Educational Administration: Theory and Practice
2024, 30(11), 3055-3061
ISSN: 2148-2403
https://kuey.net/

Research Article

Digital Policing And Due Process: Legal Challenges Of Surveillance Technologies In India's Police Mechanism

Dr. Manju Rani*

*Assistant Professor Guest Faculty ncweb. Delhi University, drmanjumeerut@gmail.com

Citation: Dr. Manju Rani (2024). Digital Policing And Due Process: Legal Challenges Of Surveillance Technologies In India's Police Mechanism, *Educational Administration: Theory and Practice*, 30(11) 3055-3061
Doi: 10.53555/kuey.v30i11.11267

ARTICLE INFO

ABSTRACT

India's police institutions are undergoing an accelerated digital transformation marked by interoperable crime databases, biometric and facial recognition deployments, platform-mediated intelligence access, and digitally captured evidentiary workflows. These shifts are frequently defended as modernization measures intended to improve investigation quality, coordination, and conviction outcomes. Yet the legal architecture governing surveillance and data-driven policing remains fragmented across constitutional doctrine, sectoral statutes, executive rules, and platform design choices, producing a structural gap between technologically intensified policing and the procedural guarantees associated with due process. This paper offers a doctrinal and normative analysis of the legality, necessity, proportionality, and procedural fairness of contemporary surveillance technologies within Indian policing. It argues that due process concerns are not confined to isolated abuses or "privacy" narrowly conceived; rather, they arise systemically from the end-to-end pipeline of surveillance-based policing: collection, aggregation, algorithmic inference, evidentiary production, and adjudicative reliance. Drawing on constitutional privacy and fairness jurisprudence, interception safeguards, emergent digital evidence infrastructures, and comparative benchmarks for lawful surveillance, the paper develops a due process framework tailored to digital policing. It concludes that India requires a surveillance governance redesign that internalizes legality and proportionality as operational constraints, mandates independent authorization for high-intrusion measures, guarantees contestability of algorithmic outputs, and supplies meaningful remedies including evidentiary consequences where surveillance violates constitutional or statutory conditions.

Keywords: *Digital policing; surveillance; due process; privacy; proportionality; interception; facial recognition; CCTNS; ICJS; NATGRID; electronic evidence; India*

Introduction

Digital policing in India is no longer a marginal modernization project; it is increasingly the institutional substrate through which "ordinary" policing is organized, recorded, and rendered legible to state actors and courts. Systems such as the Crime and Criminal Tracking Network and Systems (CCTNS) are framed as national-scale infrastructures, reportedly implemented across all States and Union Territories and covering over 21,000 police stations, with a large public outlay and extensive personnel integration. Simultaneously, the Inter-Operable Criminal Justice System (ICJS) seeks to integrate police, courts, prisons, forensics, and prosecution through "one data once entry" logic and secure platform interoperability, thereby reshaping the institutional conditions under which investigations move toward adjudication. These governance moves are not merely administrative. They embed new forms of surveillance capacity: searchable repositories, cross-database identity resolution, and the routinization of audio-visual capture as evidence through initiatives such as e-Sakshya, which is publicly described as storing videography, photography, and testimonies on an e-evidence server for prompt availability to courts.

The core legal problem is that surveillance technologies do not simply "collect" information; they restructure the conditions of suspicion, the distribution of investigative attention, and the evidentiary narratives that courts will be asked to accept. As such, the legal challenges are fundamentally due process challenges. In

constitutional terms, due process in India is mediated through Article 21's guarantee of "procedure established by law," interpreted to require justness, fairness, and reasonableness rather than formal legality alone (Maneka Gandhi v. Union of India, 1978). Within this doctrinal landscape, privacy is now a fundamental right and, crucially for digital policing, informational privacy and state data practices are placed under a legality-necessity-proportionality framework (Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017). These constitutional constraints, however, are often operationalized through executive authorizations, classified practices, and sectoral rules that may not provide robust adversarial contestability or meaningful ex post remedy.

This paper advances three claims. First, India's digital policing ecosystem has created a surveillance-evidence continuum in which investigative databases, interception powers, biometric/face recognition systems, and digital evidence platforms mutually reinforce one another, amplifying intrusiveness and error consequences. Second, existing legal controls especially executive authorization and review-committee oversight are structurally insufficient for due process in high-volume digital policing, because they do not consistently ensure individualized necessity, minimize function creep, or guarantee contestability of algorithmic outputs. Third, doctrinal developments after the recognition of privacy as a fundamental right require not only better privacy compliance but a due process redesign: independent authorization for high-intrusion surveillance, transparency-compatible oversight, and remedial doctrines that impose consequences when surveillance breaches legal thresholds.

Methodology and Scope

The paper employs doctrinal legal research and normative institutional analysis. Doctrinally, it synthesizes constitutional jurisprudence on privacy, procedural fairness, and surveillance; statutory and delegated frameworks governing interception and data processing; and evidentiary doctrine relating to electronic records and admissibility. Normatively, it evaluates whether the institutional design of digital policing systems can satisfy due process requirements, understood as a composite of ex ante authorization, legality and foreseeability, procedural safeguards against abuse, and effective remedy for rights violations.

The focus is India's police mechanism broadly conceived, including police-facing databases, intelligence access infrastructure, lawful interception regimes, biometric data collection statutes, and digital evidence tools that interface with courts. While policing is constitutionally distributed in a federal structure, national platforms and central authorizations increasingly shape state-level practice, making the due process question unavoidably multi-level.

The Architecture of Digital Policing in India: From Databases to "One Data Once Entry"

Digital policing in India is increasingly anchored in integrative platforms that render persons, incidents, and networks searchable and interoperable. CCTNS is publicly described as a nationwide project with large-scale coverage of police stations and personnel, with a project design oriented toward standardization of police data entry and access. ICJS extends this logic beyond police: the describes ICJS as integrating the five pillars of criminal justice police (via CCTNS), courts (e-Courts), prisons (e-Prisons), forensic labs (e-Forensic), and prosecution (e-Prosecution) with "one data once entry" as an institutional objective. A government communication hosted on the Ministry's platform describes the implementation of ICJS as a major central sector scheme with NCRB and NIC playing implementation roles and a multi-year budgeted program horizon.

These systems are not neutral record-keeping devices. They create new capacities for surveillance by enabling identity resolution across multiple data sources, supporting predictive or network analytics, and shifting frontline police incentives toward data capture and platform compatibility. Moreover, interoperable platforms change the evidentiary ecology: platform outputs can become "official" records, while the platform's design choices fields, categories, and linkages shape what becomes legible as suspicion or association.

The architecture also includes "real-time intelligence" aspirations. NATGRID has been analyzed in scholarship as an attached office intended to facilitate systematic government access to data sources, including private-sector data, for security objectives (Abraham, 2012). Government procurement documents associated with NATGRID signal the development and implementation of integrated technical systems via system integrators and security-cleared procurement workflows, illustrating an infrastructure-centric approach to intelligence access and data integration. Even without full public visibility into operational specifics, the existence and procurement logic of such platforms matters for due process because they increase the state's capacity to aggregate and infer sensitive information with limited individualized judicial supervision.

Constitutional Foundations: Due Process, Privacy, and the Proportionality Constraint

Due process as fairness under Article 21

The Indian constitutional order does not textualize "due process of law" in the American sense; yet Article 21 has been interpreted to require procedure that is just, fair, and reasonable rather than formal legality alone (Maneka Gandhi v. Union of India, 1978). This interpretive tradition supplies a doctrinal basis to evaluate

surveillance not merely as an executive power question but as a procedural justice question. When surveillance enables coercive state action arrest, search, prosecution, or reputational harms procedural fairness demands safeguards proportionate to the intrusion and risk of error.

Privacy as a fundamental right and the three-part test

The recognition of privacy as a fundamental right constitutionalizes constraints on state data practices. The Puttaswamy judgment affirms informational privacy as a facet of privacy and articulates a structured inquiry requiring legality, legitimate aim/need, and proportionality, emphasizing dangers to privacy in the information age and the state's obligations (Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017). For digital policing, the significance of Puttaswamy is twofold. First, it provides a doctrinal vocabulary to evaluate surveillance technologies beyond ad hoc reasonableness. Second, it implies that "law" cannot be reduced to opaque executive practice; legality requires accessible norms capable of constraining discretion.

Surveillance jurisprudence before and after Puttaswamy

Indian courts confronted surveillance in earlier constitutional contexts as well. In Kharak Singh, the Court struck down domiciliary visits under police regulations, reflecting early constitutional unease with intrusive surveillance practices even as other forms of surveillance were not fully invalidated (Kharak Singh v. State of Uttar Pradesh, 1963). PUCL's telephone tapping decision treated interception as implicating speech and privacy and imposed safeguards, illustrating judicial recognition that surveillance requires procedural constraint even when authorized by statute (People's Union for Civil Liberties v. Union of India, 1997). More recently, the Pegasus litigation demonstrates institutional difficulty in testing surveillance claims when governments invoke secrecy; the Supreme Court's order in Manohar Lal Sharma v. Union of India (2021) reflects judicial concern with credible allegations of unlawful surveillance and the limitations of executive assertions as a substitute for independent scrutiny.

The doctrinal trajectory indicates a constitutional demand for structured justification and safeguards. Yet the legal infrastructure of surveillance technologies often remains executive-centric, producing a mismatch between constitutional ideals and day-to-day digital policing practice.

Statutory and Regulatory Frameworks Governing Surveillance Technologies

Lawful interception regimes: telecommunications and computer resources

Surveillance powers in India operate through multiple legal pathways. For interception related to "computer resources," Section 69 of the Information Technology Act, 2000 authorizes directions for interception, monitoring, or decryption, subject to reasons recorded and procedural safeguards as prescribed. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 specify procedural conditions for such interception, reflecting a delegated-rule model rather than a warrant-based judicial authorization model.

For telecommunications interception, the legal landscape has been updated by the Telecommunications Act, 2023, a consolidating statute in the telecommunications domain. The Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 provide operational definitions and procedural structures, including a "competent authority" model located in the Union Home Secretary (for the central government) and state Home Department secretaries (for state governments), and a review committee mechanism. The rules also indicate a supersession logic vis-à-vis prior interception rules while preserving existing interception orders until expiry, revealing continuity of executive-authorized interception even as the statutory frame changes.

From a due process standpoint, the persistent reliance on executive authorization and internal review committees raises questions of independence, individualized necessity, and adversarial contestability. It also produces a legal fragmentation problem: the same investigative objective may be pursued through telecommunications interception, IT Act interception/decryption, or database integration, each with its own procedures and oversight design, thereby enabling forum-shopping within the surveillance state.

Biometric capture and long-term retention: the Criminal Procedure (Identification) Act, 2022

The Criminal Procedure (Identification) Act, 2022 expands the legal basis for collecting "measurements," defined to include fingerprints, palm prints, footprint impressions, photographs, iris and retina scans, physical and biological samples and their analysis, and behavioral attributes such as signatures and handwriting. It also empowers the National Crime Records Bureau to collect, store, process, and disseminate measurement records and specifies retention "for a period of seventy-five years" subject to destruction requirements in certain cases of release, discharge, or acquittal after exhausting remedies.

This statute matters for digital policing because biometric databases are increasingly integrated with platform ecosystems and can be paired with facial recognition or identity verification systems. The due process risk is not limited to collection; it extends to long-term retention, secondary use, dissemination to law enforcement agencies, and the lowered practical threshold for turning an arrested person into a long-term data subject.

Data protection law and law-enforcement exemptions: the DPDP Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) creates a general framework for processing digital personal data, defining "processing" broadly to include collection, storage, retrieval, sharing, disclosure by transmission, dissemination, and destruction. It frames lawful processing around consent or "certain legitimate uses," and establishes institutional mechanisms such as the Data Protection Board of India. At the level of principle, this is an important step toward regulating data-intensive governance. Yet the due process question is whether a general data protection statute, especially one that contemplates significant state processing, can meaningfully constrain law-enforcement surveillance systems that are designed for investigatory and security purposes rather than consumer-facing data fiduciary contexts (Digital Personal Data Protection Act, 2023).

Policy analysis of the DPDP framework has emphasized its applicability logic and the operationalization of rights and obligations, indicating that its effectiveness will depend on enforcement design and the handling of state exceptions (PRS Legislative Research, 2023). For policing, the core doctrinal challenge is that data protection law may regulate some data handling practices but may not supply the procedural safeguards traditionally demanded for intrusive surveillance, such as independent authorization, necessity in an individualized sense, and effective ex post remedy for unlawful surveillance.

Facial Recognition and Platform Surveillance: From Targeted Verification to Mass Identification Risk

Facial recognition technologies (FRT) illustrate how digital policing can shift from targeted investigation to population-scale identification. Commentary on India's FRT landscape has noted that a call for tenders for a centralized Automated Facial Recognition System (AFRS) by NCRB in 2019 signaled movement toward mass identification logics, not merely verification in limited contexts. Civil society research has documented the existence and content of AFRS procurement documents and situated them within broader governance concerns about legal basis, safeguards, and integration with other databases (Hickok, 2021).

The due process issues raised by FRT are distinct yet interlinked with interception and database integration. First, FRT introduces probabilistic identification into policing, where error rates and data quality are not evenly distributed across populations or contexts; this produces distributive consequences and potential discriminatory impacts even before formal legal coercion occurs. Second, FRT can function as a suspicion generator rather than a suspicion confirmer, reversing the traditional logic in which individualized suspicion precedes identification techniques. Third, because FRT can be integrated with CCTV and large image repositories, it risks "continuous line-up" conditions in public spaces, intensifying chilling effects on speech and association (People's Union for Civil Liberties v. Union of India, 1997). Fourth, the evidentiary status of FRT outputs is contestable: if such outputs are used to justify arrest or charge, defendants must be able to test the system's accuracy, training data constraints, audit trails, and chain of custody.

In Indian constitutional terms, these concerns must be tested against the Puttaswamy proportionality framework and Article 21 fairness. Yet the institutional tendency to treat FRT as a "technology tool" rather than a rights-restricting measure can result in under-regulated deployment particularly when procurement and pilot deployments precede legislative deliberation.

Digital Evidence Pipelines: e-Sakshya, Electronic Records, and the Proceduralization of Proof

Digital policing increasingly depends on the transformation of real-world events into digital artifacts that can travel through police systems to courts. The launch of e-Sakshya is presented publicly as an initiative where videography, photography, and testimonies are stored on an e-evidence server and made available to courts, signifying a formalization of digital capture as a default evidentiary practice. The ICJS ecosystem is explicitly described as integrating the main pillars of criminal justice to make justice delivery more effective, implying that evidentiary objects will increasingly be born-digital within an interoperable infrastructure (, Government of India, 2024).

The Section 65B line of doctrine and its due process significance

Indian evidentiary doctrine on electronic records has evolved around authenticity and certification. The Supreme Court's decisions in Anvar P.V. v. P.K. Basheer (2014) and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) affirm the centrality of certification and compliance for admissibility of electronic records (Anvar P.V. v. P.K. Basheer, 2014; Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, 2020). These cases matter for digital policing because surveillance outputs are often electronic by design. Authenticity requirements can, in principle, serve due process by forcing traceability and reducing post hoc manipulation. However, authenticity rules alone do not resolve the foundational legality question: an electronic record can be authentic yet unlawfully obtained.

Illegally obtained evidence and the remedial gap

A long-standing fault line in Indian due process concerns the admissibility of unlawfully obtained evidence. In Pooran Mal, the Supreme Court rejected an exclusionary rule as a general constitutional principle, allowing reliance on evidence even if obtained through illegal search, subject to other constraints (Pooran Mal v. Director of Inspection, 1974). Similarly, R.M. Malkani upheld admissibility of a tape-recorded

conversation as relevant evidence under evidentiary provisions, reinforcing a relevance-and-authenticity emphasis rather than exclusion based on illegality (R.M. Malkani v. State of Maharashtra, 1973).

This doctrinal posture creates a distinctive vulnerability for digital surveillance. If unlawful interception, unlawful database access, or unlawfully deployed FRT can still produce admissible evidence, the incentive structure becomes skewed: rights violations may not threaten the prosecution's case, and remedies may be limited to collateral proceedings or abstract constitutional claims. In a high-volume digital policing environment, this remedial gap risks making constitutional proportionality constraints aspirational rather than operational.

The Due Process Deficit in Surveillance Technologies: A Pipeline Analysis

A central contribution of this paper is to frame digital policing as a surveillance-evidence pipeline with distinct due process failure points.

At the collection stage, the due process question is whether surveillance is governed by accessible law, limited to legitimate aims, and authorized through procedures that ensure individualized necessity. Executive authorization models under interception rules and IT Act frameworks are vulnerable to routinization, particularly when orders are secret and affected individuals are rarely notified (Information Technology Act, 2000, § 69; Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024).

At the aggregation stage, interoperable platforms such as CCTNS and ICJS increase the state's capacity to consolidate data across contexts and time. Even if each data entry event is "lawful" in isolation, aggregation can produce new intrusions through mosaic effects: the combined dataset reveals patterns and associations that no single data point would disclose. Puttaswamy's recognition of informational privacy dangers in the digital age indicates constitutional sensitivity to such systemic effects (Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017).

At the inference stage, algorithmic tools such as FRT can generate leads without transparent reasoning. This transforms the locus of suspicion from human judgment to computational correlation. Without auditability and disclosure, defendants cannot effectively test the basis of state action, undermining adversarial fairness.

At the evidentiary production stage, tools like e-Sakshya institutionalize the creation and storage of digital artifacts. This can strengthen chain of custody if designed well, but it also concentrates power in platform administrators and creates risks of selective capture, metadata manipulation, or contextual omission, especially when police control both collection and upload.

At the adjudication stage, courts may be asked to rely on surveillance-derived evidence without being institutionally positioned to assess the legality and proportionality of upstream surveillance or the reliability of algorithmic inference. Where the law does not supply exclusionary consequences for illegality, the adjudicative stage may not correct upstream due process failures (Pooran Mal v. Director of Inspection, 1974).

Case Study Lens: Telephone Tapping Safeguards and the Limits of Executive Review

PUCL remains central because it articulates that telephone tapping implicates constitutional rights and requires procedural safeguards, including a structured authorization process and review mechanisms (People's Union for Civil Liberties v. Union of India, 1997). Subsequent scholarly analysis has argued that PUCL's influence on surveillance law is substantial but insufficient for the digital age, urging redesign rather than incremental patchwork (Ramachandran, 2014).

The due process limitation is not merely that executive review committees might be biased; it is that executive review is structurally misaligned with an adversarial justice system. Review committees operate without participation of the affected person, without public reasoning, and often without meaningful transparency. In the context of mass-scale digital interception possibilities and high-frequency data requests through integrated systems, the reliance on executive review makes individualized proportionality difficult to operationalize.

The Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 continue to embed a "competent authority" model in the executive (home secretaries) and incorporate a review committee, demonstrating continuity in design even as statutory forms change. This continuity invites a constitutional question after Puttaswamy: can executive authorization and internal review satisfy legality and proportionality for high-intrusion surveillance, especially when the practical likelihood of notice and contestation is minimal?

Digital Policing, Self-Incrimination, and the Boundary of Investigative Compulsion

Digital policing also interacts with Article 20(3)'s protection against self-incrimination and the limits of investigative compulsion. Selvi addressed the involuntary administration of scientific techniques, emphasizing the tensions between investigative efficiency and individual liberties (Selvi v. State of Karnataka, 2010). While Selvi's direct subject differs from data surveillance, its reasoning is relevant: the Court recognized that technologically mediated investigation can intensify coercion, and constitutional safeguards cannot be diluted merely because the state asserts efficiency gains.

Analogously, compelled biometric capture and long-term retention under the Criminal Procedure (Identification) Act, 2022 must be assessed not only through statutory authorization but through proportionality and fairness, particularly because the Act contemplates extensive sharing and retention that outlasts the immediate investigative context.

Toward a Due Process Framework for Digital Policing in India

A due process framework for digital policing should be understood as a set of institutional constraints that translate constitutional proportionality and fairness into operational practice. The objective is not to disable legitimate policing but to ensure that technologically amplified power is matched by procedurally robust accountability.

Independent authorization for high-intrusion surveillance

Where surveillance intrudes deeply into privacy, association, or bodily integrity, executive authorization should be replaced or supplemented by independent authorization with reasoned orders. In India, the strongest doctrinal basis for this move is the Puttaswamy legality-need-proportionality structure (Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017). Independent authorization is also a practical solution to the secrecy problem illustrated by Pegasus litigation, where the Court found executive assertions insufficient to dispose of serious surveillance allegations (Manohar Lal Sharma v. Union of India, 2021).

Contestability and disclosure for algorithmic outputs

If policing relies on algorithmic systems such as FRT, due process requires contestability. This does not entail disclosing sensitive operational details that would defeat legitimate law enforcement, but it does require disclosing sufficient information to enable meaningful challenge: the basis for a match, confidence thresholds where used, audit logs, the provenance of the query image, and known system limitations. Without these, a defendant cannot test whether an algorithmic output is probative or merely prejudicial.

The procurement-driven emergence of AFRS and related FRT deployments demonstrates the need to treat algorithmic systems as legal objects requiring procedural governance rather than as discretionary tools (Hickok, 2021).

Data minimization and retention limits tied to purpose

Long-term retention periods such as the 75-year retention rule for “measurements” under the Criminal Procedure (Identification) Act, 2022 raise proportionality concerns because they transform investigation into life-course governance and amplify function creep. A due process-compatible approach would tie retention and dissemination to purpose, require periodic necessity review, and impose heightened safeguards for individuals not convicted of serious offenses.

Platform governance and auditability in interoperable systems

Interoperable criminal justice platforms create both benefits and harms. They can reduce bureaucratic delay and improve coordination, as ICJS publicly claims through its integration design. Yet platform governance must be treated as part of “procedure established by law” because it determines how data is entered, linked, accessed, and transmitted. Due process requires auditable access logs, role-based access controls, redress mechanisms for incorrect entries, and meaningful consequences for misuse.

Remedies and the problem of admissibility

Perhaps the most difficult reform question concerns remedies. As long as unlawfully obtained evidence is generally admissible under the Pooran Mal and Malkani line of reasoning, surveillance illegality will not predictably alter case outcomes (Pooran Mal v. Director of Inspection, 1974; R.M. Malkani v. State of Maharashtra, 1973). In a digital policing environment, where surveillance-derived evidence can be central to prosecution, the absence of exclusionary consequences risks hollowing due process at scale.

A proportionate remedial approach could be doctrinally structured without adopting a rigid exclusionary rule. Courts could develop a calibrated suppression doctrine where evidence obtained through serious or deliberate surveillance illegality is excluded, while minor procedural errors without rights impact may not trigger exclusion. Such calibration would align with Article 21 fairness and Puttaswamy proportionality and could be supported by legislative reform in evidentiary statutes and criminal procedure.

Limitations and Future Research

This paper is limited by the partial opacity of operational policing technologies and classified surveillance practices. While it draws on official documents describing platform infrastructures and statutory frameworks, many critical questions particularly around algorithmic accuracy, database integration protocols, and oversight functioning require empirical access and transparency that are not always publicly available. Future research should integrate doctrinal analysis with ethnographic work on police digital workflows, quantitative auditing of algorithmic systems, and comparative institutional design studies evaluating independent authorization models in constitutional democracies.

Conclusion

Digital policing in India is moving toward a platform-mediated criminal justice ecosystem in which surveillance and evidence are increasingly co-produced. CCTNS and ICJS exemplify a governance strategy that prioritizes interoperability and data-driven efficiency, while tools like e-Sakshya institutionalize digital evidence capture and rapid court availability. At the same time, interception frameworks under the IT Act and telecommunications rules continue to rely heavily on executive authorization and internal review committees, creating a due process deficit when scaled to contemporary surveillance capacity.

Constitutional doctrine after Puttaswamy demands more than superficial compliance; it demands an operationalization of legality, necessity, and proportionality, embedded in procedures that are fair, contestable, and remedially meaningful. The persistence of broad admissibility for unlawfully obtained evidence further weakens deterrence and remedy, making the redesign of surveillance governance and evidentiary consequences central to the due process project.

The path forward is not to reject digital policing but to constitutionalize it in practice: independent authorization for high-intrusion surveillance, platform auditability, algorithmic contestability, purpose-bound retention, and robust remedies that make rights violations legally consequential. Only then can India's modernization of policing avoid becoming a technologically enhanced form of procedural injustice.

References

1. Abraham, S. (2012). Government access to private-sector data in India. *International Data Privacy Law, 2*(4), 302-311.
2. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India).
3. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) SCC OnLine SC 571 (India).
4. Criminal Procedure (Identification) Act, No. 11 of 2022 (India).
5. Digital Personal Data Protection Act, No. 22 of 2023 (India).
6. Hickok, E. (2021). *Facial recognition technology in India*. Centre for Internet and Society.
7. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
8. Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295 (India).
9. Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (India).
10. Manohar Lal Sharma v. Union of India, Writ Petition (Criminal) No. 314 of 2021 (Supreme Court of India, Oct. 27, 2021).
11. , Government of India. (2017). *Crime & Criminal Tracking Network and Systems (CCTNS): Project overview & scope (Brief)*.
12. , Government of India. (2022, February 18). *Inter-Operable Criminal Justice System (ICJS) project* (document hosted on MHA platform).
13. , Government of India. (2024, September 13). *Inter-Operable Criminal Justice System (ICJS)* (official webpage).
14. People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (India).
15. Pooran Mal v. Director of Inspection, (1974) 1 SCC 345 (India).
16. , Government of India,. (2024, August 4). *Union Home Minister and Minister of Cooperation launches e-Sakshya, Nyaya Setu, Nyaya Shruti and e-Summon App for three new criminal laws in Chandigarh today*.
17. PRS Legislative Research. (2023). *The Digital Personal Data Protection Bill, 2023: Bill summary*.
18. R.M. Malkani v. State of Maharashtra, (1973) 1 SCC 471 (India).
19. Ramachandran, C. (2014). PUCL v. Union of India revisited: Why India's surveillance law must be redesigned for the digital age. .
20. Selvi v. State of Karnataka, (2010) 7 SCC 263 (India).
21. Telecommunications Act, No. 44 of 2023 (India).
22. Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 (India).
23. . (2024). *The landscape of facial recognition technologies in India*.
24. The Information Technology Act, 2000, § 69 (India).
25. Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (India).