Page: 129-162 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 3 | Issue 2

2025

DOI: https://doi.org/10.70183/lijdlr.2025.v03.45

UNVEILING THE DARK WEB: AN EXPLORATORY STUDY OF AI-ASSISTED CYBERCRIME INVESTIGATIONS IN INDIA'S HIDDEN INTERNET

Shamik Lodh[1]

I. ABSTRACT

The rise of cybercrime in India, driven by growing indications of digitization and technological advancement, presents formidable challenges to individuals, businesses, and national security. This report brings together existing literature on the landscape for cybercrime in India and the extending role of artificial intelligence (AI) to build investigative capacity. Traditional enforcement practices face challenges to manage the breadth and sophistication of cybercrime; AI provides a set of tools for threat detection, data analysis, digital forensics, and suspect identification.

However, the move toward AI to address cybercrime in India faces legal and regulatory considerations, technical and organizational challenges and ethical considerations. This report reviews the existing legal framework for existing and anticipated cybercrime and AI laws in India, examines the technical and organizational challenges to the implementation of AI in investigations, and introduces several case studies to indicate potential and limitations of AI.

The review leads to the conclusion that whilst AI indicates significant opportunity in assisting/increasing investigations of cybercrime in India, it requires a related legal and regulatory framework, careful investments in technical capability and education and a consideration of ethical implications to ensure safe and just cyberspace.

II. KEYWORDS

Cybercrime, Digitization, AI- Artificial Intelligence, Investigations.

[1] LLM (Criminal Law)

III. INTRODUCTION

The global rise in cybercrime has developed into a crucial problem in the digital era, affecting many aspects of society, ranging from individual privacy and financial security to the integrity of national infrastructure and international relations.[2] In India, there has been a rapid expansion of its digital infrastructure and a growing number of internet users and it has, therefore, also seen a sharp increase in incidents of cybercrime across the wide variety of offenses, which include financial fraud, data breaches, cyber espionage, and online radicalization.[3]The increased complexity and scope of these cybercrimes has created pressure on traditionally structured law enforcement organizations -which often lack specialized skills and technologies to investigate and prosecute these crimes.[4]

In response, artificial intelligence (AI) has emerged as a possible disruptive tool in investigating cybercrime.[5] AI, which is broadly defined to include technologies such as machine learning, natural language processing, and computer vision, has the potential to analyse massive datasets, ascertain complex patterns and manipulate robotics for automating some time-consuming investigative tasks. All of this may lead to the cybercrime investigative process becoming more efficient and effective.[6] However, introducing AI into the Indian law enforcement system carries its own unique set of challenges. It brings into focus important questions regarding the capacity of in place systems to respond not only to the operational and technical

[2] Adam M. Bossler & Tamar Berenblum,et.al, *Introduction: New Directions in Cybercrime Research*, 42 JOURNAL OF CRIME AND JUSTICE 495 (2019).
[3]Jenna McLaughlin,"UN Debates How to Define Cybercrime", *NPR*, Sep. 13, 2023, *available at:* https://www.npr.org/2023/09/13/1199324577/un-debates-how-to-define-cybercrime (last visited May 2, 2025).
[4] Bossler and Berenblum, *supra* note 1.
[5] KAVITA SAINI, SWAROOP S. SONONE, MAHIPAL SINGH SANKHLA, NAVEEN KUMAR, *ARTIFICIAL INTELLIGENCE IN FORENSIC SCIENCE: AN EMERGING TECHNOLOGY IN CRIMINAL INVESTIGATION SYSTEMS*,206,(CRC PRESS, 2024), *available at:* https://www.routledge.com/Artificial-Intelligence-in-Forensic-Science-An-Emerging-Technology-in-Criminal-Investigation-Systems/Saini-Sonone-Sankhla-Kumar/p/book/9781032263366 (last visited Apr 4, 2025).
[6] MICHAEL STOLTZ, *ARTIFICIAL INTELLIGENCE IN CYBERSECURITY: BUILDING RESILIENT CYBER DIPLOMACY FRAMEWORKS* (arXiv,2024), *available at:* http://arxiv.org/abs/2411.13585 (last visited May 2, 2025).

readiness of law enforcement bodies, but also around the ethical questions of incorporating AI into these sensitive spaces.[7]

This report aims to produce a systemic integration of what we understand about cybercrime in India, and the new possibilities of AI in the investigation of cybercrime, from a systematic review of the relevant literature and academic scholarship. It will consider the types and patterns of cybercrimes in India, the potential uses of AI technologies at various stages of cybercrime investigation, the current legal and regulatory structures governing cybercrime and AI, and the main technical and organizational challenges to the widespread use of AI in this space.

Additionally, the report will describe and analyse selected case studies of AI supported cybercrime investigations in India, in order to provide some empirical insights into the implications and lessons of field experimentation of AI innovations in practice. As a whole, this synthesis will set the stage for informed recommendations to improve cybercrime investigations in India, through the appropriate and responsible application of artificial intelligence.

IV. AN IN-DEPTH EXAMINATION OF CYBERCRIME AND SOCIOCULTURAL DYNAMICS IN INDIA.

A. Historical Trajectory of the Cybercrime Phenomenon and its Legal Infrastructure.

The *October 2008* Mumbai Terror Attacks were significant reminders of the ever-evolving threats, likely leading to emerging concerns regarding digital security. Although not a cyber attack in nature, the event demonstrated ways terrorists used digital communications, common information dissemination of new technologies for planning, coordination, and potentially guidance in real time as the attack was unfolding. Terrorists occasionally had highly technical mechanisms for command and control that involved situational awareness through monitoring fellow attackers via

[7] Dr Shailja Thakur, *Artificial Intelligence and Criminal Justice System: A Comparative Study with India, UK, and USA*, 5 (2024).

social media or news outlets.[8] This incident also exposed intelligence collection shortcomings and the need to keep operationally sensitive information off the internet during a problem.[9]

During the period of demonetization in India in ***2016***, major implications for cybersecurity began to take shape. The sudden withdrawal of high-value currency notes created huge incentives for users to adopt digital transactions. In an environment of such rapid adoption--often by users that are completely new to digital payment technology--cybercriminals seized the opportunity. Cybercrimes and frauds manifested to a large extent in India after the demonetization of high-value currency notes.

In light of the moving climate toward a more complex cyber threat and the need to protect individual privacy with new datasets, India has seen ever-evolving regulations in the areas of data protection and cybersecurity. The users query specifically states 2018 regulations in India related to data protection and cybersecurity; however, it is important to highlight the administrative and awareness movements emerging since 2018.

The RBI Act, 2018 intended to set broad standards for the security of frameworks operated by banks and payment operators, require cyber crisis management plans, and then introduce broad mandatory notification of breached data/information. Subsequently, the Digital Personal Data Protection Act (DPDP), passed in 2023 and earlier drafted in 2018, also relates to the lawful processing of personal data, the rights of individuals, and the responsibilities of organizations when processing data.[10] Other regulatory authorities, such as IRDAI and TRAI, have also released related guidelines to inform their sectors on cybersecurity and protection of data. Therefore, it is evident

[8] Edge Staff, *Lessons Learned from the 26/11 Mumbai Terror Attacks*, EDGE (May 1, 2019), https://amuedge.com/lessons-learned-from-the-26-11-mumbai-terror-attacks/ (last visited Apr 5, 2025).

[9] ANGEL RABASA ET AL., THE LESSONS OF MUMBAI (1 ed. 2009), https://www.jstor.org/stable/10.7249/op249rc (last visited Apr 5, 2025).

[10] Top Cybersecurity Regulations in India [Updated 2025] | UpGuard, https://www.upguard.com/blog/cybersecurity-regulations-india (last visited Apr 5, 2025).

that India is currently developing regulations for a secure and trusted digital ecosystem.

B. Statistical Profile of Cybercrime in India (2022-2024).

In the last few years, there has been a troubling increase in cybercrime across India, according to various statistical reports. For example, in 2022, the National Crime Records Bureau (NCRB) indicated that there were 65,893 cases registered under Cyber Crimes, which represents a 24.4% increase from the 52,974 cases the previous year (2021). The vast majority of cyber crimes were motivated by fraud, at 64.8% of the registered cases. There was considerable growth as well for cybercrime in metropolitan cities, a 42.7% increase in the reported cases for 2022. The city with the highest number of registered cybercrime cases, among metropolitan areas, was Bengaluru. According to the Indian Computer Emergency Response Team (CERT-In) agency, 2022 had more than 5.2 million cyber incidents reported in India.[11]

This upward trend continued in 2023, with CERT-In tracking 1.59 million cybersecurity incidents for the year compared to 1.39 million in 2022. In total, India faced over 79 million cyber incidents in 2023—a clear sign of the pervasiveness and growth of the threat. The number of complaints registered through National Cybercrime Reporting Portal increased substantially in 2023, with a year-on-year increase of 61%, bringing the total number of complaints to 1.56 million. This shows there may be two reasons for the rise: either an uptick in cybercriminal activity or taditionally less awareness and previously-induced concern from victims to report their incidents. Early 2024 also indicates the upward trend in cases may not reverse, as more than 500 million cyber incidents have been reported by the end of the first three months of 2024 alone, where an average of 7,000 complaints are made daily to the National Cybercrime Reporting Portal.

[11] Understanding the Dynamics of Cybercrime in India a Comprehensive Study and Recommendations, RESEARCHGATE (2024), https://www.researchgate.net/publication/372960099_Understanding_the_Dynamics_of_Cybercrime_in_India_a_Comprehensive_Study_and_Recommendations (last visited Apr 5, 2025).

The financial aspect of cybercrime affecting businesses and individuals in India is likewise substantial and growing. According to the report issued by Reserve Bank of India (RBI) in 2023, the average cost of a data breach in India has reached $2.18 million: indicating a growth of 28% since 2020. For context, globally, costs of cybercrime are projected to reach approximately $13.82 trillion by 2028. Investment fraud topped the loss-making cybercrime in 2022 with a recorded victim loss of $70,811 per victim. By 2025, Indian entities will likely predominate losses of ₹20,000 crore related to cybercrime. In the first six months of 2024, the total loss associated with cyber fraud was over ₹11,000 crore, averaging a loss of ₹60 crore per day, in India.

When we look at the trends in major metropolitan areas we see variations, as well. Among the metro cities, Bengaluru had the most cybercrime cases in 2022; impartially, and arguably the gold standard in measuring cyber fraud, Bengaluru has dropped off and was covered in traditional scam formats such as phishing and OTP scams; scams in Bengaluru have increased accordingly with patterns of development in scams unique to the fraud landscape--specifically an increase in investment scams and digital arrest scams. In Bengaluru, individuals recorded losses of ₹1,806 crore in 2024 alone, while total loss of Karnataka was ₹2,047 crore.[12]

Mumbai was next with a total of 4,724 cybercrime's recorded investigations in 2022; in 2024 there was a trend upward with an overall increase of 22% in cybercrime cases with investment scams increased from 6 cases to 87 cases, a system development of 14 over three years. Navi Mumbai alone in 2024 lost ₹440 crore to cyber fraud. While Delhi recorded 685 cases in 2022, Delhi rated the highest per lakh population rate in reported criminal activity on cybercrime scams; Delhi had a reported 95 per lakh population. All these statistics support unbelievably widespread varieties of criminal activity and the growth of illegal scams in cyberspace and the development of and the sharing of various techniques throughout major metropolitan areas within India.[13]

[12] Ajay Sukumaran, "Rs 2,047 Cr Lost in 2024, Karnataka Set to Buff Up Against Cybercrime," *India Today*, Dec. 20, 2024, 21:00 IST.
[13] CERT, "India: Promoting internet safety amongst 'netizens" ,(UNODC,2012).

C. The Developing Nature of Cybercriminal Activity

The nature of cybercrime in India is one characterized by developing capabilities, which are being made possible by advancing technology in the hands of cybercriminals. Cybercriminals are increasingly exploiting Artificial Intelligence (AI) and Machine Learning (ML) algorithms to automate and improve the efficacy of attacks, making them very difficult to detect.[14] According to an upcoming survey, a significant 93% of Indian businesses expressed concern about AI's ability to make data breaches worse and more advanced. Such concerns are valid, as AI is already being applied to various malicious activity within the Indian digital arena.

Among the uses for AI in cybercrime, the crafting of highly believable phishing emails is one of the most significant.[15] Generative AI models can review and analyse social media and communication histories to produce personalized messages that entice recipients to divulge sensitive information. Deepfake technology is another primary area where cybercriminals are abusing AI. Cybercriminals are using deepfake technology to impersonate trusted individuals with realistic fake videos and voice recordings, which has led to substantial ongoing financial fraud. A case in India involves a known industrialist being defrauded of a substantial amount of money based on a fake Supreme Court hearing using deepfake technology the cybercriminals built.

Techniques, such as SIM-swapping and Multi-Factor Authentication (MFA) bypass, are also becoming more mainstream, using AI to exploit vulnerabilities in identity verification procedures. AI is not only being applied to smart password guessing and cracking but also making brute force attacks easier and quicker by anticipating how people typically predict passwords. AI-based ransomware exploits multiple vectors, including using AI to identify valuable files to encrypt, and to navigate and evade

[14] Sakshi C & Amit Jaju, "The Rise of AI-Powered Cyber Attacks: How Indian Businesses Can Prepare," *JD Supra*, Jan. 23, 2025,
[15] ET Edge Insights, "Barracuda Highlights Evolving Phishing Techniques to Look Out for in 2025," *Trending* (Jan. 9, 2025)

 (ISSN: 2583-7753)

endpoint security. Finally, AI is being leveraged on the dark web for automating marketplaces for stolen data and enabling fraudulent transactions.[16]

The rise of automated attack tools is also driving the increasing sophistication of cybercrime in India. Cybercriminals are now using artificial intelligence to automate the discovery of network vulnerabilities and the initiating of exploits at a quicker pace than what is achievable in developing those capabilities manually. Botnets driven by artificial intelligence are already being configured to orchestrate more effective and resilient DDoS attacks.[17] The dark web is a key facilitator of this growth — it is an enormous marketplace where multiple types of hacking tools, malware, and exploits can be bought. Even the type of sophisticated tools that allow those with varying degrees of technical ability are now reasonably easy to procure. Additionally, the emergence of models referred to as cybercrime-as-a-service (CaaS) will further erode the barrier to entry, allowing those with minimal skill to orchestrate an attack by loaning either the tools or services from established cybercriminals.

Widespread Cyber Threats and Their Consequences

- **Ransomware attacks:** are a primary concern in India as they have increased since 2020; the number of attacks slightly decreased in 2022, but this type of cyber threat means business as usual.[18] For example, ransomware attacks over the past four years before 2024 affected one industry in India, the manufacturing and production industry alone, with an impressive increase of 41%. Further, the healthcare industry in India has been particularly vulnerable in that it has regularly been the attack surface for all kinds of cyberattacks inclusive of ransomware, healthcare and ransomware has its own unique combination. A good example is the ransomware attack on AIIMS Delhi that had crippled services for an extensive period in 2022.

[16] Cyber Laws of India, ISEA, https://infosecawareness.in/cyber-laws-of-india (last visited Apr 5, 2025).
[17] CyberTalents, *What Is Cyber Crime? Types, Examples, and Prevention*, CYBERTALENTS BLOG, https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention (last visited Apr 5, 2025).
[18] The Latest Ransomware Statistics (updated January 2025) | AAG IT Support, https://aag-it.com/the-latest-ransomware-statistics/ (last visited Apr 5, 2025).

- **Phishing continues:** to be one of the higher occurrence types of cybercrime in India. Cybercriminals are using increasingly complex methodologies, including the use of Artificial Intelligence to prepare very credible and personalized phishing emails. Attackers are using even more innovative techniques to get past traditional cyber-secure environments with some examples of that being the use of text QR codes with malicious URLs, specially crafted URL links to direct person to a specific blog, among other techniques moving phishing content from the body of emails to documents like PDF attachments or other technologies like Google documents.

An aspect of cybercrime that has grown particularly concerning within India is the oversaturation of OTP (One-Time Password) scams against users of online banking services.[19]

Cyber threats against critical infrastructure in India

India's critical infrastructure, representing the sectors of significant importance to national security, the economy and public welfare is constantly being threatened by a growing list of cyber threats. These threats attack essential services like those of the banking, government, healthcare and power grid infrastructure systems and battle national security and stability. The banking systems in India are under perpetual cyber bombardment and enduring a distressingly high volume of cyber attacks. Evidence shows Indian banks sustain an average of more than 2,500 cyberattacks weekly.

Scheduled commercial banks (SCBs) remain the primary target accounting for the vast majority of reported incidents. For example, in 2024, a ransomware attack disrupted nearly 300 smaller local banks' payment systems running through a single technology service provider. In light of this, the Reserve Bank of India (RBI) has issued advisories

[19] Navigating Phishing Threats in Indian Online Banking, https://lawdocs.in/blog/phishing-attacks-in-online-banking-in-the-indian-context-unmasking-the-threat-landscape (last visited Apr 5, 2025).

and required institutions to monitor key systems including SWIFT, card networks, RTGS, NEFT, and UPI closely.

Government databases and networks are becoming more susceptible to cyber threats as well. Between 2019 and 2023, the number of cyberattacks on entities associated or related to the government of India increased 138% with the expectation of continued growth. Consequences of these attacks have included large-scale data thefts involving the personal information of millions of citizens. Aadhaar data breaches and the RailYatri e-booking service attack are examples of these attacks. Critical infrastructure (e.g., the All India Institute of Medical Science (AIIMS), the power grid, etc.) have also been threatened by cyberattacks.

In 2024, a significant data breach revealed the personal information of 750 million telecom customers, which was then offered for sale on the dark web, indicating the scope for possible breaches. Healthcare networks in India appear to be a target for cybercriminals. The volume of attacks is alarmingly high, with approximately 1.9 million cyberattacks in 2022. Notably, ransomware attacks on hospitals such as AIIMS Delhi, raise fear of interference with essential service delivery and jeopardizing sensitive patient information. These cyberattacks have ultimately lead to the compromise of private medical records and personally identifiable information.

The Function of the Dark Web in Enabling Cybercrime

The dark web is a portion of the internet that is hidden and can only be accessed with specialized software, and it has an important role in facilitating all kinds of cybercriminal behavior in India. Its anonymity can provide a haven for illicit markets and forums where stolen data, hacking tools, and illegal services are bought and sold. Some estimates suggest that a large percentage of dark web content is related to illegitimate activities, including economic fraud and cybercrime.

D. Societal Impact of Cybercrime in India

The ubiquity of cybercrime within India has a significant and intertwined societal impact on individuals, businesses, and the broader digital ecosystem. Those that are

affected by cybercrime frequently face damaging psychological consequences.[20] These can range from a general loss of confidence in online products and/or services to something more severe, such as Post Traumatic Stress Disorder (PTSD), increased anger and frustration, and even suicidal thoughts. Victims may suffer from common emotional distress, anxiety, depression, and panic attacks. In certain types of cybercrime, particularly cyberstalking and cyberbullying, victims may experience high levels of fear and anxiety. Emerging threats such as digital arrest scams may elicit strong emotional responses such as fear, guilt and shame which cause victims to comply with the scam. The social stigma associated with being a victim of cybercrime can exacerbate the psychological effects and may prevent them from accessing support or reporting the crime.

The economic impact of cybercrime in India is large and widespread. Individuals and businesses are experiencing increasing direct financial loss, with estimates suggesting annual losses in the billions of dollars. Economic losses are incurred through cybercrime in a variety of ways, including online fraud, ransomware and identity theft.[21] Further, cybercrime creates substantial barriers for innovation in India and investment in India.[22]

V. THE IMPACT OF ARTIFICIAL INTELLIGENCE ON CYBERCRIME INVESTIGATIONS

A. Artificial Intelligence for Automated Threat Detection in Cybercrime Investigations:

The increasing volume and sophistication of cyber threats has resulted in the deployment of Artificial Intelligence (AI) for automated threat detection in cyber

[20] Dr Theju Kumar C, *PSYCHOLOGICAL IMPACT OF CYBERCRIMES – AN OVERVIEW*, 11 TURKISH ONLINE JOURNAL OF QUALITATIVE INQUIRY 1370 (2020).

[21] Impact of Cyber Crimes on Indian Economy - Daily Excelsior, https://www.dailyexcelsior.com/impact-of-cyber-crimes-on-indian-economy/ (last visited Apr 5, 2025).

[22] Indian entities may lose Rs 20,000 cr to cybercrimes in 2025: CloudSEK Report, THE ECONOMIC TIMES, Mar. 1, 2025, https://economictimes.indiatimes.com/industry/banking/finance/indian-entities-may-lose-rs-20000-cr-to-cyber-crimes-in-2025-cloudsek-report/articleshow/118651127.cms?from=mdr (last visited Apr 5, 2025).

crime investigations. AI is heavily utilized in the identification and remediation of a wide variety of malicious activities in cyberspace. Machine Learning (ML), a subset of AI, involves constructing algorithms that learn from data, discover patterns, and make predictions or decisions without being explicitly programmed. In cyber crime detection, ML algorithms are trained on large datasets consisting of legitimate and malicious behaviors to detect subtle indicators of threats that a more traditional rule-based systems may miss.

Deep Learning (DL), a more complex sub-set of ML, uses artificial neural networks with multiple layers to analyze complex types of data and automatically extract relevant features.[23] This hierarchical learning process enables DL models to identify very sophisticated types of threats, such as advanced persistent threat campaigns and new malware.[24] Natural Language Processing (NLP) is another prominent branch of AI that aims to help computers comprehend, interpret, and produce human-generated language. In cybercrime investigations, NLP is especially powerful for investigating textual data like emails, chat logs, posts on social media, and dark web sites to collect threat intelligence, attribute malicious intent, and establish concealed associations involving cybercriminals.

Behavioural Analytics uses AI systems to determine norms of behavior for users, devices, and networks; activity is monitored, and any non-compliant behavior based on the set norms is flagged.[25] AI-based systems are able to observe behavioral variations that could indicate security breaches, insider threats, or other malevolence.

These techniques of using AI have been shown to work well in a number of different contexts in identifying different cyber threats. In the area of malware detection, AI, primarily ML algorithms like XGBoost, work well in considering file characteristics, system behavior in a runtime (sandbox) environment, and changes to the system for

[23] Malware Detection Using Machine Learning Techniques, https://www.einfochips.com/blog/malware-detection-using-machine-learning-techniques/ (last visited Apr 5, 2025).
[24] Dark Web Monitoring: Extracting and Analyzing Threat Intelligence, RESEARCHGATE (2024), https://www.researchgate.net/publication/384008320_Dark_Web_Monitoring_Extracting_and_Analyzing_Threat_Intelligence (last visited Apr 5, 2025).
[25] AI-Powered Incident Response: Transforming Cybersecurity, (2025), https://cyble.com/knowledge-hub/ai-powered-incident-response/ (last visited Apr 5, 2025).

the purpose of malicious software detection. XGBoost is an ensemble learning technique that utilizes high levels of accuracy and efficiency, and can withstand the high-dimensional and complex data normally present in malware analysis. In the area of intrusion detection, AI systems (towards the development of AI/ML-based Intrusion Detection Systems (IDS)) utilize neural networks to monitor traffic and identify suspicious activity and network anomalies, either per session or in real-time.[26]

Research shows that AI will have a significant impact on how cybercrime investigations will evolve. AI-based tools allow forensic specialists to rapidly and accurately analyze large volumes of data, discover complex patterns that may proceed unnoticed by humans, and identify associations that may exist between disparate digital artifacts, thus yielding more rapid and accurate investigative results.

Behavioural analysis that is made possible through Artificial Intelligence (AI) provides a valuable tool for detecting sporadic behaviour that is indicative of cybercriminal activities. By identifying a customary range of user and systems behaviours, AI can detect variations that may indicate the malicious or compromising of a system. User and Entity Behaviour Analytics (UEBA) is one application of AI in behavioural analysis and is characterized by the monitoring of user, device, or application behaviour in a network using machine-learning algorithms.[27] UEBA systems are being taught the differential nature of an activity to recognize if an object has an odd activity, possibly leading to a security breach.

The accuracy of some AI algorithms used to monitor behaviour has been high. For example, the Random Forest algorithm had accuracy levels as high as 99% for anomaly-related behaviour indicating a cyber threat (for example, a Distributed Denial of service (DDoS) attack). More importantly, financial services organizations using behavioural biometrics that leveraged machine learning have reported significant decreases in fraud losses, while processing transactions faster.[28]

[26] AI in Developing Predictive Models for Cyber Threats, https://www.allstarsit.com/blog/ai-in-developing-predictive-models-for-cyber-threats (last visited Apr 5, 2025).
[27] Simona-Nicoleta Vulpe et al., *AI and Cybersecurity: A Risk Society Perspective*, 6 FRONT. COMPUT. SCI. 1462250 (2024).
[28] Behavioral Analysis of Cybercrime: Paving the Way for Effective Policing Strategies | Request PDF, RESEARCHGATE (2024),

Behavioural analysis can be a helpful avenue to identify unusual behaviour, for example, if a user logs in from two different locations at the same time or accesses a system that they would not typically use. This can give an organization an early warning of a potential security event.[29]

B. Predictive Analytics and Machine Learning Models for Cyber Threat Forecasting

Predictive analytics utilizing machine learning (ML) models has recently emerged as an increasingly essential predictive tool in cybersecurity for forecasting the likelihood of a cyber threat. After the organization has taken the time to analyze historical data and put a pattern in place, some sort of analysis techniques can be utilized to reduce risk before an exposure risk becomes a real risk.

Another method, one of the more popular methods, is via machine learning algorithms that analyse historical threat-related data, threat intelligence feeds and network-related log data for patterns and/or anomalies pointing to potential future threat activity. Proactive predictive threat modeling using historical data and threat intelligence provides the organization an opportunity to model attack scenarios to understand attack vectors and to prepare proactive defensive measures.

Another method, one of the more popular methods, is via machine learning algorithms that analyse historical threat-related data, threat intelligence feeds and network-related log data for patterns and/or anomalies pointing to potential future threat activity.[30]

The capability to predict these attacks with in the real-world has demonstrated reliability in several research. Research has indicated deep learning models have high

https://www.researchgate.net/publication/374635705_Behavioral_Analysis_of_Cybercrime_Paving_the_Way_for_Effective_Policing_Strategies (last visited Apr 5, 2025).

[29] Predictive Analytics in Cybersecurity | DataGuard Cybersercurity, https://data-guard365.com/cybersecurity/predictive-analytics-in-cybersecurity/ (last visited Apr 5, 2025).

[30] Max Landauer et al., *A Review of Time-Series Analysis for Cyber Security Analytics: From Intrusion Detection to Attack Prediction*, 24 INTERNATIONAL JOURNAL OF INFORMATION SECURITY (2024), https://discovery.researcher.life/article/a-review-of-time-series-analysis-for-cyber-security-analytics-from-intrusion-detection-to-attack-prediction/6978f4750b9036ca99ed4cd79ebcc839 (last visited Apr 5, 2025).

fidelity in predicting cybercrime incidents, achieving upwards of 92% in predictive success with superior false positive rates compared to traditional means.[31] Time series forecasting, such as ARIMA, have demonstrated the ability to exceed naive forecasting methods in predicting the intensity of cyberattacks while also providing classes of potential insights into future activity.[32]

C. The Role of Facial and Voice Recognition Technologies in Supporting Law Enforcement

Facial and voice recognition technologies, which employ artificial intelligence in analysis, provide law enforcement agencies with some of the most useful capabilities for identifying cybercriminals. These technologies analyze unique biometric characteristics, which can be used in investigations, but they also introduce important legal and ethical dilemmas.

Facial Recognition Technology (FRT) can identify or verify an individual and characterize or measure unique patterns and shapes of their facial features detected in still images and video.[33] The efficacy of facial recognition technology (FRT) has advanced remarkably in recent years, with some prominent applications expressing confidence levels of over 99% for accuracy across various demographic groups in a controlled environment. Similarly, voice recognition technology, which is often referred to as voice biometrics, applies an individual's distinct voice signature for the purpose of confirming identity and detecting linguistic anomalies indicating possible fraud or impersonation.[34]

The legal implications of FRT in cyber incident investigation are complex and could differ by jurisdiction. Several states and municipalities have enacted laws forbidding

---

[31] The Role of Artificial Intelligence in Predicting Cyber Threats, RESEARCHGATE (2024), https://www.researchgate.net/publication/385639588_The_Role_of_Artificial_Intelligence_in_Predicting_Cyber_Threats (last visited Apr 5, 2025).

[32] Lukman Hakim & Lili Ayu Wulandhari, *Cyber Security Threat Prediction Using Time-Series Data With LSTM Algorithms*, 12 INDONESIAN JOURNAL OF ELECTRICAL ENGINEERING AND INFORMATICS (IJEEI) 1111 (2024).

[33] David Gargaro last updated Contributions from Rene Millman in Features, *The Pros and Cons of Facial Recognition Technology*, ITPROUK (2020), https://www.itpro.com/security/privacy/356882/the-pros-and-cons-of-facial-recognition-technology (last visited Apr 5, 2025).

[34] AI Voice Detection & Voice Security | Respeecher Cybersecurity, https://www.respeecher.com/cybersecurity (last visited Apr 5, 2025).

or limiting governments from using FRT due to privacy concerns. Courts are placing additional emphasis on disclosure and the right to discover FRT styles or methods, especially in criminal cases, where the court finds that the reliability of the technology is essential in determining its use in the investigation.

D. Pros of AI in Cybercrime Detection

Ultimately, the greatest benefits of AI in cybercrime detection is the huge acceleration in speed and efficiency. AI algorithms can examine and process enormous amounts of digital data in real time, something that would take humans that are evaluating months of time instead.[35]

AI also provides remarkable scalability in managing the rapidly increasing volume of digital evidence in crimes against computers. As cyber threats continue to grow in complexity and the volume of data continues to grow rapidly, AI-enabled solutions will scale with the organization, providing a large degree of assurance in security, while simplifying the analysis of large datasets that can often measure in terabytes, even petabytes of data. This democratization of volume scalability extends to threat intelligence and incident response—allowing an organization to adapt on the fly to its complex IT infrastructure and changing threat dynamics without maxing out its security teams.[36]

Academic literature and case studies in practice provide convincing evidence in support of these advantages. Studies show that, as compared to conventional approaches, AI can raise the accuracy of threat detection by nearly 95%. The abundance of case studies also demonstrates AI is effective in many forms of cybersecurity, including defending against ransomware attacks, spotting insider threats, identifying phishing campaigns, and enhancing threat intelligence, and, across the board, AI has been shown to generate greater accuracy and efficiency.

[35] EC-Council, *Role of AI & ML in Enhancing Cybersecurity Against Threats*, CYBERSECURITY EXCHANGE (Nov. 30, 2024), https://www.eccouncil.org/cybersecurity-exchange/network-security/role-of-ai-ml-in-enhancing-cybersecurity-against-threats/ (last visited Apr 6, 2025).
[36] Real-Time Threat Detection Using The Power Of AI - Cyble, https://cyble.com/knowledge-hub/real-time-threat-detection-with-ai/ (last visited Apr 6, 2025).

VI. THE LEGAL AND REGULATORY FRAMEWORK FOR CYBERCRIME IN INDIA

A. Analysis of the Existing Cyber Legal Framework in India.

The Information Technology Act, 2000: An Update Foundational Pillar

The Information Technology Act, 2000 (amended in 2008 and 2023) is India's main cybercrime legislation. Under this law, there are a number of offenses to which punishment is attached, including unauthorized damage to systems (Sec 43), tampering with computer documents (Sec 65), hacking (Sec 66), receiving stolen computer hardware (Sec 66B), identity theft (Sec 66C), cheating by personation (Sec 66D), capturing/transmitting private images without consent (Sec 66E), cyberterrorism (Sec 66F), publishing obscene material (Sec 67), and unauthorized disclosure of information (Sec 72A). The law is currently being assessed for its effectiveness against ever-evolving cyber threats.

Aspects of the Digital Personal Data Protection Act 2023: A New Protections Landscape for Cybercrime

In August of 2023, the Digital Personal Data Protection Act, 2023 (DPDP Act) was enacted which represents a first step towards establishing data protection in India, but it is still awaiting the implementation of the rules—these rules are still in draft form for public consultation and potential changes will probably result in no implementation before January 2025. The intent of the DPDP Act is to protect individuals' personal data and privacy rights, in a manner that is lawful, fair and transparent. The Act prescribes that data principals (individuals) have rights and data fiduciaries (the organizations that are processing personal data) have obligations. In the cybercrime landscape, the DPDP Act attempts to provide safeguards with a few important provisions. For example, it states that data fiduciaries must have reasonable security safeguards in place to protect the personal data against unauthorized access and disclosure. That said, the DPDP Act also stipulates that in the event of a personal data breach the data fiduciary must notify the Data Protection Board of India (DPB) and impacted individuals.

The DPDP Act provides serious financial penalties if a data fiduciary fails to secure personal data or to notify the DPB or affected individuals of breach.

Sector-Specific Cybersecurity Compliance Regulations

Many regulatory authorities have issued their own sector-specific guidance to improve cybersecurity in their respective areas, such as the Reserve Bank of India (RBI) which has published its guidelines on Information Technology Governance, Risk, Controls and Assurance Practices to supervise across all sectors which informs theirs and other customers about their data protection practice obligations, what the organization's accountability and risk obligations for its IT asset management and cybersecurity and cyber resiliency measures across it all of its IT systems, including incident reporting obligations for not only victims of cybercrime but also for affected customers and stakeholders of the organizations actual incident response by way of transparency and scrutiny. The RBI guidelines also mandate that regulated entities have measures against unauthorized access to customer data, managing threats to data systems, data breach risks where PII is compromised and has the ability to mature as new risks and vulnerabilities emerge through monitoring the IT governance process (through monitoring and supervision, incident controls, scans, audits and testing).[37]

On the same note, SEBI has published its Cybersecurity and Cyber Resilience Framework (CSCRF) for entities regulated by them in the securities market as the minimal standard of cyber risk management. CSCRF is working to improve cyber resilience, meet changing cyber threats, meet international cybersecurity standards, facilitate more efficient audits, enforce compliance by regulated entities, and establish streamlined reporting formats for cybersecurity events.[38] On 2022, CERT-In issued mandatory cyber security directions that required all service providers, intermediaries, data centers, body corporates, and government organizations to retain ICT logs for a rolling period of 180 days, and to report certain categories of cyber

[37] RBI., "RBI Guidelines for Cybersecurity Framework" ,(2016).
[38] SISA, "SEBI's New Cyber Resilience Guidelines Explained",(2024).

incidents to CERT-In within 6-hours of becoming aware of the incident or being made aware of the incident. In CERT-In also plays a part in initiatives such as the Cyber Swachhta Kendra, which focuses on botnet cleaning and malware analysis.[39]

Cybercrime Cells: Organizational Structure, Purpose and Efficacy

Under the increasing threat of cybercrime, India has initiated a series of cybercrime cells at the state level and national level. Each state police TV Department and the Central Bureau of Investigation (CBI) have developed cybercrime investigators-special teams or units-to address cybercrime cases, including online stalking, financial scams, hacking and malicious software. At the national level, the Indian Cyber Crime Coordination Centre (I4C) operates as an Office of Ministry of Home Affairs before functioning as a national super objective facility to coordinate responses to cybercrime incidents and threats across law enforcement agencies in a global and comprehensive manner.[40] The I4C is organized in distinct identifiable units, including the National Cybercrime Threat Analytics Unit to mine cyber criminality and produce operational intelligence assessments of cybercrime threats; National Cybercrime Reporting Portal (www.cybercrime.gov.in), a citizen-facing tool enabling citizens to report a variety of incidents of cybercrime, with a concentrated focus on vulnerable populations such as women and children; and Joint Cybercrime Investigation.

B. Discussion of the Challenges Related to Cyber Laws Enforcement in India.

Jurisdictional Issues

An important hurdle to enforcing cyber laws in India is related to the transnational nature of cybercrimes. In many cases, the offenders, the victims, and the very digital infrastructure used to commit the crime (the servers) may be situated across on or many different countries. The global nature of the crime makes it extremely

[39] CERT-In 2022 Guidelines – Cyber security advisory | Positka, https://positka.com/services/cert-in (last visited Apr 6, 2025).

[40] Ministry of Home Affairs | Government of India, https://www.mha.gov.in/en/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme (last visited Apr 6, 2025).

challenging to ascertain whether the law enforcement agency or investigator has jurisdiction to investigate and prosecute the offense.

Skilled cyber law enforcement shortage

A significant obstruction for effective enforcement of cyber laws in India is a significant decrease of skilled personnel within law enforcement agencies, who are entitled to special knowledge and expertise required to handle the complexities of cyber crime investigation. This includes a shortage of trained investigators in various related technical areas required to navigate the complications of digital forensic, cyber law and cyber offenses. Traditional police training programs often do not adequately equip the authorities, which effectively revolve effectively with special skills required to investigate and prosecute cyber offenses, leading to sufficient difference in capacity.

Under reporting of cybercrime

A significant obstacle to correctly assess the scale of cyber crime in India and prepare effective enforcement strategies is the prevailing under reporting of such incidents by victims. Many factors contribute to this reluctance, including a variety of cyber crimes and general lack of awareness among the public about the mechanisms available to report them. Many victims, especially people with concerns about business and their public image, may be afraid of reputed damage associated with accepting a cyber phenomenon, leading them to lead them to avoid reporting[41]. In addition, there is often a lack of confidence in the capacity of law enforcement agencies, which is to effectively investigate and resolve cyber crime cases, which discourage the victims from coming forward. The alleged complexity of the reporting process and potentially long nature can also prevent victims.

[41] How to File a Cyber Crime Complaint Online in India, SBI GENERAL INSURANCE, https://www.sbigeneral.in/blog-details/how-to-file-a-cyber-crime-complaint-online-in-india (last visited Apr 6, 2025).

VII. ACADEMIC-TECHNICAL AND ORGANIZATIONAL CHALLENGES IN AI-AUGMENTED INVESTIGATIONS

A. Technical Challenges in AI-Assisted Investigations

The Burden of Big Data: Managing Volume and Complexity in Investigative Datasets

Often, investigations involve some form of analysis within extraordinarily large datasets that may include millions of documents, multiformat multimedia files, and a range of other evidence. Traditional investigative methodologies typically find it difficult to process such substantial amounts of data in any meaningful way [User Query]. A successful implementation of AI tools would require the assurance of a formidable model and a scalable infrastructure that can manage the data at this volume [User Query].

There is an increased adoption of cloud-based solutions as a strategy to manage these large datasets with more efficiency while decreasing the costs of hardware. It is expected to manage more than 10 petabytes of digital evidence in just law enforcement, which demonstrates the expanding need for improved data management capability. One of the most compelling values of AI is its natural ability to rapidly and accurately manage these large datasets. Furthermore, the dramatic increase in the amount of digital evidence in modern investigations is driving a necessity to move to AI solutions to appropriately manage and analyze data.[42]

Algorithmic Limitations

Present-day AI systems are not without drawbacks, since they may exhibit bias, a lack of generalizability, and brittleness when applied to investigative data [User Query].

- **Bias:** Bias in AI can emerge from several avenues, including the data used to train the models, inherent flaws in the algorithms themselves, or due to the unconscious biases of its human developers. Historical biases lurking within criminal justice data can be encountered and learned and reinforced via AI

[42] Cloud Solutions for Law Enforcement: Scalable & Secure, https://vidizmo.ai/blog/cloud-solutions-for-law-enforcement-secure-and-scalable (last visited Apr 6, 2025).

models, which can create harmful policing practices if used for predictive policing, among other things. For example, facial recognition systems have been identified to have larger error/mistake rates in recognizing people with darker skin - clearly a significant flaw. This risk of spreading existing disparities indicates that AI-based models will perpetuate and increase social inequalities instead of aiding justly.[43]

- **Generalizability:** It is essential that AI models are able to perform correctly across various datasets and contexts for them to be useful for investigations. However, models that are trained on specific datasets, or for a specific context, may not generalize to out-of-distribution data or new investigation contexts.[44] Overall performance and generalization of models are affected by the training data's quality and representativeness.
- **Brittleness:** AI models can exhibit brittleness, meaning the model may work under specific circumstances in a controlled environment but fail or behave unexpectedly when placed in a scenario or with data that is even slightly different from what it has been trained on. The existence of out-of-distribution (OOD) data, which is substantially dissimilar to the training data of the model, can significantly affect model capabilities, with the model exhibiting high confidence in the wrong classifications[45].

Navigating the Threat Landscape

The use of AI systems in investigations poses a host of security risks and vulnerabilities that need to be carefully considered. Adversarial attacks on AI systems can occur when an input is changed to persuade the AI to create incorrect or unintended outputs. Along with this, network security vulnerabilities can allow for the sensitive information related to the investigation to be exposed by the AI systems

[43] AI Bias Examples | IBM, (2023), https://www.ibm.com/think/topics/shedding-light-on-ai-bias-with-real-world-examples (last visited Apr 6, 2025).
[44] Frank Morales Aguilera, *The Frontiers of Intelligence: Navigating Open Problems in AI*, AI SIMPLIFIED IN PLAIN ENGLISH (Jan. 22, 2025), https://medium.com/ai-simplified-in-plain-english/the-frontiers-of-intelligence-navigating-open-problems-in-ai-9e6f6a8e3a51 (last visited Apr 6, 2025).
[45] Taktile - How LLMs are becoming investigative partners in fintech fraud detection, https://www.taktile.com/articles/llms-investigative-partners-fraud-detection (last visited Apr 6, 2025).

storing or processing that information. For example, unauthorized access to sensitive data requiring Facial Recognition or predictive policing program evidence can provide bad actors with access to investigative process manipulation opportunities, possibly compromising the integrity of evidence or jeopardizing witness protection programs.

B. Organizational Barriers and Resource Constraints to Adopting AI

The Expertise Gap

The effective incorporation of AI into investigative processes may be hampered through the potential absence of requisite training among investigators and IT staff [User Query]. The investigators may not be sufficiently trained to use AI tools effectively, and IT staff may lack the subject-specific knowledge required to deploy and maintain such systems [User Query], and training to close this skills gap can disrupt existing workflows and lead to added costs [User Query]. The lack of trained AI professionals is a challenge that exists in law enforcement, in addition to other professional areas. The world lacks adequate trained professionals to meet the increasing demand in AI skills.

The application of AI tools may exacerbate existing skills gaps within organizations, while creating demand for new and specialized skills. Therefore, organizations will need to develop ongoing training and professional development programs to support the use and skill development of the civilian personnel that will utilize AI tools in their investigative processes.[46]

The Cost Factor

Any fiscal implications related to the implementation of AI systems - acquisition, specialized training, and maintenance - can be a substantial barrier to many organizations. The upfront expense related to implementation can mean borrowing or allocating significant resources for hardware and related operational expenses. In

[46] (Opportunities and Challenges of AI Adoption by the Abu Dhabi Police: A Review Study, RESEARCHGATE (2025), https://www.researchgate.net/publication/384143952_Opportunities_and_Challenges_of_AI_Adoption_by_the_Abu_Dhabi_Police_A_Review_Study (last visited Apr 6, 2025).

particular, smaller law enforcement agencies are challenged by the costs related to budget. While the costs associated with hardware may be a hurdle, it is worth noting that there are cloud deployment options that may alleviate some of the upfront hardware costs. However, studies indicate that, after the initial investment, careful planning for the implementation of AI might result in significant long-term savings in operational costs.[47] Budgetary constraints can limit many organizations' opportunities to invest in state-of-the-art AI solutions. Identifying scalable and cost-effective solutions (e.g., cloud or hosted models, grant possibilities, or statewide licensing agreements) can address budgetary constraints that may inhibit AI use in investigative settings.

Investment in Human Capital

In order to address the skill gaps that limit the possible use of AI in investigations, organizations should make investments in training and education that will promote a sufficient understanding of the technologies. This type of educational initiative needs to be interdisciplinary, targeting investigative personnel, legal professionals, and information technology teams and enabling collaboration across domains of expertise. Training should ultimately offer clarity about the capabilities and shortcomings of AI technologies, and indicate that AI expands upon human input rather than supplanting it. Hands-on and practical experience with AI tools is a critical factor in developing confidence and familiarity for users.

Ongoing training and professional development are also necessary to stay current with the expanding field of AI and how it may be utilized in investigations. In addition, a larger program of AI literacy will aid in ensuring various stakeholders within the organization are familiar with the basic concepts and ethical implications of AI implementation.[48]

Building a Solid Foundation

[47] Jared Blistein, *IBM Cost of a Data Breach Report: AI Security Cost Reduction*, VEZA (Aug. 28, 2024), https://veza.com/blog/ibm-cost-of-a-data-breach-report-ai-security-cost-reduction-veza/ (last visited Apr 6, 2025).
[48] Cloud Solutions for Law Enforcement: Scalable & Secure, *supra* note 130.

The large amount data utilized in AI-assisted investigations requires utilizing scalable and secure infrastructure solutions. Cloud-based solutions are particularly effective in this respect, as they can scale to efficiently manage large amounts of data while minimizing the upfront costs of installing hardware. Cloud solutions offer significant advantages regarding scalability, affordability, and flexibility, enabling organizations to manage infrastructure and resources in response to fluctuating investigative workload demands. For organizations that deal with extremely sensitive or classified data, hybrid cloud solutions provide a middle ground between the advantages of cloud, such as scalability, and the security advantages of an on-premises solution.[49]

C. Utilization of AI in Investigations: Established Investigation of Particular Case

In **United States v. Loomis (2016),** the legal issue involved the possible use of artificial intelligence (COMPAS), as a pre-sentencing report to assess the gravity of the crime, and potential imprisonment. Importantly, the defendant claimed the use of the black-box algorithm/imperfect AI assessment was unconstitutional, as he could not contest the algorithm at the hearing. Significance: Serious issues were raised regarding the transparency and fairness of outcomes produced by AI. The decision highlighted: there is a compelling need to make AI models explainable if they are to be relied upon as one consideration in the context of a legal system and investigation or in deciding possible decisions that could be considered by a legal system.[50]

D. BIG Brother Watch v. United Kingdom (2021)

- **Court:** European Court of Human Rights (ECHR)
- **Issue:** Mass surveillance incorporating AI-aided interception systems
- **Outcome:** Violated rights under Articles 8 & 10 (right to privacy and expression)

[49] Employing Effective Cybersecurity Solutions for Data Protection Against AI-Assisted Attacks | Arcserve, https://www.arcserve.com/blog/employing-effective-cybersecurity-solutions-data-protection-against-ai-assisted-attacks (last visited Apr 6, 2025).
[50] hlr, *State v. Loomis*, HARVARD LAW REVIEW (2017), https://harvardlawreview.org/print/vol-130/state-v-loomis/ (last visited Apr 18, 2025).

- **Significance:** Illustrated that technical surveillance tools, if employed without balance, can interfere with rights. Encouraged a global conversation surrounding advancing independent oversight and establishing frameworks on the purpose, limitations, and accountability for use of AI delivery models.[51]

The Central Information Commission (CIC) condemned the Delhi Police for "wrong" and dubious responses to RTI queries about the sources of facial recognition data, its authenticity, and the use of this data to investigate riots in North-East Delhi. The **Anushka Jain v. Delhi Police (2022)** case exposed the Delhi Police's use of facial recognition technology and its lack of transparency. The CIC emphasized the importance of being open and instructed the Delhi Police to exercise greater caution when responding to such RTI Act information requests in the future.[52]

Bombay A Suo Moto PIL (2021) Issue occurred at the Bombay High Court: The cut back of Resources on Cybercrime has led to a rise of Cyber Crime as a consequence of not what has been added to effective policing practice.

- **Observation:** The high court has pointed out the low conviction rates being the outcomes of a cyber "cells" lack of technical resources and qualified personnel.
- **Significance:** highlighted the need to resource the (hardware and training) AI infrastructure for law enforcement and to allow the law enforcement agencies to coordinate their training and use enough people in a Cmsn.[53]

E. Murder investigation cases by Delhi Police (January, 2024)

In January, 2024, the Delhi Police made a significant advancement in investigative practices by using artificial intelligence in a murder investigation. This case involved the identification of a decedent male unknown to the police and found near the Geeta

[51] Big Brother Watch v. United Kingdom, https://www.justiceinitiative.org/litigation/big-brother-watch-v-united-kingdom (last visited Apr 18, 2025).
[52] Anushka Jain vs Delhi Police on 4 July, 2022, https://indiankanoon.org/doc/125677646/?type=print (last visited Apr 18, 2025).
[53] Bombay High Court Slams Mumbai Police For Delay In Elderly Woman's Case Who Lost 32Lakh In Digital Fraud Case, (2025), https://lawchakra.in/high-court/bombay-high-court-slams-mumbai-police/ (last visited Apr 19, 2025).

Colony flyover, which was almost immediately complicated in the (re)establishment of the decedent's identity [user query]. The use of AI indicated an increasing trend among law enforcement agencies in large Indian metropolitan centres to employ advanced technologies to assist with tackling increasingly complex criminal investigations. - The major AI technique employed by Delhi Police was facial image enhancement. Its purpose was to change a picture of the deceased victim, whose face was closed and the signs of dirt were converted into a recognizable image, which could potentially lead to identification. The process included several major stages: fixing facial malaise, especially the restoration of natural colors that were turned into blue; Removing dirt and restoring the feeling of freshness on the face; And, most importantly, digitally to create an image that looks like a living person to "open" the victim's closure eye.[54].

According to the Deputy Commissioner of Police (North), Manoj Meena, Delhi Police collaborated with an AI specialist and used a suit of equipment to achieve this facial reconstruction. Its purpose was to cross the boundaries of the original picture and generate an image that would be more likely to be identified by someone who knows the deceased. The entire AI-manufacturing process to recreate the victim's face allegedly took about two hours.

Increased image, a "hue and cruel" notice was included in the notice, then widely broadcast across Delhi. Delhi Police published about 2,000 posters characterized by AI-based image and strategically placed them in major public places such as bus stops, police stations and railway stations.

The tireless efforts of the Delhi Police achieved an important success when the victim's brother Rahul displayed one of these posters outside a police station when he was there to file a report about his missing brother. Recognizing the face as his brother, Hitandra Singh in the poster, he immediately approached the Kotwali Station House Officer (SHO).

[54] Delhi Police Uses AI to Crack Murder Case and Bring Victim Back to Life | Delhi News - Times of India, https://timesofindia.indiatimes.com/city/delhi/delhi-police-uses-ai-to-crack-murder-case-and-bring-victim-back-to-life/articleshow/107127666.cms (last visited Apr 6, 2025).

This identification enabled authorities to identify a murder conspiracy involving three people- allegedly strangled Hitande after a one-month dispute, Paravveer Singh, Herneet Singh and Priyanka. All three defendants were arrested within a week of the identity of the victim. This case is a strong and compelling example of the potential power of AI in the investigation of serious crime, specifically in situations where answering the question of identity may otherwise be reduced. In cases involving unknown dead individuals with compromised physical characteristics, AI-operated facial growth may provide an important lead that may otherwise be unattainable, potentially revolutionizing how such an investigation occurs.[55]

VIII. CONCLUSION

As the analysis below hammers on —confirming a starker reality of mounting cybercrime backlash in India that multiple traditional law enforcement methods are barely able to contain well enough. Machine learning, being an important tool in computer forensics Analysis and cybercrime investigation can automate processing large sets of digital data providing enhanced efficiency, fast speed with higher accuracy to trace complex patterns. Yet this move of incorporating AI in Indian cybercrime investigations is not a magic bullet and has several constraints. Three things determine how successful AI will be, data quality and the possibility of algorithmic bias combined with new generations of cyber attacks.

Adopting AI in cybercrime investigations requires a strong legal and regulatory framework to give assurance for responsible use of the technology. The ongoing legal framework, mainly under the IT Act may need to be either amended or fresh legislation brought in such as those addressing data protection, algorithm control and fundamental right safeguarding tendencies of AI. Additionally, there are technical and organisational challenges that need to be addressed in order for organisations to successfully embrace AI. This involves a mixture of strategic investments in technical infrastructure, creating structures for new kinds of training programs specifically

[55] Delhi Police uses AI to construct the face of a dead man to solve murder mystery - Delhi Police uses AI to construct the face of a dead man to solve murder mystery BusinessToday, https://www.businesstoday.in/technology/news/story/delhi-police-uses-ai-to-construct-the-face-of-a-dead-man-to-solve-murder-mystery-414821-2024-01-25 (last visited Apr 6, 2025).

tailored to law enforcement and improving the ability for agencies to share intelligence with each other.

The absence of some public case studies that document AI-led cybercrime investigations in India showcase the necessity for more transparency here, though taking into account operational confidentiality. The implications of such cases, even if only anecdotally true, underline the necessity for AI experts to be in bed with law enforcement and keep at it as trained professionals – maintaining ethical considerations above all.

In the years to come, one can expect cybercrime in India being carried out via more advanced methods that are highly elusive and hence will require for its investigation an increasing dependency on sophisticated technology like AI. It is, therefore, important for India to address these challenges and leverage the opportunities of AI in a clearly demarcated legal and ethical framework would be crucial in securing its cyber ecosystem while keeping mother India safe at digital border.

IX. RECOMMENDATIONS

A. Policy Improvements

- **Legislative Reforms:** Identify the deficiencies within laws and amend necessary provisions in IT Act, 2000 regarding AI technology-related cybercrime investigation including data privacy safeguards (CONSENT), algorithmic transparency requirements and accountability of autonomous decision making.
- **AI Ethics Guidelines:** AI-specific guidelines, based on successful international practices and principles in line with the national interest of India, for harmonization to guide law enforcement agencies in ethical use of Artificial Intelligence should be developed and enforced.
- **Data Protection Framework:** Amend and augment Indian data privacy and protection laws for operationalization in the context of AI-based

investigations, clearly specifying processes related to collection, storage, processing, sharing etc[56].

- **International Cooperation:** Promote greater International initiatives as opportunities for State engagement with all cybercrime and AI investigation oversight practices Competition, meaning common task collaboration across borders.[57]

B. That is how AI implementation gets through technical as well as organizational hurdles

- **Close-Up Investments:** Support its upstream commitment to invest in the technical infrastructure, AI Tools and data storage it will require for effective use of AI-led cybercrime investigation by budgeting enough funds. [Implied need with resource provision]
- **Training:** Create uniform, multi-level training programs to help law enforcement personnel (and facilitated by appropriate trainers) effectively use AI-powered tools in investigations — Training needed from the get-go.
- **Inter-Departmental:** Implement strong inter-departmental coordination mechanism and data sharing across various LEAs as well as cybersecurity agencies for comprehensive cybercrime response.
- **Promote public awareness and trust:** Launch a series of campaigns to inform the public about how AI technology is embedded in cybercrime investigation use cases, making sure that ethical considerations are addressed sufficiently for these technologies while promoting their fairness and accountability.[58]

[56] The Digital Personal Data Protection Act, 2023
[57] Isha Sharma, "A Legal Study on Role of AI in Criminal Justice System in India," 10(8) *Int'l J. Emerging Tech. & Innovative Res.* a678–a700 (Aug. 2023), available at http://www.jetir.org/papers/JETIR2308092.pdf.
[58] Thakur, *supra* note 6.

C. Improving the Performance in India of Cybercrime Investigations

- **Best Practice Development:** Publicise & develop best practices, as well as industry standard methodologies for the utilisation of different AI technologies in cybercrime fighting — backed by evidence and case studies [implies need for a norm regarding protocols].
- **Continuous Evaluation:** Develop tools and processes for the ongoing evaluation of AI technologies in use for cybercrime investigations to ensure that they are fit-for-purpose, adaptive against new types of threats and any discrimination free.
- **Knowledge Sharing Platforms:** Establish platforms for law enforcement entities to share their knowledge, experiences and best practices from the property while illustrated cyber crimes supported by AI technologies which would help in creating a community of practice that leads towards perpetual learning.
- **Academia and industry partnerships:** Enable collaborations amongst law enforcement agencies, academia havens on the new cutting edge AI solutions with technology sector to work together against addressing specific challenges of cybercrime in India.

X. REFERENCES

A. Primary Sources

Statutes

- Information Technology Act, 2000.
- Indian Penal Code, 1860.
- Code of Criminal Procedure, 1973.
- Indian Evidence Act, 1872.
- Constitution of India, 1950.
- Personal Data Protection Act, 2023.

- The Digital Personal Data Protection Act, 2023.

Reports

- CERT-In Guidelines 2022.
- India's Strategic Options in a Changing Cyberspace.
- Report on Cybercrime Detection and Time Sensitivity.
- Report on AI-Driven Phishing Attack (2024).
- RBI Cybersecurity Framework Report (2023).
- Impact of Cyber Crimes on Indian Economy – *Daily Excelsior*.
- Indian Government Cybersecurity Budget 2024 Report.
- Indian Cybercrime Coordination Centre (I4C) Report.
- India's New Cybersecurity Standards (2023).
- Cyber Resilience Guidelines – SERT (2024).
- Cloud Solutions for Law Enforcement – Positka (2023).
- Cyber Threats Report – Cyble Labs.
- Psychological Impact of Cybercrime Report.
- The Role of AI in Predicting Cyber Threats – NITI Aayog Brief.
- Cybercrime Trends in India – NCRB Annual Report 2023.

B. Secondary Sources

Books

- Sharma, R. & Singh, P., *Cyber Crimes in Indian Law*, Universal Law Publishing, New Delhi, 2020.
- Bakshi, P.M., *Cyber Laws of India*, Eastern Book Company, Lucknow, 2021.
- Gautam, R., *Cybercrime and Digital Forensics: An Introduction*, Sage Publications, 2019.
- Tyner, H., *Cybersecurity for Decision Makers*, Wiley, 2022.

- Frankel, M., *AI and Crime: How Artificial Intelligence is Advancing Crime Prevention*, Routledge, 2023.
- Narayan, S. & Shikha, K., *Indian Legal System and Mental Health*, PMC Books, 2022.

Articles

- Siva Vignesh, "Legal Challenges of Artificial Intelligence in India's Cyber Law Framework: Examining Data Privacy and Algorithmic Accountability Via a Comparative Global Perspective," *IJFMR* (2024).
- Ashish Sharma & Dr. Yogender Singh, "Cyber Frauds In India's Digital Payment Ecosystem: Risk, Impacts, And Regulatory Responses," 30 *Educational Administration: Theory and Practice*, Article 15326 (2024).
- Lukman Hakim & Lili Ayu Wulandhari, "Cyber Security Threat Prediction Using Time-Series Data With LSTM Algorithms," 12(1) *IJEEI* 1111 (2024).
- David Gargaro, "The Pros and Cons of Facial Recognition Technology," *ITPROUK* (2020).
- FNU Jimmy, "Reducing False Positives in Cybersecurity with Interpretable AI Models," *ResearchGate* (Dec. 2024).
- Dorcas Esther, "The Role of Artificial Intelligence in Predicting Cyber Threats," 11(08) *IJSRM* 935 (Nov. 2024).
- Narinder Singh & Moirangmayum, "Challenges of Cyber Crime in India," *International Journal of Social Science Studies* (Jan. 2014).
- Fr. Vineeth George, "Digitalization of Payments Post Demonetization of Currency: Prospects and Challenges," *International Journal of Research and Analytical Reviews (IJRAR)* 130 (Feb. 2019).
- Steven Legacy, "Cyber Forensics and Cyber Crime Investigation: Utilizing AI for Faster and More Accurate Results," *ResearchGate* (Nov. 2022).
- Theju Kumar C, "Psychological Impact of Cybercrimes – An Overview," 11 *Turkish Online Journal of Qualitative Inquiry* 1370 (2020).

- Adam M. Bossler & Tamar Berenblum, "Introduction: New Directions in Cybercrime Research," 42(5) *Journal of Crime and Justice* 495 (2019).

Websites

- www.ndl.iitkgp.ac.in (National Digital Library of India (NDLI))
- CERT-In 2022 Guidelines – Cyber security advisory| Positka (CERT-In Official Portal)
- www.mha.gov.in (Ministry of Home Affairs, India)
- www.india.gov.in (National Portal of India)
- www.interpol.int (INTERPOL-led operation targets growing cyber threats)
- www.cytrain.ncrb.gov.in (Cyber Training Platform)
- www.legalserviceindia.com
- www.rbi.org.in (RBI Guidelines)
- cybercrime.gov.in (Reporting Portal)
- timesofindia.indiatimes.com (Delhi Police Uses AI to Crack Murder Case and Bring Victim Back to Life | Delhi News - Times of India)