International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 06-04-2025, Accepted: 07-05-2025, Published: 22-05-2025
Volume 11, Issue 5, 2025, Page No. 75-78

Liability and accountability in ai-driven policing: Revisiting the doctrine of command responsibility in cyberspace

Pratyaksh Joshi[1], Dr. Yogesh Wamankar[2]
[1] Research Scholar, Department of Law, Mansarovar Global University, Sehore, Madhya Pradesh, India
[2] Assistant Professor, Department of Law, Mansarovar Global University, Sehore, Madhya Pradesh, India

Abstract
The rise of artificial intelligence (AI) in Indian policing has transformed surveillance and predictive enforcement strategies. However, this technological evolution has also raised critical legal questions regarding liability when AI systems infringe upon constitutional rights or cause wrongful outcomes. This paper explores the doctrinal applicability of the command responsibility principle in cases of AI misuse in policing within the Indian context. Drawing from constitutional protections under Articles 20, 21, and 22, this study engages with landmark Supreme Court rulings such as Nilabati Behera v. State of Orissa (1993) [10], D.K. Basu v. State of West Bengal (1997) [5], and K.S. Puttaswamy v. Union of India (2017) [9]. It evaluates statutory instruments including the Information Technology Act, 2000 [8], Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 [2], and Bharatiya Sakshya Adhiniyam (BSA), 2023 [3]. By analyzing ethical concerns such as algorithmic bias and opacity, along with institutional mechanisms like the NHRC and Police Complaints Authorities, the paper proposes extending supervisory liability principles to the digital domain. It concludes with recommendations for statutory reforms, algorithmic audits, and clear accountability mandates to uphold constitutional values in AI-assisted law enforcement.

Keywords: AI-driven policing, command responsibility, algorithmic bias, constitutional rights, accountability

Introduction
Artificial intelligence (AI) is reshaping the operational frameworks of law enforcement in India. AI-driven systems such as facial recognition technology (FRT), predictive analytics, and real-time surveillance tools are increasingly utilized by police agencies to monitor, identify, and apprehend suspects (Pol & Karthik, 2024) [13]. While these technologies enhance operational efficiency, they simultaneously raise significant questions about constitutional rights, ethical boundaries, and, most critically, accountability.

India's constitutional scheme provides robust protections for individual liberty and procedural fairness under Articles 20, 21, and 22. These protections are particularly relevant when automated systems make decisions that affect individual freedoms. Yet, the legal regime remains largely silent on who bears responsibility when an AI system—authorized, deployed, or supervised by police—leads to wrongful arrest, unlawful detention, or breach of privacy. This gap highlights the need to explore doctrines traditionally applied in custodial and military contexts, particularly the doctrine of command responsibility.

Though rooted in international criminal law, the doctrine of command responsibility has doctrinal relevance in Indian policing. It posits that superiors can be held liable for the unlawful acts of subordinates when they fail to prevent or punish those acts, especially when they knew or ought to have known about them (Singh, 2016) [19]. Applying this principle to AI-based policing, it is pertinent to ask whether a supervisory officer or institution can be held accountable when an AI tool—used under their command—violates an individual's rights.

This paper attempts to bridge the existing gap in legal scholarship by examining whether the doctrine of command responsibility can be adapted to AI-driven policing in India. It studies Indian statutes such as the Information Technology Act, 2000 [8], and the recently enacted Bharatiya Nagarik Suraksha Sanhita (2023) [2], as well as constitutional jurisprudence developed in seminal Supreme Court decisions. It also highlights ethical concerns and suggests a framework for institutional and individual liability in cyberspace governance.

Objectives
- To analyze the constitutional and statutory safeguards under Articles 20, 21, and 22 of the Constitution of India and evaluate their application to AI-assisted policing through existing Indian laws such as the IT Act, BNSS 2023 [2], and BSA 2023 [3].
- To examine the doctrinal relevance of the command responsibility principle in assigning liability to police supervisors for violations arising from the use or misuse of AI systems in law enforcement.

Constitutional and Statutory Framework
a. Constitutional Protections: Articles 20, 21, and 22
The Constitution of India provides foundational rights that are directly implicated when AI-driven policing tools are used. Article 20(3) protects individuals from being compelled to self-incriminate. This is particularly relevant when biometric systems (e.g., fingerprint or facial recognition) are used to unlock personal devices without consent. In Selvi v. State of Karnataka (2010) [17], the Supreme Court held that involuntary techniques like narcoanalysis, brain mapping, or lie detector tests violate Article 20(3), as they extract personal knowledge from an accused (Selvi v. State of Karnataka, 2010) [17].

Article 21, which guarantees the right to life and personal liberty, has been expansively interpreted to include the right to privacy, dignity, and procedural fairness. In K.S.

Puttaswamy v. Union of India (2017) [9], the Supreme Court unequivocally recognized privacy as a fundamental right under Article 21, stating that any intrusion must satisfy legality, necessity, and proportionality (K.S. Puttaswamy v. Union of India, 2017) [9]. This interpretation imposes constraints on AI-based surveillance systems, which often operate in opaque, non-consensual, and unregulated ways.

Article 22 protects individuals against arbitrary arrest and detention. AI systems used for facial recognition or predictive policing could potentially bypass procedural safeguards such as informing the accused of the grounds of arrest or ensuring legal counsel. These fundamental guarantees are often compromised when technology is treated as infallible and not subject to human oversight (Rajagopal v. State of Tamil Nadu, 1994) [15].

b. Information Technology Act, 2000 [8]

The Information Technology Act, 2000 [8] governs electronic records, data protection, and cyber operations. Section 66E penalizes the capturing or transmission of private images without consent, which is highly relevant in the context of mass surveillance through AI-powered CCTV and drone systems (Information Technology Act, 2000) [8]. Sections 69 and 69B permit lawful interception and monitoring but are meant to be executed with appropriate governmental authorizations.

Despite these provisions, the IT Act is silent on algorithmic accountability. It does not mandate any audit trail, documentation, or explainability of AI processes, thereby offering limited recourse to individuals who may be wrongly profiled or targeted by automated policing systems (Pol & Karthik, 2024) [13].

c. Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 [2]

The BNSS, which replaces the Code of Criminal Procedure (CrPC), has implications for AI-assisted investigations. For instance, Section 187 of BNSS (replacing CrPC Section 167) extends the period of police custody even after judicial remand, potentially aggravating wrongful detention risks if based on flawed AI predictions (BNSS, 2023) [2]. Section 194, which governs the sanction required to prosecute public servants, may protect officers unless it is shown that the misuse of AI was beyond the scope of their official duty.

Courts have held that such protection is not absolute. In Shiv Sagar Tiwari v. Union of India (1996) [18], the Supreme Court clarified that acts committed outside the scope of duty—such as unauthorized surveillance—do not enjoy statutory protection under old Section 197 CrPC (Shiv Sagar Tiwari v. Union of India, 1996) [18].

d. Bharatiya Sakshya Adhiniyam (BSA), 2023 [3]

The BSA modernizes evidentiary rules to accommodate digital records. Section 63 reaffirms the importance of certificates for the admissibility of electronic records, a continuation of Section 65B of the Indian Evidence Act, 1872. However, in the context of AI, questions persist about how to certify data processed through black-box algorithms, where the origin and transformation of data are not easily verifiable (Bharatiya Sakshya Adhiniyam, 2023) [3].

Cases such as Anvar P.V. v. P.K. Basheer (2014) [1] have mandated strict compliance with certification norms, which may pose challenges when AI outputs are presented as evidence without human validation (Anvar P.V. v. P.K. Basheer, 2014) [1].

AI Tools in Indian Policing and Ethical Concerns

a. Deployment of AI in Indian Law Enforcement

In recent years, Indian police departments have incorporated AI-based technologies for tasks such as facial recognition, predictive policing, and real-time surveillance. The Delhi Police have used Automated Facial Recognition Systems (AFRS) during riot investigations, including the 2020 Northeast Delhi riots and the 2022 Jahangirpuri clashes (Santoshini, 2022) [16]. Similarly, Uttar Pradesh Police have adopted tools like Trinetra and Staqu's ABHED to identify suspects through image and video analysis (Ulmer, 2019) [21].

Predictive policing tools are also being tested to forecast crime-prone zones based on historical and socio-economic data. While these developments aim to enhance policing efficiency, they risk over-surveillance, targeting of specific communities, and opacity in decision-making (Indian Express, 2023) [7].

b. Algorithmic Bias and Disproportionate Impact

One of the most pressing ethical challenges in AI-driven policing is algorithmic bias. AI systems trained on historical data often inherit the prejudices embedded in past practices. In India, this risk is compounded by socio-economic stratification. For instance, the deployment of facial recognition in Delhi reportedly resulted in disproportionately high targeting of Muslims during riot-related investigations (Santoshini, 2022) [16].

Globally, such concerns have been corroborated by empirical evidence. The American Civil Liberties Union (ACLU) documented several instances in the United States where Black individuals were wrongfully arrested due to flawed facial recognition matches (Wessler, 2024) [22]. While similar large-scale audits are unavailable in India, anecdotal patterns raise concerns about replicating these injustices domestically.

c. Opacity of AI and Due Process Violations

Most AI policing tools in India function as "black boxes"—their logic is proprietary, inaccessible, and unexplainable in court. This undermines the due process of law, as individuals are unable to challenge the reasoning behind their arrest or surveillance. The Supreme Court in *Puttaswamy v. Union of India* (2017) [9] emphasized that any invasion of privacy must pass the tests of legality, necessity, and proportionality. However, opaque AI tools rarely meet these standards when used without statutory authorization or judicial oversight (K.S. Puttaswamy v. Union of India, 2017) [9].

Further, in the ongoing Pegasus spyware case, the Supreme Court noted the state's obligation to inform affected individuals about surveillance, reiterating the need for transparency and accountability in digital policing (Pradhan, 2025) [14].

d. Empirical Instances of AI Misuse

Evidence from news reports and human rights organizations illustrates the growing misuse of AI tools in India. After the Delhi riots, media investigations revealed that over 2,000 arrests were made, many of which were allegedly based on CCTV footage processed by facial recognition software without independent verification (The Hindustan Times, 2022) [20]. While police claimed these tools reduced wrongful arrests, human rights groups warned that the systems lacked audit trails and risked misidentifying innocent civilians (Indian Express, 2023) [7].

In Uttar Pradesh, officials claimed that facial recognition helped in narrowing down suspects during anti-CAA protests. However, the absence of public oversight and third-party audits raises red flags about potential abuse (Ulmer, 2019) [21].

e. Legislative and Institutional Gaps

Despite these risks, there is no comprehensive legal framework in India that regulates the use of AI in law enforcement. The Ministry of Electronics and Information Technology (MeitY) has issued non-binding guidelines and advisories, but no binding legislation mandates transparency, accountability, or audit of AI systems in policing (Fazal, 2025) [6].

Moreover, police officers using these systems are rarely trained in data ethics or algorithmic limitations. Without mandatory ethical and legal training, reliance on automated tools can lead to over-policing, wrongful arrests, and erosion of public trust.

Doctrine of Command Responsibility and Indian Legal Context

a. Doctrinal Overview and Relevance to AI Policing

The doctrine of command responsibility, primarily established in international criminal law, holds superiors liable for the unlawful acts of their subordinates when they knew, or ought to have known, about the commission of such acts and failed to prevent them (Singh, 2016) [19]. Although not codified in Indian criminal law, Indian constitutional and administrative jurisprudence reflects similar principles, particularly in the context of state accountability for police misconduct.

The relevance of this doctrine to AI-driven policing lies in the fact that decisions made by automated systems are often enabled, approved, or ignored by supervisory officers. If such systems infringe upon rights or lead to wrongful arrests, the accountability should extend to those in command.

b. Judicial Interpretation of Supervisory Liability

In Nilabati Behera v. State of Orissa (1993) [10], the Supreme Court imposed liability on the state for custodial death, recognizing the failure of superior officers to safeguard constitutional rights (Nilabati Behera v. State of Orissa, 1993) [10]. This principle was expanded in D.K. Basu v. State of West Bengal (1997) [5], where the Court issued binding guidelines for arrest and detention, thereby establishing command-level responsibility for procedural compliance (D.K. Basu v. State of West Bengal, (1997) [5].

The same logic applies to AI-based law enforcement. If facial recognition or predictive tools are deployed without due oversight and lead to wrongful detention, the superior officer’s negligence in ensuring procedural safeguards must attract liability.

In Shiv Sagar Tiwari v. Union of India (1996) [18], the Court observed that bureaucratic hierarchies do not absolve senior officers from liability when their negligence facilitates subordinates' illegal actions (Shiv Sagar Tiwari v. Union of India, 1996) [18]. This forms a strong foundation for extending the doctrine of command responsibility to AI-enabled misconduct.

c. Surveillance Jurisprudence and Technological Accountability

In People’s Union for Civil Liberties (PUCL) v. Union of India (1997) [12], the Supreme Court struck down unregulated phone tapping and laid down procedural safeguards, affirming that the right to privacy extends to communications (PUCL v. Union of India, 1997). The rationale can be extended to digital surveillance technologies such as facial recognition, gait analysis, and social media monitoring.

Similarly, in R. Rajagopal v. State of Tamil Nadu (1994), the Court emphasized the individual's right to control personal information, a concept directly threatened by unregulated AI surveillance (Rajagopal v. State of Tamil Nadu, 1994) [15].

d. NHRC, Police Complaints Authorities, and Oversight Mechanisms

The National Human Rights Commission (NHRC), established under the Protection of Human Rights Act, 1993, plays a critical role in investigating rights violations, including custodial torture and illegal detention. NHRC data shows persistent patterns of police excesses, though specific oversight of AI-related abuse remains underdeveloped (NHRC, 2023) [11].

Following Prakash Singh v. Union of India (2006), the Supreme Court directed states to establish Police Complaints Authorities at state and district levels to address grievances against police officers. These bodies can potentially hear complaints related to wrongful actions stemming from AI tools (Commonwealth Human Rights Initiative, 2010) [4].

Despite these mechanisms, institutional oversight remains weak due to lack of awareness, enforcement, and legislative mandate to regulate AI systems. Capacity-building, legal reform, and judicial interpretation are needed to adapt existing institutions to new technological realities.

Conclusion and Suggestions

Artificial Intelligence in Indian policing offers efficiency, data-driven decision-making, and predictive capability. Yet, its unregulated use without legal safeguards poses serious threats to individual liberties, equality, and procedural fairness. The Indian legal system—anchored in Articles 20, 21, and 22 of the Constitution—places a high premium on human dignity, autonomy, and accountability. The doctrine of command responsibility, though originally rooted in military and international law, offers a compelling framework for ensuring that supervisory officers do not evade responsibility when AI tools under their watch cause harm.

From Nilabati Behera to Puttaswamy, the Indian judiciary has laid a rich foundation for state accountability and procedural safeguards. The use of AI in policing now requires these principles to be extended to a digital context. Failure to do so risks eroding public trust, deepening systemic biases, and undermining the rule of law.

Suggestions

1. **Statutory Regulation of AI in Policing:** Enact specific legislation regulating AI use in law enforcement. It should include guidelines for deployment, algorithmic explainability, third-party audits, and mandatory oversight mechanisms.

2. **Integration of Command Responsibility Doctrine:** Amend the Police Acts and BNSS to codify supervisory liability for misuse of AI tools by subordinates. Departmental rules should treat algorithmic abuse as serious misconduct.

3. **Algorithmic Transparency:** Police departments must maintain logs, explainability reports, and accuracy metrics for AI tools used in investigations or surveillance.

4. **Judicial and Institutional Oversight:** The NHRC and State Police Complaints Authorities should be empowered and trained to investigate complaints involving AI misuse. The Supreme Court can issue AI-specific guidelines akin to D.K. Basu.

5. **Capacity Building:** Incorporate AI ethics, data protection laws, and procedural safeguards into police training curricula. Officers must understand both the strengths and limits of AI tools.

With such reforms, India can ensure that the deployment of AI in policing enhances justice rather than undermines it, reaffirming constitutional values in the age of technology.

References

1. Anvar PV. v. P.K. Basheer, (2014) 10 SCC 473.
2. Bharatiya Nagarik Suraksha Sanhita, 2023 (India).
3. Bharatiya Sakshya Adhiniyam, 2023 (India).
4. Commonwealth Human Rights Initiative. Seven steps to police reform: Implementation of Supreme Court directives in Prakash Singh. CHRI, 2010.
5. Basu v DK. State of West Bengal, (1997) 1 SCC 416.
6. Fazal I. MeitY to present AI impact report to Parliamentary Committee on March 5. Storyboard18, 2025.
7. Indian Express. Racist, sexist, casteist: Is AI bad news for India? The Indian Express, 2023.
8. Information Technology Act, 2000 (India).
9. Puttaswamy v KS. Union of India, (2017) 10 SCC 1.
10. Nilabati Behera v. State of Orissa, (1993) 2 SCC 746.
11. National Human Rights Commission (NHRC). Annual Report 2022-2023. NHRC, Government of India, 2023.
12. People’s Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
13. Pol R, Karthik A. Can India’s new evidence act address the challenges posed by artificial intelligence? The Secretariat, 2024.
14. Pradhan B. “Nothing wrong in country using spyware”: Supreme Court on Pegasus row. Business Standard, 2025.
15. Rajagopal v R. State of Tamil Nadu, (1994) 6 SCC 632.
16. Santoshini S. Indian police use facial recognition to persecute Muslims and other marginalized communities. Coda Story, 2022.
17. Selvi v. State of Karnataka, (2010) 7 SCC 263.
18. Shiv Sagar Tiwari v. Union of India, (1996) 6 SCC 558.
19. Singh A. Command responsibility in international criminal law: India’s perspective. Indian Law Review,2016:8(2):130–145.
20. The Hindustan Times. 2 yrs after Delhi riots: 2,456 held, 2 convicted, 2022.
21. Ulmer A. India’s use of facial recognition tech during protests causes stir. Reuters, 2019.
22. Wessler NF. Police say a simple warning will prevent face recognition wrongful arrests. American Civil Liberties Union, 2024.