COMPREHENSIVE ANALYSIS: THE ROLE OF ARTIFICIAL INTELLIGENCE IN DIGITAL EVIDENCE AND CRIMINAL INVESTIGATION

by

Dr. Manoj Sharma
Advocate
Allahabad High Court, Lucknow Bench

ABSTRACT

Globally, the integration of Artificial Intelligence (AI) is fundamentally transforming the paradigms of criminal justice, forensic science, and the management of electronic proof. Law enforcement agencies, intelligence organizations, and judicial bodies are increasingly incorporating sophisticated algorithmic systems to address the geometric expansion of electronic data generated by modern society. Technologies such as deep-learning-based facial recognition, automated text processing via Natural Language Processing (NLP), predictive policing algorithms, machine learning behavioral models, and automated digital forensics tools are rapidly transitioning from conceptual experiments into core operational infrastructure. These innovations offer unprecedented advancements in processing velocities, pattern-matching accuracy, and proactive crime prevention strategies. However, this algorithmic revolution is not without critical points of friction. The pervasive deployment of autonomous and semi-autonomous systems within the criminal justice apparatus introduces severe systemic risks. These encompass profound constitutional and ethical challenges, including the erosion of individual privacy rights, the weaponization of mass state surveillance, the persistence of socio-economic and racial biases within algorithmic training datasets, an absolute lack of transparency in "black-box" decision-making architectures, and the subsequent threat to due process and fundamental human rights. This comprehensive analysis deconstructs the structural, operational, statutory, and ethical dimensions of AI's burgeoning role in digital evidence management and criminal investigations, evaluating both its disruptive potential and the urgent necessity for robust human-centric regulatory frameworks.

1. INTRODUCTION: THE DIGITAL METAMORPHOSIS OF SOCIETY AND CRIMINALITY

The digital revolution has transformed human civilization, permeating all aspects of living through computing infrastructure, interwoven networks, and ubiquitous mobile sensors. This dependence on the digital world has changed the way that people communicate, transact, work and govern. This pervasiveness of the social change has also created a very scalable, anonymous and borderless space for malicious actors. Traditional criminal operations have evolved over time into well-developed digital versions, and new types

of purely digital threats have sprung up. Police forces no longer just police the streets, they now have to deal with the distributed nature of cyber fraud, complex identity theft operations, weaponized ransomware networks, deep-web illicit marketplaces and state-sponsored cyber-terrorism.

The magnitude of this transformation is particularly pronounced in India. According to the National Crime Records Bureau's 'Crime in India 2023' report, cybercrime cases in the country rose by 31.2 per cent in 2023 as compared to the previous year, with registered cases climbing from approximately 52,000 in 2021 to over 86,000 in 2023. Fraud constituted the dominant motive, accounting for approximately 68.9 per cent of all reported cybercrime incidents, while conviction rates at trial remained below three per cent, revealing acute systemic limitations in the detection, investigation, and prosecution of digitally enabled offences.[1]

TRADITIONAL CRIMINALITY	MODERN CYBER-CRIMINALITY
Localized geographic footprints with physical boundaries.	Borderless, distributed operations running across multiple jurisdictions.
Tangible physical evidence trails subject to physical decay.	Transitory, highly volatile digital data stored on virtual servers.
Linear, easily interceptable communication channels.	Encrypted, anonymized peer-to-peer networks and darknets.
Manual execution mechanics requiring physical proximity.	Automated, highly scalable exploit scripts and malware packages.

The amount, types and pace of information created during these contemporary crimes is an overwhelming hurdle for manual human investigation. Even after a routine investigation, hundreds of gigabytes of encrypted communication, location data, financial transactions, app metadata may be found in a single smartphone. At the aggregate level, in complex transnational investigations, data grows at a fast pace into the terabyte and petabyte area. You're in a place where you're taking a lot of bullets and there's no old school police work. AI has thus been transformed from a so-called "luxury" technology to a must-have basic tool. In addition to their ability to quickly ingest, clean, parse and analyse vast numbers of multi-modal, unstructured data with unparalleled speed and granularity, AI frameworks can fill the tactical intelligence gap between raw data collection and actions.

2. THEORETICAL FOUNDATIONS AND THE NATURE OF DIGITAL EVIDENCE

Conceptualizing Electronic Proof

[1] National Crime Records Bureau, 'Crime in India 2023' (Ministry of Home Affairs, Government of India, 2025) <https://ncrb.gov.in> accessed 15 June 2026.

Digital evidence is any information with particular probative value, stored, processed or transmitted electronically and presented in court to prove or disprove a disputed fact. Physical evidence, which includes fingerprints, ballistics, and biological evidence, has clearly discernible, physical characteristics while digital evidence is made of numbers and binary configurations (0s and 1s) that are interpreted by hardware and software layers.

Classifications of Digital Evidence

Digital evidence exists within a wide range of sources as described in modern forensic models:

- **Communications Data:** Electronic mail packets, instant messaging applications (end-to-end encrypted and clear text), voice-over-IP (VoIP) logs, social media communications.
- **Media and Surveillance Records:** HD closed circuit television (CCTV) video, dash camera video, body-worn camera video, and digital photos.
- **Transactional and Financial Metadata:** Online banking ledgers, Credit Card Processing Logs, Cryptocurrency blockchain Ledgers, E-commerce transaction histories.
- **System and Network Metadata:** IP routing tables, Wi-Fi handshake logs, Cell-tower ping data, Operating system registry files, and file system timestamps (Creation, Modification and Access times).
- **Cloud and Remote Repositories:** : Distributed server data, off-site backed up archives and synced device profiles.

Core Legal and Technical Vulnerabilities

Digital evidence has special ontological characteristics that make collection and admittance of this type of evidence to a court process very complex:

Fragility ‖ Malleability ‖ Volatility

1. **Extreme Fragility:** Unintended interaction with a running system may alter or overwrite important information or metadata at any time, thereby rendering it irretrievably unpreserving.
2. **Malleability and Manipulation Risk:** Digital files can be copied, altered, or even completely fabricated and without easily detectable macroscopic evidence. This is worsened by the advent of generative AI models, which allow for the easy generation of hyper-realistic fake media (or ‘deepfakes').
3. **The Volatility Challenge:** Critical information stored in the device's Random Access Memory (RAM) or temporary network buffers is immediately destroyed when the device is powered down or when the system is booted or restarted, and requires “live forensics” interventions.

Thus, it is crucial to obtain the absolute authenticity, integrity, and uncorrupted chain of custody for digital

evidence in order for it to be admissible under the modern rules of evidence.

3. THE PRACTICAL APPLICATIONS OF ARTIFICIAL INTELLIGENCE IN CRIMINAL INVESTIGATIONS

AI is not a single solution, but rather a set of several different related methodologies that mimic human thought, recognize, or learn from patterns and relationships. Create complex designs and make own judgments.

3.1 Crime Pattern Analysis and Predictive Policing

Predictive policing uses crime logs, socio-demographic information, meteorological data and spatial-temporal information to uncover unique geographical correlation and forecasting crime trends. AI systems process years of Revenue Watch's incident data enables the identification of hotspot areas with the help of high-tech Machine Learning (ML) architectures such as Risk. Terrain Modeling (RTM) and Hot Spot Analysis to detect where particular offenses (e.g., residential burglary) are most likely to occur.

A certain period of time has the highest risk statistic for burglaries, vehicle thefts or violent conflicts. That enables police departments to make the best use of resources—dispatch patrol units to areas where crimes are likely to occur before they happen—instead of relying on simply a reactive approach to policing and move toward a proactive deterrent approach.

3.2 Facial Recognition Technology (FRT)

Biometric AI models have revolutionized the way that human faces are represented as unique mathematical vectors, which can then be compared to the faces of known suspects. Advanced Convolutional Neural Networks (CNNs) locate key facial features on the human face, like the exact distance between the eyes, the depth of the eye sockets, the shape of the cheek bones and the symmetry of the jaw line. These algorithms can quickly and automatically compare, for example, images taken by urban CCTV systems or low-res images of individuals in photographs, with large centralized databases of criminal images (with millions of images) or civil identity information. FRT allows investigators to monitor the movements of known fugitives in a very populated public space, identify unconscious victims and scan extensive crowds for people on watchlists.

In the Indian context, the deployment of automated facial recognition systems by state police forces has proceeded without a dedicated statutory framework. Several state agencies, including those in Delhi, Bengaluru, Hyderabad, and Maharashtra, have operationalised facial recognition systems, while India has yet to enact specific legislation governing the conditions of permissible use, data storage, or redressal mechanisms. Civil society organisations, including the Internet Freedom Foundation, have called for a moratorium on biometric facial recognition systems pending the establishment of stronger legal safeguards. The risks attendant to unregulated deployment were concretely illustrated in 2024 when a breach of the Tamil Nadu Police Facial Recognition Portal exposed over 800,000 lines of data, including personal

information of more than 50,000 individuals.[2]

3.3 AI in Cybercrime Detection and Mitigation

Generative Tools.3.5 AI and the Evolution of Computer Forensics. Modern cyber attack moves are automated and so will be the defence and cyber attack counter measures. AI models run in the background of network environments, detecting phishing attacks, unauthorized network intrusions, identity theft syndicates, high-tech forms of malware, and complex online financial frauds. Unsupervised machine learning algorithms can detect anomalies in real time, such as when a micro-transaction is executed across thousands of shell accounts or a database extraction is attempted at an odd time of day that hasn't been seen before, by using a baseline of "normal" system behavior defined by Anomaly Detection models. This will enable security systems to isolate affected nodes and limit any breaches in data before human analysts are even aware of a compromise.

3.4 Digital Forensics and Advanced Evidence Analysis

At the scene of a crime, when digital media devices are retrieved, forensic experts may find themselves in the difficult position of having to manually process broken up storage drives. AI utilities speed this process up a great deal with automated data triage:

- **File Carver Automation:** AI-powered tools can identify file structures and reconstruct and carve out corrupted or deleted files in unallocated drive space using advanced heuristics.
- **Computer Vision Triage:** This function automatically scans millions of images and videos captured and extracts them, instantly sorting and flagging those that contain illicit material, weapons, narcotics, currency or missing persons. This reduces manual human investigators hours of work by hundreds.
- **Deepfake Audits:** Highly specialized adversarial neural networks compare media at the pixel and frame level to identify anomalies in lighting and unnatural eye blinking and facial boundary artifacts to determine if a digital video or sound recording is synthetically created or modified.

3.5 Voice Recognition and Natural Language Processing (NLP)

Criminal enterprises often use technical terms, code words or several languages to blend their activity into unreadable messages during intercepted communications. The NLP engines are specifically developed to accept huge amounts of text and voice data, and perform real-time translation, keyword spotting, and semantic sentiment analysis. Moreover, biometric speaker identification algorithms can be applied to voice from wiretaps or audio files that have been stolen. The system can use different vocal metrics, including fundamental pitch frequency changes, formant shifts, and behavioral speech cadences, to accurately recognize a person's ‘voiceprint' even when they are using voice-modulating software, speaking in a

[2] Software Freedom Law Centre, ‘Analysis of the Facial Recognition Technology-enabled Surveillance Landscape in India’ (SFLC, November 2024) <https://sflc.in/analysis-of-the-facial-recognition-technology-enabled-surveillance-landscape-in-india/> accessed 15 June 2026; Anisha Hingorani, ‘Indian Police Adopt Facial Recognition Despite Risk of Massive Data Breaches’ (Biometric Update, 7 May 2024) <https://www.biometricupdate.com/202405/indian-police-adopt-facial-recognition-despite-risk-of-massive-data-breaches> accessed 15 June 2026.

whisper, or using a foreign speech pattern.

4. MODERNIZING DIGITAL EVIDENCE MANAGEMENT SYSTEMS (DEMS)

In addition to the tactical use of Artificial Intelligence in the field investigation, AI has a key structural role in the administrative processes of evidence on its way to court. Structural inefficiencies, data silos and human weaknesses plague traditional evidence management systems. By incorporating AI, Digital Evidence Management Systems (DEMS) can enhance various critical aspects of their operation, addressing these challenges, including the following:

1. **Automated Ingestion and Semantic Indexing:** 2. Automated Ingestion and Semantic Indexing: As varied data streams like body-worn camera footage, dashcam media, audio interrogations and scanned documents are ingested into a secure DEMS, AI automatically generates descriptive metadata tags. It keeps the files sorted by date, location, case number, involved persons, the objects or words that have been recognized. It is an extremely informative searchable repository.
2. **Mitigation of Manual Error:** Manual data entry is always susceptible to errors, omissions and typos. AI also handles the indexing process, which automatically detects inconsistencies, missing information and more. or files that are not properly cross-referenced, guaranteeing that crucial evidence is not lost due to bureaucratic mistakes.
3. **Algorithmic Chain-of-Custody Tracking:** To meet the rigorous requirements for evidence to be admissible in court, evidence should have an unbroken and verifiable chain of custody that documents each person who accesses, views, or transfers the asset. The access log automatically gets continuously reviewed by AI-powered DEMS and it uses the anomaly detection algorithm to detect unauthorized access to viewing, abnormal export commands, or non-compliant modifications, which helps protect the legal integrity of the record.
4. **Accelerated Case Assembly and Legal Retrieval:** In the discovery phase of a trial, prosecutors and defense attorney will need to review thousands of pages of documentation. With AI search engines, attorneys can query case systems semantically and get instant access to contextually relevant evidence from all media types.

5. THE INDIAN LEGAL LANDSCAPE GOVERNING DIGITAL EVIDENCE

The Statutory Framework

- **Information Technology Act, 2000 (IT Act):** IT Act is the cornerstone of Indian cyber law, offering the general legal framework for the recognition of electronic transactions, digital signatures, and electronic records. It explains what constitutes cyber crime and spells out the Criminal Code of the United States for illegal access to data, identity theft and data breaches.
- **Bharatiya Sakshya Adhiniyam, 2023 (BSA):** supersedes the old Indian Evidence Act 1872, which was enacted under British colonial rule, and is a structural change to make evidentiary rules more

responsive to the modern digital world. The BSA greatly broadens the definition of "documents" to expressly include electronic and digital records, which helps to make it easier to admit the evidence of a smartphone, cloud record, or server log.

- **Digital Personal Data Protection Act, 2023 (DPDP Act):** DPDP Act brings in a robust compliance framework for the protection of data in India. The Act imposes specific formulating restrictions and exemptions for the state law enforcement and national security agencies to enable proper criminal investigations, but at the same time it imposes very important restrictions on the processing, storage and protection of citizens' personal data.

The Constitutional Mandate and Judicial Oversight

The application of algorithmic methods and digital collection approach should always be in keeping with the general constitutional safeguards embodied in the constitution of India. The fundamental Rights to Life and Personal Liberty are guaranteed in Article 21. The definition of this article has been greatly broadened by the Supreme Court of India in the landmark case of *Justice K.S. Puttaswamy v. Union of India (2017).* The nine judge bench unanimously ruled that the Right to Privacy is an inherent and fundamental part of Article 21.

The Puttaswamy case sets out a three-part test for the states' intervention and surveillance regime to be constitutionally acceptable:

Legality (Statutory Authority) × Need (Legitimate State Aim) × Proportionality

An AI based police system that does not meet this three-fold test is unconstitutional and a violation of Article 21.

6. STRUCTURAL ETHICAL REALITIES, LEGAL PITFALLS, AND SYSTEMIC VULNERABILITIES

Algorithmic Bias and Data Pollution

Artificial Intelligence models are not conscious but they learn to predict based on the historical data. The AI will learn, repeat, and validate these human biases with a veneer of mathematical objectivity if they are embedded in the historical data that it is trained to recognize.If the biases, systemic discrimination or disproportionate policing trends are present in the historical data that the AI is trying to learn, it will do so and perpetuate them under the guise of mathematical objectivity. If predictive policing models are based on past arrest data that. If someone is targeted disproportionately by the algorithm, then over time police patrol is going to be concentrated in those areas. This is an "extraordinary feedback loop.

The Black-Box Problem and the Loss of Transparency

The contemporary deep learning models work through hugely complex multi-layered neural networks.

These systems are very good at prediction, but the way they make their decisions, is in many cases, completely opaque, which is called by the "black-box problem". It is difficult for a human investigator, defense counsel or the sitting judge to follow The exact reasoning or weightings the AI uses to conclude that a suspect is a high-risk suspect. The absence of explainability Contrary to the fundamental law principle of the Principles of Natural Justice and Right to a Fair trial.

Case Study: The Pegasus Spyware Controversy

In short, the Pegasus spyware scandal developed by the NSO Group warns of the risks of sophisticated spyware. digital surveillance technologies. Pegasus is a category of sophisticated cyber weapons that are capable of carrying out “zero-click” attacks, and These simply could infect the smartphones without any user input and be able to intercept communications, real-time audio and video. Data on video feeds, location, or encrypted messages. This use of Pegasus against journalists, political opposition There were three significant structural weaknesses that were demonstrated by leaders, civil rights activists and judicial officials: accountability of the State, risk of over-surveillance, and susceptibility of civil Digital infrastructure.

In India’s specific experience, a technical committee appointed by the Supreme Court under the supervision of Justice R.V. Raveendran (retired) examined twenty-nine mobile devices submitted by alleged victims. The committee, which submitted its report in July 2022, found malware in five of the twenty-nine devices but was unable to conclusively attribute the malware to Pegasus spyware, in part because the Union of India declined to cooperate with the committee’s investigation. The court noted explicitly that the government had not extended the required cooperation, and the committee’s recommendations regarding legal and policy frameworks for the protection of privacy remained unimplemented. Subsequent forensic analysis by Amnesty International in December 2023 identified further attempts to target Indian journalists using the NSO Group’s BLASTPASS exploit, corroborating the concerns that had prompted the original petitions.[3]

7. THE LIMITS OF AUTOMATION: WHY ARTIFICIAL INTELLIGENCE CANNOT REPLACE HUMAN JUDGMENT

The potential of AI is growing and there is a very real danger that it will be used to create a fully automated justice system, with algorithms taking the place of human investigators, prosecutors and judges. This vision is born out of a fundamental misunderstanding of the capabilities of AI, which has cognitive limitations.There is an absolute cognitive limitation in AI that makes this vision fundamentally incorrect.

The Absence of Empathy and Moral Reasoning: AI systems are basically mathematical optimization systems, computing statistical relationships from binary data inputs. They lack any ability to display real human empathy, compassion or moral judgment. The administration of justice can not be conducted on the

[3] Manohar Lal Sharma v Union of India, Writ Petition (Civil) No 314 of 2021; Deccan Herald, ‘Pegasus Snooping Case: Malware Found in 5 Phones but No Conclusive Proof That It Had Spyware, Says Supreme Court’ (Deccan Herald, 25 August 2022) <https://www.deccanherald.com/national/pegasus-snooping-case-malware-found-in-5-phones-but-no-conclusive-proof-that-it-had-spyware-says-supreme-court-1139110.html> accessed 15 June 2026.

basis of a binary logic applied to a set of facts. It requires an understanding of human suffering, structural socio-economic mitigations and the specific nature in terms of moral complexity of the offence.

The Disconnect Between Correlation and Causation: Machine learning algorithms are great at finding correlations – that is, that Variable A is often seen with Variable B. Correlation cannot be taken as causation. An AI can identify a geographic location or an individual that has specific statistical patterns, but it doesn't have a cognitive ability to make inferences on the causal relationships. This is a space that must be filled in by the discretion of man.

Judicial Accountability and the Democratic Mandate: In a democratic society, the power to limit a person's freedom. The arrest or incarceration of a person or object in order to secure one's freedom is profound in the moral sense. This is an electrical power that must be connected to an institutional accountability. Algorithms can't be blamed. You can't lock up a software or software program without finding them guilty of something. There should never be technology that serves as the main basis for asserting the legitimacy of democratic institutions.

8. INTERNATIONAL DEVELOPMENTS: COMPARATIVE FRAMEWORKS

When analysing the strategies and approaches of various country-states in incorporating AI into their criminal justice Artificial Intelligence in Digital Evidence & Criminal Investigation Different priorities for security, efficiency and human rights are found in systems:

- **United States of America:** First country to use predictive policing software (Geolitica/Predpol). Pre-trial and sentencing risk assessment tools based on algorithms (COMPAS). This broad use, however, has led to an inordinate amount of internal litigation and, as a result, academic debate about the extent of the racial bias.
- **United Kingdom:** the Government has deployed large-scale Automated Facial Recognition (AFR) systems in major cities, primarily under the Metropolitan Police Service (MPS). This has given rise to important legal questions about the consistency of the scanning of biometrics in real time with the provisions of privacy laws.
- **People's Republic of China:** Embarked on an extremely top-down approach towards embedding AI in state surveillance, creating gigantic urban surveillance initiatives such as Sharp Eyes. In this context, AI is an overt means of mass social control and preemptive political surveillance.
- **Republic of Estonia:** At the global level, Estonia is pioneering with the use of "AI judges" in its justice system for resolving small-claims disputes within a financial limit. Importantly, it is a system based on clear rules which are immediately subject to de novo review by a human judge.

European Union: The European Union enacted Regulation (EU) 2024/1689, commonly known as the EU Artificial Intelligence Act, which entered into force in August 2024 and represents the world's first comprehensive risk-based statutory framework for AI governance. Under the Act, AI systems deployed in

law enforcement contexts, including predictive policing, real-time biometric identification in public spaces, and AI tools used to evaluate the reliability of criminal evidence, are classified as high-risk and subject to stringent pre-deployment conformity assessments, transparency obligations, and mandatory human oversight requirements. The Act further prohibits, without exception, the use of AI systems to profile individuals for the purpose of predicting criminal offences based solely on demographic characteristics, establishing a categorical red line that reflects a broader commitment to the protection of fundamental rights in algorithmic governance.[4]

9. STRATEGIC RECOMMENDATIONS FOR A ROBUST NATIONAL FRAMEWORK

1. **Codification of Dedicated AI Governance Legislation:** There is a need for a dedicated and comprehensive law "Artificial Intelligence Regulation Act" for the criminal justice sector. The rules and regulations have to be clearly stipulated regarding allowable and non-allowable use scenarios of AI.
2. **Mandating Algorithmic Transparency and Explainability:** Before the violation of a defendant's right to a fair trial, proprietary ‘trade secret' exemptions must never be permitted to override the need for transparency and explainability. The law should require any AI tool used to create investigative leads to be based upon open source logic or full disclosure of the source code.
3. **Establishment of an Independent Algorithmic Audit Commission:** A multi-disciplinary, independent algorithmic audit commission, consisting of (digital forensic) experts, human rights lawyers, data scientists and retired judges, should be established to carry out regular, mandatory audits before and after deployment.
4. **Specialization of Investigator Training and Digital Literacy:** Specialization of Investigator Training and National and state police academies need special curricula to educate on advanced data and its applications. Specialized curricula is needed in national and state police academies to educate the need for advanced data and its applications. Forensics, the workings of machine learning and constitutional limits on electronic surveillance.

10. CONCLUSION

The criminal investigation and digital evidence are being transformed by the use of AI. management. AI provides law enforcement officers with an unprecedented suite of tools for facing the challenges of increasingly common incidents. The sophistication of cybercrime, especially in terms of processing great amounts of data in a short time frame, as well as the ability to identify intricate criminal activities, is what makes the situation so challenging. Networks, and transform court administrative procedures. But the

[4] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence [2024] OJ L 1689 (EU AI Act), arts 5 and 6 and Annex III; European Parliament, ‘EU AI Act: First Regulation on Artificial Intelligence’ (European Parliament, 9 June 2023, updated 2024) <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence> accessed 15 June 2026.

implementation of these powerful technologies can't take place in a legal void. Algorithmic bias, algorithmic decision making and algorithmic mass state surveillance. If not well monitored, they can pose a danger to individual liberty, due process and the right to privacy. The It is not appropriate that criminal justice's future be left in the hands of 'total technological determinism'. It is critical to have AI always.AI should always be there. Supervised by humans in order to maintain democratic principles.

11. FUTURE SCOPE: HORIZON SCAN OF AI IN THE JUSTICE ECOSYSTEM

The future of AI in criminal justice is one in which it's deeply integrated in a number of new technological horizons:

- **Real-Time Behavioral Analytics and Geospatial Monitoring:** Future platforms will not only be based on However, the idea of historical data review has been swapped with the urban IoT sensor arrays and computer vision networks. Geospatial, real-time threat modelling capabilities.
- **Blockchain Integration with Digital Evidence Lifecycle:** Once again, the future will see more integration of blockchain with the Digital Evidence Lifecycle, this time merging the two with AI diagnostics. Blockchain Integration – decentralized blockchain ledgers (a complete tamper-proof chain-of-custody record): Digital Evidence Lifecycle is designed to address the problems of authenticity.
- **Generative Adversarial Deepfake Detection Systems:** to identify such frauds. Customized "Generative Adversarial Deepfake Detection Systems" will be relied upon by law enforcement to detect such frauds. Adversarial Networks" (GANs) that have been specifically developed to identify fake media and disinformation Created with the help of generative AI models.
- **Autonomous Cybercrime Hunting Frameworks:** Independent cybercrime hunting models will be constantly uploaded to the Internet to detect malicious activity. Discovering dark web addresses, monitoring forums underground and mapping of cryptocurrency laundry addresses are automated. decentralized networks: Autonomous Cybercrime Hunting Frameworks.
- **Smart Courtrooms and Automated Case Management:** ntelligent judicial assistants will streamline full legal research and cross-reference with precedents, optimize dockets and provide multi-lingual transcriptions on the spot to clear massive backlogs.

REFERENCES

1. Information Technology Act, 2000 (India).

2. Digital Personal Data Protection Act, 2023 (India).

3. Bharatiya Sakshya Adhiniyam, 2023 (India).

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

5. Research Publications on Artificial Intelligence and Criminal Justice Frameworks, Global Forensic Review.