ARTIFICIAL INTELLIGENCE POWERED PREDICTIVE POLICING OF CYBER CRIME: DIGITAL PAYMENTS INFRASTRUCTURE OF INDIA AS A CASE STUDY

Mr. Achint Dubey, Assistant Professor, School of Law, Centurion University of Technology and Management, Odisha

Ms. Shraddha Suman Paikray, Assistant Professor, School of Law, Centurion University of Technology and Management, Odisha

ABSTRACT

The evolution which took place in India to become a world digital payments leader lead by the Unified Payments Interface (Hereinafter UPI) crossing ₹200 trillion in transaction value annually, is an economic achievement as well as forensic challenge. The unprecedented rise of digital transactions has resulted in rise in cyber financial crimes from mule accounts to crypto frauds calling for cutting investigative and legal measures.

This paper examines the role of artificial intelligence in predictive policing with a focus on its integration into forensic science and legal framework of India. The paper covers latest tools such as MuleHunter.AI of Reserve Bank of India, Federated learning models of National Payment Corporation of India and predictive systems at State level assessing their effectiveness in fraud detection, forensic auditing of transactions and cross border evidence tracking. In addition to this the paper also covers the admissibility of AI produced evidence under law of India as well as constitutional issues pertaining to privacy, due process and proportionality.

Findings of the research reflects that though tools such as MuleHunter.AI exhibit up to 95 percent accuracy for mule account detection, rural forensic capacity remains short of gaps, cross border crime investigation and standardized procedures for the presentation of AI based evidence in courts is also not properly dealt. The researcher proposes an integrated framework of AI, Forensic Sciences and Law designed for socio economic diversity of India emphasizing not only technological innovation but also judicial supervision and forensic reliability. Such an approach will make proper use of potential of AI simultaneously safeguarding justice and human rights in the modern world.

I. Introduction

A. The Digital Payments Revolution in India

India has become a global leader in digital payment ecosystem with the UPI leading this transformation. In the year 2024 UPI recorded approximately 17,220 crore transactions valued at ₹246.83 lakh crore representing a 46 percent increase in volume and 35 percent increase in value compared to 2023.[1]This exceptional growth had made India responsible for roughly 49 percent of the digital payment transactions around the world.[2]

The UPI system managed by the National Payments Corporation of India (Hereinafter NPCI) has expanded from enabling 17.9 million transactions in 2017 to over 172 billion transactions in 2024. A compound annual growth rate of 89.3 percent in volume and 86.5 percent in value over five years.[3] In 2024 December it reached a historic milestone with 1,673 crore transactions managing an average of 535 million digital payments per day.[4]

B. The Dark Side of Digital Prosperity: Cyber Financial Crime

However this amazing digital growth brought along with it increase in cyber financial crimes. Between 2024 April and 2025 January 24 lakh reported digital fraud cases took place resulting in losses of ₹4,245 crore a 67 percent spike from the previous year.[5] High value frauds exceeding ₹1 lakh multiplied to 29,082 cases causing losses of approximately ₹175 crore. According to the National Crime Records Bureau (Hereinafter NCRB) online financial frauds constitute 67.8 percent of all cybercrime complaints.[6]

UPI fraud specifically rose 85 percent in FY 2023 to 24 amounting to losses of ₹1,087 crore.[7] Bank frauds has risen three times from 8,752 incidents (₹9,298.4 crore) in FY22 to 32,363

[1] UPI Shines In 2024, Transactions Cross 17,000 Cr Mark, INC42 (Jan. 4, 2025), https://inc42.com/features/upi continues to shine in 2024 transactions cross 17000 cr mark/.
[2] UPI Statistics By Transaction, Usage, Apps and Facts [2024], ELECTROIQ (Dec. 4, 2024), https://electroiq.com/stats/upi-statistics/.
[3] United Payments Interface (UPI) Dominates Digital Payments, Sees Explosive Growth Over Five Years, IBEF (Jan. 28, 2025), https://ibef.org/news/united-payments-interface-upi-dominates-digital-payments.
[4] National Payments Corporation of India, Fraud Risk Management, NPCI, https://www.npci.org.in/who-we-are/risk-management/fraud-risk-management (last visited Oct. 20, 2025).
[5] India's Digital Gold Rush Turns Risky: AI Called In to Police ₹200 Trillion Payments, THE420.IN (Aug. 21, 2025), https://the420.in/financial-fraud-ai-driven-compliance-india-digital-payments/.
[6] MuleHunter.ai, RBI INNOVATION HUB (Feb. 24, 2025), https://rbihub.in/mule-hunter-ai/.
[7] NPCI's AI-Driven Risk Scoring to Help Banks Combat UPI Fraud, MEDIANAMA (Apr. 3, 2025), https://www.medianama.com/2025/04/223-npci-ai-upi-fraud-detection/.

incidents (₹2,714.64 crore) in FY24.[8] The difficult nature of these crimes ranging from mule account operations and phishing attacks to advanced persistent threats requires advance investigative responses.

C. Enter Artificial Intelligence: A Paradigm Shift in Crime Prevention

Traditional rule based fraud detection systems have proven insufficient against the scale, velocity and sophistication of modern cyber financial crimes. These systems characterized by high false positive rates and long turnaround times leave number of fraudulent accounts undetected.[9] Artificial intelligence particularly machine learning algorithms offers a transformative approach by analyzing massive datasets in real time identifying complex patterns invisible to human analysts and keeping up to evolving criminal techniques. The use of AI driven predictive policing technologies in the context of digital payment security by India with particular emphasis on three critical dimensions: (1) technological efficacy and implementation challenges; (2) legal admissibility and evidentiary standards under law of India; and (3) constitutional safeguards for privacy, due process and proportionality has been analyzed in this paper. With the comparative analysis with international systems and careful evaluation of new initiatives of India, this paper proposes an inclusive framework for combining AI, forensic science and law in the unique socio legal context of India.

II. AI Driven Fraud Detection Infrastructure in India

A. MuleHunter.AI By RBI: Architecture and Efficacy

MuleHunter.AI is an AI system developed locally by Reserve Bank of India through its subsidiary known as Reserve Bank Innovation hub. It is an AI/ML based system made to deal with money mule accounts. These are the bank accounts used by criminals to transfer illegal money usually operated by unsuspicious people lure by promises of easy money or force into participation which serve as pillar for cyber financial crime. The transfer of funds through interconnected mule accounts makes tracing and recovery efforts difficult for the agencies.

[8] Business Standard, "Explained: RBI is using an AI tool MuleHunter.ai to cut down digital frauds" (December 9, 2024),https://www.business-standard.com/finance/personal-finance/explained-rbi-has-a-new-ai-tool-mulehunter-ai-to-reduce-digital-frauds-124120900250_1.html

[9] Reserve Bank Innovation Hub, *supra* note 6, at 2.

1. Technical Framework

MuleHunter.AI use advance machine learning algorithms to examine transaction patterns and account details predicting mule accounts with better accuracy and speed as compared to traditional rule based systems.[10] In the development process of this AI consultations were done with various banks to understand existing identification methods and their limitations. Through the cooperation with various institutions the team of developers understood that there are nineteen distinct patterns of mule account behaviour and eventually the same was included into the AI model.[11]

This AI model processes real time as well as near real time transactions producing model scores from behavioural analytics.[12] Key differentiating features includes:

1. **Pattern Recognition**: Identifying anomalous patterns in transactions, unusal movements of money and questionable connections between accounts.

2. **Velocity Analytics**: Detecting fast and back to back transactions that suggest someone is trying to hide where money came from indicating layering strategies are used.

3. **Network Analysis**: Mapping of accounts which are interconnected to detect criminal networks

4. **Adaptive Learning**: Continuous learning of new types of fraud typologies as well as carefully examining the feedback loops

2. Pilot Implementation and Results

At the initial phases of the project which was conducted with the cooperation with two major public sector banks gave encouraging results showing the capability of system to correctly detect mule accounts that had dodged the traditional mechanisms.[13] While the exact accuracy of the model is still unknown industry experts suggest the systems are about 95 percent accurate

[10] BUS. STANDARD, supra note 8.
[11] IndiaAI, RBI's AI Initiative MuleHunter.ai: AI Solution to Tackle Digital Fraud in India, INDIAAI (Dec. 10, 2024), https://indiaai.gov.in/article/rbi-s-ai-initiative-mulehunter-ai-ai-solution-to-tackle-digital-fraud-in-india.
[12] National Payments Corporation of India, Fraud Risk Management, NPCI (Dec. 10, 2024), https://www.npci.org.in/who-we-are/risk-management/fraud-risk-management.
[13] What is MuleHunter.ai, RBI's Latest Initiative to Tackle Financial Frauds, BUS. TODAY (Dec. 6, 2024), https://www.businesstoday.in/personal-finance/banking/story/what-is-mulehunterai-rbis-latest-initiative-to-tackle-financial-frauds-456480-2024-12-06.

with fewer false alerts than old systems. The participating banks in the pilot study got real time alerts through web based mechanism helping to take prompt investigative measures. The fraud reporting feature of system helps in data collection and analysis of trend supporting which in turn helps authorities and organizations take action across the entire system[14]

B. Federated Learning Framework NPCI

To support the initiatives of RBI, NPCI has also developed a federated model with the cooperation of selected banks to increase fraud detection capabilities across the network of UPI.[15] This mechanism integrates internal risk scores of customers of the banks based on demographic features such as age, occupation and history of transactions with own transactions and device profiling scores of NPCI.

1. Federated Architecture

The approach of working together offers several advantages:

1. **Preservation of Privacy**: The data of customers kept safe within respective bank systems while contributing to collective intelligence

2. **Cross Institutional Insights**: Aggregated pattern recognition without direct data sharing

3. **Real Time Risk Assessment**: AI/ML driven fraud scores provided to banks at no cost, enabling real time transaction blocking

2. Fraud Risk Management System

The Fraud Risk Management (FRM) solution of NPCI processes transactions in real time and near real time modes using machine learning and artificial intelligence.[16] The system analyzes fraud reports submitted by member banks to identify trends and initiate corrective actions.

[14] National Payments Corporation of India, Fraud Risk Management, NPCI, https://www.npci.org.in/who-we-are/risk-management/fraud-risk-management (last visited Oct. 20, 2025).
[15] UPI Fraud: How It Works & How Financial Institutions Can Prevent UPI Related Frauds, BANKIQ (June 12, 2025), https://bankiq.co/upi-fraud-how-it-works-and-how-can-financial-institutions-prevent-it/.
[16] National Payments Corporation of India, Fraud Risk Management, NPCI, https://www.npci.org.in/who-we-are/risk-management/fraud-risk-management (last visited Oct. 20, 2025).

Additional security measures include:

1. **Device Binding**: Mandatory linking of devices to bank accounts or Aadhaar cards for UPI app onboarding

2. **SIM Binding**: Active SIM verification to prevent unauthorized account access

3. **Scam Account Flagging**: Warning messages sent to customers before transferring money to accounts flagged as fraudulent by other users.[17]

C. State Level Implementations and Hybrid Models

Several states of India have initiated predictive policing programs though adoption remains uneven. Uttar Pradesh and Delhi have deployed AI applications for crime prevention including predictive policing, video surveillance analysis and investigation support.[18] However comprehensive data regarding state level efficacy remains limited partly due to confidentiality concerns and inadequate data sharing protocols.

The collaboration between NPCI and the Institute for Development and Research in Banking Technology (IDRBT) multiplies efforts to strengthen cybersecurity infrastructure through specialized training programs addressing cybersecurity best practices, operational resilience and data privacy.[19]

III. Legal Framework for AI Evidence in India

A. The Indian Evidence Act, 1872 and Electronic Evidence

The admissibility of AI generated evidence in Indian courts hinges primarily on provisions governing electronic evidence under the Indian Evidence Act, 1872 and its successor the Bharatiya Sakshya Adhiniyam, 2023.

[17] NPCI's AI-Driven Risk Scoring to Help Banks Combat UPI Fraud, MEDIANAMA (Apr. 3, 2025), https://www.medianama.com/2025/04/223-npci-ai-upi-fraud-detection/.
[18] AI Policing in India: Existing Research and Where to Begin Future Research, ACADEMIA.EDU (Sept. 1, 2024), https://www.academia.edu/123442551/.
[19] Banks, RBI Unite to Launch Digital Fraud Detection Platform, COINGEEK (Jul. 25, 2025), https://coingeek.com/banks-rbi-unite-to-launch-digital-fraud-detection-platform/.

1. Section 65B: The Cornerstone of Electronic Evidence

Section 65B of the Indian Evidence Act, 1872 represents the statutory foundation for electronic evidence admissibility.[20] This provision establishes that information contained in electronic records, printed on paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be deemed a document and is admissible in proceedings without further proof or production of the original provided certain conditions are satisfied.

Critical Conditions under Section 65B(2):

- The computer output must be produced during regular course of activities by persons with lawful control over the computer
- Information must be regularly fed into the computer in the ordinary course of activities
- The computer must have been operating properly during the material period or any improper operation must not affect the accuracy of electronic record
- Information in the electronic record must derive from information fed into the computer in the ordinary course of activities[21]

2. The Certificate Requirement: Section 65B(4)

Section 65B(4) mandates a certificate identifying the electronic record describing the manner of production and providing particulars of the device. This certificate must be signed by a person in charge of the computer or relevant activities.[22] The Supreme Court in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) confirmed that Section 65B constitutes a complete code for electronic evidence admissibility superseding other provisions.[23]

3. Bharatiya Sakshya Adhiniyam, 2023: Evolution and Expansion

The Bharatiya Sakshya Adhiniyam, 2023 which replaces the previous evidence act

[20] Indian Evidence Act, 1872, § 65B.
[21] *Ibid.*, § 65B(2).
[22] *Ibid.*, § 65B(4).
[23] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 3 SCC 216.

significantly expands the scope of electronic evidence. Section 63 of BSA (corresponding to Section 65B of IEA) classifies electronic records as primary evidence rather than secondary evidence.[24] This represents a substantive upgrade in the legal status of digital evidence.

Key BSA Innovations:

1) Expanded definition of electronic records to include information stored in semiconductor memory or any communication devices (smartphones, laptops)

2) Inclusion of emails, server logs, smartphones, locational evidence, and voice mails

3) Recognition that electronic or digital records have the same legal effect as paper records

4) Provision for Examiner of Electronic Evidence to assist courts in forming opinions on such evidence[25]

B. Information Technology Act, 2000: Complementary Framework

The Information Technology Act, 2000 provides complementary provisions for cyber investigation and digital evidence. As a primary cybercrime legislation of India, it was enacted to provide legal recognition to electronic transactions and facilitate electronic governance while preventing cybercrime.[26]

1. Key Investigative Provisions

Section 69A: Empowers authorities to intercept, monitor or decrypt information in computer resources if necessary for sovereignty, integrity, defense, security or public order.[27] The provision includes procedural safeguards and has been upheld by the Supreme Court despite privacy concerns with the Court holding that national security takes precedence over individual privacy in certain contexts.

Section 78: Establishes investigative authority providing that police officers not below the rank

[24] Bharatiya Sakshya Adhiniyam, 2023, § 63.
[25] Electronic Evidence under Bhartiya Sakshya Adhiniyam, 2023, DRISHTI JUDICIARY, https://www.drishtijudiciary.com/bharatiya-sakshya-adhiniyam-&-indian-evidence-act/electronic-evidence-under-bhartiya-sakshya-adhiniyam-2023 (last visited Oct. 20, 2025).
[26] Information Technology Act, 2000.
[27] *Ibid.*, § 69A.

of Inspector may investigate offenses under the Act.[28] This provision ensures cybercrimes are investigated by experts while keeping proper supervision in place.

Search and Seizure: The police officers authorized to conduct search and seizure, can now search and seize computer devices or data related to cyber crime after following the proper procedural requirements under the Code of Criminal Procedure, 1973(Now BNSS, 2023).[29]

2. Amendments and Evolution

In 2008 major amendments were introduced in the Information Technology Act, 2000[30] to strengthen fines/penalties and making certain cyber crimes as serious category offences. Under section 43A[31] the concept of corporate liability was introduced for the failure to take reasonable security measures for sensitive personal data.[32] Section 79[33] introduced the concept of safe harbor protection to intermediaries from liability for third party content, subject to certain conditions imposed by government.

C. Challenges in AI Evidence Admissibility

Even though there are detailed framework, there exist several challenges which complicates AI evidence admissibility:

1. The Problem of Black Box

Deep learning neural networks deployed by AI operate as black boxes where the process of decision making remains opaque even to their creators.[34] This decision making process conflicts with basic evidentiary principles requiring transparency, verifiability and cross examination rights. Courts need to check if AI evidence is real and reliable even though they can't always understand how the AI reached its conclusions.

---

[28] *Ibid.*, § 78.
[29] Introduction to Cyber Crimes: Relevant Provisions Under The Information Technology Act, 2000, LEGAL SERV. INDIA, https://www.legalserviceindia.com/legal/article-14379-introduction-to-cyber-crimes-relevant-provisions-under-the-information-technology-act-2000.html (last visited Oct. 20, 2025).l
[30] Information Technology Act, 2000, No. 21 of 2000.
[31] Information Technology Act, 2000, § 43A (as amended 2008).
[32] Information Technology Act, 2000, § 43A (as amended 2008).
[33] Id.
[34] AI-Generated Evidence in Indian Courts: Admissibility and Legal Challenges, LAW JURIST (Jul. 1, 2025), https://lawjurist.com/index.php/2025/07/02/ai-generated-evidence-in-indian-courts-admissibility-and-legal-challenges/.

2. Certificate Compliance for AI Systems

The certificate rules were designed for traditional computer systems with human operators. However modern AI fraud detection systems work very differently they operate across multiple networks, use cloud storage and continuously learn from data shared between different systems. This creates problems: Who is responsible? In a system spread across many computers and locations, it is unclear who the "person in charge" is. How to certify a changing system? Traditional certificates assume the computer system stays the same. But AI systems constantly learn and update themselves so how can someone certify that it is working properly when it keeps changing? Section 63(4) of BSA 2023[35]**:** The new law has similar challenges but adds more requirements now two signatures needed **of** both a responsible official and a technical expert must sign the certificate. The problem remains even with these new rules it is still unclear how to certify AI systems that are distributed, constantly learning and have no single person in charge.

3. Reliability and Validation Standards

The courts must check the credibility and reliability of data quality on which a model is trained, bias reduction efforts and accuracy parameters of an AI system. The lack of standard forensic protocols for the validation of AI system results in inconsistency in judicial treatment. The Supreme Court of India in the case of *State of Maharashtra v. Dr. Praful B. Desai*[36] *noted*, that courts must adapt to technological changes while ensuring that no tampering of electronic records took place during investigation.[37]

4. Chain of Custody in AI Generated Evidence

Traditional chain of custody rules must be changed to keep up with the AI systems. Also mechanism needs to be evolved to check whether AI generated alerts or risk scores are genuine or not.

IV. Constitutional Dimensions: Privacy, Due Process and Proportionality

A. Right to Privacy as a Fundamental Right

[35] Bharatiya Sakshya Adhiniyam, 2023, § 63(4).
[36] *State of Maharashtra v. Dr. Praful B. Desai*, (2003) 4 SCC 601.
[37] Id.

The Supreme Court of India in the judgment of *Justice K.S. Puttaswamy v. Union of India*[38] held that privacy holds the position of fundamental right as it is an intrinsic part of Article 21[39] of the Constitution.[40] This decision has deeply affected the AI driven surveillance and predictive policing.

1. What are the components of Right to Privacy?

The Court identified multiple dimensions of privacy which are also relevant from the perspective of AI policing:

1) **Bodily Privacy**: Biometric data cannot be forcefully collected from an individual
2) **Informational Privacy**: Control over sensitive data and its circulation in the market
3) **Decisional Privacy**: State cannot interfere with personal choices of Individual
4) **Locational Privacy**: Freedom of movement, state cannot constantly keep surveillance on the movement of individual[41]

2. The Proportionality Test

For any infringement to identify as a valid infringement of privacy, it must satisfy a proportionality test:

1. **Legality**: The action of State must be carried as per the law
2. **Legitimate Aim**: The action of state must lead to a legitimate state objective
3. **Necessity**: For achieving that objective the action of the state is necessary
4. **Proportionality**: The action must be in proportion to the objective it wants to achieve
5. **Procedural Safeguards**: sufficient procedural protections must be provided against

[38] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[39] Constitution of India, art. 21.
[40] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[41] Right to Privacy as a Fundamental Right in AI Era, LAWBHOOMI (Aug. 29, 2025), https://lawbhoomi.com/right-to-privacy-as-a-fundamental-right-in-ai-era/.

arbitrary state action[42]

AI driven predictive policing systems involving mass data collection, profiling and surveillance must satisfy each element of this test. The wholesale surveillance of communities and individuals as practiced in some predictive policing implementations potentially violates privacy rights absent compelling justification and procedural safeguards.[43]

B. Equality and Non-Discrimination: Article 14

Article 14 of the Constitution of India guarantees equality before law and equal protection of laws. AI systems trained on biased historical data risk perpetuating and amplifying existing discriminatory patterns.[44] In context of India where marginalized communities have historically experienced disproportionate policing, AI algorithms may reinforce caste based, religious or socio economic discrimination.

1. Algorithmic Bias Concerns

AI crime prediction systems that learn from old police data may keep sending police to the same neighbourhoods that were heavily policed before, turning predictions into reality and continuing unfair treatment. This is called algorithm bias when the data itself is not fairly collected. Since there is no transparency about what data was used to train these systems, how they work or what triggers their decisions. It is impossible to properly check if they violate constitutional rights.

2. Equal Access to Justice

AI fraud detection systems should not unfairly target certain groups of people by wrongly flagging them as fraudsters more often than others. This leads to innocent people having their bank accounts frozen, being denied banking services or even being falsely prosecuted for crimes. The constitution guarantees equal treatment for everyone which means AI systems must treat all people fairly regardless of their background.

---

[42] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[43] Opiniolegal India, Predictive Policing — A Threat to Legal and Constitutional Rights?, MEDIUM (Nov. 19, 2022), https://medium.com/@opiniolegal.india/predictive-policing-a-threat-to-legal-and-constitutional-rights-fc071d9cc879.
[44] AI, Privacy & Fundamental Rights, LAWBHOOMI (Sept. 2, 2025), https://lawbhoomi.com/ai-privacy-fundamental-rights/.

C. Due Process and Fair Trial Rights: Article 21 and 22

Articles 21 and 22 guarantee the right to fair legal treatment and a fair trial including protection from being arrested without proper reason and the right to know why you are being arrested.[45] AI systems that predict crime and label people as likely criminals based on computer risk scores may weaken these constitutional protections.

1. Presumption of Innocence

Predictive policing goes against the basic principle that everyone is innocent until proven guilty by labeling people as high risk before they commit any crime. When these computer predictions influence whether someone gets arrested, whether they get bail or where police focus their attention the AI stops being just an investigation tool and becomes a decision maker. This transfers power from human decision makers to hidden computer programs that cannot be held accountable in the same way.[46]

2. Right to Challenge Algorithmic Decisions

Fair legal treatment requires that people have a real chance to challenge decisions that harm them. When AI systems mark bank accounts as fraudulent or label people as high risk those affected must have:

1) Information that an AI system made the decision about them
2) An explanation of how and why the AI made that decision
3) A chance to provide evidence that proves the decision is wrong
4) The right to have a human review and change the AI decision[47]

Most AI systems being used today do not have these protections raising serious concerns about whether they provide fair legal treatment as required by the constitution.

[45] Constitution of India, Arts. 21, 22.
[46] AI Governance in India: Balancing Constitutional Rights, Algorithmic Fairness, and Ethical Regulation, FASTRACK LEGAL SOLS. (Mar. 21, 2025), https://fastracklegalsolutions.com/ai-and-indian-constitution/.
[47] AI, Surveillance and Privacy in India: Human Rights in the Age of Technology, OXFORD HUM. RTS. HUB, https://ohrh.law.ox.ac.uk/ai-surveillance-and-privacy-in-india-human-rights-in-the-age-of-technology/ (last visited Oct. 20, 2025).

D. The Digital Personal Data Protection Act, 2023: Gaps and Limitations

The Digital Personal Data Protection Act (DPDPA), 2023 represents primary data protection legislation of India. However it contains significant limitations regarding AI surveillance and predictive policing.[48]

Critical Deficiencies:

1. Section 17 allows the government to ignore the law for broad reasons like national security and public order
2. No strong protections against surveillance practices
3. No independent agency with power to enforce the law against government departments
4. Weak rules about AI decision making and profiling

These weaknesses allow AI surveillance systems to work without proper oversight potentially enabling widespread surveillance that violates constitutional privacy rights.

V. Comparative Global Perspectives on AI Predictive Policing

A. United States: Pioneer and Cautionary Tale

The United States has been a leader in using predictive policing. Companies like Palantir and PredPol have created and used these systems in major cities such as Chicago, Los Angeles, New Orleans and New York since 2012.[49]

1. Technical Implementation

U.S. systems usually use one of two methods one predicting where crimes will happen or two predicting which people will commit crimes again. For example the Chicago Police Strategic Subject List (SSL) gave risk scores to individuals claiming to predict how likely they were to

[48] Digital Personal Data Protection Act, 2023, No. 22 of 2023.
[49] AI & Global Governance: Turning the Tide on Crime with Predictive Policing, U.N. U. (Sept. 5, 2023), https://cpr.unu.edu/publications/articles/ai-global-governance-turning-the-tide-on-crime-with-predictive-policing.html.

be involved in violent crime.

2. Critical Backlash and Discontinuation

Many cities stopped using predictive policing after widespread complaints about racial discrimination, lack of openness and doubts about whether it actually worked. In 2020 Santa Cruz California became the first U.S. city to ban predictive policing tools because of concerns about civil rights.[50] Studies demonstrated that these systems disproportionately targeted minority communities reinforcing discriminatory policing patterns rather than reducing crime.

B. European Union: Regulatory Leadership

The European Union has taken a more careful approach, focusing on government supervision and protecting basic rights.

1. The EU AI Act: Comprehensive Regulation

The EU Artificial Intelligence Act which takes effect in February 2025 creates rules for AI systems based on how risky they are.[51] Most importantly article 5 bans the use of AI systems that predict whether someone will commit a crime based on their profile, location or past criminal record recognizing that such systems pose serious threats to basic human rights.[52]

Prohibited Practices under EU At:

- Predictive policing systems based on profiling, location, or past criminal behavior.
- Emotion recognition systems in law enforcement, border management, workplace and educational institutions.
- Indiscriminate scraping of biometric data from social media or CCTV footage for facial

[50] Surveillance and Predictive Policing Through AI, DELOITTE, https://www.deloitte.com/global/en/Industries/government-public/perspectives/urban-future-with-a-purpose/surveillance-and-predictive-policing-through-ai.html (last visited Oct. 20, 2025).
[51] AI Act: A Step Closer to the First Rules on Artificial Intelligence, EUR. PARL. (May 11, 2023), https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence.
[52] The Promises and Perils of Predictive Policing, CIGI, https://www.cigionline.org/articles/the-promises-and-perils-of-predictive-policing/ (last visited Oct. 20, 2025).

recognition databases.

2. GDPR and Law Enforcement Directive

The General Data Protection Regulation (GDPR) and Law Enforcement Directive (LED) provide comprehensive data protection frameworks applicable to policing contexts mandating:

1. Data minimization and purpose limitation
2. Transparency regarding data processing
3. Rights of access, rectification and erasure
4. Independent supervisory authority oversight
5. Data protection impact assessments for high risk processing[53]

C. United Kingdom: Pioneering and Contested

UK police forces have emerged as global pioneers in algorithmic policing technologies including live facial recognition, geographic hotspot mapping and individual risk assessment tools.[54]

1. Implementation Examples

The Harm Assessment Risk Tool (HART) of Durham Constabulary employs machine learning to predict recidivism likelihood over two years informing referral decisions for rehabilitation programs.[55] Manchester police utilized predictive measures to reduce robberies, burglaries and vehicle thefts by double digits in initial implementation.[56]

[53] Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [General Data Protection Regulation]; Council Directive 2016/680, 2016 O.J. (L 119) 89 (EU) [Law Enforcement Directive].
[54] How Algorithmic Policing Challenges Fundamental Rights Protection in the EU: Lessons from the United Kingdom, SPRINGER, https://link.springer.com/chapter/10.1007/978-3-031-86813-9_9 (last visited Oct. 20, 2025).
[55] AI in Policing and Security, POST (Nov. 22, 2024), https://post.parliament.uk/ai-in-policing-and-security/.
[56] Artificial Intelligence is Used for Predictive Policing in the US and UK – South Africa Should Embrace It, Too, THE CONVERSATION (Jun. 25, 2024), https://theconversation.com/artificial-intelligence-is-used-for-predictive-policing-in-the-us-and-uk-south-africa-should-embrace-it-too-191266.

2. Legal Challenges and Regulatory Gaps

Despite operational deployment UK implementations face significant legal challenges regarding:

1. Compliance with Human Rights Act provisions protecting privacy and non discrimination
2. Ensuring proper impact assessments are done under the Data Protection Act 2018
3. Being open about how algorithms make decisions
4. Systems to hold people responsible when rights are violated[57]

The Equality and Human Rights Commission has warned that facial recognition technology and predictive policing algorithms are developing faster than laws can keep up with creating gaps in regulation that threaten basic human rights.

VI. Synthesis: Challenges and Opportunities in Context of India

A. Technological Efficacy: Promise and Reality

The AI fraud detection programs of India especially MuleHunter.AI and the shared learning system of NPCI show great potential. However several problems make it difficult to be fully optimistic about them.

1. Data Quality and Availability

AI systems need large amounts of good quality data to work properly. Indian banks face problems with their data. It is not organized in the same way across banks, is often incomplete and banks do not share information well with each other. Banks in rural and semi urban areas often do not have the digital systems needed to collect complete data creating gaps where fraud

[57] How Algorithmic Policing Challenges Fundamental Rights Protection in the EU: Lessons from the United Kingdom, SPRINGER, https://link.springer.com/chapter/10.1007/978-3-031-86813-9_9 (last visited Oct. 20, 2025).

goes undetected.[58]

2. Resource Constraints in Forensic Capacity

While urban centers may access sophisticated AI tools, rural forensic laboratories lack technical expertise, hardware infrastructure and trained personnel for AI assisted investigations. This capacity gap creates uneven fraud detection and prosecution capabilities across jurisdictions.

3. Cross Border Crime Investigation

Digital financial crimes often cross-country borders. Indian AI systems need to work together with law enforcement and financial intelligence agencies from other countries. However current systems lack strong methods for sharing data across borders providing legal help to other countries and coordinating investigations. This makes it harder to fight criminal networks that operate internationally.

B. Legal and Procedural Gaps

1. Absence of AI Specific Evidentiary Standards

Neither the old Indian Evidence Act nor the new Bharatiya Sakshya Adhiniyam has specific rules for evidence created by AI. Courts do not have standard procedures for:

1. Checking if an AI model is reliable and accurate
2. Evaluating the quality of data used to train the AI and whether it contains bias
3. Reviewing changes made to the AI model over time and its settings
4. Certifying AI systems that work across multiple computers and networks under Section 65B(4) requirements.

2. Inadequate Discovery and Disclosure Mechanisms

Defense lawyers must have access to details about AI systems including the data used to train

[58] Impacts and Ethics of Using Artificial Intelligence (AI) by the Indian Police, EMERALD INSIGHT (Sept. 12, 2024), https://www.emerald.com/insight/content/doi/10.1108/PAP-06-2023-0081/full/html.

them, how they work, their accuracy rates and how often they make mistakes in order to effectively challenge AI evidence. Current legal procedures do not give lawyers enough rights to access this information which may violate the right to fair legal treatment.

3. Judicial Capacity for Technical Evaluation

Judges need training in how AI works, how to understand statistics and how to spot bias so they can properly evaluate AI evidence in court. Without organized training programs there is a risk that judges will either accept AI evidence without questioning it or reject it inappropriately.

C. Constitutional Safeguards: Implementation Imperatives

1. Mandatory Privacy Impact Assessments

All AI predictive policing systems must undergo thorough privacy impact assessments that examine:

1. Whether collecting data is necessary and reasonable for the purpose
2. Whether there are other methods that would invade privacy less
3. Protections to prevent the system from being used for purposes beyond what it was originally designed for
4. Ways to ensure the system operates openly and responsibly

2. Independent Algorithmic Auditing

AI systems that affect basic rights must be checked by independent outside auditors to verify:

1. The system is tested for bias and steps are taken to reduce it
2. The system works accurately for all groups of people
3. The system follows constitutional and legal requirements
4. The system and its data are secure and have not been tampered with

3. Robust Appellate and Review Mechanisms

People affected by AI decisions must be able to:

1. Get a clear explanation of how and why the AI made its decision
2. Have a human review the decision and change it if the AI was wrong
3. Appeal the decision through government departments or courts
4. Get compensation and other remedies if the AI decision was wrong

VII. Proposed Framework: Integrating AI, Forensics and Law

A. Multi Stakeholder Governance Model

For AI predictive policing to work properly it needs organized oversight from multiple groups:

1. **Technical Standards Body:** Sets rules for how AI systems should work, how to test them and certifies they meet standards
2. **Regulatory Oversight Authority:** Checks that rules are being followed, conducts inspections and holds violators accountable
3. **Judicial Training Academy:** Creates training programs for judges, prosecutors and defense lawyers on AI systems
4. **Civil Society Advisory Council:** Ensures openness, allows public input and protects rights of the people
5. **Research and Evaluation Wing:** Conducts studies to check if AI works whether it discriminates and how it affects rights of people

B. Graduated Risk Based Framework

Using a risk based approach similar to the EU AI Act:

Banned Uses:

1. Spying on large numbers of people without specific suspicion about individuals

2. Predicting behaviour based only on caste, religion, or ethnicity
3. Using facial recognition in public places in real time except in emergencies

High Risk Uses (need strict rules and safeguards):

1. AI scoring people as fraud risks which leads to freezing their accounts
2. Systems that automatically monitor and block transactions
3. Sharing financial intelligence information across countries

Medium Risk Uses (need transparency and accountability):

1. Analyzing overall fraud patterns and trends
2. Identifying geographic areas with high fraud
3. Analyzing networks to detect organized crime

Low Risk Uses (need basic oversight only):

1. Detecting unusual activity for humans to review
2. Tools that show patterns visually
3. Using AI to improve administrative efficiency

C. Forensic Standards and Protocols

Creating forensic standards specifically for India that cover:

1. **Testing AI Systems:** Requirements for testing AI before it is used, minimum accuracy levels and checking for bias against different groups of people
2. **Recording Evidence:** Rules for tracking AI created evidence from start to finish keeping records of system versions and settings
3. **Expert Witnesses:** Standards for who qualifies as an AI expert in court what

information they must share and how they can be questioned

4. **Lab Certification:** Requirements for labs that analyze AI evidence to be officially approved

D. Legislative Reforms

Proposed statutory amendments:

Indian Evidence Act/Bharatiya Sakshya Adhiniyam:

1. A new law section dealing with evidence produced by AI systems
2. Rules to verify and certify that AI systems are trustworthy
3. Requirement to reveal how the AI works when used in criminal trials
4. Right for the accused to contest AI based evidence

Information Technology Act:

1. Clear rules about how AI can be used in cyber investigations
2. Privacy protections when AI is used for surveillance
3. Systems to hold AI decision making accountable
4. Agreements for cooperation between countries

Digital Personal Data Protection Act:

1. End the ability of government to ignore data protection laws without limits
2. Clear rules specifically for AI profiling and automated decisions
3. Create an independent Data Protection Authority with power to enforce laws
4. Required assessments of how AI systems affect people

VIII. Conclusion

India is at an important moment in using AI to predict and prevent cyber financial crimes. Programs like MuleHunter.AI, federated learning model of NPCI and various state level projects show that India has both advanced technology and serious commitment to fighting online fraud. Digital payment system in India is massive it handles nearly half of all real time transactions worldwide. Because the system is so large and processes payments so quickly it needs equally powerful mechanism to protect it. However advanced technology alone cannot guarantee fair and effective crime prevention. Using AI in policing and investigations must be supported by strong laws that ensure evidence is reliable complete constitutional protections for privacy and fair treatment and systems that ensure accountability and transparency.

There are several problems right now like no clear rules for AI evidence in court, judges lacking the technical knowledge to evaluate AI systems, weak privacy protections when AI is used for surveillance and different regions having different abilities to analyze digital evidence. These problems harm both how well AI systems work and constitutional rights of people. The Data Protection Act gives the government too many exemptions and has too few rules to hold AI systems accountable missing important chances to protect rights of people. The legal system of India is built on constitutional values like dignity, freedom and equality which provides a solid base for creating a unique way for India to regulate AI. One that uses new technology while protecting the basic rights of people. The suggested solutions including shared governance involving multiple groups, rules based on risk levels, forensic standards and legal changes provide a plan for achieving this balance. As India continues to become more digital the decisions made today about using AI in law enforcement will affect not only how well crime is prevented but also the very nature of Indian democracy. The challenge is to make sure that AI is used as a tool for justice not just for speed and efficiency. AI should support human judgment while remaining accountable to human values and constitutional principles. Only by integrating AI in this balanced way can India unlock the full potential of AI while staying true to its commitment to justice, equality and human rights in the digital age.