Page 3522 - 3542 **DOI:** *https://doij.org/10.10000/IJLMH.1111774*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 2

2026

Historical Evolution of AI in Criminal Investigations in India

APOORVA CHAUDHARY[1]

ABSTRACT

This study examines the historical evolution of Artificial Intelligence in criminal investigations in India, tracing the transition from manual policing to data-driven and AI-enabled systems. It highlights key developments such as NCRB, CCTNS, ICJS, predictive policing, and AI surveillance technologies, while analysing the legal and ethical frameworks governing their use. The paper argues that technological advancement must be balanced with privacy, accountability, and constitutional safeguards to ensure fair and transparent criminal justice.

Keywords: *Artificial Intelligence; Criminal Investigation; Digital Evidence*

I. EARLY FOUNDATIONS: PRE-DIGITAL AND EARLY DIGITAL POLICING IN INDIA

The gradual development of police systems in India has been influenced by the colonial past of the country, the nature of its institutions, and the specific ways in which technology has been integrated in the last twenty years. Pre-digital Indian police systems were completely analogue and characterised using paperwork, registers, and a human-driven process. Investigative systems were also entirely colonial, as they were designed under the Indian Police Act of 1861, which was focused on order maintenance and the suppression of investigative administrative efficiency and modernity. Analysts argue that the colonial legacy left a system that was heavily dependent on hierarchy, bureaucracy, and manual systems, which, in a paradoxical manner, guaranteed operational inefficiency, slow recording, and state coordination/communication. As a result of the expanded and diversifying society, early dynamics of policing showed the desire to explore and use technology in colonial policing systems reform[2].

By the 1970's and 1980's, the national policy bodies started to understand the structural inefficiencies that resulted from the heavy reliance on paper-based workflow systems and the limited flow of information. For example, the National Police Commission (1977–1981) suggested modernizing police functions, and other reforms, including upgrading police record management and improving the investigative support. However, during that time, because of

[1] Author is an LL.M. Student at Amity Institute of Advanced Legal Studies, Noida, Uttar Pradesh, India.
[2] David H. Bayley, *Police and Political Development in India* (Princeton University Press, 1969).

 [ISSN 2581-5369]

the existing infrastructural constraints and the absence of adequate institutional technical capacities, digitization efforts were scant. Therefore, the early decades of post-independence policing were characterized by an incremental and not a systematic approach to the adoption of technology, as only a few isolated units or specialized branches adopted rudimentary communication and computation devices tools[3].

The establishment of the National Crime Records Bureau (NCRB) in 1986 marked a significant milestone with India's first major effort at institutional crime centralisation and investigative computing. It brought together the Directorate of Coordination Police Computers, the Inter State Criminals Data Branch, and the Central Fingerprint Bureau. It aimed to provide the country's law enforcement agencies with a national network of crime and criminal information and investigative support across state lines. The NCRB's creation first signified the modern use of information and data systems in policing and set the stage for future AI- based systems, analytic databases, and national systems. While NCRB was the first agency to computerise processes, it was also the first to become a national standard for report standardisation, fingerprint digitisation, and the technical training of police officers states[4].

While efforts were made to improve police activity in previous decades, the 1980s and 1990s remained analog. Many police stations used handwritten diaries, created extensive records on paper, and stored evidentiary materials physically. These acts were not only time-consuming, but made obtaining relevant information much more difficult. Former police officials in conjunction with contemporary studies, describe the Indian police organizations reliance on analog systems as "pre-digital" in reference to the advanced global technology. Because many police structures have reliance on outdated systems, investigators were unable to search previously stored records, unable to confirm if a person had a criminal record, and unable to communicate with multiple police jurisdictions. These issues were extremely prevalent with inter-state criminals and organized criminal networks. Additionally, states used varied procedures to collect, record, and report criminal activity. The varied procedures created a lack of uniformity in the practices of policies and ultimately the instructions given to police officers on the ground.

While all of this was ongoing, some limited forms of technology were being adopted in law enforcement. Wireless communication and radios were some of the first forms of technology that were used in the field to create a more modernized system of communication. These types

[3] Arvind Verma & K.S. Subramanian, *Understanding the Police in India* (LexisNexis Butterworths, 2009).
[4] National Police Commission, *Reports of the National Police Commission (1977–1981)*, Ministry of Home Affairs, Government of India.

of technologies did not have significant advanced capabilities, but they improved the overall coordination between police and officers in the field. All of this was noted to be the first step towards modernization. Some states adopted these technologies faster than others. The rapid shifts in the view of police administrators showed that they knew police organizations should not be using structures that had been in place for years.

The 1990s also experienced a lack of changes to police activity. The police structure was shaped by India's economic liberalization and personal computing, which brought developments to law enforcement. State police departments began to examine the implementation of computerised record management systems. During this time, digital crime mapping was trialed, FIR (First Information Report) record digitisation was initiated at select urban stations, and attempts were made to digitise case file archives. All of these developments, however, were isolated. Police leaders were localising modernisation efforts, but there was no digital policing framework at the national level. As retired police leaders have observed, these attempts lack depth, planning, and coordination at the national level, as well as a lack of integrated approaches to criminal justice policy[5].

This era's importance comes less from the technologies used and more from the incremental changes in the institutional framework. For the first time, policing agencies began to critically examine the sufficiency of the traditional paradigm, the investigation and automation of processes and the digital value of evidence. Record digitization and the use of communications and Information and Communication Technology (ICT) for investigation set the stage for later integrated systems at the national level. Numerous scholars have argued that in the 1990s, for the first time, technology became an “integral part” of the administration of justice in India, paving the way for more systematic reforms in the 21st century.

During this time, there was a growing recognition that crime, and especially technology enabled crime, was becoming more intricate and sophisticated. The purely manual investigative approaches were insufficient for cyber crime, electronic fraud, and transnational criminal networks. There was an appreciation among police agencies that their operational approaches required administrative computing, as opposed to simple mechanization of routine activities. This marked the paradigm shift from technology as a supplementary tool of policing to a primary, integral component of crime investigation, prevention, and intelligence.

In addition, this period also created the foundation for integrated systems that were to be built later, for example in the Crime and Criminal Tracking Network & Systems (CCTNS) and the

[5] National Crime Records Bureau, *About NCRB*, Ministry of Home Affairs, Government of India.

 [ISSN 2581-5369]

Inter Operable Criminal Justice System (ICJS).

Although the systems implementation started in the late 2000's after the Mumbai attacks, the principles of those systems are based on data standardisation, digital record keeping, interstate coordination, and centralized crime databases. These principles started in the early decades of digital development. If it weren't for the NCRB's formation in the 80's, and the employment of computer systems in police in the 90's, then the systems discussed in the 2000's would not have been implemented as rapidly.

Within the same time frame of the NCRB's formation and its computerised fingerprinting, a new police biometrics digitisation system was being developed at the Central Fingerprint Bureau. When the bureau was incorporated into the NCRB in 1986, it allowed for the new automated fingerprint comparisons, and new databases for easy allocation and retrieval of fingerprints. This new system digitised the investigative biometrics for police use at the time, which was a large conceptual innovation and represented a large shift for the police data[6].

As the year 2000 approached, the comprehensive effects of these activities had given rise to a transitional\policing landscape: one in which manual processes were still dominant but were beginning to consider\more digitally based processes as integral to modern-day policing. Analysts highlight that even with\progress in policing technology, the police remained burdened with antiquated systems and\bureaucratic stagnation that inhibited widespread change. The absence of national technology\infrastructures, inadequate and ununiformed training and adoption across states resulted in a stagnant and slow\progress. Regardless, this era laid the groundwork needed to the wide-ranging digital reforms that\occurred in the 2000s and 2010s. The reforming of Indian Policing, through central mandates, mission mode projects, and integrated systems, took a leap as it entered the digital era Ro 2000s.

Looking back, the early digital and pre-digital era of policing in India has to be evaluated as a formative\stage of policing which involved a lot of 'trial and error' processes, structural barriers and a slow\progress in the administrative thought process. Although the systems used in this period had\significantly less sophistication than those of later A I Based systems, these systems were still important that they created and institutionalized the ideals that were the basis of the set of technological reforms that were to come later. The NCRB, the first steps of the use of IKs, the first experiments in the\computerization of the police functions, the first recognition of the technology's potential in the\investigative processes, all of these factors were instrumental in paving the way for India's\inevitable ending with highly digitized, datacentric,

[6] K.S. Subramanian, *Political Violence and the Police in India* (Sage Publications, 2007).

 [ISSN 2581-5369]

and algorithmic policing. without the early building blocks, the later developments of national databases, predictive analytics, AI based surveillances, and automated digital forensics, would have had no the institutional framework that was essential for the development and large scale adoption

II. ESTABLISHMENT OF NATIONAL DATABASES AND INTEGRATED POLICING SYSTEMS

India's development of national databases and national integrated policing systems marks a significant turning point in the country's criminal justice system development continuum. The transformation began in 1986 with the National Crime Records Bureau (NCRB), which was established to assist investigators in linking crimes and cross jurisdictional offenders. To achieve this, the NCRB merged the Directorate of Coordination Police Computer (DCPC), the Inter State Criminals Data branch, and the Central Fingerprint Bureau of the CBI. The purpose of the NCRB was to assist the police in modernizing their information and management systems through standardization of data collection and analysis. Over the years, the mandate of the NCRB has expanded with the advent of the Automated Fingerprint Identification System (AFIS), the National Automated Fingerprint Identification System (NAFIS), and the Digital Police Portal, which was developed in 2017. These systems and services provided law enforcement personnel and the general public with real time, on-thespot matching of fingerprints, forensic assistance, and access to centralized databases. However, as crime became more and more complex, the NCRB transitioned from a basic manager of databases to the national leading technological anchor for making and/or technological decision support systems, analytics and cross agency collaboration or convergence provide a foundation for the policing framework based on Artificial Intelligence (AI) systems[7].

One of NCRB's most significant contributions came with the launch of the Crime and Criminal Tracking Network & Systems (CCTNS) in 2009, an ambitious missionmode project under the National e-Governance Plan. Conceived in the aftermath of the 2008 Mumbai attacks, CCTNS aimed to resolve the longstanding fragmentation of crime records across India by interconnecting police stations nationwide through a unified Core Application Software. The project sought to digitize key police processes including FIR registration, investigation records, and charge sheets to enable seamless access to real-time crime data[8]. The initiative aimed to create a unified system in which Indian police services would be accessible on a national scale,

[7] K.S. Subramanian, *Political Violence and the Police in India* (Sage Publications, 2007).
[8] Bureau of Police Research and Development (BPR&D), *Modernisation of Police Forces in India*

 [ISSN 2581-5369]

and which would include advanced record-keeping and analytical capabilities, user-friendly service portals for citizens, and the digital conversion of legacy paper records. Over the years, the CCTNS made remarkable progress, especially in connecting 16,000 police stations and thousands of higher police offices, and from 2013 to 2022, it became possible for citizens to register over 99% of police reports (FIRs) online. Nevertheless, as a national initiative, it has faced a number of problems, including varying software integration around the country, a lack of infrastructure in remote and rural areas, and insufficient training of police personnel to use the digital tools.

Operational performance differences in each state, as seen in the country in states like Bihar and Rajasthan, demonstrates that while a number of states have been able to implement the initiative, some have not been able to effectively bring in system integrators and/or migrate legacy systems. These gaps reinforce the need for more systematic human resource development, enhanced cybersecurity, and continuous improvements outlined by the emerging CCTNS 2.0 frameworks, including cloud technologies, automated biometric identification, and improved data validation for enhanced accuracy and completeness. Fundamentally, CCTNS represents India's first substantive shift from manual policing towards digital policing, and provides the foundational framework for data-driven and integrated justice policing mechanisms[9].

ICJS builds on the groundwork established by the CCTNS. It represents the next development of India's integrated policing system. Directed by the eCommittee of the Supreme Court, ICJS aims at integrating the police, judiciary, correctional services, forensics, and prosecution services through a single digital network. One of the ICJS objectives is to do away with repetitive data entry and facilitate seamless, instantaneous sharing of data, including case First Information Reports (FIRs), charge sheets, case diaries, forensics and related court case documents. The slogan 'one data, one entry' speaks to the principle that data that is entered into a police system becomes available to the other segments of the system without the data being entered multiple times into other systems.

In Phase I of the ICJS, stand-alone IT systems were integrated for eCourts and ePrisons; however, in Phase II, which was approved in 2022 for an outlay of ₹3,375 crores, the ICJS focuses on advanced integration, analytical dashboards, cross search solutions, and adherence to the new criminal laws, including the Bharatiya Nyaya Sanhita and concomitant legislation.

[9] M.P. Singh, "Information Technology and Criminal Justice System in India," *Journal of the Indian Law Institute*, Vol. 45, No. 3 (2003).

 [ISSN 2581-5369]

Arguably, for the purpose of enhancing investigation, the proposed integration is likely to solve the problem of the 'information delay syndrome, where it is possible for the judiciary to have on the record an FI Report [First Information Report] that has been uploaded by the police, and to have the corresponding and cross-referencing collaboration of forensic laboratories and prosecuting services efficiently[10]. However, implementing ICJS nationwide also presents challenges related to technological readiness, data privacy, legal procedural harmonisation, and the need for specialised training across agencies. Despite these hurdles, ICJS is widely regarded as a milestone in India's transition to a modern, coordinated, and transparent criminal justice system.

Simultaneously, large-scale digitisation efforts transformed courts and prison administration, complementing the integration goals of ICJS. The e-Courts Project, initiated in 2007 and currently in Phase III with a total outlay of ₹7,210 crore, represents India's flagship judicial digitisation programme. Digitisation of case records, e-filing systems, video-conferencing infrastructure, cloud-based data storage, National Judicial Data Grid dashboards, and virtual courts are some of the key components that have drastically improved accessibility and reduced pendency. The integration of AI-powered tools such as automated case scheduling, predictive analytics for adjournment forecasting, and machine-assisted legal research has further modernised court processes, making justice delivery more efficient and citizen friendly. Parallel to this, the e-Prisons system modernised prison management through biometric identification, inmate tracking, digital case management, online visitation, and grievance redressal systems, enabling real-time sharing of prisoner data with courts, prosecutors, and police agencies. The combination of e-Courts and e-Prisons demonstrates how digital transformation across different justice pillars amplifies efficiency, accountability, and transparency, ensuring that each institution operates with up-to-date information and synchronised workflows within a unified national ecosystem.

The cumulative impact of these systems has brought about a fundamental shift in India's investigative capabilities. For the first time, police forces, forensic teams, prosecutors, and courts can access standardised data through interoperable networks, dramatically improving the speed and quality of investigations. The integration of national databases enhances the ability to identify repeat offenders by linking FIRs, biometric records, and forensic findings across states, a function strengthened by NAFIS through its unique 10-digit fingerprint identification numbers[11] . The standardisation of records also mitigates discrepancies that

[10] Pavan Duggal, *Cyber Law in India* (Wolters Kluwer, 2014).
[11] Ministry of Home Affairs, *Crime and Criminal Tracking Network & Systems (CCTNS) Guidelines* (2009).

 [ISSN 2581-5369]

previously arose from varied reporting formats and paper-based documentation across states. This consistency strengthens decision-making by enabling accurate trend analysis, predictive policing strategies, and resource allocation based on reliable nationwide data. Studies on technological integration in investigations emphasise that digitised and standardised data whether from CCTNS, CCTV networks, or forensic labs enhances evidentiary accuracy, improves the admissibility of digital evidence in courts, and increases the precision of suspect identification. Further, integrated systems support law enforcement agencies in overcoming historically entrenched barriers such as bureaucratic delays, siloed information, and incomplete records, thereby accelerating case progress and reducing opportunities for manipulation or data loss[12].

Nevertheless, while interoperability offers immense advantages, it also introduces concerns related to privacy, data protection, and ethical governance. Legal scholarship notes that expanding digital surveillance, large-scale data storage, and biometric identification must be balanced with constitutional privacy guarantees and compliance with emerging legislation such as the Digital Personal Data Protection Act, 2023. As India's justice system embraces integrated and AI-enabled systems, these concerns highlight the need for strong data governance frameworks, transparent audit mechanisms, and strict safeguards against misuse. But despite these important considerations, the overarching trend remains clear: national databases and integrated systems have fundamentally modernised India's investigative architecture, enabling a shift from fragmented, manual processes to a coherent, data-driven, and technologically resilient criminal justice ecosystem[13].

III. TRANSITION TO ADVANCED ANALYTICS AND AI-ENABLED POLICING

The Indian police agencies are evolving from rudimentary digitized data storage systems to sophisticated systems employing data analytics and artificial intelligence (AI) due to the growing diversity of data sources accessible to them. Rapid advancements made in police data capture from documents, selective dissemination of information (SDI) and local social media data support this claim. A marked growth in the police data capture systems and the establishment of the Crime and Criminal Tracking Network and Systems (CCTNS) within the police data ecosystem occurred. Authorities are now able to utilize a diverse range of data sources, including person-level SMS, call data records and legitimate investigations, and CCTV video feeds, social media data (Facebook, Instagram, WhatsApp, X, Telegram) and

[12] Ibid.
[13] National Crime Records Bureau, *Fingerprint Bureau and Automation Initiatives*, Government of India Reports.

 [ISSN 2581-5369]

public safety apps, and time-framed and geo-located data from smart traffic systems. There has been an increasing establishment of social media monitoring units within the police forces of Indian states. The Russian invasion of Ukraine in 2022 and the subsequent information wars highlighted the importance of these units. The need to monitor disinformation, detect social movements, and respond to cybercrime in real time is expected to drive growth from approximately 262 in early 2020 to 365 by 2024. Data flows between police, prosecutors, courts, prisons, and forensic laboratories have become standard practice due to the integration of the Indian judiciary's e-Court system and the police's Crime and Criminal Tracking Network and Systems (CCTNS) along with the Interoperable Criminal Justice System (ICJS) Stack. This has made it possible to implement systems and analytical dashboards based on data lakes with "one data, one entry" principles.

The merging of these data streams with artificial intelligence (AI) pertaining to video analytics, biometric scanning, and cyber forensics is beginning to alter the speed and nature of investigations, and is creating a more efficient process for the identification of suspects and evidence streams, as well as the transition from manual to more efficient and risk-based operational resource targeting. The most important example of big data in policing is the consolidated use of metropolitan CCTV networks and sophisticated analytics.

Take, for instance, the "Safe City" Extension in Delhi. Under the City Safe initiative, the Delhi Government is integrating police departments with AI-enabled facial recognition, as well as the construction of command-and-control centers. The project will see hundreds of arrests in the pilot districts in relation to real-time as well as historical facial recognition systems with criminal face recognition databases. On certain high-security alert occasions, such as Republic Day, police officers equipped with AI smart glasses that allow for real-time face recognition and matching with the police watchlist are deployed. Delhi police are the first to be reported using such technology in Indian policing. There is also a similar case of artificial intelligence application in SMI. The police social media monitoring cells equipped with artificial intelligence (AI) monitor social media for viral content, implement direct social media interventions, operate under the framework of the IT Rules of 2021, and activate the police in relation to the offline movements at the place of interventions. This kind of policing is also visible in the latest public policy briefings based on BPR&D and DoPO.

The application of AI in policing also relates to the lessening of due process, errors, and the associated biases. For the last several years of a lack of civil liberties, India has seen the most

 [ISSN 2581-5369]

extreme application of AI and Big Data in policing[14].The second pillar of this transition is predictive policing and algorithmic crime mapping. In this case, predictions of When, Where, What are made based on historical FIRs, Incident Logs, Seasonality, and micro place attributes, to aid in the pre-emptive deployment of personnel. Deployments in India have been more cautious than those in the United States, but the pace is picking up. spanning operational narratives and practitioner case studies, are indicative of weekly hotspot forecasts and dashboards for allocation of resources as well as alerts that recompute risk if and when new incidents have been added to the CCTNS/ICJS fabric. Management consultancies working with state programmes have reported rapid changes in the configuration of the predictive models from early on-premise installations to cloud- based systems with API's to the ICJS allowing for centralized documentation and realtime reporting, analytics, and model retraining loops as well as a more developed construct for gap analyses. predictive models for India have aligned with 'big data', and more specifically, with the spatiotemporal clustering, regression trees, and ensemble models] of predictive analytics. Regarding model performance, the India predictive models do not defy context: it is absolutely necessary that the inputs and criteria be the standard where nation databases have improved, but still,inter-state variation persists. Therefore, the policy literature is calling for better model explanations, documentation of audits and "human in the loop" interaction, where the recommendations actions, which are guided by the model, are not determined by it[15].

Concrete state-level initiatives illustrate both ambition and diversity in approach. In Maharashtra, the government established MARVEL (Maharashtra Advanced Research and Vigilance for Enhanced Law Enforcement) as a special-purpose vehicle to integrate AI into policing statewide, and partnered with industry to launch Maha Crime OS AI a platform showcased in December 2025 as accelerating cybercrime investigations from months to hours through automated data triage, link analysis, and case guidance. Mumbai Police have publicised an AI-based predictive system (developed with K J Somaiya Institute of Technology) that mines five years of crime data to forecast theft-prone zones and time bands, feeding weekly and monthly analytics to station officers; media reports cite early pilots with notable accuracy and prevention claims, alongside integration of facial recognition and ANPR across an expanding surveillance grid. In Telangana, Hyderabad Police have coupled dense CCTV infrastructure with experimental AI features ranging from mask-compliance detection during

[14] Second Administrative Reforms Commission, *Fifth Report on Public Order* (2007).
[15] Andrew Guthrie Ferguson, *The Rise of Big Data Policing* (NYU Press, 2017); Rashmi Ranjan Das, "Predictive Policing and Big Data Analytics in India," (2020) 12 *Indian Journal of Law and Technology* 45.

 [ISSN 2581-5369]

the pandemic to newer plans for AI-assisted investigation and, more recently, have deployed TG-QUEST, an AI-integrated drone policing system positioned as a "digital beat officer," including proactive crowd analytics, ANPR, and collaborations with platforms like Google Maps for traffic intelligence. Large-scale field deployments have followed: in January 2026, Telangana Police used TG-QUEST at the Medaram Jatara an event expecting ~20 million devotees—combining AI people-counting, balloon-mounted cameras, and dronebased advisories for real-time crowd and traffic management[16]. The 2026 Republic Day plan for Delhi incorporates the use of AjnaLens smart glasses that have the ability to share data with the police for real-time processing of data in rapidly moving crowds. These glasses also have thermal imaging and facial recognition to minimize the need for person to person checking. These also come in conjunction with pilot algorithms on the district level, such as Akola, Maharashtra's marketed as India's first repeat offender system via Project Trinetra which does offender scoring but claims to do so with a "no profiling" approach and internal audits to minimize bias.

As the technology stack continues to evolve, so does the role of private and public partnerships in AI-enabled policing. Vendors and start-ups provide video analytics (object detection, and behavior recognition), as well as FRS wearables, drones, and case workflow co-pilots. Systems integrators connect these to the CCTNS and the ICJS, and the cloud providers offer elastic computing for model training and cross-agency dashboards. AI in Maharashtra's MahaCrimeOS is co-developed with Microsoft ISV CyberEye, the state's MARVEL SPV, and Microsoft's India Development Center, exemplifying partnerships of three or more focused on a specific domain AI[17].

For the rollout of smart glasses scheduled for 2026 in Delhi, reports detailing the locationbased city reporting, and other press sources, state that the collaboration is with AjnaLens, an Indian startup that is developing the wearable device and the integration for facial recognition matched with police databases. Ecosystem other than this collaboration, for example, the open call for police technologies by the Centre for Police Technology partnerships with police technology OEMs, startups, and academic institutions for 50 areas within "smart policing," shows that the vendor structuring in India is developing for forensic, cyber intelligence, AI operational analytics, and operational tech under one framework. In addition, there is concern in the media and commentary from various experts that when the procurement of technologies is ungoverned, outpaces the mechanisms of control, or when gaps occur, there is a loss of public

[16] United Nations Interregional Crime and Justice Research Institute (UNICRI), *Artificial Intelligence and Robotics for Law Enforcement* (2019).

[17] Government of Maharashtra, *MARVEL Initiative and AI in Policing Reports* (2025); Microsoft India Development Center, *AI for Public Safety Initiatives* (2025).

 [ISSN 2581-5369]

confidence in the systems that detect, arrests, or surveils people, and the AI systems used for the surveillance or policing are not transparent.

The addition of analytics and biometrics to police video technology is one area in which the operational use of AI is very apparent. On one end, the technology used in mobile and stationary digitale video surveillance systems is able to produce "hits" which are actionable enough to assist the police to perform an investigatory function that would be impossible for them to conduct for the volume of people interacting with the city's infrastructure. Examples of the pilots conducted by the Delhi Police revealed the identification and arrest of multiple people in a very short timeframe, some of whom were identifiable in very poor video images, and provided the police with the ability to perform what are called "rolling" video surveillances of high traffic areas. On the other end, activist and investigative reporting have documented multiple instances in which facial recognition was the central component used to justify the arrest of an individual in relation to a protest, which has reignited discussions about the need for threshold controls, demographic discrimination, and due process when the technology is used as the primary means to decide an outcome.

These concerns are evident not only in Delhi. In other major metropolitan areas, rapid Frontline (FR) expansion, and the "distress detection" technologies (based on micro expression, sound, and crowd anomaly detection) have prompted the need for statutory guardrails, auditing, and use-case proportionality requirements. However, the policing side argues that AI can be a "force multiplier" and, if used properly, will allow sparse personnel to cover more areas and fill more gaps, particularly in massive events and in areas where manual policing is too dangerous or simply not feasible. An example is the drone-based aerial patrols that the Telangana DGP describes as first responders that can arrive at an incident more quickly than ground teams, providing streaming video that is tamper proof for evidentiary purposes, an operational rationale that is in alignment with the command and control approaches to policing that are in vogue in many parts of the world [18].

Telecom and messaging data are sensitive layers in this ecosystem and are usually touched under court sanctioned or statutory processes. Though the public domain is operationally detailed, the logic is simple. Call data record (CDR) analysis, tower dumps, and geofencing analytics can prove presence and movement. SMS messages and application telemetry assists with crisis triage and crowd control. Social media Open Source Intelligence (OSINT) analytics

[18] Mumbai Police & K. J. Somaiya Institute of Technology, *Predictive Policing Pilot Studies* (reported in media sources, 2024–2025).

 [ISSN 2581-5369]

identify influence networks, misinformation outbreaks, and flash-mob threats. Policy briefs merging data from the Directorate of Public Order (DoPO) and internal security commentary suggest that the rise of specialised monitoring cells correlates with the volume and velocity of activity in this domain, with internal Standard Operating Procedures (SOPs) designed to keep situational awareness from open-source surveillance that requires a lower legal threshold for intrusive surveillance. Indian researchers studying police use of social media note that citizen engagement and tip inflows via Online Social Media (OSM) monitoring create a situation where digitally generated complaints, leads to a missing person, and reports of a crisis are channeled directly into policing Customer Relation Management (CRM) systems, while also creating new burdens around content verification and trust.

In this context, "big data" in Indian policing is not only surveillance, but also a communications public-facing framework that when designed well enables service delivery and transparency. The next phase is also being shaped by two additional trends. First, edge AI and wearables are bringing analytics to the scene via body worn cameras with on-device redaction, patrol smartphones running licence plate and facial recognition matching, and low-connectivity situations query glasses that are linked to local watchlists.Delhi's AjnaLens deployment exemplifies this "edge first" approach, with a local report stating that user privacy is preserved through the use of local (encrypted) phone databases that support independent operation during the crowd control sweep. Second, AI copilot(s) for investigators—already tested in MahaCrimeOS AI in Maharashtra—are expected to accelerate processes such as complaint reading, timeline generation, suggest link charts, and digital forensic triage on seized devices and cloud accounts, with some level of human oversight. Participants in state briefings and media reports about the launch make claims of unprecedented reductions in the cycle time for recovery of fraud-related crimes in the digital space. They also intend to extend this to 1,100 police stations, but independent assessments will be necessary to determine the actual effect and to assess the extent of automation bias in decision-making[19].

The sustained trust of the public on governance systems relies on the multiple model vendor standards (data shareability, portability, auditability) algorithmic accountability, bias, and accuracy audits, and impact assessments, which many people have mentioned as being part of international research on the data governance of the law enforcement system. Indian scholars explain that the privacy jurisprudence of the Supreme Court of India established the concepts of "proportionality," "legitimacy," and "necessity," which must anchor the cross border state

[19] Internet Freedom Foundation, *Automated Facial Recognition Systems in India: Policy Brief* (2021).

 [ISSN 2581-5369]

policing using advanced technology and artificial intelligence (AI) powered surveillance systems and operational AI (co-pilot) systems on autonomous operational workflows. Emerging practical integrations from field pilots include ethically logging and validating prealert actions as well as setting alerts to avoid behavioral pattern profiling of known repeat offenders. That operational approach balances augment and replace; corroborate and conclude and effectively balances operational trade-offs with the protection of civil liberties.

India's adoption of advanced analytical and AI based policing technologies is predicated on the confluence of four transformations: the proliferation of data sources; predictive and riskbased resource distribution systems becoming standard; the expansion of state-sponsored initiatives employing AI-powered tools, such as drones and collaborative case management systems; and the increasing combination of public and private partnerships furnishing the necessary hardware, software, and cloud solutions. The advantages of improved identification, proactive intervention during major public gatherings, and faster cyber fraud detection are counterbalanced by interstate conflict, reliance on probabilistic associations, and the need to establish a legal framework to maintain public confidence.

With India advancing further into AI policing, the challenge for policymakers and police executives will be to combine oversight with realism to ensure that AI is an operational force for the extension of justice and not an operational end that compromises justice.

IV. LEGAL AND POLICY MILESTONES SUPPORTING TECHNOLOGY-DRIVEN POLICING

India's current model of architecture and technology-based policing rests on a number of legislative, constitutional, and policy frameworks that define the scope of the legal frameworks in which digital technologies, systems of surveillance, and AI involved policing operate. The most important of the extensive frameworks is the Information Technology Act of 2000, which provided a legal framework for electronic documentation, cybercrimes, and digital evidence for the first time in India. Primarily aimed at legalising electronic transactions and supporting e-governance, the IT Act provided that electronic records and digital signatures were to be treated as equivalent to paper-based documents and, thus, enabled police and investigative agencies to use digitally produced evidence in a case. The Act's establishment and regulation of digital signature frameworks and the resolution of cyber disputes through the establishment of the Controller of Certifying Authorities and the Cyber Appellate Tribunal, as well as the criminalisation of hacking, online fraud, and identity theft, which provided an early outline of cybercrime investigations, were all driven by the IT Act. The 2008 amendments, as well as the

 [ISSN 2581-5369]

most recent ones, provided the IT Act with an extension, and in particular, an updating of the policy and procedural powers in relation to the criminal use of electronic devices. The cumulative effect of the aforementioned frameworks provided the police, for the first time, with a legally defensible framework within which to handle electronic evidence, conduct cyber forensics, and use digital technologies in the investigation processes, thus providing the legal framework for the use of AI technology in policing systems[20].

The Supreme Court's significant privacy ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) brought a new fundamental right (that of privacy) to the constitution, identifying it as one that rests on the fundamental aspect of dignity, liberty, and the right to be left alone. It was a nine judge bench that brought to the judgement a new consideration of the right to privacy as something that for the first time expressly recognised the constituent elements of informational privacy, bodily privacy, autonomy discretion/closure/exclusionist (essentially) privacy). This new proposition on privacy created a new frontier (and arguably, a constitutional framework) on the boundaries of state surveillance, biometric data collection, and state data processing. The Court's rule of three (or trilogy) on legality, necessity, and the less intrusive means, and greater public good, advocates, was in their own words, the first jurisprudence on privacy in India, where they empirically argued that privacy should be respected. This new privacy doctrine created a new and fundamental set of principles and constructions for Puttaswamy and Justice Puttaswamy underpin the aforementioned public good that set the basics for state secret (or state surveillance) reasoning on the constituent boundaries of privacy in India. Puttaswamy, though the intrusiveness of the implementation of the processes, gave a new 'rights-based' articulate basis that post-Puttaswamy India, gave the basis from which all policing technologies in India had to work[21].

India's data governance evolved with the completion of the Digital Personal Data Protection Act (DPDP Act) of 2023, a highly anticipated milestone based on the case of Puttaswamy. The Act has been the result of extensive drafting and a public discussion of the known and unknown elements of the Act. The length of time taken suggests the Act's components remain contentious. The Act prioritises Puttaswamy's core principles, vesting data subjects with fundamental rights of access, rectification, erasure, and restriction of data processing, as well as fiduciary responsibilities of data controllers (affecting public data controllers) to ensure the processing of data is safe, transparent, and responsible. Conversely, broad government

[20] Telangana Police, *Use of AI and Surveillance Technologies in Hyderabad* (official releases and reports, 2020–2024).
[21] Telangana State Police, *TG QUEST Drone Policing Initiative* (2025).

 [ISSN 2581-5369]

exemptions, primarily contained in Section 18, allow for the processing of personal data without consent by law enforcement and intelligence agencies for national security, public order, and crime control purposes. There is a significant gap in the oversight of the processing of personal data, which could allow for unrestricted surveillance. Scholars agree the DPDP Act has improved prior protection regimes, but remain concerned that the DPDP Act's exemptions will prevail over the proportionality protections identified in Puttaswamy, particularly in the contexts of AI. Concerns exist with the DPDP Act's lack of protection on data processing with the integration of AI and the ongoing advancements by states, such as Delhi's Safe City project, which is AI-enabled, and Maharashtra's crime platform, MahaCrimeOS. The DPDP Act leaves fundamental issues of auditability, algorithmic discrimination, and lawful processing to be covered by sectoral policies as opposed to a dedicated AI law[22].

Concurrent with data protection laws, the Ministry of Home Affairs (MHA) has become a principal architect of the technology-driven reform of policing, issuing guidelines, sanctioning pilot projects, advocating forensic and AI policing, and seeking implementation at an unprecedented scale. A notable development is the creation of AI Task Forces in state police organizations, coming as a result of a 2026 (upcoming) order from the Prime Minister insisting that all states and union territories establish dedicated AI units, and that at least 70% of police personnel be trained in AI via the ingot digital learning portal. The MHA is also designing an overarching national Artificial Intelligence (AI) policy to facilitate intelligence fusion, real time threat assessment, automated tagging, predictive analytics and modeling, and other operational mechanisms to support policing and internal security functions— particularly, extensive operational integration with NATGRID, India's data fusion and analytics system for crossborder and internal security. This is perhaps the largest leap toward algorithmic policing in India, and reflects an operational strategy for making data-driven decision-making a core element of the Country's national security and law enforcement strategy. The Ministry has also coupled the forensic modernization with the AI expansion: there is a new national scheme to establish a modern forensic lab in every district, a mobile forensic investigation subsystems, and the requirement that forensic investigations be conducted for all serious crimes, thereby, making science and technology standards in policing. These changes are in tandem with the three new criminal laws—Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita, and Bharatiya Sakshya Act—that are heavily dependent on forensic and digital evidence, thereby creating a climate to incorporate technology and science into the criminal process. During policy forums, senior officials at the MHA have outlined these developments as initiatives

[22] Press Information Bureau, Government of India, *Deployment of Technology at Medaram Jatara* (2026).

 [ISSN 2581-5369]

intended to position India's criminal justice system as the most advanced globally in the next five years, with emphasis on integrated AI, forensic expansion, and countrywide training[23].

These laws and policies are milestones in India's modern transformation of policing. The IT Act has the legal basis for digital investigations and policing of cybercrimes; Puttaswamy sets out the constitutional parameters that curb surveillance; the DPDP Act with huge enforcement exclusions gives the governance and rights framework on data; and the policy push of the MHA is the policy push that covers the broad adoption of AI, modernization of forensics, and the building of unified country-wide capacity. These frameworks together underscore the transformation of India's criminal justice system through technology, while also indicating the need to prioritise and balance privacy, accountability, and constitutional restraints on policing in the automation and data-centric age.

V. CRITICAL REFLECTIONS AND FUTURE DIRECTIONS

India's relatively recent technological infusion in policing (the last 20 years) is an example of how difficult it is for complex institutions to integrate new innovations. India has adopted technology in policing in response to crises, capacity gaps, political priorities, and the public's demands. Initiatives for early integration of technology in the justice system, including the CCTNS, ICJS integration, and e-governance of the judicial system, taught us that technology must be paired with structural changes such as the development of procedures, the provision of adequate training, the establishment of reliable technological and institutional systems, and the engagement of the institution. The uneven integration of technology in policing systems in the individual state systems in India also shows us that the technology will only be as good as the data that is fed into it. Outdated records, outdated procedures, and manual backlogs placed limits to the full integration of the system. It also taught policymakers the importance of systems being designed with an interoperability focus, and the importance of unified systems/standards. One of the most persistent lessons has been that the implementation of new technology without clear rules (legal) and without adequate ethical consideration will magnify systemic problems and existing biases.

India showed us that while the implementation of new systems and new technologies is necessary, it must be done with adequate governance. Overall, India has also shown that the integration of technology into policing is largely dependent on the people/ the culture[24].With India advancing into a new era of technology-augmented policing, there are a number of new

[23] Delhi Police, *Republic Day Security Arrangements and Technology Deployment* (2026); media reports on AjnaLens collaboration.
[24] Maharashtra Police, *Project Trinetra Documentation and Pilot Reports* (2024–2025).

 [ISSN 2581-5369]

trends on the horizon which will change the manner in which security agencies operate. One such trend is the fast `development` of generative artificial intelligence, which will change the facets of intelligence processing, assistance in investigations, and the construction of cases. Generative models can already aid in the summarising of complaints, analysing trends and patterns of thousands of First Information Reports (FIRs), translating reports and other types of evidence in various languages, aiding investigators in identifying and explaining the gaps and references that are difficult for a normal human being to identify.

In the near future they can likely aid in crime scene reconstruction, preliminary reports of investigations, and synthesising various pieces of data to generate investigative leads. Along with this, there is the development of multimodal forensics, which is in other words the combined analysis of audio, video, text, biometrics, and other sensor data as opposed to the analysis of these data types in isolation. In the near future India will likely be forced to develop systems that will be able to utilise various types of data as a result of the widespread CCTV systems and other video recording equipment) in order to develop a coherent timeline of investigative events. Also, data and evidence from satellite images, social media, and the extraction of data from mobile devices will also over the coming years be combined in order to develop a timeline of investigative events.

While these technologies will enable improvements in real-time threat identification, emergency responses, and situational awareness, the extent of surveillance and technologies used to identify and track devices is likely to exceed the limits of law enforcement's manpower. Technologies such as drone surveillance, ground robotic drones, automatic number plate readers (ANPR), and body-worn devices with artificial intelligence (AI) operate surveillance technologies which may normalise the surveillance environment.All these evolving technologies indicate that India is embarking on a new phase in which policing will be more focused on predictive, pre-emptive, and automated methods, where human decision-making will be supplemented by, and in some cases, usurped by, artificial intelligence.[25].There is an urgent need for solid legal protections as well as ethical frameworks to match growing technological capabilities. Existing laws, while essential, do not cover autonomous analytics, AI-driven profiling, or widespread biometric systems.

More detailed and specific statutes are necessary for clarifying what data is able to be collected, how long data sets can be held, how investigative agencies are to justify their algorithm-assisted decisions, and what independent oversight balances are to be in place. AI systems' transparency

[25] Ministry of Home Affairs, *Inter-Operable Criminal Justice System (ICJS) and CCTNS Reports* (2019 onwards).

 [ISSN 2581-5369]

is made to be profoundly important.If AI systems make decisions or judgments that are related to bail, risk, or even the identification of suspects, the individuals affected should have the opportunity to challenge the decision and understand the reasoning behind the different AI assessments. In addition to this ethical transparency, the frameworks should be in place for potential algorithmic bias and discrimination that AI systems may derive from historical crime and related police data (i.e. trained data for the police) that may reproduce police data injustices of the past. Mandatory audits, algorithmic impact assessments, and other third-party assessments should become the "norm" for the technological justice system. Surveillance technology and collateral abuse are becoming intertwined, as the system's technology incorporates AI that learns and acts in an autonomously decision-making environment. India will need legal frameworks established that focus on areas of individual rights, and the recognition that people do have privacy, dignity, and a process that is equitable and just. Those concepts are not antipolicing; they are concepts that must be a central and critical part of legitimate, good faith policing.

India's biggest challenge will be balancing national security with privacy and individual rights in an increasingly digital world. Data collection and use demand increased and more sophisticated technology. The use of restraint and transparency and accountability become challenging. In order to effectively implement this process, rights and security should be perceived as values that reinforce each other. Public trust is imperative for any security plan to be effective, and without trust, any goal is rendered impossible. The goal should be to synthesize competing values of security, privacy and citizen rights. In some cases, citizen rights will be protected better with more assertive policing, as opposed to a more relaxation or passive approach to policing. When AI and other techno-automation practices are deployed, it is essential that citizen rights are protected. Integration of modern policing technology and citizen rights will involve a combination of effective oversight, judicial approval of automated technopolicing, and, audit and accountability systems.

In some cases, citizen rights will be protected better with more assertive policing, as opposed to a more relaxation or passive approach to policing[26]. Considering the course of India's evolving technologies, the AI-based innovations on the horizon, the urgency for ethical and legal frameworks, and the persistent balancing act between security and rights, India is at a critical juncture. The path India selects will either result in technology being a tool for justice, efficiency, and public trust, or result in technology being a contributor to unmitigated

[26] Microsoft India & CyberEye, *MahaCrimeOS AI Collaboration Reports* (2025).

 [ISSN 2581-5369]

surveillance and institutional overreach. The future will require not only improved technologies, but also a greater focus on governance, increased public participation, and a rekindling of the constitutional principles that will be needed to support any contemporary criminal justice system. The extensive impact technology-driven policing has had on the criminal justice system in India is indicative of the system's ability to understand the processing and response to crime in a digitally driven society. From digitization of police records and the building of a national police record system and ICT infrastructures to the use of advanced analytical tools and artificial intelligence surveillance and forensic technologies, police systems are modernizing to enhance speed, accuracy, and efficiency. Each technology, institutional, and legislative development has a positive and negative impact on police agencies and modern law enforcement's structural, ethical, and legal challenges.

While all the chapters explore specific technology-driven law enforcement challenges, they all agree that policing is an area that technology has no throughput impact. The CCTNS and ICJS as digital platforms have demonstrated that digital integration requires not just advanced technology, but standardized data, trained personnel, and cooperation between law enforcement agencies. The use of surveillance drones, predictive policing and facial recognition technologies are forms of artificial intelligence that have been shown to reinforce the strengths and weaknesses of the institutions being surveilled. If oversight and adequate data are available, these technologies can substantially improve law enforcement. If there is a lack of oversight, training, and data, then these technologies may increase the risk of discriminatory profiling, opaque decision-making, and misidentification. The incremental progress of legal and constitutional advancements of late, particularly through the Puttaswamy judgement and the recent Digital Personal Data Protection Act, Constitutional recognition of the right to privacy, have offered some respite to developments in technology and the policing of people. These developments advance the understanding that the policing of people in democratic societies must be carried out in a rights respectful manner, even in the face of emerging and increased risks. They also articulate the growing balance that needs to be struck between the rights and obligations of the state to protect national security and the constitutional protection of individual rights and freedoms, especially when policing, as a technology, becomes increasingly data driven, automated, and interconnected.

The next wave of technologies (including generative artificial intelligence (AI), multimodal forensics, autonomous surveillance systems, and advanced data fusion technologies) will revolutionise the speed and accuracy of investigations. While there is optimism for incredible advancements in the practice of policing, there is a corresponding concern that it will also

 [ISSN 2581-5369]

introduce normalised surveillance, weaken or remove the protection of rights, and diminish the trust of the people if new technologies for policing are deployed without legal, ethical, and institutional boundaries. While predictive and preemptive policing introduced new, unimagined, and advanced models for policing, it will introduce new challenges for accountability, transparency, and community policing.

India has come to a critical point in its development. The groundwork has been done in technology, institutions are being built, and policies are beginning to address contemporary issues. The most important focus moving forward is the assurance that democratic control keeps pace with technological advances. Building this balance will require ongoing reforms, training, impact assessments, accountability, and a commitment to dignity, privacy, and fairness. The potential that technology has in policing is not in supplanting human decision making. It should be used to enhance that decisioning, so that the future of policing is not only more efficient, but more equitable.

*****

 [ISSN 2581-5369]