DOI: 10.21088/ijlhb.2454.7107.12226.6

Indian Journal of Law and Human Behavior
Volume 12 Number 2 / July - December 2026

REVIEW ARTICLE

Digital Governance and Use of AI-Policing in Uttar Pradesh

Rajeev Kumar Singh[1], Shivam Mishra[2]

HOW TO CITE THIS ARTICLE:

Rajeev Kumar Singh, Shivam Mishra. Digital Governance and Use of AI-Policing in Uttar Pradesh. Indian J Law Hum Behav 2026; 12(2): 122-134.

ABSTRACT

Artificial intelligence is beginning to reshape policing in Uttar Pradesh through crime analytics, predictive patrolling, facial recognition, natural-language search, AI-assisted reporting, case-tracking platforms and traffic-management systems. This paper examines these developments not merely as technological upgrades but as a form of digital governance in which police discretion is increasingly mediated by data, algorithms and privately developed platforms. Using a doctrinal and qualitative policy-analysis method, the study reviews the constitutional framework, the Criminal Procedure (Identification) Act, 2022 and Rules, the Digital Personal Data Protection Act, 2023 and Rules, relevant criminal procedure and evidence laws, official police circulars, practitioner accounts and international AI-governance standards. It evaluates the operational value of systems such as the Crime Analytics and Predictive Policing Portal, FAI, AI-enabled document management, EBITA, Trinetra 2.0, Crime GPT and YAKSH. The paper finds that these tools may improve information retrieval, supervision, resource allocation and response time, but their legitimacy depends on data quality, purpose limitation, proportionality, human review, auditability and effective remedies. India's present legal framework remains fragmented and does not create a complete accountability structure for AI-assisted police decision-making. The paper therefore proposes a rights-respecting governance model based on prior impact assessment, classified risk levels, documented human oversight, independent audits, secure retention practices, vendor accountability and accessible grievance redressal. Such safeguards can support efficient policing without weakening constitutional liberty, equality or public trust.

KEYWORDS

• AI-enabled policing • Digital governance • Uttar Pradesh Police • Algorithmic accountability • Constitutional privacy

AUTHOR'S AFFILIATION:

[1]Associate Professor, Amity Law School, Amity University, Lucknow, Uttar Pradesh, India.
[2]Ph.D. Scholar, Amity Law School, Amity University, Lucknow, Uttar Pradesh, India.

CORRESPONDING AUTHOR:

Rajeev Kumar Singh, Associate Professor, Amity Law School, Amity University, Lucknow, Uttar Pradesh, India.

E-mail: rksingh2@lko.amity.edu

➢ **Received:** 03-08-2026 ➢ **Accepted:** 05-09-2026

Creative Commons Non Commercial CC BY-NC: This article is distributed under the terms of the Creative Commons Attribution NonCommercial 4.0 License (http://www.creativecommons.org/licenses/by-nc/4.0/) which permits non-Commercial use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the Red Flower Publication and Open Access pages (https://www.rfppl.co.in)

INTRODUCTION

Policing is one of the clearest sites at which the promise and danger of artificial intelligence become visible at the same time. A well-designed system may help an officer locate a missing person, identify a recurring crime pattern, retrieve an old circular within seconds, or send an emergency vehicle through a congested crossing. The same system, when built on inaccurate data or used without clear limits, may repeatedly direct police attention towards already over-policed neighbourhoods, wrongly match an innocent person's face, or create a permanent digital shadow around someone who was never convicted. The real question is therefore not whether the police should use technology. The more important question is how public power should be organised when technology begins to shape who is watched, questioned, stopped, classified, investigated or treated as a risk.

Uttar Pradesh offers a particularly important setting for this inquiry. The State has a large and administratively diverse police system, ranging from metropolitan commissionerates to rural police stations and specialised units. In recent years, its policing architecture has increasingly relied on digitised records, Crime and Criminal Tracking Network and Systems (CCTNS) data, geographic crime mapping, facial recognition, mobile applications, automated document retrieval and AI-assisted search. Some initiatives operate across the State, while others have emerged as district-level innovations or operational pilots. Taken together, they show a movement from basic computerisation towards data-led and AI-enabled policing. That movement is also part of a wider shift towards digital governance, in which decisions are produced through a combination of legal rules, institutional practices, databases, software design and human judgement. The central argument is that AI-enabled policing is sustainable only when it strengthens both operational capacity and constitutional legitimacy. Efficiency without safeguards may produce quick decisions, but it cannot produce durable public trust.

The paper makes three connected contributions. First, it maps the emerging uses of AI and data-intensive systems in the Uttar Pradesh Police, including crime analytics, predictive policing, social-media alerts, AI-assisted first information reporting, document management, evidence tracking, facial recognition, natural-language search and traffic management. Secondly, it identifies the constitutional and statutory rules that should govern these systems, particularly Articles 14, 19 and 21 of the Constitution, the Criminal Procedure (Identification) Act, 2022, the Digital Personal Data Protection Act, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023. Thirdly, it proposes a practical governance framework for Uttar Pradesh based on risk classification, impact assessment, human oversight, auditable decision-making, data minimisation, security, transparent procurement and accessible remedies.

Research Questions, Objectives and Methodology

The study is guided by four questions. How is AI presently being used, or proposed to be used, across the policing cycle in Uttar Pradesh? In what manner do these systems alter police discretion and administrative responsibility? Are existing constitutional, criminal-procedure and data-protection rules sufficient to govern high-impact police uses of AI? What institutional safeguards can enable innovation without weakening individual rights or public confidence? These questions move the discussion beyond a simple list of technological applications and place AI policing within the broader law of public administration and constitutional governance. The objectives are correspondingly practical and normative. The paper seeks to distinguish low-risk administrative assistance from high-risk uses that affect identification, surveillance, liberty or criminal investigation; to assess the public value and legal risks of major Uttar Pradesh initiatives; to explain the gaps between general data law and the specific needs of algorithmic policing; and to develop a State-level model that can be implemented through police standing orders,

procurement conditions, technical protocols and independent oversight.

Methodologically, the paper adopts a doctrinal and qualitative policy-analysis approach. It studies constitutional principles and relevant legislation, reads judicial decisions on privacy, fair procedure, surveillance and bodily or biometric evidence, and examines responsible-AI frameworks developed by Indian and international institutions. It also draws upon official Uttar Pradesh Police circulars and press material, together with the practitioner account by Kumar and Chaudhary, to understand how particular systems are expected to function. Since publicly available descriptions do not always disclose technical architecture, training data, error rates or procurement terms, the analysis does not claim to conduct a technical audit.

AI-Enabled Policing as a Form of Digital Governance

Digital governance refers to more than the online delivery of public services. It describes the manner in which administrative power is reorganised through data, digital platforms and automated processes. In policing, this reorganisation is especially consequential because the institution already possesses coercive authority. This produces a redistribution of discretion rather than its disappearance. Traditional police discretion rests mainly with officers and supervisors, who are expected to act within law and record reasons where required. AI-enabled policing adds new actors and influences: software developers determine classifications; database administrators define access and retention; vendors may control proprietary models; data-entry practices affect accuracy; and officers decide how much weight to give a recommendation. Responsibility can become dispersed across this chain. A sound governance model must prevent this diffusion from becoming an accountability vacuum.

The literature on algorithmic regulation explains that automated systems can continuously monitor conduct, classify risk and trigger interventions at a scale that ordinary administration could not achieve (Yeung, 2018). For governance purposes, AI-enabled police systems can be placed on a spectrum. At one end are administrative tools that organise circulars, translate instructions or assist with routine drafting. In the middle are analytical and supervisory tools that identify patterns, track deadlines or suggest statutory provisions. At the high-risk end are systems used for facial recognition, predictive targeting, continuous surveillance, biometric linkage or decisions that materially affect liberty. The closer a system moves towards identification, suspicion or coercive action, the stronger the requirements of legal authority, accuracy testing, explainability, human review and redress must become.

Emerging AI-Policing Architecture in Uttar Pradesh

1. Crime Analytics, Hotspot Mapping and Predictive Patrolling

The Crime Analytics and Predictive Policing Portal is among the clearest examples of data-led deployment in Uttar Pradesh. Official circular material refers to trend analysis of CCTNS crime data plotted on maps, including patterns of theft, burglary and robbery during specified night hours. The underlying administrative idea is understandable: police resources are finite, while crime is distributed unevenly across time and place. Mapping recurring incidents may help supervisors plan patrol routes, identify vulnerable stretches and respond before a pattern becomes entrenched. Used carefully, such analysis can support evidence-based deployment instead of relying entirely on intuition or informal local knowledge.

The difficulty begins when a descriptive map is treated as an objective prediction of future conduct. Crime data are produced through reporting, registration and police activity. Areas where residents report more frequently, where cameras are concentrated or where officers patrol intensively are likely to generate more records. Offences that remain unreported, particularly those occurring within homes or involving marginalised victims, may appear less significant in the dataset. A predictive portal can therefore reproduce

institutional visibility rather than actual incidence. Before hotspot scores influence deployment, the department should examine registration practices, missing-data patterns, socio-economic proxies and the possibility that repeated patrolling itself is creating the data used to justify further patrolling.

2. Social-Media Risk Alerts and Emergency Response

The practitioner paper describes an arrangement under which content indicating suicide risk on Facebook or Instagram may generate an alert to the Uttar Pradesh Police social-media centre, followed by location-based coordination through UP-112 and the local police. The public value of timely intervention is evident. In a genuine emergency, minutes can matter, and a structured alert may help officers or family members reach a distressed person before irreversible harm occurs. This is an example of AI functioning not as a criminal-prediction tool but as an early-warning mechanism directed towards the preservation of life. At the same time, such public-private coordination requires a carefully defined emergency protocol. Location information and sensitive content should be shared only where the alert meets a clearly documented threshold of imminent harm. Data received for life-saving intervention should not silently enter criminal-intelligence databases or be retained for unrelated policing.

3. FAI and AI-Assisted Registration of Information

The FIR Artificial Intelligence system, described as an initiative of Agra Police, is intended to analyse the text of a complaint, identify important terms and suggest relevant legal provisions along with directions that may assist the investigating officer. Such a tool can be useful at the reporting stage. Police personnel often work under pressure, and a structured prompt may help them notice a legal ingredient, ask a necessary follow-up question or avoid a routine clerical omission. It may also support officers who are adapting to the transition from the Indian Penal Code to the Bharatiya Nyaya Sanhita.

Nevertheless, registration of a first information report is a legal act, not a classification exercise alone. The correct provision depends on facts, context, intention, relationship between parties and judicial interpretation. Keyword matching can easily confuse similar expressions or miss facts conveyed in local language. More seriously, an officer may treat the software's suggestion as a safe default and stop exercising independent legal judgement. This is automation bias: the human remains formally responsible but psychologically defers to the machine. The system should therefore be designed as a checklist and research aid, not as an automatic section-allocation mechanism. Every accepted or rejected suggestion should be traceable, and the final decision must remain with an identified officer who records reasons in significant cases. Language design is equally important in Uttar Pradesh, where complaints may be made in Hindi, Urdu, English or regional dialects and may initially be narrated orally. Training data should reflect local linguistic variation, not merely standardised legal phrases.

4. AI-Enabled Document Management and Institutional Memory

The proposed AI-powered Document Management System is a comparatively lower-risk but institutionally valuable use. Optical character recognition and natural-language processing can help digitise physical documents, classify them, produce short summaries and answer natural-language queries. The original document must, however, remain controlling. AI-generated summaries can omit exceptions, confuse amendments or invent plausible-sounding propositions. The interface should therefore display the source circular, date, issuing authority, amendment history and confidence warning alongside every summary.

5. EBITA and Evidence-Based Investigation Tracking

The Evidence Based Investigation Tracking Application, also described in the Agra Police account, brings together case management, evidence logging, task allocation, supervisory

notes and real-time monitoring. Digital tracking can respond to delays that arise when investigation files move slowly through physical channels or when supervisory directions are not recorded in a consistent manner. Time-bound tasks, status dashboards and a clear history of changes may help senior officers identify neglected steps and allocate support where an investigation has stalled. The legal value of such a platform depends on the integrity of its records. Evidence metadata, timestamps and chain-of-custody information must be protected against unauthorised alteration. The system should distinguish between a contemporaneous entry and a later correction, preserve both versions and identify the person making each change. Access should follow the principle of least privilege: an officer should see only what is necessary for the assigned role. Where the application links with AI-generated suggestions from FAI or ranks cases for supervisory attention, the criteria should be documented and reviewable.

6. Trinetra 2.0, Crime GPT and YAKSH

Trinetra 2.0 represents the identification and intelligence layer of Uttar Pradesh's digital policing. The practitioner paper describes a large digitised repository containing criminal histories, FIR details, photographs, interrogation material, reward information, incarceration details and seizure records. It further describes facial-recognition search and a Crime GPT feature that allows officers to retrieve information through natural-language queries. Official Uttar Pradesh Police material has separately recognised Trinetra 2.0 and the Crime Analytics and Predictive Policing Portal as major policing initiatives. These tools can shorten the time required to compare a photograph, locate a previous record or connect information held across cases.

The YAKSH application, introduced through official directions in 2026, adds AI-powered facial recognition and voice search and supports verification or monitoring of specified categories of offenders. Circulars concerning beat verification, data entry, supervisory features, correction where naming was found wrong or an accused was acquitted, and SOS or broadcast functions show an attempt to create operational rules around the platform. The correction-related circular is especially significant because criminal databases often preserve suspicion longer than the legal process permits. A person who has been acquitted, discharged or wrongly named should not continue to appear to every user as an undifferentiated 'criminal' merely because an old record remains searchable. Facial recognition is a high-risk use because a similarity score is not an identification in the legal sense. Research has shown that some facial-analysis systems produce uneven error rates across groups (Buolamwini & Gebru, 2018; Grother et al., 2019). A possible match should therefore be treated only as an investigative lead requiring independent verification. Officers should be shown several candidate matches, similarity levels and warnings, and every search should create an audit trail.

7. Traffic Management and Urban Governance

AI-supported traffic management sits at the intersection of policing, urban administration and sustainable development. Adaptive signals can use live traffic data to alter signal phases, identify congestion, detect pedestrians, recognise a stalled vehicle or create priority for ambulances, fire services and police response vehicles. Predictive tools may also anticipate unusual traffic during a procession, examination, public event or emergency. In a densely populated urban setting, even modest improvements can reduce delay, fuel consumption and the risk created by unmanaged intersections.

A sustainable approach would assess the system against safety, accessibility and environmental outcomes rather than only average vehicle speed. This is an area where well-governed AI can produce visible public benefit and build confidence in responsible innovation.

Table 1: Selected AI-enabled policing applications and governance concerns in Uttar Pradesh

Application	Primary function	Potential public value	Main governance concern
Crime analytics and predictive policing	Maps patterns and supports deployment or patrolling	Better allocation of limited personnel and faster preventive response	Feedback loops, discriminatory concentration of surveillance, uncertain accuracy
FAI and legal-section suggestion	Analyses complaint text and suggests relevant penal provisions	Faster registration support and greater consistency	Automation bias, incomplete facts, incorrect legal classification
AI-enabled document management	Summarises, categorises and retrieves circulars and regulations	Institutional memory, accessibility and compliance	Hallucinated summaries, confidentiality and over-reliance
EBITA and digital case tracking	Tracks evidence, tasks, supervision and case progress	Time-bound investigation and audit trails	Data integrity, chain of custody, access control and function creep
Trinetra 2.0, Crime GPT and YAKSH	Searches criminal records using photographs, text or voice; supports identification and monitoring	Faster suspect and missing-person searches	False matches, outdated records, stigma, opaque ranking and mass surveillance
Adaptive traffic and emergency systems	Optimises signals, detects incidents and prioritises emergency vehicles	Safer roads, reduced delay and improved response time	Continuous camera data, vendor security and unequal deployment

Source: *This compilation is based on official Uttar Pradesh Police material and Kumar and Chaudhary (n.d.).*

Constitutional and Statutory Framework

1. Articles 14, 19 and 21: Legality, Fairness and Proportionality

Article 14 is central because an algorithmic classification may distribute police attention or risk unequally. A model based on irrelevant proxies, unrepresentative data or unreviewable assumptions may produce arbitrary outcomes even where no officer intends to discriminate. Equality review must therefore examine both the stated rule and the operational effect of the system. Consistent computer output is not necessarily equal treatment if the underlying categories are defective.

Article 21 protects life and personal liberty and requires procedure that is just, fair and reasonable, as developed in Maneka Gandhi v. Union of India. In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court recognised privacy as a fundamental right and emphasised legality, legitimate State purpose, proportionality and procedural safeguards. AI policing engages privacy not only when data are collected secretly, but also when separate records are combined to infer identity, association, movement or risk. A photograph that appears ordinary in one file can become highly revealing when matched across a large database. The constitutional inquiry must accordingly address the full data lifecycle collection, linking, analysis, sharing, retention and deletion. Article 19 is relevant where surveillance or predictive monitoring chills lawful expression, association or assembly. Systems used around public gatherings should have a specific operational purpose, limited retention and heightened authorisation rather than becoming a routine record of political participation.

Due process also requires contestability. When an AI output materially contributes to an adverse action, the affected person should have a meaningful opportunity to challenge the factual basis through ordinary legal proceedings. This does not necessarily require disclosure of source code in every case. It does require preservation of the relevant input, model or version used, search parameters, output, officer action and audit log so that a court or oversight body can reconstruct what occurred.

2. Biometric and Behavioural Data under the Criminal Procedure (Identification) Act, 2022

The Criminal Procedure (Identification) Act, 2022 expands the State's authority to take 'measurements' for identification and investigation. The expression covers fingerprints, palm-print and footprint impressions, photographs, iris and retina scans, physical and biological samples and their analysis, as well as specified behavioural attributes. The Act authorises collection from broad categories of persons and gives the National Crime Records Bureau a central role in collecting, storing, processing, sharing and destroying records. The prescribed retention period of seventy-five years creates a long-term biometric infrastructure capable of supporting future analytics and cross-database matching. The Act is highly relevant to AI policing even though it does not specifically regulate artificial intelligence. AI systems become more powerful as the volume and variety of identification data increase. Facial recognition may use photographs, while other tools may combine biometric records with FIR histories, geographic information or behavioural data. The legal authority to collect a measurement does not automatically answer whether it may be used to train a model, linked with unrelated databases or repeatedly searched for new purposes. These secondary uses require a separate assessment of purpose, necessity and proportionality. The statutory framework contains provisions for destruction in specified cases, including where a person without a previous conviction is released without trial, discharged or acquitted, subject to applicable conditions and judicial direction. The governance protocol must identify which data are legally retained, which are operationally necessary, and which should be removed because continued availability creates unjustified stigma.

The constitutional debate over physical and testimonial evidence also acquires a new dimension. Selvi v. State of Karnataka protected mental privacy against involuntary techniques such as narcoanalysis and brain-mapping, while later decisions have distinguished physical characteristics such as voice samples from compelled testimonial communication. In an AI environment, apparently non-testimonial data can be aggregated to generate detailed inferences about behaviour or association.

3. The Digital Personal Data Protection Act, 2023 and Rules

The Digital Personal Data Protection Act, 2023 introduces a general framework for processing digital personal data, but its relationship with policing is limited by both exemptions and phased commencement. Section 17(1)(c) exempts processing undertaken in the interest of preventing, detecting, investigating or prosecuting an offence from several obligations and rights under the Act. Section 17(2) also permits notification-based exemptions for specified State instrumentalities in interests that include State security and public order. These clauses recognise legitimate law-enforcement needs, but they also reduce the extent to which the general data-protection statute can function as a complete rights framework for police AI. At the time of writing in July 2026, the Act and the Digital Personal Data Protection Rules, 2025 are being brought into force in phases. The November 2025 commencement notification provides an eighteen-month period before many substantive provisions, including sections 3 to 17, take effect. It would therefore be inaccurate to assume that the complete consent, notice, rights and exemption architecture is already operational. Even after commencement, offence-related processing will remain partly exempt. Constitutional standards, criminal-procedure safeguards, departmental rules and judicial review will continue to perform a major role.

Law-enforcement exemption should not be read as permission for unstructured data use. The wording is tied to the interest of prevention, detection, investigation or prosecution. Processing that is merely convenient, speculative or unrelated to a defined policing purpose should not automatically claim the benefit. Basic duties such as security safeguards, accuracy, access control, retention discipline and breach response are also necessary for

operational reliability, not only privacy. A database corrupted by weak security or outdated records harms investigation as well as individuals.

4. Criminal Procedure, Electronic Evidence and Administrative Accountability

The Bharatiya Nagarik Suraksha Sanhita, 2023 encourages the use of electronic communication and digital processes at several stages of criminal procedure, while the Bharatiya Sakshya Adhiniyam, 2023 recognises electronic and digital records within the law of evidence. These developments make reliable digital systems increasingly important. They do not, however, convert an AI-generated prediction or facial match into proof. Admissibility, relevance, authenticity and evidentiary weight remain separate questions. An investigative lead must be supported by legally obtained evidence capable of being tested in court.

The principles in D.K. Basu v. State of West Bengal and People's Union for Civil Liberties v. Union of India remain instructive because they demonstrate the constitutional value of documented procedure and external oversight in coercive State action. Technology should strengthen these protections by creating accurate time-stamped records, not create invisible routes around them. When AI contributes to an arrest, search or surveillance decision, the officer's legal grounds must be independently recorded. A generic statement that 'the system identified the person' cannot replace statutory satisfaction.

Major Governance Risks

1. Historical Data, Bias and Self-Reinforcing Predictions

Police data are shaped by social behaviour, reporting patterns, legal priorities and past enforcement. They may contain spelling errors, duplicate identities, outdated addresses, unresolved allegations or categories created for an earlier administrative purpose. A model trained on such data can make historical inequality appear scientifically inevitable. Predictive policing scholarship repeatedly warns that arrest and incident records may reflect where police looked as much as where harm occurred (Brayne, 2017; Lum & Isaac, 2016; Meijer & Wessels, 2019). This is particularly important in a socially diverse State where caste, class, migration and locality may correlate with seemingly neutral variables.

2. Opacity, Automation Bias and the Problem of Reasons

Complex machine-learning models may generate an output without an explanation that is meaningful to an officer, court or affected person. NITI Aayog has identified the 'black box' problem as a central concern in high-stakes decision-making. Opacity is not only technical. A rule-based system may also be opaque where the department does not disclose criteria, the vendor claims trade secrecy or users do not understand how information is ranked. The appropriate level of explanation depends on the use, but a high-impact output must at least identify the relevant factors, limitations and confidence.

3. Privacy, Function Creep and Persistent Digital Suspicion

Function creep occurs when information collected for one purpose is gradually used for another. A photograph collected during investigation may later enter a facial-recognition gallery; a traffic camera may become a general surveillance device; or a welfare alert may be retained as intelligence. Each additional use appears modest in isolation, but the combined system can create continuous visibility of individuals who have never been convicted. Long retention periods intensify this risk because old and context-poor data remain available to new tools.

4. False Matches, Cybersecurity and Data Integrity

A false facial match or erroneous identity link can redirect an investigation and expose an innocent person to stigma or coercive questioning. The harm is greater where officers are not told the error rate or where the same incorrect data appear across multiple connected systems. Confidence thresholds should be calibrated to the operational context, and low-quality images should not be searched merely because the software permits

it. Independent corroboration must precede coercive action.

5. Accountability, Vendors and the Right to a Remedy

Public-private collaboration can bring technical expertise, but it can also place key decisions inside confidential contracts. A police department must retain control over data, system configuration and audit access. Proprietary claims should not prevent testing for bias, security or accuracy. Contracts should identify which party is responsible for defective performance, unauthorised access, delayed correction and preservation of records required in litigation. The department should have a workable exit plan so that public functions do not become dependent on a single vendor.

AI, Public Value and Sustainable Development

The conference theme rightly connects AI governance with sustainable development. Sustainable policing is not simply policing that uses advanced equipment. It is policing that can maintain safety, legality and public confidence over time. An efficient system that produces repeated rights violations is institutionally unsustainable because it generates litigation, distrust, resistance and poor-quality evidence. Conversely, a rights-conscious system may improve cooperation and reporting, which are essential to effective criminal justice.

AI-enabled policing is most directly connected with Sustainable Development Goal 16, which calls for peaceful and inclusive societies, access to justice and effective, accountable institutions. Crime-pattern analysis, case tracking and searchable legal instructions may improve institutional effectiveness. Transparent rules, correction mechanisms and independent audits strengthen accountability. The connection is therefore two-sided: AI can contribute to Goal 16 only where the institution itself remains answerable for the way AI is used.

Traffic management and emergency response also relate to safer and more inclusive cities under Goal 11. Adaptive signals can reduce congestion and improve ambulance or police response, while incident detection may support road safety. Yet benefits must reach peripheral and lower-income areas rather than only high-visibility urban corridors. Digital infrastructure should be evaluated for accessibility, local language support and the needs of persons with disabilities. Inclusive design is not an optional social addition; it affects accuracy and public usability.

A Rights-Respecting Governance Framework for Uttar Pradesh

The following model is designed for adoption through a consolidated police AI and data-governance policy, supplemented by system-specific standing orders.

1. System Inventory and Risk Classification

The first step is a complete inventory of digital and AI-enabled systems used by the department, including district-level pilots and vendor-operated platforms. Each entry should record purpose, owner, data sources, user categories, technical method, deployment status, affected population, retention period, vendor role and audit history. Systems can then be classified as low, medium or high risk. Administrative search and document summarisation may be low or medium risk; facial recognition, predictive targeting and biometric linkage should be high risk because they can affect liberty, equality and privacy.

2. Prior Algorithmic and Human-Rights Impact Assessment

A high-risk system should not move from pilot to operational use without a written impact assessment. The assessment should identify the legal basis, necessity, less intrusive alternatives, expected benefit, data quality, error consequences, affected groups, security controls, human-review arrangement and redress process. It should include field testing in representative conditions rather than rely solely on vendor laboratory results. A summary can be made public, with redaction of details whose disclosure would genuinely compromise security or investigation.

3. Purpose Limitation, Data Quality and Retention

Every dataset and model should have a defined purpose. Data collected for emergency welfare contact, traffic optimisation or internal administration should not be transferred to criminal intelligence without fresh legal justification. Data-quality procedures must include duplicate detection, source verification, regular updating, acquittal and discharge status, correction requests and deletion workflows. Retention should be tied to law and operational need. Where the Criminal Procedure (Identification) Act requires or permits long retention, access and secondary use should still remain controlled.

4. Meaningful Human Oversight and Recorded Reasons

No person should be arrested, searched, detained or subjected to coercive action solely because an AI system produced a match, prediction or recommendation. The officer must independently establish the legal grounds and record the role played by the system. For high-impact uses, the record should include query parameters, model or database version, output, confidence indicator, corroborating material and final decision. Officers should be protected, not penalised, for reasoned disagreement with an automated suggestion.

5. Independent Testing, Audit and Performance Review

Accuracy claimed by a vendor should be verified under local conditions. Testing should include false-positive and false-negative rates, performance across image quality and relevant demographic conditions, robustness to language variation, cybersecurity and misuse scenarios. Independent academic or technical institutions can conduct periodic audits under confidentiality safeguards. Audit findings should lead to correction, retraining, restricted use or suspension. A system that repeatedly fails should not continue merely because significant funds have been invested.

6. Transparent Procurement and Vendor Accountability

Procurement documents should define the public purpose and performance standard before a product is selected. Contracts must preserve government ownership or control over police data, prohibit unauthorised reuse, require breach notification, permit independent audit, specify model-update procedures and ensure data portability on termination. Intellectual-property protection can coexist with public accountability, but no vendor should be able to block a court or authorised auditor from examining material necessary to assess a consequential decision.

7. Access Control, Security and Audit Trails

Role-based permissions should be granular. A beat officer, investigator, supervisor, technical administrator and external vendor do not require identical access. Sensitive searches should be logged with user identity, time, purpose and result, and unusual patterns should trigger review. Facial-recognition and criminal-history searches should require a case or incident reference except in a documented emergency. Logs must themselves be protected against alteration and retained long enough for disciplinary, judicial or audit review.

8. Transparency, Community Engagement and Grievance Redressal

The department should publish a plain-language register describing high-risk systems, their purpose, broad data categories, safeguards and contact point for correction or complaint. Operationally sensitive details may be withheld, but the existence and legal basis of the system should not remain secret. Consultation with civil-society organisations, lawyers, technologists and representatives of affected communities can identify risks that a purely internal process may miss. A time-bound grievance mechanism should permit correction of identity, status and other factual errors.

9. Training and Professional Responsibility

Technology literacy must become part of police training. Officers need to understand what a confidence score means, how bias can arise, why correlation is not proof and when a system should not be used. Training should combine technical instruction with constitutional rights, evidence law and practical case studies.

10. Sunset Clauses and Measurable Public Value

Every pilot and high-risk deployment should have a review date. Continuation should depend on evidence that the system achieves its stated purpose, remains lawful and does not create disproportionate harm. Metrics should include error, correction, security incidents, rights complaints and distribution of benefits, not only the number of matches or arrests.

Table 2: Proposed lifecycle safeguards for AI-enabled policing

Lifecycle stage	Minimum governance safeguards
Planning	Clear legal purpose; alternatives analysis; risk classification; stakeholder identification
Data preparation	Source verification; minimisation; representative testing; correction and deletion rules
Procurement/ development	Audit rights; security standards; data ownership; explainability and exit clauses
Pilot testing	Local validation; false-match analysis; rights impact assessment; officer training
Operational use	Role-based access; documented human review; case-linked searches; protected audit logs
Monitoring	Independent audit; disparity testing; cyber review; complaint and correction statistics
Renewal or retirement	Public-value evaluation; sunset review; secure deletion or migration; vendor handover

CONCLUSION

Artificial intelligence can help the Uttar Pradesh Police manage information, identify patterns, supervise investigation and respond more quickly to public needs. These benefits do not remove the need for constitutional discipline. AI systems are built from past data, designed through human choices and used within institutions that may already contain inequality or error. When a prediction or match influences coercive power, the consequences are too serious for uncritical reliance. Legal authority, necessity, proportionality, data quality, meaningful human oversight, independent audit and effective correction must be treated as operational requirements rather than abstract ethical aspirations. High-risk systems should be subject to prior impact assessment, local validation, documented reasons, strict access, vendor accountability, public rules, independent review and sunset clauses. AI-enabled policing will be judged not by the sophistication of its software but by the quality of justice it produces. A future-ready police service must be capable of using data intelligently while recognising that every data point may represent a person whose dignity and liberty remain constitutionally protected. When innovation is guided by that understanding, digital governance can make policing both more efficient and more legitimate. Without it, technology may merely automate old weaknesses at a larger scale.

AI Assistance Disclosure

OpenAI ChatGPT was used for language refinement, structural organisation and drafting assistance. The author remains responsible for verifying sources, legal propositions, factual descriptions and the final analysis and conclusions.

REFERENCES

1. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).
2. Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, India Code (2023).
3. Bharatiya Sakshya Adhiniyam, No. 47 of 2023, India Code (2023).
4. Brayne, S. (2017). Big data surveillance: The case of policing. American Sociological Review, 82(5), 977–1008. https://doi.org/10.1177/0003122417725865
5. Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, 81, 1–15.
6. Council of Europe. (2024). Framework convention on artificial intelligence and human rights, democracy and the rule of law. https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

7. Criminal Procedure (Identification) Act, No. 11 of 2022, India Code (2022). https://www.indiacode.nic.in/handle/123456789/19029
8. Criminal Procedure (Identification) Rules, 2022, Gazette of India (2022).
9. D.K. Basu v. State of West Bengal, (1997) 1 SCC 416 (India).
10. Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India (2023). https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
11. Digital Personal Data Protection Rules, 2025, Gazette of India, G.S.R. 846(E) (2025). https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf
12. European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. Official Journal of the European Union.
13. Grother, P., Ngan, M., & Hanaoka, K. (2019). Face recognition vendor test (FRVT), Part 3: Demographic effects (NISTIR 8280). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8280
14. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
15. Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. University of Pennsylvania Law Review, 165(3), 633–705.
16. Kumar, S., & Chaudhary, U. (n.d.). Artificial intelligence (AI) in policing [Unpublished practitioner paper].
17. Lum, K., & Isaac, W. (2016). To predict and serve? Significance, 13(5), 14–19. https://doi.org/10.1111/j.1740-9713.2016.00960.x
18. Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (India).
19. Margetts, H. (2022). Rethinking AI for good governance. Daedalus, 151(2), 360–371. https://doi.org/10.1162/daed_a_01922
20. Meijer, A., & Wessels, M. (2019). Predictive policing: Review of benefits and drawbacks. International Journal of Public Administration, 42(12), 1031–1039. https://doi.org/10.1080/01900692.2019.1575664
21. Ministry of Electronics and Information Technology. (2025). Notification bringing provisions of the Digital Personal Data Protection Act, 2023 into force in phases, G.S.R. 843(E). Gazette of India. https://www.meity.gov.in/static/uploads/2025/11/c56ceae6c383460ca69577428d36828b.pdf
22. NITI Aayog. (2021a). Responsible AI #AIForAll: Approach document for India Part 1: Principles for responsible AI. Government of India. https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf
23. NITI Aayog. (2021b). Responsible AI #AIForAll: Approach document for India Part 2: Operationalizing principles for responsible AI. Government of India. https://www.niti.gov.in/sites/default/files/2021-08/Part2-Responsible-AI-12082021.pdf
24. People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (India).
25. Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 33–44. https://doi.org/10.1145/3351095.3372873
26. Richardson, R., Schultz, J. M., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. New York University Law Review Online, 94, 15–55.
27. Ritesh Sinha v. State of Uttar Pradesh, (2019) 8 SCC 1 (India).
28. Selvi v. State of Karnataka, (2010) 7 SCC 263 (India).
29. UNESCO. (2021). Recommendation on the ethics of artificial intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000381137
30. United Nations. (2015). Transforming our world: The 2030 agenda for sustainable development (A/RES/70/1).
31. United Nations Interregional Crime and Justice Research Institute & INTERPOL. (2019). Artificial intelligence and robotics for law enforcement.
32. Uttar Pradesh Police. (2023). DGP Circular No. 39: Trend analysis and predictive policing using CCTNS crime data [Circular]. https://uppolice.gov.in/article/en/dgp-up-circulars
33. Uttar Pradesh Police. (2024). DGP Circular No. 29: Updating data relating to offenders involved in unresolved crimes in the Trinetra application [Circular]. https://uppolice.gov.in/article/en/dgp-up-circulars
34. Uttar Pradesh Police. (2025). Major policing initiatives and FICCI Smart Policing Awards

[Press release]. https://www.uppolice.gov.in/site/writereaddata/UploadedPressRelease/pdf/PRP_20250310192851532 1.pdf

35. Uttar Pradesh Police. (2026a). YAKSH application: AI-powered facial recognition and voice search [Press release]. https://uppolice.gov.in/site/writereaddata/UploadedPressRelease/pdf/PRP_20260105205126760 6.pdf

36. Uttar Pradesh Police. (2026b). DGP circulars concerning YAKSH verification, data entry, supervision, correction and SOS/broadcast features [Circulars]. https://uppolice.gov.in/article/en/dgp-up-circulars

37. Yeung, K. (2018). Algorithmic regulation: A critical interrogation. Regulation & Governance, 12(4), 505–523. https://doi.org/10.1111/rego.12158