THE EVOLUTION OF POLICING IN THE 21ST CENTURY: TECHNOLOGY, SURVEILLANCE, AND THE CHANGING NATURE OF CRIME CONTROL

Diksha Kharbanda[1] & Haneri[2]

ABSTRACT

Policing in the present day has entered a transformative phase which is defined by digital systems, advanced surveillance tools, as well as data-driven intelligence models. The shift is neither incremental nor cosmetic as it represents a deep restructuring of how crime is detected, interpreted, as well as governed. The traditional frameworks that relied on physical patrol, eyewitness accounts, as well as manual investigations are steadily being replaced by the modern algorithmic assessment, sensor-based monitoring, biometric identification, and cloud-anchored evidence ecosystem. Therefore, this paper examines the structural, technological, and legal evolution of policing during this transition with special focus on India's rapidly changing criminal justice landscape.

The drastic rise of cybercrime, transnational fraud, and encrypted communication, as well as digital financial offenses, which are embedded with technologically switched criminal networks, has exposed the limits of 20th century policing methods. To this response, contemporary agencies are deploying facial recognition systems, CCTV-federated networks, AI-driven pattern analysis, predictive policing algorithms, as well as mobile forensic capabilities. At the same time, these tools also introduce concerns regarding accuracy plus discriminatory impact plus digital governance and data governance. Altogether, this analysis traces how these tensions shape modern policing practice as well as public accountability.

India's new criminal laws like the Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS), and Bharatiya Sakshya Adhiniyam (BSA) form an important dimension of this study. These statutes incorporate digital warrants, electronic documentation, mandatory forensic procedures, and updated evidentiary rules, signaling the country's first attempt to legislate technology-ready policing. The paper evaluates how these reforms

[1] Assistant Professor, University Institute of Legal Studies, Chandigarh University.

[2] Assistant Professor, University Institute of Legal Studies, Chandigarh University.

reconfigure investigative powers, procedural safeguards, and digital-evidence requirements.

In order to frame these developments, the analysis draws on criminological theories, surveillance studies, as well as judicial doctrine and privacy, proportionality, as well as comparative insight from international policing reforms. This research altogether concludes that while technology enhances operational efficiency and investigative precision, it also magnifies ethical dilemmas and legal vulnerabilities. Effective 21st-century policing will require not only technological capacity but also constitutional discipline, transparent governance, and a robust oversight structure, which when coupled together will ensure that innovation strengthens security without eroding liberty.

Keywords: Artificial Intelligence, cybercrime, criminology, modern day crime, new criminal laws, data analytics.

1. Introduction

Policing in the modern era has undergone an extremely vivid transformation, which is marked by integration of digital technologies, data analytics, as well as advanced surveillance infrastructure. As the purpose of this study is to examine how policing has shifted in this era, majorly from largely reactive manpower-driven operations to modern technologically augmented intelligence-led systems. Contemporary scholarship notes that the defining characteristic of modern policing is its reliance on digital systems, algorithmic tools, and big data platforms. A development discussed extensively by Barron and Hammer in their analysis of “technology-driven policing models”.[3]

The core problem addressed in this research is mismatch between traditional policing frameworks as well as the structure of 21st century crime. Criminal activity nowadays is mainly diffused and distributed among cyberspace, which is often transnational, frequently encrypted, and technologically sophisticated. Cyber fraud, identity theft, phishing, ransomware, dark-net marketplaces, and online radicalization furthermore exemplify these crimes, and they altogether cannot be addressed through conventional policing models. Intelligence-led policing and data-centric methodologies are therefore increasingly central to law enforcement strategy.

[3] Georgios Gkougkoudis et al., Intelligence-Led Policing and the New Technologies Adopted by the Hellenic Police, 2 Digital 2020, 143, 143–63 (2022), https://doi.org/10.3390/digital2020009

Scholars such as Gkougkoudis emphasize that policing has shifted from institution-based decision-making to "intelligence-led, technology-assisted crime governance".[4]

A key dimension of this transformation is pointed at the rise of predictive policing, in which machine learning algorithms analyze historical crime data to forecast potential hot-spots or suspect patterns. While the systems do promise efficiency, side-by-side they also raise concerns about algorithmic bias, discriminatory profiling, and lack of transparency. Digital evidence has similarly become indispensable. Metadata, device extraction report, IP logs, server record, and cloud storage data now form the backbone of criminal investigation. All of this reflects a fundamental shift in evidentiary structures.

In India, the urgency of studying this transformation is heightened by the introduction of new criminal laws. The ***BNSS*** (Bharati Nargarik Suraksha Sanhita), ***BNS*** (Bharatiya Nyaya Sanhita), and ***BSA*** (Bharatiya Sakshya Adhiniyam). All of these are a comprehensive overhaul of the criminal law framework implemented in 2024. As these laws replace colonial era IPC, CRPC, and Evidence Act, as well as formally incorporate digital processes such as electronic warrant, digital reference system, forensic mandate, and electronic record integrity standards. A detailed doctrinal analysis of the statutes by the Square Circle Clinic describes them as "India's first structurally modern technology-ready criminal codes".[5]

At last, the scope of this study spans conceptual, technological, and legal dimensions. The evolution of policing practices, the role of surveillance in crime control, the statutory mechanism regulating the modern enforcement, as well as foundational constitutional constraints. Limitations also include varying state capacities, limited empirical data on newly adopted technologies, and the nascent implementation of India's new criminal courts.

The research is guided by four central questions:

1. How has technology transformed policing practices?

2. What role does surveillance play in contemporary crime-control mechanisms?

[4] James Byrne & Don Hummer, Technology, Innovation and Twenty-First-Century Policing, 25 Policing 8 (2016) (available via ResearchGate).

[5] The Square Circle Clinic, India's New Criminal Laws: A Substantive Analysis (Oct. 22, 2025), https://thesquarecircleclinic.org/2025/10/22/new-criminal-laws-substantive-analysis

3. How do the new criminal laws regulate and constrain policing powers?

4. How does the IT Act structure digital-crime enforcement and prosecution in India?

This introduction establishes the conceptual and legal foundation for analysing the evolution of policing in the twenty-first century.

2. Historical Evolution of Policing

2.1) Policing in the 20th vs 21st century

The present-day professionalized policing involves centralized forces, be it patrol, human intelligence, and organizational reforms, which are aimed at *bureaucratic efficiency* and public order. Contemporary police work, on the other hand, is *digitally saturated*. Patrols are supplemented by sensor networks, digital records, and inter-agency data-sharing platforms, where in the 20th century, policing relied solely on *human guardianship* and neighborhood presence. But in the 21st century, policing increasingly relies on *technological guardianship*, CCTV arrays, mobile data extraction, biometric databases, as well as a cloud evidence system. This drastic institutional shift is discussed in reviews of policing history and modernization.[6]

2.2) Development of modern policing models

Several governance models are marking the transition. Compstat introduced performance-driven data-led management, which (originated in NYPD in the 1990s) and also spread internationally as a performance and accountability tool. Furthermore, *intelligence-led policing ILP* prioritized targeted response informed by intelligence product and risk assessment rather than blanket patrol. It also grew after 1990s, especially after the 9/11 attack, which links policing to national security information flows. These models transformed everyday decision-making, as commanders now use dashboards, heatmaps, and intelligence briefs, as back then commanders used to rely on officer reports and solely on their own experience.[7]

2.3) Shift from reactive to preventive policing

[6] Callie Marie Rennison & Mary Dodge, The History of Policing, in Introduction to Criminal Justice: Systems, Diversity, and Change 107 (5th ed. SAGE Publ'ns 2015).

[7] David Weisburd, Stephen D. Mastrofski, Rosann Greenspan & James J. Willis, The Growth of Compstat in American Policing (Police Found'n Apr. 2004).

The old reactive paradigm responding after harm now has been superseded by preventive and predictive frameworks. *Situational Crime Prevention and routine activity* ideas were repurposed through technology: sensors act as guardians, data analytics predict hotspots, and patrols are directed proactively rather than randomly. Predictive policing tools, however, import historical bias into automated forecasts unless carefully governed. Empirical studies show mixed effectiveness: data can concentrate resources efficiently but can also reproduce structural inequalities when the training data reflect biased enforcement.[8]

2.4) Criminological theories influencing modern policing

Classic theories still animate practice, but their application is reframed by tech. *Routine Activity Theory* (Cohen & Felson) explains why digital routines (e-commerce, mobile banking) create new target opportunities and new guardianship needs. *Broken Windows* (Wilson & Kelling) influenced order-maintenance policing and its technological cousins (rapid response via cameras and sensors), yet critics caution that such approaches can lead to over-policing of marginalized communities. In short, the theory toolbox is the same, but the instruments like algorithms, sensors, metadata are new.[9]

3. Technological Transformation in Policing

3.1) Surveillance Technologies

The policing arena has been radically reshaped by surveillance architectures that overlay physical spaces with digital sensing. The deployment of closed-circuit television (CCTV) networks across Indian cities has become a ubiquitous pillar of modern crime control. A recent government-commissioned study found CCTV to be the most frequently used surveillance tool by police, even while public anxiety about privacy remains elevated.[10] For instance, in Bengaluru, over 530,000 geo-tagged CCTV cameras are now operational—an indicator of the scale of digital guardianship. Facial Recognition Systems (FRS) further augment CCTV by converting image data into actionable intelligence. In New Delhi markets, the FRS enabled identification of 70 suspects within nine days during a major shopping festival, illustrating how

[8] Lawrence E. Cohen & Marcus Felson, Social Change and Crime Rate Trends: A Routine Activity Approach, 44 Am. Sociological Rev. 588 (1979).

[9] James Q. Wilson & George L. Kelling, Broken Windows: The Police and Neighbourhood Safety, 249 The Atlantic 29 (Mar. 1982).

[10] Sarasvati N.T., More People in India Support Surveillance Tech than Those Critical of It: Study, MediaNama (Mar. 31, 2023), https://www.medianama.com/2023/03/223-surveillance-tech-study-public

biometric surveillance changes the speed and scope of policing responses.[11] Drones and Unmanned Aerial Vehicles (UAVs) extend surveillance into aerial space: for crowd monitoring, border control, and situational awareness, police now rely on sky-borne sensors as much as foot patrols. The use of drones in Indian policing is reported in public-policy reviews as a technology that enjoys majority support (~55 %) among respondents, yet also raises significant civil-liberties concerns.[12] The **Automatic Number Plate Recognition** (ANPR) system completes the quartet: by digitally recording and analysing vehicle movement data, ANPR transforms cars from anonymous transport into data-points within policing networks, enabling rapid vehicle tracking and linking mobile suspects to crime scenes.

3.2) Forensic and Investigative Technologies

The drastic shift from analog to digital evidence is marking a profound sea change in investigative practice, as **DNA profiling** now routinely supplements the traditional detective work. But in a more radical manner, **cyber-forensic tools** enable law enforcement to extract mobile phone data, plus tap-in to cloud logs, as well as map *digital footprints*. As previous decades had mobile device data extraction only limited to call records, it now also encompasses geolocation metadata, app usage logs, as well as allows deleted file retrieval, which altogether renders the smartphone a *rich forensic mine*. Recent research emphasis shows how **digital footprint analysis** is stitching together the disparate device traces, metadata trails, and social media records. It altogether has become central in crime reconstruction and prevention.[13] These forensic techniques shift the locus of policing from street to data center, which altogether creates an **evidence ecosystem** in which every byte is a potential clue.

3.3) Predictive Policing & Big Data

Perhaps the most controversial dimension of technological transformation can be considered as **predictive policin**g, which is a paradigm in which law enforcement agencies use big data

[11] Abhay, Delhi Cops Use Face Recognition System to Curb Market Crime, The Times of India (Oct. 31 2024), https://timesofindia.indiatimes.com/city/delhi/facial-recognition-technology-transforms-crime-prevention-in-delhis-markets/articleshow/114788109.cms

[12] Common Cause & Lokniti-CSDS, Status of Policing in India Report 2023: Surveillance and the Question of Privacy (Mar. 2023), https://ruralindiaonline.org/as/library/resource/status-of-policing-in-india-report-2023-surveillance-and-the-question-of-privacy/

[13] Priya Vedavalli et al., Facial Recognition Technology (FRT) in Law Enforcement in India: Concerns and Solutions, DGN Policy Brief No. 13 (Artha Global Apr. 22, 2021), https://artha.global/wp-content/uploads/2025/01/Facial-Recognition-Technology-FRT-in-Law-Enforcement-in-India-Concerns-and-Solutions.pdf

analytics, machine learning models, and risk assessment tools in order to forecast the crime, rather than waiting for it to occur. The adoption of *Compstat* in the United States is a prototype of data-driven policing models that promotes performance metrics, crime mapping, and accountability[14]. In Indian cities, machine learning systems have also reported above 90% predictive accuracy for hot-spot forecasting using geo-spatial and demographic features[15]. Moreover, AI-driven crime pattern prediction also holds promise but also raises **ethical concerns** like profiling, discrimination, false positives, and algorithmic opacity altogether threatens procedural fairness. A study also remarks that in India, "inferior-quality datasets have ended up reinforcing and amplifying police biases in law enforcement."[16]

Predictive policing tools require three elements: historical crime data, analytics platforms, and operational response mechanisms. Without proper safeguards, these become structures of over-policing rather than prevention. The term **algorithmic guardianship** aptly describes the new role of police data systems: algorithmically guided guardians that iterate over past patterns to inform future enforcement.

3.4) Body-Worn Cameras (BWCs)

In the domain of accountability and transparency, **body-worn cameras (BWCs)** stand out as a technological innovation that links frontline policing to public trust. These devices serve dual roles: evidence collection (capturing arrests, search-operations, and custodial interactions) and deterrence (reducing use-of-force incidents). In crowded railway stations in Delhi, the procurement of over 100 BWCs alongside 2,000 CCTV cameras reflects how Indian policing treats BWCs as **force-multipliers and accountability tools.**[17]

Their presence encourages **procedural transparency**, ensures recording of interactions, and supports digital-trail creation for oversight purposes. They shift policing from watching over

[14] Youngsub Lee, Ben Bradford & Krisztián Pósch, The Effectiveness of Big Data-Driven Predictive Policing: A Systematic Review, 5 Justice Evaluat. (2024), https://www.tandfonline.com/doi/full/10.1080/24751979.2024.2371781

[15] Amrita Sarkar et al., Real-Time Crime Prediction in India Using Machine Learning, IJRASET (2025), https://www.ijraset.com/research-paper/real-time-crime-prediction-in-india-using-machine-learning

[16] Antara Vats, Building the Case for Restricted Use of Predictive Policing Tools in India, 32 Int'l Rev. Info. Ethics (Nov. 2022), https://informationethics.ca/index.php/irie/article/view/487

[17] Khushi Bhuta, Crowd-Control Systems To Boost Security At Rly Stns, The Times of India (June 15, 2025), https://timesofindia.indiatimes.com/city/delhi/crowd-control-systems-to-boost-security-at-rly-stns/articleshow/121854843.cms

to being watched by, thereby embedding a reciprocal surveillance logic within officer-citizen interaction.

Figure: 1.1

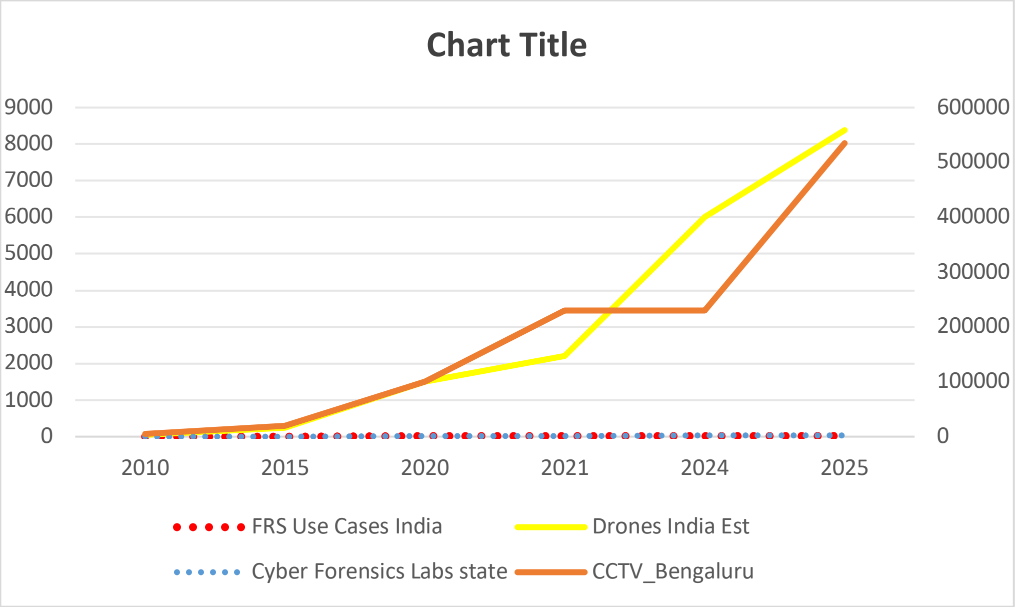


Figure 1.1: Trends in technology-enabled policing mechanisms in India (2010–2025), based on secondary data from TOI, Artha Global, MarketsandMarkets, and MHA-CCPWC datasets.

The figure compares the growth of CCTV cameras, drone deployments, FRS use-cases, and state cyber-forensic laboratories over time.

At last, the rapid technological transofrmation of policing is not all about new gadgets. It is more about a **reconfiguration of the policing paradigm** from human based guardianship to more of an algorithmic surveillance. While these technologies enhance operational capacity and efficiency, they simultaneously amplify complexities of governance, ethics, privacy and bias. In summary for this, the questions of *who watches the watchers, how algorithms decide, and what safeguards exist* become ever more urgent.

4. Legal Framework: Indian Criminal Law Reforms & Technology

4.1) Overview of New Criminal Laws

India's criminal-justice architecture has recently undergone a **paradigmatic overhaul**. With effect from July 1, 2024, the colonial-era legal edifice comprising the Indian Penal Code (IPC), the Code of Criminal Procedure (CrPC) and the Indian Evidence Act was supplanted by three landmark statutes: the Bharatiya Nyaya Sanhita (BNS) which replaces the IPC, the Bharatiya Nagarik Suraksha Sanhita (BNSS) which replaces the CrPC, and the Bharatiya Sakshya Adhiniyam (BSA) which replaces the Evidence Act[18].

These statutes aim to align India's substantive and procedural criminal law with 21st-century realities like **digital evidence, algorithmic investigations, cross-border crime, and cyber-enabled threats**. While also addressing longstanding concerns about colonial legacies in legal language and structures[19].

For instance, the BNS (2023) is described as "an Act to consolidate and amend the provisions relating to offences and for matters connected therewith or incidental thereto." Thus this new legal framework forms the *statutory backbone* of modern policing in India.

4.2) Key Provisions Affecting Policing

Several critical provisions within the new statutes directly influence policing, particularly in relation to technology and investigative power.

Firstly, under the BNSS, **electronic evidence** is now explicitly recognised: digital FIRs, e-summons and electronic warrants are provided for culminating in a modernised process in which policing operations can issue warrants, summons and record statements in digital form. Training materials note that these provisions are facilitating real-time chain-of-custody tracking for crime-scene data[20].

Secondly, the expansion of police power is visible through enhanced provisions for **preventive detention**, broad search and seizure powers aided by technology as well as elevated roles for forensic units. The police are now authorised to use *mobile forensic vehicles*, audio-video recording of searches/seizures and linkages between police stations, forensic labs and courts

[18] India, Ministry of Home Affairs, New Criminal Laws (last updated July 9, 2024), https://www.mha.gov.in/en/commoncontent/new-criminal-laws

[19] Drishti IAS, New Criminal Laws Come into Force (July 1, 2024), https://www.drishtiias.com/daily-updates/daily-news-analysis/new-criminal-laws-come-into-force

[20] Khushi Bhuta, 7.3 k FIRs Filed by Noida Cops in 1 Year Since BNS Rollout but Digital Evidence Only in 13 %, The Times of India (Aug. 12, 2024), https://timesofindia.indiatimes.com/city/noida/7-3k-firs-filed-by-noida-cops-in-1-year-since-bns-rollout-but-digital-evidence-only-in-13/articleshow/124056031.cms

via video-conferencing[21].

Thirdly, technology for s*earch and seizure is fortified*: under BNS/BSA, every arrest, search or seizure must be recorded electronically; statements by women witnesses are to be recorded by female officers and provisions emphasise digital evidence upload to central platforms. The Noida example displays that although 7,322 FIRs were filed in one year, only 13% had digital evidence uploaded via the mandated system thus highlighting the implementation gap. These changes collectively shift policing from paper-based, human-intelligence models to digital-forensic, tech-enabled architectures which is **a tectonic shift in policing practice**.

4.3) Information Technology Act, 2000 (IT Act) and Its Amendments

In a parallel aspect to the overhaul of criminal laws, the **IT Act, 2000** continues to be extremely important to policing of digital crime in India. Section 66 of the IT Act criminalises various forms of misuse of computer resources like identity theft, hacking and fraudulent access[22]. Furthermore, Section 67 penalises transmission of obscene material in electronic form. The Act's intermediary-liability regime under section 67 C and section 69A empowers the Government to issue directions for interception, monitoring or blocking of computer resources tools which law-enforcement regularly invokes for cyber surveillance. An illustrative case for this to consider can be Shreya Singhal v. Union of India, in which section 66A[23] of the Act was struck down for violating free speech.

Thus, the IT Act provides a **specialised cyber-crime framework**, while BNS/BNSS/BSA provide the **general criminal regime** in which modern policing functions; together they regulate digital-crime enforcement, digital evidence handling, and technological surveillance.

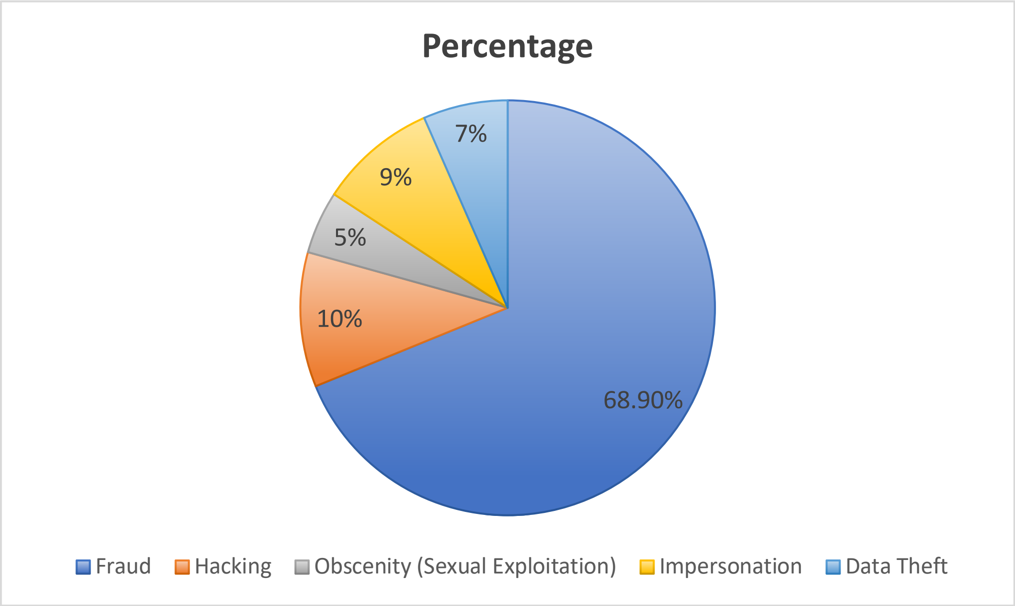
Figure 2.1: Distribution of IT Act Prosecutions (Fraud, Hacking, Obscenity, Impersonation, Data Theft).

[21] Khushi Bhuta, SPs to Monitor Mob Lynching, Terrorism: CM, The Times of India (June 1, 2024), https://timesofindia.indiatimes.com/city/bhubaneswar/sps-to-monitor-mob-lynching-terrorism-cm/articleshow/120972518.cms

[22] Cybersecurity Laws and Regulations – India 2025, ICLG (Nov. 6, 2024), https://www.iclg.com/practice-areas/cybersecurity-laws-and-regulations/india

[23] A Background to Section 66A of the IT Act, 2000, PRS India (Apr. 12, 2021), https://prsindia.org/theprsblog/a-background-to-section-66a-of-the-it-act-2000?page=2&per-page=1

Data drawn from NCRB Crime in India 2023 (fraud and sexual exploitation figures) and category-allocation estimates for other offence types.



The legal framework now positions Indian policing for the digital era: from the recognition of electronic warrants and digital FIRs under new criminal laws to specialised cyber-crime provisions under the IT Act. The efficacy of these reforms will majorly depend on implementation+technological capacity alongside of comprehensive training of investigators otherwise the laws risk being form over function.

5. Jurisprudence Shaping Policing & Surveillance

Table: Key Judicial Precedents Shaping Policing, Surveillance, and Digital Rights in India

Case Name	**Court & Year**	**Core Holding / Principle**	**Impact on Policing & Surveillance**
Justice K.S. Puttaswamy (Retd.) v. Union of India	Supreme Court, 2017	Recognised **privacy as a fundamental right** under Article 21; established tests of legality, necessity, proportionality.	Police surveillance now requires stronger constitutional justification; mass surveillance & data collection must satisfy proportionality.

Case Name	**Court & Year**	**Core Holding / Principle**	**Impact on Policing & Surveillance**
K.S. Puttaswamy (Aadhaar) v. Union of India	Supreme Court, 2018	Upheld Aadhaar but struck down Section 57; limited private-sector use; emphasised data-minimisation.	Restrains police from seeking Aadhaar-based authentication except where authorised by law; limits biometric overreach.
Anuradha Bhasin v. Union of India	Supreme Court, 2020	Held that **internet access is integral to free speech**; shutdowns must be temporary, proportionate, and reviewable.	Police cannot impose indefinite shutdowns; ensures judicial scrutiny of digital policing tools like shutdowns during protests.
People's Union for Civil Liberties (PUCL) v. Union of India – Telephone Tapping Case	Supreme Court, 1997	Laid down **procedural safeguards** for phone interception—necessity, duration limits, review committees.	Becomes the benchmark for lawful interception; police must follow strict tapping protocols under the Telegraph Act & IT Act.
Kartar Singh v. State of Punjab	Supreme Court, 1994	Upheld TADA but mandated safeguards against abuse—legal aid, judicial oversight, reasoned detention.	Influences anti-terror policing; requires higher thresholds before surveillance, detention, or special-law powers used.
Shreya Singhal v. Union of India	Supreme Court, 2015	Struck down **Section 66A of the IT Act** as vague & unconstitutional.	Prevents police from arresting for online speech; narrows misuse of digital policing powers.
Delhi High Court FRT Matters (*Saron v. GNCTD*, *Roshni v. Delhi Police*, pending)	Delhi High Court, 2021–2024	Questions legality, accuracy, and bias of Facial Recognition Technology; seeks due-process safeguards.	May restrict blanket FRT deployment; pushes transparency reports, accuracy disclosures, and warrant requirements.
Various High Court rulings on electronic evidence	Multiple, 2020–2024	Stress on **Section 65B certificate**, chain-of-custody, and authenticity for digital evidence.	Directly shapes police investigation methods under the Bharatiya Sakshya Adhiniyam (BSA) and BNSS.

6. The Future of Policing: Integration, Innovation & Safeguards

The upcoming era of policing in India is being shaped by fast-paced technological adoptions like AI Tools, digital evidence system, drones, predictive analytics, as well as quantum-era forensic upgrades. All of these shifts are already visible. For example, the Delhi police has deployed f**acial recognition systems (FRS)**[24] across major markets, in which automated facial matching are now part of Delhi policing.

Similarly, **Hyderabad police uses AI-backed tools like TSCOP[25] and Hawkeye**, which are able to integrate the real-time CCTV footage and analyze them at large. However, not all consequences of technological policing are positive. The **Status of Policing in India Report (SPIR) 2023**, released by Common Cause, warns that India's increasing use of facial recognition, data integration, and predictive policing raises privacy and fairness issues as the ***ruralindia*** report argues that many technologies are deployed without safeguards, legal standards, or transparency.

Predicitive Policing is being conducted by using statistical patterns in order to forecast crime location and even high-risk individuals and it is slowly being moven from pilot projects to active use that too specifically in the metropolitan cities. But researches at international or global level also indicate as well as demonstrate that predictive models are bale to mirror the historic biases in the data to train them. When Indian FIR datasets fluctuate widely between states and districits, predictive analytics can also generate skewed risk sources without any issue which in total will further intensify scrutiny in already over-policed regions[26].

Unless India mandates bias-testing, transparent documentation, and human review of algorithmic outputs, predictive policing could compromise public trust instead of improving safety.

Quantum Era Forensics, it means India's digital-evidence ecosystem is facing a major transformation as the country advances under the National Quantum Mission. Quantum

[24] Facial Recognition Technology Transforms Crime Prevention in Delhi's Markets, Times of India (Nov. 5, 2025), https://timesofindia.indiatimes.com/city/delhi/facial-recognition-technology-transforms-crime-prevention-in-delhis-markets/articleshow/114788109.cms

[25] Telangana Police, TSCOP & HawkEye Crime Analytics Platform, Telangana Police Official Website, https://tspolice.gov.in

[26] Information Society Project, Yale Law School, Predictive Policing Info Pack (2023), https://law.yale.edu/sites/default/files/area/center/mfia/document/infopack.pdf

computing will eventually render many existing encryption and hashing tools obsolete. Forensics labs depending on traditional hashing for chain-of-custody will find their methods vulnerable once quantum decryption becomes commercially viable[27].

Scientific research anticipates this shit as studies in forensic science which includes recent work being published in MDPI is warning that digital timestamps, hashing integrity, and secured logs will require quantum-resistant cryptography to remain admissible and reliable in court. The Bharatiya Sakshya Adhiniyam (BSA), which integrates digital evidence into mainstream criminal trials, makes quantum-secure infrastructure even more critical.

Digital courts and Virtual Policing, refers to India's justice delivery system is moving toward full digital integration. The E-Courts Phase III Programme, launched by the Ministry of Law & Justice, lays out a plan for a unified digital case-flow pipeline connecting police stations, forensic labs, prisons, and courts. The E-Committee of the Supreme Court has further explained that virtual hearings, e-summons, digital filing, and real-time access to electronic evidence will form the backbone of 21st-century justice[28].

BNSS accelerates this shift by embedding electronic FIRs, digital warrants, online investigation reports, and remote testimony directly into procedural law. However, India's digital divide remains a major obstacle. People in rural and economically weaker regions often lack devices or stable connectivity, making it difficult for them to participate meaningfully in virtual hearings. Digital justice cannot expand without simultaneous investment in public access infrastructure.

Drone Enabled Surveillance means police drones fleets are expanding at extremely promt pace that too in metropolitan cities like Delhi, Mumbai, Hyderabad, Bengaluru and Noida. Drones are now being used for monitoring the crowd-flow+provide perimeter security as well as emergency operations. A 2024 report[29] highlighted their increasing role in protecting railway stations and high-density public spaces. While drones enhance situational awareness, they also raise questions about high-resolution aerial monitoring, storage of drone footage, automated

[27] Department of Sci. & Tech., National Quantum Mission (2023), https://dst.gov.in/national-quantum-mission

[28] Press Info. Bureau, Government of India, Launch of e-Courts Mission Mode Project Phase III (Apr. 2024), https://pib.gov.in/PressReleasePage.aspx?PRID=2009020

[29] Times of India, Crowd-Control Systems to Boost Security at Railway Stations (2024), https://timesofindia.indiatimes.com/city/delhi/crowd-control-systems-to-boost-security-at-rly-stns/articleshow/121854843.cms

object tracking, and covert surveillance. India does not yet have a law that sets boundaries for persistent aerial observation or defines retention periods for drone-captured data.

Urgent need for a comprehensive surveillance law[30], this aspect is mainly about India's current surveillance framework is fragmented which is relying on Telegraph Act rules for phone interception, Section 69 of the IT Act for digital interception, PUCL (1997) safeguards for wiretapping, and CERT-In notifications for incident reporting. None of these statutory tools anticipate modern policing technologies such as FRS, drones, predictive algorithms, biometric networks, or automated surveillance systems. Policy organisations such as Vidhi Centre for Legal Policy, Common Cause, and the Internet Freedom Foundation have repeatedly stressed the need for a standalone Surveillance Regulation Act rooted in the constitutional principles of K.S. Puttaswamy v. Union of India (2017).

Recommendations:-

1. Enact a National Surveillance Regulation Act with warrant standards+transparency rules, retention limits, and specific provisions for FRS, drones, and predictive policing.

2. Mandate algorithmic accountability for example bias audits, model documentation, and human-in-the-loop decision control for all AI systems.

3. Upgrade digital-evidence infrastructure under BSA with quantum-secure hashing and automated chain-of-custody systems.

4. Introduce drone-governance rules including geofencing, public flight logs, and judicial authorisation for sensitive surveillance.

5. Strengthen digital-justice access with rural virtual-court centres, digital assistance desks, and offline procedural access.

6. Adopt a quantum-ready policing roadmap aligned with the National Quantum Mission.

[30] Common Cause & Lokniti-CSDS, Status of Policing in India Report 2023: Surveillance and the Question of Privacy (2023), https://ruralindiaonline.org/en/library/resource/status-of-policing-in-india-report-2023-surveillance-and-the-question-of-privacy/

7. Conclusion

The drastic change and evolution of policing in 21st century is reflecting a decisive transition from traditional manpower which is centering models to a technologically complex ecosystem which is driven by data, algorithms, and digital evidence. Altogether, the integration of surveillance infrastructure, artificial intelligence, forensic digitization, as well as predictive analysis has reshaped not only investigative capacity but as well as the fundamental logic through which the police can understand crime, also identify threats, alongside deploying the resources at efficient and effective manner. Furthermore, India's recent criminal law reforms institutionalize this transition by embedding electronic warrants, digital FIRs, forensic first mandates, as well as chain of custody requirement directly into statutory procedure. All of these coupled together can provide us with the developments which signal a structural reorientation of policing apparatus toward a technologically enabled and intelligence-led model.

However, the transformation is not without risk as predictive policing, facial recognition system, and role surveillance is introducing concerns related to algorithmic bias, opacity disproportionate targeting, as well as mass monitoring. Thus, the absence of comprehensive surveillance regulation act creates a legal vacuum in which high-risk technology can be deployed without uniform safeguards. All of this underlines that any policing practice affecting privacy, speech, movement, or autonomy must meet the test of legality, necessity, as well as proportionality, yet the gap between token station doctrine and field-level police practice remains wide.

Looking ahead, the core challenge for India is balancing technological capability with democratic restraint. Technology can strengthen policing, but only if its use is transparent, audited, and constitutionally compliant. Without strong guardrails, the same tools that enable faster detection and efficient investigation can also facilitate unprecedented forms of surveillance and discriminatory enforcement.

Thus, the future of policing requires a rights-based framework that integrates statutory clarity, algorithmic accountability, digital-justice access, forensic modernisation, and institutional oversight. Only through such a calibrated approach can India harness technological advancement while safeguarding civil liberties, ensuring that crime control in the twenty-first century remains both effective and just.