

FUTURE CRIMES IN INDIA 2026: ARTIFICIAL INTELLIGENCE, PRIVACY AND LEGAL REFORM

Saood Khan

Research Scholar At Sage University, Bhopal
Contact at: saood369@gmail.com

ABSTRACT

The blistering development of digital technologies has changed the opportunities and the threats linked to technological progress. Artificial intelligence (AI) is being progressively applied in the financial systems, governance systems, and social communication systems in India. Although these developments increase the growth and efficiency of the economy, they provide a new source of criminal activity. The paper investigates the emerging connection between artificial intelligence and the novel crime manifestations in India. Special focus is put on cyber fraud, identity theft, deepfake manipulation, and automated misinformation campaigns. The study also determines the suitability of the existing legal system in combating AI-related crimes and outlines the gaps in the current laws. Based on the qualitative analysis of the secondary data, policy discourse, and the trend of cybercrimes in 2021-2025, the study identifies the increasing complexity of digital crimes and their influence on the right to privacy. The research indicates that the existing legal regulations are not adequate to combat the problems of autonomous technologies and algorithmic decisions. The paper concludes that forward-thinking legal reforms that optimize the balance between technological innovation and the protection of privacy, accountability, and constitutional principles in the digital age should be implemented in India

KEYWORDS

Artificial Intelligence, Cybercrime, Privacy Rights, Legal Reform, Digital Crime, India

1. INTRODUCTION

Digital technology has entered the daily routine of the Indian lifestyle in the past few years. Online banking and digital payments, social media communication, and government services are only a few examples of how technology has affected the way people communicate, work, and get information. This fast digitization has resulted in new avenues of economic growth, innovation, and better services to the people. Meanwhile, however, it has also transformed the character of crime. Crimes that were previously perpetrated using conventional physical means are now being perpetrated in digital space.

The increasing application of artificial intelligence is one of the most important technological changes that have taken part in this shift. Artificial intelligence can be defined as computer systems that are able to learn through data, detect patterns, and conduct activities that would otherwise be handled by human intelligence. Such systems are currently in extensive use in areas like finance, health care, governance, and communication. Although AI usage has resulted in efficiency and technological growth, it has also brought about new dangers in case such technologies are used improperly.¹

As access to sophisticated digital tools becomes more and more commonplace, crime is turning increasingly more inventive and harder to detect. Artificial intelligence-driven technologies can be applied to automate fraudulent activities, produce fraudulent content of high quality and authenticity, as well as to manipulate personal information. As an illustration, deepfake video-generating and human voice cloning tools may be abused to impersonate a person during a financial transaction or even to disseminate misinformation. On the same note, phishing attacks can be done on a large scale by automated systems that target an individual with a personalised digital message.

The second critical issue has a connection with the security of personal privacy. Artificial intelligence systems are largely based on gathering and processing large amounts of data. Any personal data presented online, financial dealings, and online services may be processed and analysed in a manner that an individual may not completely comprehend or regulate. The

¹H. Sayyed, Artificial Intelligence and Criminal Liability in India: Exploring Legal Implications and Challenges, 10(1) Cogent Soc. Sci. art. 2343195 (2024).

misuse of this information by bad actors can result in identity theft, loss of money, and any other grave breach of privacy.²

Simultaneously, governments and law enforcement agencies are also adopting artificial intelligence to enhance crime detection and investigation. Predictive analytics, facial recognition, and automated data analysis technologies are getting more and more popular to help track and spot potential criminal behaviour. In spite of the fact that these tools can improve efficiency within law enforcement, they also lead to concerns regarding transparency, accountability, and the abuse of surveillance technologies.

The legal systems face significant issues with these developments. Most of the current cybercrime laws were formulated when artificial intelligence technologies were not extensively applied. Consequently, some of the novel challenges, including the responsibility of autonomous systems, the regulation of deepfakes, and the responsibility for decisions based on algorithmic methods of algorithms, are not a priori covered in existing legal systems.³

Against this backdrop, there is a need to analyse the impact of artificial intelligence on shaping crime in the future in India and the effectiveness of the current legal systems to match this development. This paper will thus examine the connection between AI, new digital offenses, and privacy issues. It also analyses the suitability of the existing law in India and underscores the fact that legal changes are required which can respond to technological changes and protect individual rights in the digital age.

1.1. Research Objectives

The following objectives guide the present study:

1. To explore the way artificial intelligence is contributing to the development of cybercrime in India.
2. To examine the privacy threats posed by AI-powered technologies.
3. To assess the sufficiency of the current Indian laws to deal with AI-related offenses.

²Tasnimul Md Hassan, The Perils and Promises of Artificial Intelligence in Criminal Sentencing, 19(2) Indian J. L. & Tech. 1 (2024).

³Puneet G. & Sony R., The Role of Artificial Intelligence in Improving Criminal Justice: Indian Perspective, 8(4) NUJS J. Regul. Stud. 2 (2024).

4. To determine the possible legal changes needed to control future criminal acts of technology.

1.2. Research Methodology

The study employs the qualitative form of analytical research using secondary sources of information as its main data source. The paper is based on academic articles, government publications, debates on technology policy, and publicly available statistics on cybercrime.

The secondary data that covered cybercrime cases in 2021-2025 were reviewed to determine the developing technological trends. These trends were examined in order to establish how artificial intelligence can enable new digital crime.

Also examined in the study are the applicable legal provisions in current Indian law, such as internet crime laws and systems of criminal law, as a way of assessing their role in criminalizing AI-led crimes.

2. ARTIFICIAL INTELLIGENCE AND NEW DIGITAL CRIMES.

The continued expansion of the use of artificial intelligence in digital systems has not only been efficient and automated but also led to new types of technologically facilitated criminal activity. Due to the increased availability and technical capabilities of AI tools, they are becoming open to abuse by individuals and organised criminal groups. Such technologies enable criminals to robotize fraud, copy the behaviour of humans, and process digital data with more precision and magnitude.

Table 1 presents key categories of crimes that are increasingly associated with the misuse of artificial intelligence. The table outlines the nature of each offence and highlights the potential consequences that such activities may have on individuals, institutions, and society. By identifying these emerging patterns, the study aims to demonstrate how artificial intelligence is reshaping the methods through which cyber offences are committed.⁴

Table number 1: Types of AI-driven crime and their possible impact.

⁴A. Sharma et al., Artificial Intelligence in the Indian Criminal Justice System: Advancements, Challenges, and Ethical Implications, 5(1) J. Lifestyle & SDGs Rev. e04877 (2025).

Type of AI-Driven Crime	Description of the Offence	Possible Impact
Deepfake Manipulation	Use of AI tools to create realistic fake videos or voice recordings that imitate real individuals.	Can be used for fraud, misinformation, political manipulation, or reputational harm.
AI-Assisted Financial Fraud	Automated phishing emails, scam calls, and fraudulent digital transactions generated using AI algorithms.	Financial loss to individuals and institutions; increase in online banking fraud.
Identity Theft	Use of stolen personal or biometric data to impersonate individuals in digital platforms or financial systems.	Unauthorized access to accounts, financial exploitation, and privacy violations.
Data Manipulation	AI tools used to alter or analyse datasets for illegal purposes such as market manipulation or information distortion.	Economic disruption, manipulation of decisions, and loss of trust in digital systems.
Cyber Manipulation	AI-generated bots and automated accounts used to spread misinformation, harassment, or propaganda on social media.	Influence on public opinion, social instability, and misinformation spread.

The statistics in Table 1 suggest that the field of artificial intelligence has increased the breadth and depth of cybercrime. Among the most important events, the advent of deepfake manipulation should be mentioned, in which AI-based audio or video content is created in which real people are imitated. Financial fraud, misinformation campaigns, or reputation damage can be committed with such technology, and it is becoming harder and harder to verify the authenticity of the information or the presence of a fake one.

The other trend worth mentioning is the development of AI-based financial fraud. Phishing systems and scam activities are automated to enable a criminal to reach many victims at a time.

These systems are able to scan the data of the users and create personalised messages of a fraudulent nature that are likely to make the victims trust and act on those messages.

Another important issue in the online world is identity theft. Online platforms and data breaches permit criminals to make comprehensive digital portraits of people based on the availability of their personal data. This information can be analysed using artificial intelligence and used to impersonate victims and gain access to financial accounts or other sensitive systems. Artificial intelligence is also abused in the manipulation of data. By manipulating or manipulation of digital data, criminals can affect financial decisions, corporate processes, or institutional processes. These operations may weaken the stability of digital information infrastructure and cause more significant economic destabilization.

Lastly, the development of cyber manipulation by means of AI-controlled bots and automated accounts proves that one can use technology to disseminate false information and control the way people talk. Such automated systems have the power to share misleading information on social media in a short period of time and impact people, as well as lead to the destabilisation of the social and political climate.

The data provided in Table 1 indicates that the crimes committed with the help of AI are growing more complex and harder to identify. The automation of the work of artificial intelligence allows offenders to work on a scale that would not have been possible with traditional criminal means. The ensuing development places more emphasis on the need to bolster the legal framework, enhance digital literacy, as well as augment the technological capacity of law enforcement agencies to comply with the emerging cyber threats.

3. THE PRIVACY ISSUE WITH ARTIFICIAL INTELLIGENCE.

Artificial intelligence machines can be utilized, but basically by collecting, processing, and analysing large amounts of data. The personal data of people is being stored and processed in automated systems as digital platforms continue to proliferate into various sectors like finance, communication, healthcare, and governance. Although AI technologies are effective in enhancing efficiency and improving decision-making, the matter of individual privacy and data security concerns remains quite important.⁵ Table 2 points out the biggest privacy threats posed by the extensive use of artificial intelligence and how it might impact people and organizations.

⁵O. Ruhil, The Legal Assembly Line: A Critique of AI in Indian Law, 15(3) J. L. & Tech. 210 (2023).

Table 2: Privacy Risks Associated with Artificial Intelligence

Privacy Issue	Description	Possible Consequences
Mass Data Collection	AI systems require large datasets including personal, behavioural, and financial information.	Increased risk of data misuse and unauthorized data access.
Data Breaches	Storage of large datasets makes digital systems attractive targets for cybercriminals.	Identity theft, financial fraud, and exposure of sensitive personal information.
AI-Based Surveillance	Technologies such as facial recognition and behavioural tracking monitor individuals in public and digital spaces.	Potential violation of privacy rights and excessive monitoring.
Algorithmic Bias	AI systems may produce biased or unfair decisions due to flawed datasets or algorithms.	Discrimination in areas such as employment, finance, or law enforcement.
Lack of Transparency	Automated decision-making processes are often complex and difficult to understand.	Reduced accountability and limited ability for individuals to challenge decisions.

The information presented in Table 2 illustrates that privacy concerns associated with artificial intelligence extend beyond simple data misuse. AI technologies depend heavily on the collection and analysis of personal information, which increases the risk of privacy violations when adequate safeguards are not in place. Large-scale data collection and storage make digital systems vulnerable to cyberattacks and data breaches, potentially exposing sensitive personal information. The use of AI-powered surveillance technologies further intensifies these concerns. Systems such as facial recognition and behavioural tracking allow institutions to monitor individuals continuously, raising questions about the balance between security and personal freedom. Additionally, algorithmic bias and lack of transparency in automated decision-making processes may lead to unfair outcomes that are difficult to challenge.

Overall, the data highlights that while artificial intelligence offers substantial technological advantages, it also introduces complex privacy risks. Addressing these challenges requires stronger data protection regulations, improved transparency in AI systems, and clear

accountability mechanisms to ensure that technological innovation does not compromise fundamental privacy rights.

4. LEGAL FRAMEWORK THAT CURRENTLY EXISTS IN INDIA.

India controls cybercrime and digital crimes by implementing a blend of laws in technology law, criminal law, as well as data protection legislation. The main law that regulates activities in cyberspace is the Information Technology Act, 2000, which gives legal status to electronic records and creates punishment to different cybercrimes. Some parts of this Act specifically refer to digital crimes. An example is that in Section 43, unauthorized access, downloading, or extracting data in computer systems are criminalized, whereas in Section 66, hacking and other computer-related crimes are criminalized. Section 66C directly deals with identity theft that involves the misuse of electronic signatures, passwords, or unique identification information, whereas Section 66D punishes cheating by personation through computer resources that is widely used in online fraud and phishing schemes. Also, Section 66E is concerned with breach of privacy by taking or spreading images of private spaces without permission. Despite addressing numerous types of cybercrime, the provisions have been implemented prior to the accelerated development of artificial intelligence technologies and thus do not specifically address such crimes as the manipulation with deepfakes or the fraud introduced by artificial intelligence.⁶

It was a landmark case that the Right to Privacy was declared a basic right in Article 21 of the Constitution of India. The Supreme Court highlighted that there is informational privacy and the protection of personal data are part of privacy. The case is of interest to the discourse on the issue of artificial intelligence and digital surveillance since AI systems are often based on the mass collection and processing of individual information. The Court decided that any infringement on privacy has to meet the concepts of legality, necessity, and proportionality.⁷

Other than the Information Technology Act, some offences that encompass digital deception and fraud can also be tried in accordance with the Bharatiya Nyaya Sanhita, 2023, which substituted the Indian Penal Code. The provisions referring to cheating, impersonation, and criminal misrepresentation may be applied in instances when digital technologies are applied to deceive other people or receive financial gains. As an example, crimes where fraudulent

⁶M. Rani, Impacts and Ethics of Using Artificial Intelligence (AI) by the Indian Police, 47(2) Policing: An Int'l J. 345 (2024).

⁷Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

representation or manipulation of finances is conducted by digital means can be covered by general provisions pertaining to cheating and fraud as a criminal case. Section 66A of the Information Technology Act, 2000 was declared unconstitutional by the Supreme Court, which said that it contravened the constitutional right to freedom of speech and expression in Article 19(1)(a). The Court concluded that indistinct limits on online communication may result in arbitrary application. This ruling is significant to the AI governance problem since automated surveillance and algorithmic editing of digital text should also observe the constitutional liberties.

Besides criminal laws, the Digital Personal Data Protection Act, 2023 is also significant regarding the protection of personal data in the digital world environment. This Act sets forth responsibilities of data fiduciaries with respect to lawful collection and processing as well as storage of personal data. It also acknowledges the rights of individuals to their personal information and provides penalties against unauthorized processing or misuse of personal information. As artificial intelligence systems usually presuppose the existence of large datasets that involve personal data, the safety of data in the context of this law is especially applicable to the prevention of privacy breaches and data misuse.⁸

There have also been institutional mechanisms that have been established to bolster cybercrime enforcement in India. The investigation and coordination of offences related to technology is aided by the Indian Cyber Crime Coordination Centre (I4C), which is set up by the Ministry of Home Affairs, and other special cybercrime police stations and digital forensic laboratories. In addition, people can report online fraud and identity theft, among other online crime activities, through the National Cyber Crime Reporting Portal.⁹

Whether electronic evidence created by the defendant under Section 65B of the Indian Evidence Act, 1872, is admissible. According to the Supreme Court, electronic records are supposed to be supported by a certificate of authenticity of the electronic evidence. The case is of particular significance in cases that involve AI research since digital evidence, algorithmic information, and electronic documents are frequently at the center of cybercrime prosecution.

⁸A. Narayanan, M. Agarwal & S. Bansal, Artificial Intelligence Inroads into the Indian Judicial System, 9(4) Indian J. Legal Stud. 200 (2023).

⁹M. Ojha, Legal, Ethical and Social Ramifications of the Use of Artificial Intelligence in Decision-Making: A Comparative Analysis of the EU and Indian Law, 31(3) Int'l J. L. & Info. Tech. 220 (2023).

The case was related to the problem of data privacy and the liability of online platforms related to criminal investigations. The Delhi High Court considered the issue of whether the social media companies could be compelled to provide user information in connection with the investigation, but weighed the privacy matters. The case points to the increasing legal issues concerning online platforms, information management, and privacy of personal data.¹⁰

Although these legal and institutional actions exist, this still leaves a number of regulatory loopholes when it comes to dealing with new AI-based crimes. Existing laws are mostly concerned with the old cybercrimes like hacking, data theft, and online fraud, yet are not explicit about the concerns of autonomous AI systems, algorithmic accountability, or misuse of deepfake technologies. Since artificial intelligence is still impacting the digital world as well as criminal behaviour, it is possible that the current legal system may need additional changes to tackle the issues of sophisticated technological offenses.

5. OBSERVED PATTERNS OF AI-RELATED CRIMES

The growing use of artificial intelligence and automated digital tools has significantly influenced the pattern of cybercrime in recent years. Technological advancements allow offenders to conduct fraudulent activities more efficiently and on a larger scale than traditional criminal methods. AI-based systems enable criminals to analyse data, automate communication, and imitate human behaviour, making digital crimes more sophisticated and difficult to detect.¹¹ To better understand these emerging patterns, Table 3 outlines key forms of AI-related crimes, their nature, and the trends observed in recent years.

Table 3: Observed Patterns of AI-Related Crimes

Type of Crime	Nature of Offence	Observed Trend
Financial Fraud	AI-assisted phishing attacks, automated scam calls, and fraudulent digital transactions	Rapid growth with the expansion of digital banking and online payment systems
Identity Theft	Misuse of personal, financial, or biometric data to impersonate individuals online	Increasing incidents due to frequent data breaches and large-scale data collection

¹⁰Karmanya Singh Sareen v. Union of India, W.P. (C) 7663/2016 (Delhi High Court).

¹¹S. Dhiman & S. Singh, Cybercrime and Computer Forensics in Epoch of Artificial Intelligence in India, 2(4) Cyber L. Rep. 13 (2023).

Deepfake Manipulation	AI-generated voice or video content used to impersonate individuals or spread misinformation	Emerging threat in financial fraud, misinformation campaigns, and reputational harm
Data Exploitation	Unauthorized collection, sale, or misuse of personal information obtained from digital platforms	Closely linked with social media platforms, digital services, and data marketplaces
Cyber Manipulation	Use of AI-generated bots or automated accounts to spread misinformation or harassment	Expanding rapidly across social media networks and online communities

As seen in Table 3, artificial intelligence has caused a substantial change in the level and character of cybercrime. Among the most outstanding types of financial fraud seems to be the one that has increased in number as a result of the growing preference gained through using digital banking and other online payment systems. Intelligent phishing applications and robots working on the scam allow criminals to attack a vast number of people at the same time, making them more likely to be exploited financially.

Another significant issue of the digital world is identity theft. The mass gathering of personal information by Internet sources and organizations has enhanced criminals' convenient access to and abuse of confidential information. This process is also developed with the help of AI tools, which analyse stolen data and form detailed computer images of possible victims. The advent of deepfake technology is a new aspect of cybercrime. Real people can be effectively impersonated by AI-generated audio and video content, which can result in fraud and misinformation or harm their reputation. On the same note, the abuse of personal information for commercial interests or any other illegal act underscores the increased problem of data abuse in the digital ecosystem.

Last but not least, AI-created bots and automated social media accounts have become a more apparent form of cyber manipulation. These systems are able to disseminate misinformation, harassment, and propaganda on social media fast and this may affect people's opinions and social structure. Altogether, the tendencies noticed in the table indicate that lawbreakers are turning towards technological automation and executing crimes on a bigger scale without losing some anonymity. This tendency also shows the increasing complexity of cybercrime and

the necessity of more effective regulatory mechanisms, better technological skills of law enforcement agencies, and increased awareness of people about the security of the Internet.

6. IMPLICATION ON PRIVACY AND SECURITY

The high-speed adoption of artificial intelligence into digital infrastructures has made a huge difference in the world of privacy and security in contemporary societies. Artificial intelligence systems rely on the constant gathering, processing, and analysing of massive data volumes, which makes them effective. In a digitally interconnected world like India, where people are gradually becoming more dependent on online platforms to carry out financial transactions, communication, e-commerce, healthcare services, and government interactions, a colossal amount of personal information is being created on a daily basis. Such a data-driven ecosystem allows AI technologies to enhance efficiency and decision-making, as well as deliver personalized digital services. Those same processes that bring about these technological developments have, however, posed a huge threat to privacy protection and the security of digital systems.¹²

The massive amount of gathered and processed personal information is one of the biggest privacy issues related to artificial intelligence. AI systems frequently utilize massive data sets that contain sensitive data about biometrics, financial data, web history, social media usage, and geographic data. Such data sets are often gathered using digital platforms, mobile apps, and web-based services that people engage with on a regular basis. A lack of strong protection mechanisms when this type of data is stored or processed makes it susceptible to theft, abuse, or misuse by criminals. Cyber intrusions and data breaches may result in sensitive personal information being exposed, resulting in identity theft, financial fraud, and a damaged reputation. Besides being criminally abused, the large-scale collection of personal information by companies and organizations brings up the issue of mass surveillance and diminishes personal control over online spaces.¹³

This further adds to the implications for privacy since more advanced technologies like facial recognition systems, biometric authentication, and behavioural tracking algorithms are being used. These technologies enable organizations to track and scan the movements of people with

¹²K. Mukhija & S. Jaiswal, Digital Personal Data Protection Act 2023 in Light of the European Union's GDPR, 4 *Jus Corpus* L.J. 638 (2023).

¹³S. Dubey, A Comparative Analysis of Data Privacy Laws Across India, EU and USA, 10(1) *J. Legal Stud. & Res.* 52 (2024).

accuracy never before witnessed. Though the introduction of such tools is usually done in the name of security or efficiency, it might confuse the line between lawful use of data and invasive surveillance. Without effective regulatory procedures and transparency processes, users are likely to lack the knowledge or even control over how their personal data are gathered, archived, and utilized. Such loss of control negatively affects the concept of informational privacy and questions the very meaning of personal autonomy in the digital era.¹⁴

Artificial intelligence is also accompanied by a set of complex problems as far as cybersecurity is concerned. Artificial intelligence can automate, analyze trends, and seek to adjust to ever-evolving circumstances, which can dramatically increase the possibilities for cybercriminals. If an example, AI-based software can be employed to carry out phishing attacks at scale by creating the most personalized fake messages that are authentic to the receiver. Such systems can use publicly available information on social media or online databases to customize deceptive messages and therefore enhance the chance of success. Subsequently, victims will find it more challenging to differentiate between authoritative messages and attempts aimed at acquiring sensitive information used by malicious individuals.

Another security challenge being developed is advanced impersonation technologies. The use of AI technology to clone the voice or face of a person and generate deepfake videos allows the person to be imitated with high accuracy in terms of voice, facial expressions, or appearance. Fraudulent messages can be made in audio or video and fabricated with the help of these technologies to seem like they were made by trusted persons or institutions. Such capabilities can be used by criminal actors to distort financial transactions or disseminate fake information or harm the reputation of individuals and organizations. Since the deepfake content can be too similar to the real media, it poses great problems for law enforcement and digital platforms that need to detect and stop fraudsters.¹⁵

Besides the direct act of cybercrime, artificial intelligence is also involved in the manipulation of information in digital ecosystems. The algorithms of AI and automated bots are capable of producing huge amounts of online content and spreading it within social media network, fast. Such systems can be employed to exaggerate misinformation, undermine the discourse of the people, or even control the opinion of the people. The fast dissemination of false or misleading news may destroy people's confidence in digital channels of communication and cause

¹⁴S. Bhattacharya, Deepfake Evidence and Judicial Accountability in India, 16 NUJS L. Rev. 87 (2023).

¹⁵Pavan Duggal, Cyber Law (Universal Law Publishing, New Delhi, 2023).

confusion in scenarios that need information that require reliable information. There can also be more social and political implications to such activities, especially during elections or any form of emergencies in society where accurate information is imperative in making informed decisions.¹⁶

The other aspect of the security challenge is the susceptibility of AI systems per se. Data poisoning, adversarial attacks, or algorithmic exploitation are some of the methods of manipulating artificial intelligence models. When this occurs, attackers willingly inject false data or alter system inputs to alter the behaviour of the AI system. This can lead to the use of automated decision-making procedures giving wrong or detrimental results. To illustrate, the integrity and validity of vital online infrastructure might be jeopardized because manipulated data might be introduced to automated financial systems, biometric authentication systems, or surveillance systems.

Also, the growing trend of using AI-based decision-making systems casts doubt on accountability and transparency. In cases where algorithms are used in making decisions that influence people, including financial approvals, security checks, or risk analyses, it is not easy to tell the manner in which such decisions were made. Complex AI models cannot be challenged by individuals due to a lack of transparency. Such opaqueness may raise legal and ethical issues, especially where automated systems are not under proper supervision or human control.

All in all, the growing role of artificial intelligence in digital infrastructures has provided a multifaceted landscape where technological advantages are accompanied by novel types of vulnerability. On the one hand, AI technologies have tremendous economic development opportunities, better governance, and improved security capabilities, but on the other hand, their abuse and unintentional effects can be a serious threat to privacy protection and cybersecurity. The further advancement of AI systems in gathering and processing huge amounts of data prompts the necessity of more resilient regulatory frameworks, all-encompassing data protection legislation, and more sophisticated approaches to cybersecurity. Transparency, accountability, and responsible governance of artificial intelligence will become

¹⁶Criminalizing Deepfakes: Legal Challenges and the Future of Cybercrime Law in India, Indian J. L. & Legal Res. (2025).

a critical element of protecting the rights of individuals and ensuring the continued faith of the population in digital technologies as societies enter the era of intelligent systems.

7. MAJOR FINDINGS, REGULATORY PROBLEMS, AND THE LEGAL REFORM.

The discussion in this paper can help reveal some key points about the connection between AI and new cybercrime in India. According to the findings, artificial intelligence is rapidly changing the way and the magnitude of crime in the digital world. Artificial intelligence-driven technologies help criminals computerise fraudulent processes and analyse huge amounts of data, as well as simulate human behaviour more effectively. Through this, cyber offences are now more effective and capable of being conducted over more digital networks as compared to the conventional types of crime. Among the many types of online crimes, financial fraud and identity theft still stand out as the most dominant ones. The high rate of digital banking, online payment systems, and internet-based communication platforms has provided criminals with a chance to exploit loopholes in these platforms. Furthermore, novel technologies like deepfake machines and voice cloning through AI have posed new risks in the form of impersonation, misinformation, and damage to reputation. Such advancements imply that advances in technology as a source of innovation provide a range of benefits, but, at the same time, they widen the opportunities for complex cybercrimes.¹⁷

The paper also shows that the existing law enforcement structure in India is not well-prepared to control most of the types of crimes perpetrated by AI. The current legislation mainly addresses the conventional cybercrimes that include hacking, identity theft, as well as internet fraud. Nevertheless, the blistering development of artificial intelligence technologies poses new legal issues, which are not explicitly covered in the existing laws. The problem of accountability of the algorithms, the liability of the autonomous systems, and the regulation of deepfake technologies are rather unclear issues in the current legal regulations. This technological-legal mismatch is a symptom of the necessity to have a more flexible and proactive legal solution.¹⁸

Controlling AI-controlled crimes also has a number of practical and institutional problems. The identification of offenders in the digital environment can be considered one of the greatest

¹⁷Ravinder Kumar & Gaurav Goyal, *The Right to Privacy in India: Concept and Evolution* (Eastern Book Company, Lucknow, 2023).

¹⁸Law Commission of India, *Report on Digital Evidence and AI*, Report No. 280 (Ministry of Law & Justice, 2024).

challenges. Crooks tend to act via anonymous networks, coded communication, and advanced digital instruments that hide their identities. This makes it very difficult for investigative agencies to track down the origin of cyber offences by investigative agencies. The transnational character of cybercrime is also another challenge. Numerous AI-assisted crimes take place throughout international digital networks, with the offenders, victims, and digital infrastructure potentially being in various jurisdictions. This poses legal and procedural difficulties for law enforcement agencies that come to investigate and prosecute such offenses.

Along with the question of jurisdiction, the enforcement of AI-related offences is also influenced by the shortage of technical knowledge in the traditional investigating bodies. Researching crimes encompassing machine learning systems, automated algorithms, and advanced data analytics is knowledge- and technology-intensive. Most law enforcement agencies can experience challenges in obtaining the required training and digital forensic skills that can enable them to counter such sophisticated crimes. Moreover, due to the lack of legal definitions of artificial intelligence technologies that are accepted worldwide, it is difficult to define responsibility when the automated systems are harmful or used to engage in criminal activity.¹⁹

Considering such results and issues, the research highlights the importance of legal change in India regarding the changing character of technologically motivated crimes. To ensure proper regulation, it is necessary to create more practical legal definitions of AI-related crimes to allow new types of online criminal activities to be detected and addressed accordingly. It is also necessary to strengthen data protection regulations so that the personal information gathered and processed with the help of AI systems could be sufficiently protected. Moreover, it can be effective to create a system of accountability for the developers, technology firms, and digital platforms to make sure that the abuse of artificial intelligence will be effectively resolved.²⁰

Another key element of regulatory reform is the promotion of ethical conditions in the creation and application of AI technologies. Bias, discrimination and abuse of automated systems can be mitigated through transparent and responsible algorithmic decision-making. Simultaneously, better technological training and digital forensic capacity of cybercrime investigation units can lead to the ability of law enforcement agencies to identify and respond to AI- based offences. All of these in aggregate would help in developing a balanced regulatory

¹⁹Data Security Council of India, India Cyber Threat Report 2025 (DSCI, New Delhi, 2025).

²⁰Shyam Divan, Digital Privacy and India's DPDP Act (LexisNexis 2024).

society where technological innovation will be allowed to flourish without sacrificing privacy, security and basic legal rights.

8. CONCLUSION

The evaluation of the recent trends in cybercrime and policy shows that the character of crimes in India is undergoing a radical shift because of the high-speed technological development. The analytical reports of cybercrime during the period between 2021 and 2025 indicate the continuous rise in technology-supported offenses, especially in the field of financial fraud, identity theft, and misuse of data. As the use of artificial intelligence in digital systems continues, the offences are increasingly becoming automated, advanced, and challenging to detect.

The analysis of the data provided in this work indicates that financial fraud is the most commonly reported cybercrime, which occurs mostly because of the development of digital payment systems and online financial services. The cases of identity theft and unauthorized access to personal data also increase, and in most cases, they are associated with giant data breaches and poor data protection measures. Moreover, the new threats of deepfake technology, voice cloning using AI, and automated phishing systems also show that manipulation and deception have become technologically advanced.

Analytically, the paper highlights 3 key trends. To begin with, the extent and pace of crime have greatly increased with the application of artificial intelligence, as criminals can use these systems to reach many victims through automation. Second, growing dependence on digital information has raised the level of concerns in regard to privacy, surveillance, and abuse of personal information. Third, the current legal system in India, and especially the legal provisions of the Information Technology Act, 2000, fails to encompass the specificities of AI-driven crimes, which makes some spheres of regulation open to interpretation.

As indicated in the findings, even though artificial intelligence can help law enforcement by better analyzing data and enabling predictive policing, it also poses the risks of algorithmic bias, transparency, and possible excessiveness in surveillance practices. These technologies can undermine the basic tenets of privacy and personal freedom, unless they are regulated properly.

All in all, the information and discussion in this paper show that India needs to be proactive in their legal and policy approach to deal with the changing landscape of AI-related crime. The reinforcement of data protection protocols, setting legal accountability for AI systems, and

creating dedicated investigation powers would all be necessary moves in addressing the emerging challenges posed by technology in the future. A middle ground that promotes innovation and, at the same time, maintains accountability and protection of constitutional rights will be instrumental in determining how Indian law will react to the new digital offenses.