INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 3, March 2026 | ISSN: 2456-4184 | IJNRD.ORG

AI in the Courtroom: The Admissibility of Cyber-Forensic Evidence in Narcotics Trials.

Nazia Shabbir
LLM
Amity University, Noida, India

Abstract:

The high development of digital technologies has dramatically changed the quality of narcotics trafficking in the world. The illicit networks of drugs have started using encrypted communication platforms, social media, and the dark-web platforms that allow transactions and coordination across the borders anonymously. The developments have posed a big challenge to law-enforcement agencies because the use of conventional investigative techniques is usually not enough to identify and unravel technologically advanced networks of traffickers. As a result, law enforcement agencies have been implementing AI and other sophisticated cyber-forensic technologies more frequently to process large amounts of digital evidence and extract criminal behaviour patterns.

Artificial intelligence allows researchers to analyze electronic evidence including emails, chat history, the record of transactions and geolocation information more effectively than traditional forensic tools. Nevertheless, the increasing use of AI-supported cyber-forensic analysis has become a source of major legal concerns about the admissibility, reliability, and transparency of such evidence in the criminal proceedings. In the Indian legal system, the admissibility of the electronic evidence has developed or rather changed through the judicial interpretation of the Indian Evidence Act, Section 65B, and the further enactment of the Bharatiya Sakshya Adhiniyam, 2023. Although these legal changes have enhanced procedural protections of digital evidence, the growing application of algorithm analysis presents new difficulties of the evidence.

This is of special concern in cases prosecuted under the Narcotic Drugs and Psychotropic Substances Act, 1985 that sets forth rigid penalties and statutory presumptions on possession and culpable mental state. The given paper will discuss the admissibility of AI-assisted cyber-forensic evidence in the narcotics cases, analyze the changing statutory landscape, and suggest the legal changes that could help to establish a sense of transparency, reliability, and fairness involving the use of algorithmic evidence in the context of the criminal justice system.

Keywords: Artificial Intelligence, Cyber-Forensics, NDPS Act, Electronic Evidence, Bharatiya Sakshya Adhiniyam, Dark Web.

I. Introduction:

The fast change of digital technologies has had a great impact on the organization and functioning of illegal drug trafficking on the planet. Historically, the distribution of narcotics was based on physical distribution channels, go-between, and physical interaction between buyers and sellers. Nevertheless, the invention of the internet, coded communication systems, and electronic methods of paying money have changed the way narcotics are manufactured, sold and supplied. Currently, drug trafficking systems are becoming more and more online based, using encrypted message applications and dark-web markets where anonymous money can be conducted across borders. This has led to new problems with the law-enforcement agencies in their apprehension and prosecution of drug-related crime.

The dark web has resultingly emerged as a large marketplace in illicit drugs. The functionality of these marketplaces on the Internet is based on the anonymising networks that hide the identity and location of users. Buyers and sellers use encrypted channels to transact business with the sellers advertising narcotic substances on pseudonymous profiles. Cryptocurrencies are frequently used to make payments and offer an extra degree of anonymity as well as complicate financial tracking. Consequently, electronic devices, online transactions

and digital communication data have become very important sources of evidence in recent narcotics investigations.[1]

Cyber-forensic methods of collecting and analysing digital evidence have therefore become more important to investigative agencies in response to these developments. Cyber-forensics can be described as a scientific endeavour of the identification, preservation, extraction and analysis of the electronic information of digital devices with the aim of criminal investigation. Smartphones, laptops, cloud storage platforms, and other online gadgets are often full of valuable data concerning communication patterns, financial activities, location history and internet behaviour. Such data when studied well can expose how narcotics trafficking networks work.[2]

The artificial intelligence has gone ahead to increase the scope of cyber-forensic investigations. Analytical tools that are powered by AI can handle large amounts of digital data in a few seconds. Machine learning, automated pattern recognition, and data mining are some of the techniques that allow investigators to pick out suspicious patterns of communication, discover hidden relationships among people, and recreate criminal activity timelines.[3] These functions come in especially handy when the investigator has to examine massive amounts of data in the form of emails, chat logs, financial records, and geolocation data.

With such benefits, there exist serious legal issues of using artificial intelligence in criminal investigations. A significant problem is associated with transparency and explainability of an algorithmic analysis. Most artificial intelligence systems are based on complicated computational mechanisms by which big datasets are processed and produce predictive or analytical outcomes. The associated reasoning, however, can be very challenging to comprehend or describe, especially the reasoning behind these algorithms. This has been termed as the black box problem and this poses a challenge to the courts that have to determine the reliability and value of such technological findings as evidence.[4]

Admissibility of electronic evidence in India has gone through the process of both law reforms and judicial interpretation. In the case of Anvar P.V. v. P.K. Basheer[5] and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal[6] gave the procedural requirements of admitting electronic records under the Indian Evidence Act. However, more recently, Bharatiya Sakshya Adhiniyam, 2023, has proposed new provisions, with specific regard to electronic evidence and electronic documentation in a criminal trial.[7]

These changes get very important especially in the prosecutions that are done under the Narcotic Drugs and Psychotropic Substances Act, 1985. The NDPS Act is full of strict terms such as harsh statutory penalties and statutory presumptions meant to cover possession and culpable mental condition.[8] Under these conditions, reliability and authenticity of the digital evidence take of paramount importance to make sure that the accused is given a fair trial.

It is against this backdrop that the current paper will discuss admissibility of AI-aided cyber-forensic evidence in narcotics cases in the Indian legal system. It examines the changing legislative acts that govern electronic evidence, discusses the application of artificial intelligence to cyber-forensic investigations, and discusses the issues surrounding an algorithmic evidence in a criminal trial. The paper also puts into consideration the developments on comparative legal developments and offers reforms to achieve transparency, accountability and fairness in the application of artificial intelligence in criminal justice system.

[1] O. Dunsin, A. Adeyemi & K. Olaitan, "Artificial Intelligence and Digital Forensics in Cybercrime Investigations," *Journal of Digital Forensics, Security and Law*, Vol. 19, 2024.
[2] R. Singh & S. Gautam, "Artificial Intelligence Techniques in Cyber-Forensic Investigations," *Indian Journal of Law and Technology*, Vol. 18, 2022, pp. 65-82.
[3] Id.
[4] K. Kelly, T. McBride & L. Sanders, "Explainable Artificial Intelligence in Legal Decision-Making," *Artificial Intelligence and Law*, Vol. 28, 2020.
[5] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
[6] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
[7] Bharatiya Sakshya Adhiniyam, 2023, s. 63.
[8] Narcotic Drugs and Psychotropic Substances Act, 1985, ss. 35, 54.

II. The Statutory Framework: From the Indian Evidence Act to the Bharatiya Sakshya Adhiniyam, 2023:

The admissibility of electronic evidence in India has been changing with the current explosive growth of digital technologies and the further involvement of electronic communication in contemporary criminal investigation. Computers, smartphones, and cloud storage systems usually have important information associated with communications, financial transactions, and online activities. Given that this type of information can easily be modified or manipulated, the law has come up with special procedures intended to ascertain authenticity and reliability of electronic evidence prior to the court of law admitting it. The abolition of Indian Evidence Act, 1872 and the implementation of the Bharatiya Sakshya Adhiniyam, 2023 is an essential step towards controlling digital evidence in India.[9]

Prior to the advent of mass digital technology the Indian Evidence Act dealt mainly with the old forms of evidence like oral evidence and written evidence. Nevertheless, the steep rise in electronic communication necessitated the need to identify the digital records as a valid type of evidence. In response to this requirement, the Information Technology Act, 2000 made amendments on Indian Evidence Act. Among the most significant changes was the addition of Section 65B that introduced a special process of the admissibility of electronic records in a court of law.[10]

Section 65B stated that electronic records were admissible to evidence in case they were accompanied by a certificate that testified to authenticity of the record and the reliability of the means by which the record was produced. This certificate was to be given by an individual that was in charge of running the said computer system or management of the digital equipment. The certification requirement was meant to assure the court that the electronic evidence provided was not altered and manipulated in the process of collection or reproduction.[11]

Although the statutory terms exist, some uncertainty arose out of how Section 65B should be interpreted first. In State (NCT of Delhi) v. Supreme Court ruled that an electronic evidence would be admissible without a Section 65B certificate, but the authenticity of such electronic evidence should be determined otherwise.[12] This ruling brought about confusion on whether the certification requirement was binding or not.

Supposedly later on, the Supreme Court explained the issue in Anvar P.V. v. P.K. Basheer. The Court decided that Section 65B was a full code on the admissibility of electronic evidence and that its certification provision was obligatory.[13] The Court pointed out that electronic records are prone to manipulation and thus, a tight procedural protection is necessary to safeguard the evidentiary value of electronic records.

Arjun Panditrao Khotkar v. is a case, in which the Supreme Court reinstated this principle. Kailash Kushanrao Gorantyal where it was held that the certificate pursuant to Section 65B is one of the necessary condition to admit electronic evidence.[14] This ruling closed the case on the legal front and Tipped the scales in favour of the procedural framework of digital evidence.

In India, a modernised evidentiary system, with electronic evidence expressly identified, was established with the adoption of the Bharatiya Sakshya Adhiniyam, 2023. The new law section 63 gives the procedural requirements used to admit electronic records and the relevance of authenticating the digital data integrity.[15] The use of hash values is an important characteristic of the new framework that operates as digital fingerprints to facilitate in establishing the authenticity of electronic records.

The Bharatiya Sakshya Adhiniyam further explains the difference between a primary and a secondary electronic evidence. In case the original device on which digital information is stored is manufactured prior to

[9] A. Malik, "Digital Evidence and the Bharatiya Sakshya Adhiniyam: A New Framework for Electronic Records," *Journal of Indian Law and Society*, Vol. 15, 2024.
[10] Information Technology Act, 2000, s. 92 (amending the Indian Evidence Act, 1872).
[11] Indian Evidence Act, 1872, s. 65B.
[12] *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600.
[13] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
[14] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
[15] Bharatiya Sakshya Adhiniyam, 2023, s. 63.

the court, it can be considered a primary evidence. Nevertheless, presentation of copies of digital records should be accompanied by proper certification in order to determine authenticity.[16]

Altogether, the replacement of the Indian Evidence Act with the Bharatiya Sakshya Adhiniyam is an attempt to adjust the evidentiary law to the conditions of the digital era. The new framework aims at enhancing the credibility of digital evidence in a criminal case by creating better protocols on how to authenticate and verify electronic records.

III. AI Applications in Cyber-Forensics:

The high pace of development of digital technology of communication has greatly increased the amount of electronic information used in criminal investigations. When it comes to investigating the cases involving narcotics trafficking, investigators are often presented with vast amounts of electronic evidence stored on the electronic infrastructure in the form of smartphones, laptops, tablets, and the cloud-based systems. These devices might harbor communication history, money transactions, location history, web histories and other types of computer-generated evidence that can be useful in crimes. Traditional methods of investigating such large data are usually slow and unproductive. Due to this, police organizations are increasingly implementing artificial intelligence systems to help them in cyber-forensics.[17]

Artificial intelligence can be defined as a computer system that is used to accomplish functions that usually involve human intelligence such as pattern recognition, language processing and data analysis. AI-enabled tools in the context of cyber-forensics apply machine learning algorithms and data mining algorithms that are fully Automated to process digital evidence in a more efficient way. These tools help the investigators to trace the trends in communication, suspicious behaviour, and recreate the chronology of events related to criminal activities.[18] Such analytical abilities are specifically helpful in the context of narcotics studies, as drug trafficking organizations tend to engage heavily in online transactions and digital communication services.

Pattern recognition in online communication is one of the greatest applications of AI in cyber-forensics. The algorithm of machine learning is able to scan emails, chat messages, call records and social media communications and recognise the patterns that can signify criminal behaviour. To illustrate, AI applications can identify recurrent contact between the individuals suspected to be involved in the networks of narcotics trafficking or identify the strange communication patterns that might hint at the organized illegal actions. The ability to identify patterns that a human investigator might not easily identify by looking at the data enables AI tools to examine large amounts of data more quickly to reveal the relationships within it.[19]

Electronic discovery is another useful application of artificial intelligence, also referred to as e-discovery. Millions of documents, messages and files can be stored in digital devices and they need to be investigated. It can be very time consuming to go through these materials by a manual review. E-discovery tools which are based on AI can automatically classify, group and rank digital documents based on their relevance to the investigation. AI systems assist investigators to narrow down on the most valuable evidence in a case by sifting through large volumes of data and pinpointing the evidence that could be the most important.[20]

Network analysis of criminal organisations is also commonly applied to artificial intelligence. It is a typical case where drug trafficking activities are conducted by a number of people who play various roles in a distribution network. The AIs can be used to analyze the communication patterns of people and draw visual social network maps. These maps demonstrate the manner in which the various members of the criminal network relate to one another and assist the investigators to identify the key organisers, intermediaries as well as distributors of the activity. This knowledge of these relationships is very important in breaking down the organised drug trafficking networks.

The other significant field in which AI has been applied in cyber-forensic investigations is in transaction analysis of cryptocurrency. Narcotics marketplaces online are often supported by cryptocurrencies like Bitcoin

[16] Id.
[17] R. Singh & S. Gautam, "Artificial Intelligence Techniques in Cyber-Forensic Investigations," *Indian Journal of Law and Technology*, Vol. 18, 2022.
[18] Id.
[19] Id.
[20] Id.

to perform financial operations. Even though the use of blockchain technology traces everything in a ledger that is publicly accessible, it may be quite challenging to establish the identity of users behind cryptocurrency wallets. Tools based on AI will be able to study transaction patterns in blockchain networks and track the relationship between various digital wallets. This study can assist investigators to track financial transactions relating to illegal drug markets and those engaging in such transactions.

Artificial intelligence could also be seen as the key to monitoring the so-called dark-market places where illegal narcotics are actively sold. Dark-web stores function by encrypted networks where the users and the whereabouts of the servers on which the marketplace is housed are not known. Artificial intelligence can be used to scan the listings of vendors, the history of transactions, and user activity in such websites. Machine learning can identify new markets of drugs, suspicious traders and price trends in various markets. The data is useful in informing investigators about the arrangement and operations of internet drug trafficking groups.[21]

One more useful AI usage in cyber-forensics is the ability to rebuild digital timeline. Investigations of criminals are usually the cases where it is important to determine the sequence of events that resulted into the occurrence of an offence. Timestamps across the different digital sources like emails, messaging applications and location data can be analysed with AI tools and help to recreating a timeline of activities in chronological order. Integrating the news of various online sources would allow investigators to comprehend the way a criminal operation evolved and how various people were involved in it.

Language analysis and translation can also be done with the help of artificial intelligence. Drug traffickers frequently make sure that they communicate in a coded language or slang to hide the real meaning behind the communication. There is the use of natural language processing technologies to enable AI systems to process textual communications and detect patterns that could signal criminal intent. These tools are also capable of translating messages in various languages and this is very crucial especially when it comes to dealing with international drug trafficking cartels.

Along with these merits, it should be noted that AI-based forensic tools can be utilized as investigational tools but not as sources of proof in the first place. The outputs of such systems have to be confirmed by undertaking the due forensic measures and in addition to this they have to be supported by the testimony of an expert when they are presented in the court. The investigators should make sure that the digital evidence obtained by the aid of AI-enhanced analysis is appropriately preserved, documented and authenticated according to the law. In Som Prakash v. State of Delhi, the Supreme Court observed that scientific methods can assist courts in determining the guilt of an accused person when properly explained and verified.[22]

In general, AI has significantly increased the capacity of the police force to research intricate digital data concerning narcotics cases. AI can assist investigators by allowing them to conduct fast analysis of massive amounts of data, uncovering concealed relationships, suspecting activities, and re-creating criminal events. Yet, these technologies should be used in relation to the proper legal protection as the applicability and admissibility of cyber-forensic evidence in the trials should be provided through the appropriate legal protection.

IV. Admissibility and Reliability Challenges:

The increased application of the artificial intelligence to cyber-forensic investigations has opened new avenues to the analysis of digital evidence in a criminal case. It has also simultaneously brought a number of legal problems on the admissibility and reliability of such evidence in the courts of law. In the criminal cases especially where the offence committed is narcotics, the courts are required to make sure that the evidence produced meets the standard of proof beyond reasonable doubt. Although the AI-based tools may help the investigator detect trends and examine the mass data, the findings of such systems will have to pass the set evidentiary standards prior to being trusted in the court ruling.[23]

[21] O. Dunsin, A. Adeyemi & K. Olaitan, "Artificial Intelligence and Digital Forensics in Cybercrime Investigations," *Journal of Digital Forensics, Security and Law*, Vol. 19, 2024.
[22] *Som Prakash v. State of Delhi*, (1974) 4 SCC 725.
[23] R. Meghwal, "Artificial Intelligence and the 'Black Box' Problem in Criminal Evidence," *Journal of Law and Emerging Technologies*, Vol. 3, 2026.

The lack of transparency in the decision-making process by an algorithm is one of the most important issues associated with AI-generated evidence. Several artificial intelligence applications are based on sophisticated machine-learning algorithms, which process vast amount of data and give out analytical results. The rationale process of these outputs, however, is not always easy to comprehend. This is usually referred to as the black box problem.[24] Since the inner workings of such algorithms cannot be described easily, it can be hard to assess the court, how a certain conclusion was made. This is a serious concern when it comes to the validity of AI-generated findings in a legal system that bases its judicial decision-making on reasoned decisions.

The other critical problem is associated with the capability of the defence to challenge algorithmic evidence. The criminal trials are conducted on the basis that the accused is entitled to test and interrogate the evidence brought forward by the prosecution. The defence should also be allowed to investigate the process through which the results are obtained when the analysis created by AI is presented in court as evidence. Assuming that the algorithm that was applied to perform the analysis is proprietary or not fully publicised, it will be hard to assess by the defence whether the system made correct conclusions. Such a scenario may end up compromising the impartiality of the trial process.

Another problem is the reproducibility of the AI results. Scientific evidence is said to be reliable in most cases where it can undergo independent verification by repetition of the similar procedure under similar conditions. The use of traditional forensic procedures like chemical analysis or matching of fingerprints can often be copied by other experts. Nevertheless, AI models usually are based on concrete training samples and complicated algorithmic parameters not easily reproducible.[25] In the event that the same dataset or algorithm is not accessible to the defence or independent experts then the accuracy of the AI-generated results may become hard to verify.

The reliability of algorithmic evidence is also highly dependent on the quality and integrity of the data, which is used to analyse AI. Machine-learning systems become very reliant on the data that is used to train them and run them. In the event that the data is incomplete, incorrect or biased, the conclusions that are generated by the system can be unreliable as well. To illustrate, an AI agent that examines patterns of communication can falsely alert about innocent communication when the training data sets are biased towards criminal behaviour. These inaccuracies may be of grave consequences to the accused in the process of criminal proceedings.

The integrity of the digital evidence is another important issue. Without proper protection, electronic data is easily modified, manipulated or created. Such advanced technologies as deepfakes and digital editing tools have enabled the production of highly convincing but fake. There is a chance that distorted information will give false results when such digital materials are processed by AI tools. Courts should therefore be careful in making sure that digital evidence has been appropriately taken, maintained and verified and then they can use AI-assisted analysis.[26]

Another critical aspect concerning admissibility is the chain of custody of digital evidence. When carrying out criminal investigations, one should record all steps involved in the evidence management since the time of data collection to its presentation in court. Proper chain of custody will make sure that the evidence has not been manipulated or disturbed in the course of the investigation. During cyber-forensic investigations, this can be done in the form of imaging of digital devices, generation of hash values, and storage of data in a secure manner. The chain of custody could have any holes or loopholes that might cast doubt on the authenticity of the evidence.

The issue of expert testimony in the interpretation of AI-generated evidence also has to be addressed by courts. Judges and lawyers might not always have the expertise to process such evidence on their own since artificial intelligence systems require specialised technical processes. The expert witnesses thus become very important in providing the mechanism under which AI tools operate and the interpretation of the findings that the tools

[24] K. Kelly, T. McBride & L. Sanders, “Explainable Artificial Intelligence in Legal Decision-Making,” *Artificial Intelligence and Law*, Vol. 28, 2020.
[25] P. Singh & R. Devi, “Reproducibility and Reliability Issues in AI-Based Digital Forensics,” *International Journal of Cyber Criminology*, Vol. 19, 2025.
[26] S. Sahibpreet & R. Shikha, “AI Governance and Criminal Justice: Ethical and Regulatory Challenges,” *Computer Law and Security Review*, Vol. 46, 2025.

provide. There is also the question of the credibility and impartiality of the experts though when there is a difference in the interpretations of the same data provided by different experts.

Finally, AI-assisted cyber-forensic evidence is admissible, but only to the extent that the technology applied was reliable, transparent, and documented. Courts should make sure that the AI systems are only taken as investigative tools and not as infallible sources of truth. Close judicial examination, procedural protection, and defence capability against algorithmic evidence are all critical in ensuring fairness of trials in criminal courts. With the ever-changing nature of the digital technologies, the legal system has to remain abreast of the changes in its evidentiary guidelines, so that technological innovation becomes the source of empowerment of the justice system to be administered but not a threat to its safety.

V. Specific Challenges in NDPS Trials:

The application of cyber-forensic evidence with the help of the artificial intelligence causes certain concerns in the prosecution in the frame of the Narcotic Drugs and Psychotropic Substances Act, 1985 (NDPS Act). The NDPS Act has a reputation of being very strict in law, having serious penalties, strict procedural protections and statutory presumptions that may influence the burden of proof. Due to the fact that the sentences given under this law can lead to lengthy prison sentences and tough bail provisions, the importance of evidence scrutiny has continually been stressed by courts.[27] In such situations, when digital evidence that is processed by artificial intelligence is presented, the issues of reliability, authenticity and fairness will be of particular importance.

Among the main obstacles is the statutory assumptions of the NDPS Act 35 and 54. Such provisions enable courts to assume that there was an operative mental state or that the knowledge of possession where it is determined that the prosecution has proven a few underlying facts. In the contemporary investigations, digital evidence like chat messages, email messages, records of financial transactions and location data can be used to determine these underlying facts.[28] In case such evidence has been processed or analysed using artificial intelligence software, the courts need to critically review whether the technology involved is sound, transparent and well authenticated before being permitted to aid statutory presumptions that place the burden of guilt on the accused.

The other issue is the apparent evidences of the AI-generated outputs of the analysis. AIs can determine trends in digital information, like common communication between people or suspicious activity elsewhere. Although these insights could help an investigator depict the criminal networks, they do not necessarily make up direct evidence of involvement in the narcotics smugglings. Courts should thus decide whether the results of AI use should be considered substantive evidence or simply as assistive evidence to other types of evidence. The excessive use of the algorithmic analysis that lacks independent verification may pose a threat of false conclusions.

Digital evidence has other significant challenges in the NDPS investigations in terms of chain of custody. In contrast to physical evidence, digital data can be stored in the remote server, in the cloud-based environment, or on the encrypted communication platform. To prove the authenticity of such evidence, it is necessary to have a continuous trail of the way such evidence was recorded, stored, and examined. The integrity of the evidence produced in court may be questioned in case any anomalies are detected in the documentation of this process.

Moreover, numerous cases of narcotics have become subject to cross border digital activity such as communication with people residing in different jurisdictions or transactions made via international online platforms. Such data could be challenging to collect and verify without the collaboration of several law-enforcement bodies and adherence to the international legal procedures.

The courts in this regard are to be especially careful when analyzing AI-aided cyber-forensics evidence during NDPS trials. The transparency of technological procedures, the presence of the chain of custody, and the need

[27] A. Soni, "Presumptions under the NDPS Act and the Burden of Proof in Criminal Trials," *Indian Bar Review*, Vol. 51, 2024.
[28] Narcotic Drugs and Psychotropic Substances Act, 1985, ss. 35, 54.

to have the algorithmic results checked by another person are all the necessary steps ensuring the integrity of the fairness concept and safeguarding of the rights of the accused.

VI. Comparative Jurisprudence and Ethical Standards:

The growing trend of artificial intelligence in cyber-forensic studies has made the legal systems of nations worldwide consider the regulation of algorithmic technologies in criminal justice procedures. As police departments embrace AI to examine digital evidence, transparency, reliability, and accountability issues are the key topics of legal debate. Comparative jurisprudence will thus yield some useful information concerning the ways various jurisdictions are approaching these issues and how ethics can help shape the responsible application of AI-based forensic technologies.[29]

The European Union Artificial Intelligence Act (EU AI Act) is one of the most important developments in the field internationally. The EU AI Act provides a risk-based regulation system of artificial intelligence systems. The applications of AI in both law enforcement and criminal justice are thus commonly defined as high-risk systems under this approach. These systems should be in accordance with rigorous criteria connected with transparency, documentation, accuracy, and human supervision. The law enforcement agencies using such technologies should keep records justifying the operation of the system, the process of working with the data, and the threats address technique. This model is aimed at making sure that AI systems applied in criminal investigations do not compromise key rights or procedural fairness.[30]

One of the main principles focused in most of the international structures is the necessity of a human control. The usage of AI technological tools is likely to support, but not to displace human decision-making skills in the legal domain. Courts and investigators have to be able to scrutinize and doubt the results of the work of the algorithmic systems. This principle acknowledges the fact that technological tools, despite being potent, still can lead to errors or biased conclusions in case they are not closely monitored.

Alongside legislative frameworks, there are a number of professional organisations that have come up with ethical principles of the responsible application of artificial intelligence in forensic science. Other organisations like the Institute of electrical and electronics engineers (IEEE) and other international research organisations advocate fairness and transparency and accountability in the process of designing and implementing AI systems. These ethical principles drive developers and investigators to report the data sets they used to train AI models, describe the mechanism of the algorithms at work, and make sure that the technology does not generate discriminatory or incorrect results.[31]

The next significant idea that is brought up by international scholarship is the emergence of explainable artificial intelligence. Explainable AI is a concept of methods that make the algorithms processes of algorithms easier to understand by human users. Explainability is important in the context of criminal trials since the judges and lawyers need to be in a position to assess the rationale behind the technological findings. Scenario-based reasoning models and Bayesian networks are among the approaches that have been suggested to provide AI-generated conclusions in a comprehensible form.[32]

The significance of protecting and ensuring privacy of data, when applying artificial intelligence in the criminal investigation, is also emphasized in comparative jurisprudence. Most jurisdictions mandate law enforcement agencies to conduct rigorous protocols in gathering, storing and analysing digital data. These are the measures aimed at securing the rights of individuals and making sure that technological devices are employed in a responsible way in the legal framework.

The comparative experience has thus shown that there should be a delicate balance where the technology innovation is carefully balanced with legal responsibility in relating the artificial intelligence in criminal justice. Through the application of values and principles, including transparency, human control, explainability, and ethical management, legal frameworks can make sure that AI-based forensic technologies

[29] S. Sahibpreet & R. Shikha, “AI Governance and Criminal Justice: Ethical and Regulatory Challenges,” *Computer Law and Security Review*, Vol. 46, 2025.
[30] Regulation (EU) 2024/1689 (Artificial Intelligence Act).
[31] IEEE, *Ethically Aligned Design: A Vision for Prioritizing Human Well-Being with Autonomous and Intelligent Systems*, IEEE Standards Association, 2019.
[32] K. Kelly, T. McBride & L. Sanders, “Explainable Artificial Intelligence in Legal Decision-Making,” *Artificial Intelligence and Law*, Vol. 28, 2020.

can be used to bring about justice and prevent the infringement of basic rights and procedural fairness when it comes to criminal prosecution.

VII. Proposed Legal Reforms:

The growing trend of artificial intelligence in cyber-forensic investigations demonstrates that proper legal and procedural restrictions are required to control the admissibility and reliability of digital evidence in a criminal trial. Even though the Bharatiya Sakshya Adhiniyam, 2023 has also made significant changes regarding how electronic evidence is treated, the increasingly popular AI-assisted forensic tools need additional reforms to make the criminal justice system more transparent, accountable, and fair.[33] Such reforms are especially essential in prosecutions of narcotics under the NDPS Act, where the punishment that comes with conviction is extremely harsh and the standards to be used to prove such a case should be exercised with extreme caution.

Among the reforms, the design of standard operating procedures in AI-assisted electronic evidence should be mentioned. The law enforcement agencies ought to implement elaborate guidelines that govern the application of artificial intelligence in a cyber-forensic investigation. Such measures must compel investigators to record all the steps in the digital evidence process, these approaches comprise the source device, data extraction method, the forensic software employed, and the algorithmic model employed to analyze it. Effective documentation will allow the courts to check the authenticity and reliability of the digital evidence and will also allow the defence to look into the investigation procedure in an effective manner.

The second reform will be related to the strengthening of the certification and expert verification tools within the Bharatiya Sakshya Adhiniyam. The certification that comes with the use of AI-based tools to analyse digital data should make clear the technology process in play. Expert certificates must define the type of software that is being used, what kind of data is being analysed, and any restrictions that are related to the algorithmic approach. The provision of such information will enlighten courts on the credibility of the evidence, and allow useful cross-examination by the defence.

The other major change is judicial education in digital forensics and artificial intelligence. With technology quickly becoming a central point of criminal investigation, judges need to gain a general knowledge of digital forensic investigations and algorithm manipulation. Judges can be offered specific training programs and continuing legal education to get acquainted with such technical concepts as data extraction, hash values, algorithmic pattern recognition, and digital chain of custody. This information will help courts to get a better assessment of complex cyber-forensic evidence.

Lastly, the expert testifying needs to be encouraged in open and transparent situations concerning AI-generated evidence. The forensic experts appearing to present such evidence must be able to explain their findings in a way that can be comprehended by the judges and lawyers who may not be technically savvy. It must be clearly mentioned in reports what methods were applied, what conclusions were made, and which limitations of the technology in question might be there. These reforms will assist in making sure that artificial intelligence reinforces the performance of cyber-forensic investigations and that it does not compromise fairness and due process in criminal trials.

VIII. Conclusion:

Due to the high rate of development of the digital technology, there have been major changes not only in nature of criminal activity but also in the investigation process of such activities. With the advent of encrypted-communication services, dark-marketplaces and cryptocurrency transactions, the law-enforcement agencies have developed complex challenges in the context of narcotics trafficking. The conventional methods of investigation usually prove not enough to identify and destroy technologically advanced drug trafficking groups. This has made cyber-forensic investigation aided by artificial intelligence a more significant instrument in criminal justice systems today.[34]

Artificial intelligence is highly beneficial to digital evidence analysis. Electronic information can be subsequently analyzed with the help of AI-based tools and assist in detecting patterns of communication

[33] Bharatiya Sakshya Adhiniyam, 2023, s. 63.
[34] O. Dunsin et al., "Artificial Intelligence and Digital Forensics in Cybercrime Investigations," *Journal of Digital Forensics, Security and Law*, Vol. 19, 2024.

networks, rebuilding timelines of criminal activities, and revealing concealed connections between the figures of the criminal activities involved. Such capabilities can help investigators reveal organised narcotics trafficking networks that would otherwise be hidden in large data sets of electronic data. In this regard, artificial intelligence can enhance the ability of law enforcing agencies to react appropriately to the new manifestations of technologically-related criminal behaviour.

Meanwhile, it can be concluded that artificial intelligence in criminal investigations raises multiple legal and ethical issues. Transparency, reliability and accountability frequently pose difficulties in the algorithmic character of AI systems. The so-called black box problem, or the lack of understanding of the reasoning process underlining the algorithmic conclusions, may make the work of the courts that have to assess the credibility and the evidentiary worth of digital examination complex. Unless it is possible to provide a clear explanation of the methods adopted by AI systems along with the possibility of their verification independently, courts might have a hard time when it comes to ruling whether this kind of evidence can pass the standard of proof needed in criminal trials.[35]

Such issues are even greater in the prosecution of Narcotic Drugs and Psychotropic Substances Act, 1985. The NDPS Act is very severe with penalties and also has statutory presumptions that can cause shift of the burden of proof against the accused when such other background facts have been proved. When dealing with such circumstances the authenticity and credibility of the digital evidence comes into its own to give the accused a fair trial and convict them based on valid and well proven evidence.

The modification of the Indian Evidence Act to the Bharatiya Sakshya Adhiniyam, 2023, by India is a noteworthy attempt to bring the country to date in terms of the legal framework on electronic evidence. The law is expected to enhance the credibility of electronic evidence presented in a court by identifying the digital records and offering protection measures like the need to have certification and verification of hash values. Nevertheless, the growing application of the use of artificial intelligence during cyber-forensic investigations necessitates further elaboration of legal norms and procedural protection.

In sum, artificial intelligence is to be treated as the potent investigational tool instead of the alternative to human discretion in the justice delivery. The courts need to make sure that the evidence that is supported by AI should be transparent, verifiable, and open to meaningful questioning. Mediating between the technological innovation and the most significant tenets of fairness, due process and evidentiary reliability, the criminal justice system will be able to address the demands of the digital era and ensure the rights of the persons that are subject to criminal trials.

Bibliography:

Books and Journal Articles:

- Kelly, K., McBride, T. & Sanders, L., Artificial Intelligence and Legal Decision-Making, Oxford University Press, Oxford, 2020.
- Meghwal, R., Artificial Intelligence, Evidence and Criminal Justice, Routledge, London, Dunsin, O., Adeyemi, A. & Olaitan, K., "Artificial Intelligence and Digital Forensics in Cybercrime Investigations," Journal of Digital Forensics, Security and Law, Vol. 19, 2024.
- Malik, A., "Digital Evidence and the Bharatiya Sakshya Adhiniyam: A New Framework for Electronic Records," Journal of Indian Law and Society, Vol. 15, 2024.
- Sahibpreet, S. & Shikha, R., "AI Governance and Criminal Justice: Ethical and Regulatory Challenges," Computer Law and Security Review, Vol. 46, 2025.
- Singh, P. & Devi, R., "Reproducibility and Reliability Issues in AI-Based Digital Forensics," International Journal of Cyber Criminology, Vol. 19, 2025.
- Singh, R. & Gautam, S., "Artificial Intelligence Techniques in Cyber-Forensic Investigations," Indian Journal of Law and Technology, Vol. 18, 2022.
- Soni, A., "Presumptions under the NDPS Act and the Burden of Proof in Criminal Trials," Indian Bar Review, Vol. 51, 2024.2026.

[35] R. Meghwal, "Artificial Intelligence and the 'Black Box' Problem in Criminal Evidence," *Journal of Law and Emerging Technologies*, Vol. 3, 2026.

Reports:

- European Parliament and Council, Regulation (EU) 2024/1689 on Artificial Intelligence (Artificial Intelligence Act), 2024.
- Institute of Electrical and Electronics Engineers (IEEE), Ethically Aligned Design: A Vision for Prioritizing Human Well-Being with Autonomous and Intelligent Systems, IEEE Standards Association, 2019.