to find out who is behind that message or what the intention behind that is. This requires reliable and valid digital evidence, which is not easy to find. And it can be found out by effective cooperation between the

investigators and the institutions involved, and if there are stringent laws which can deal with AI-related crimes.

- **Deepfakes and Cloned Voices**

Deepfakes have gained attention because of their ability to make people appear or show people things that never actually happened. Deepfakes are fake things that are genuinely, or we can say, at present, not in existence. They are totally fake, such as AI-generated audio that can simply reproduce the aspect of any person's voice, which is relatively equal to their voice. Any videos with respect to any person, which actually do not belong to him, but are created by using his identity, are deepfake videos.

Their consequences can be serious because, in such types of incidents, a criminal can impersonate any company executive as well, who is highly dignified, and by using his identity, he can instruct the employee to transfer the money. Because of that, there may be a huge loss that can be suffered. Another incident is that a cloned voice can be used to convince the family member of that person or any relative of that person that he is in an emergency and is in need of something, and their family can suffer the loss. Any manipulated video of someone's reputation can also destroy his life because of that deepfake video.

So, the problem is that people trust familiar faces and voices. It is not their fault. They cannot recognize whether it is fake or not. It is the common belief that people trust familiar faces and voices. So, they will trust them. A victim who receives any call or anything related to deepfakes cannot suspect it. So, there will be a huge, serious consequence that can be suffered by them.

Indian laws have some provisions to deal with them, but they are not completely sufficient. They are not exhaustive laws. Indian laws have the IT Act, BNS, and IT Rules. They may be prevalent, but the government has also not been able to recognize deepfakes as a form of cybercrime. And it is not a random statement. This is reported by the National Cybercrime Reporting Portal. So, when the government cannot recognize such a form of deepfake cybercrime, then how can a common man recognize it?

Therefore, there is a difficulty that there is still no single, exhaustive, or complete statutory framework that can deal with such types of deepfake crimes.

- **AI-Assisted Cyberattacks**

Deepfakes have gained attention because of their ability to make people appear or show people things that never actually happened. Deepfakes are fake things that are genuinely, or we can say, at present, not in existence. They are totally fake, such as AI-generated audio that can simply reproduce the aspect of any person's voice, which is relatively equal to their voice. Any videos with respect to any person, which actually do not belong to him, but are created by using his identity, are deepfake videos.

Their consequences can be serious because, in such types of incidents, a criminal can impersonate any company executive as well, who is highly dignified, and by using his identity, he can instruct the employee to transfer the money. Because of that, there may be a huge loss that can be suffered. Another incident is that a cloned voice can be used to convince the family member of that person or any relative of that person that he is in an emergency and is in need of something, and their family can

suffer the loss. Any manipulated video of someone's reputation can also destroy his life because of that deepfake video.

So, the problem is that people trust familiar faces and voices. It is not their fault. They cannot recognize whether it is fake or not. It is the common belief that people trust familiar faces and voices. So, they will trust them. A victim who receives any call or anything related to deepfakes cannot suspect it. So, there will be a huge, serious consequence that can be suffered by them.

Indian laws have some provisions to deal with them, but they are not completely sufficient. They are not exhaustive laws. Indian laws have the IT Act, BNS, and IT Rules. They may be prevalent, but the government has also not been able to recognize deepfakes as a form of cybercrime. And it is not a random statement. This is reported by the National Cybercrime Reporting Portal. So, when the government cannot recognize such a form of deepfake cybercrime, then how can a common man recognize it?

Therefore, there is a difficulty that there is still no single, exhaustive, or complete statutory framework that can deal with such types of deepfake crimes.

- **Attacking AI-Based Security Systems**

By increasing the use of AI, it is also being used as a defensive tool. Banks use it to identify transactions, email providers use machine learning to detect suspicious communications, and organizations use it to monitor their usual day-to-day activities. However, defensive AI systems can also become targets. Attackers can identify the weaknesses of these systems, gather information about them, manipulate their inputs, and, by hacking them, misuse them. In cybersecurity, this is a broader problem, and the legal implications of such attacks can be significant. If an organization is heavily reliant on such AI tools, then the consequences can be very serious. Their financial transactions, personal information, critical infrastructure, communication strategies, and security can be at higher risk. So, it is not safe to use AI in such systems.

INDIA'S LEGAL FRAMEWORK

- **Information Technology Act, 2000**

This Act is the central legislation governing cyber law in India. The Act provides legal recognition to electronic records and electronic transactions and contains provisions dealing with various types of cybercrimes and cyber misconduct. This Act is not new legislation. It was enacted in 2000, and at that time, the digital environment was very different from what it is today. We cannot deny the fact that this legislation has dealt with cybercrime significantly over the years. However, for modern AI-driven crimes, this Act is not sufficient.

The major merit of this Act is that it is technology-neutral, which means that it is applicable to computer resources using AI as well as to other computer devices, regardless of whether they are AI-generated or not. Therefore, it can be considered technology-neutral. This neutrality is necessary because the law cannot be changed every time a new technology emerges. Thus, it is one of the biggest advantages of the Act. However, it also creates various uncertainties for courts and investigators while dealing with

cybercrimes and situations arising from crimes that cannot be adequately addressed under this enactment.

- **Bharatiya Nyaya Sanhita, 2023**

  The BNS replaced the IPC. The IPC was a very old law that was introduced in India during British rule. At present, the BNS is the primary criminal law in the Indian legal system. It is relevant here because many technology-related or AI-enabled offenses, such as misconduct, cheating, impersonation, defamation, etc., are dealt with under the BNS.

  When technology is used to commit a crime, it does not mean that it changes the essential character of the offense. The motive behind the offense remains the same. It does not automatically or completely change the nature of the offense simply because technology is used to commit that crime. For example, if a person deceives another person by using an AI-generated voice message, it is still deception carried out by that person against the victim. Just because an AI-generated voice is used, it does not change the fundamental nature of the crime.

  So, we can say that the BNS adopts a flexible approach and is also relevant in this context. However, it cannot be said that the BNS itself can solve all technological problems. Nevertheless, it can be used to curb and tackle cybercrimes and other technology-related offenses.

- **Digital Personal Data Protection Act, 2023**

  This Act primarily deals with the protection of personal data, particularly digital data, so that it cannot be leaked or misused. It is relevant because, in the world of AI, a large amount of information and a large number of systems are dependent on AI. In such cases, data can be leaked, which can cause major and irreparable loss. Such risks can be addressed through this Act.

  Criminals use personal data to exploit victims. They use this information to create fraudulent identities, through which they can target the public by convincing them through those fraudulent identities. The DPDP Act is a general data protection statute. Its purpose is to govern data and protect it. Therefore, the misuse of AI requires data protection rules to curb such crimes. Therefore, this Act is relevantly applicable here.

- **Information Technology Rules**

  See, the IT Rules provide some obligations, which deal with online platforms as well as intermediaries. Their relevance is increased by the increased use of synthetic media and because of manipulated content, which is shared widely, worldwide. That is why this Act is relevant to control such things. The government addresses these issues and tries to stop the misuse of such information of common people and deepfakes and misleading content, which are widespread by criminals. That is controlled by the government by the use of such rules. Therefore, Information Technology Rules are required. The government recognizes such things and takes measures to control such harmful acts. We can say that, by seeing such developments, India, the Indian legal system, is developing its cybercriminal laws by making such Information Technology Rules, so that the challenges which are faced by society or the

government because of such cybercriminals on the platforms can be managed. So, therefore, to control such activities, this Act plays a significant role. This Information Technology Rules Act plays a significant role.

MAJOR CHALLENGES IN THE EXISTING FRAMEWORK

- Identifying the accused Person

  Because in AI-generated crimes, it is not easy for the investigators to find out by whom the crime is committed, and therefore it is very difficult for the investigating officers. So, there should be some measure or there should be some method which should be involved, or there should be some law which can be used to identify that person.

- Cross-Border Investigations

  The second major issue which is faced by the investigating agencies is that there are geographical boundaries while doing the investigation related to cross-border crimes. So, it is very difficult to find out the victim, the offender, which service is used to commit that crime, which internet infrastructure is used, because the crimes can be committed from different jurisdictions, which can be located sometimes outside the country as well. So, it's a major issue to obtain or to find out the evidence related to such crimes and to identify such criminals who commit that cybercrime. So, there should be some law to deal with this also.

- Reliability of Digital Evidence

  The third major issue is that we can't rely on the digital evidence because it can also be fabricated. Because now the audio and videos cannot be reliable sources because, with the use of AI, they can also be fabricated. So, how can we rely on the digital evidence? So, that's also the major issue which is faced nowadays.

- Responsibility of Platforms and Technology Providers

  The fourth major issue is that there are so many companies, technological companies, which provide various services, which can be used for both legitimate as well as illegitimate purposes. But it's difficult to locate them and to find out who is responsible behind such things. So, the developers of such platforms also encourage such cybercrimes, and it's very difficult to deal with them.

Critical Gaps in the Current Framework

From the Indian legal framework, it can be seen that the following gaps are prevalent:

- There is no law specifically defining or criminalizing deepfakes for the purpose of fraud, extortion or harm.
- No law states the criminal and civil liabilities of the technology companies for developing and deploying AI technologies that could foreseeably be used in committing crimes.
- No law mandates companies that deploy AI technologies to keep auditable and unalterable logs of the process through which the AI system was deployed in committing the crime.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 12 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

- No law mandates the digital labeling or watermarking of AI-generated content to allow the identification and tracing of that content.
- The jurisdiction rules under the IT Act are insufficient when the AI system, the operators of the system, and the victims of the crime reside in separate nations.
- There are no explicit protections for the security researcher when the offensive AI tools are used during security tests.

Country / Region	Main Law	Year Written	Covers AI Crime?
United States	Computer Fraud and Abuse Act	1986	No
United Kingdom	Computer Misuse Act	1990	No
India	Information Technology Act	2000	No
International	Budapest Convention	2001	No
European Union	EU AI Act	2024	Partially
China	Cybersecurity Law	2017	Partially

What New Laws and Policies Do We Need?

Table of the key reform areas and recommendations:

Area of Reform	Current Gap in India	Recommended Change
AI Fraud & Phishing	IT Act 2000 does not define AI-generated fraud	Add specific provisions for AI-enabled fraud in BNS/IT Act
Deepfake Crimes	No dedicated deepfake law; only indirect provisions	Enact a standalone Deepfake Prohibition and Regulation Act
Corporate Accountability	No liability for AI tool developers	Introduce product liability for negligent AI deployment

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 12 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Area of Reform	Current Gap in India	Recommended Change
Evidence & Logs	No requirement to maintain AI audit logs	Mandate tamper-proof AI activity logs for legal proceedings
Jurisdiction	Cross-border gaps under IT Act	Bilateral cybercrime treaties and MLAT modernization
AI Watermarking	No law requiring AI content labelling	Mandate digital watermarks on all AI-generated content

Conclusion

Cybercrimes are not a new term or a thing with which we are not familiar. Cybercrime, in its traditional form, or we can say in the past, was also a prevailing crime, but the nature of cybercrime has changed just because of AI. Now we can say that AI is also another tool which is used by criminals to add another technological tool to commit the crime. But here, the concern is that AI can do such types of crimes, such as fraud or any cyberattack, which is faster and very easier to do, but we can't track them easily. Their investigation is very, very difficult and complicated just because of the use of AI. So, it gives an edge to criminals to commit more cybercrimes.

Although India has various legal Acts or provisions, we can say, which effectively deal with cybercrimes, such as the IT Act, BNS, DPDP Act, and IT Rules, which give a good foundation to the cyber laws of the Indian system. But there is a gap in such laws, which can't say that AI-related cybercrime can be dealt with by these laws effectively, because these laws are not exhaustive if we talk in respect of AI-related cybercrimes. So, it's a need of the hour that we should create some modern laws which comply with AI-related laws.

Because AI-related crimes are very difficult to investigate, investigating agencies face very difficulty, and if we talk about the evidence also, it's very difficult to produce evidence and it's very difficult to find out who the person is behind that crime and who committed that crime, from where he committed that crime, and what's the intention behind that. Because by the use of AI, it's very easy to manipulate the identity of the criminal. So, by using AI, a person can manipulate the identity of the victim as well as the criminal as well. So, it's the biggest issue which we can say in the existing criminal system, which we can't effectively deal with by the existing laws.

At the same time, there should be stronger agencies, we can say forensic agencies, which should be AI-friendly, or we can say, should be so much advanced that they can, you know, track AI-related cybercrimes effectively. So, there is jurisdictional error as well as sometimes, like, for example, one person sitting in Canada and by using AI or AI-related tools, he is committing the crime in India. So, now it's very difficult to find out who committed that crime or find that person who is responsible behind that crime. So, it's a very major issue.

Therefore, we need such laws in the Indian system which should be neutral in manner. We can call them technology-neutral laws which can curb out all these gaps, which are prevalent in the existing legal system. The existing laws are, you know, general laws, which we can say that are available to deal with the cyber laws. But because now AI is also present or prevalent, so with the progress of such technological development of AI, law should also be developed in such a way that we can curb out or we can deal with AI-related laws effectively.

And it's not about only India. If we talk on a broader level also, it's a worldwide issue. So, countries must work together to curb all these issues. Countries should help each other to come out from this problem. For example, developed countries can help the developing countries, so that they can make technology-effective laws, which can effectively deal with AI-generated laws. Therefore, we can say it's not only an Indian problem. It's a worldwide problem, and every country must take suitable measures for such AI-related crimes.

Reference List

1. Government of India, The Information Technology Act, 2000, Act No. 21 of 2000.
2. Government of India, The Bharatiya Nyaya Sanhita, 2023, Act No. 45 of 2023.
3. Government of India, The Bharatiya Sakshya Adhiniyam, 2023, Act No. 47 of 2023.
4. Government of India, The Digital Personal Data Protection Act, 2023, Act No. 22 of 2023.
5. Ministry of Electronics and Information Technology, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended.
6. Ministry of Electronics and Information Technology, Government of India, materials concerning synthetically generated information and intermediary obligations.
7. Ministry of Home Affairs, Government of India, materials relating to the National Cyber Crime Reporting Portal and cybercrime prevention.
8. Indian Computer Emergency Response Team (CERT-In), cybersecurity advisories and guidance on emerging cyber threats.
9. Ministry of Home Affairs, Government of India, materials relating to the Indian Cybercrime Coordination Centre (I4C).
10. European Union, Regulation (EU) 2024/1689 — Artificial Intelligence Act.
11. Council of Europe, Convention on Cybercrime (Budapest Convention).