INDEPENDENT OVERSIGHT IN BIOMETRIC GOVERNANCE: A MISSING LINK IN INDIAN CRIMINAL PROCEDURE

Abdus Sami Osman Chaus, Yashwantrao Chavan Law College & Ph.D. Research Centre, Pune

ABSTRACT

The increasing reliance on biometric technologies in criminal investigation has significantly expanded the scope of State power over the individual. The Criminal Procedure (Identification) Act, 2022 institutionalises large-scale collection, storage, and retention of biometric and biological data within the Indian criminal justice system. While the legislation aims to modernise investigation and enhance forensic capacity, it provides limited mechanisms for independent oversight or accountability. This raises serious constitutional and institutional concerns in a democratic system committed to the rule of law.

This article examines the oversight architecture of the Criminal Procedure (Identification) Act, 2022 through the lens of constitutional principles, particularly Articles 14 and 21 of the Constitution of India. It argues that internal executive supervision is insufficient to regulate data-intensive and intrusive biometric practices. Drawing upon Supreme Court jurisprudence, administrative-law principles, and comparative models from jurisdictions such as the United Kingdom and the European Union, the article demonstrates that independent oversight bodies are central to rights-based biometric governance.

The article contends that the absence of an independent supervisory authority constitutes a structural deficiency in India's biometric framework. It proposes that an oversight authority with supervisory, audit, and grievance-redressal functions would enhance transparency, protect fundamental rights, and strengthen public trust without undermining investigative efficiency. The article concludes that independent oversight is not merely a policy choice but a constitutional necessity for ensuring that biometric governance operates within the limits of legality, proportionality, and democratic accountability.

Keywords: Biometric Governance; Criminal Procedure (Identification) Act, 2022; Independent Oversight; Data Protection; Criminal Justice Administration; Privacy and Accountability; Rule of Law; Surveillance Regulation; Human Rights.

This article is an outcome of independent doctrinal and comparative research and forms part of the author's doctoral study on biometric identification, criminal procedure, and human rights. The views expressed are purely academic and personal.

I. Introduction: Biometric Power and the Problem of Accountability

The modern criminal justice system increasingly relies on scientific and technological tools to enhance the accuracy and efficiency of investigation. Among these tools, biometric identification occupies a central position, offering the State unprecedented capacity to identify, track, and categorise individuals. Fingerprints, facial recognition, iris scans, and DNA profiles have become integral to contemporary policing practices, reshaping the evidentiary landscape of criminal procedure.[1] While such technologies promise improved investigative outcomes, they also concentrate significant power in the hands of law-enforcement agencies.

The Criminal Procedure (Identification) Act, 2022 represents India's most comprehensive legislative effort to institutionalise biometric identification within criminal procedure.[2] By expanding the scope of permissible "measurements" and establishing a centralised database maintained by the National Crime Records Bureau, the Act enables large-scale collection and long-term retention of biometric data. The legislation is premised on the assumption that technological modernisation will strengthen investigation and deter crime. However, the Act simultaneously raises pressing questions concerning accountability, transparency, and control over the exercise of biometric power.

A defining feature of biometric systems is their invisibility. Unlike traditional coercive practices, biometric governance does not operate through overt force or visible intrusion alone. Its impact lies in data accumulation, algorithmic processing, and long-term storage—processes that are often opaque to the individuals affected. Once biometric data enters State databases, the individual typically loses control over how, when, and for what purpose the data is used. This asymmetry of power between the State and the individual renders oversight mechanisms constitutionally significant.

In constitutional democracies, the expansion of State power is ordinarily accompanied by

[1] David Lyon, *Surveillance Studies* (Polity Press, 2007) 1–10.
[2] The Criminal Procedure (Identification) Act, 2022, ss. 2, 3, 4.

corresponding safeguards.[3] Judicial review, legislative scrutiny, and independent regulatory bodies function as checks against arbitrariness and abuse. In areas involving surveillance, data processing, and deprivation of liberty, independent oversight plays a particularly vital role.[4] It ensures that discretionary powers are exercised within legal bounds and that rights violations are detected and remedied. The absence of such oversight risks transforming efficiency-driven governance into unchecked authority.

The Criminal Procedure (Identification) Act, 2022, however, largely entrusts oversight of biometric collection and data management to executive agencies themselves. While the Act and the Rules prescribe certain procedural conditions, they do not establish an independent supervisory authority with the power to audit practices, adjudicate grievances, or enforce compliance. Oversight is thus internal rather than external, administrative rather than independent. This design choice distinguishes the Indian framework from many international biometric and data-protection regimes, where independent regulators serve as institutional guardians of rights.

The lack of independent oversight becomes especially problematic given the breadth of the Act. Biometric data may be collected not only from convicted persons but also from undertrials and other categories of individuals who continue to enjoy the presumption of innocence.[5] The long retention periods authorised under the Act further amplify the potential for misuse, error, or function creep. Without an independent body to monitor retention, access, and deletion, individuals have limited recourse against arbitrary or disproportionate data practices.

This article argues that independent oversight is the missing institutional link in India's biometric governance under criminal procedure. It contends that the legitimacy of biometric identification does not depend solely on statutory authorisation, but on the presence of robust accountability mechanisms that operate independently of investigative agencies. By examining constitutional principles, comparative models, and the functional role of oversight institutions, the article seeks to demonstrate that independent supervision is not antithetical to effective investigation. On the contrary, it is essential to maintaining public trust, protecting fundamental rights, and ensuring that technological power remains subordinate to the rule of law.

[3] A.V. Dicey, *Introduction to the Study of the Law of the Constitution* (Macmillan, 10th ed., 1959) 188–193.
[4] National Law University Delhi, "Biometrics, Surveillance and the Law", *available at* https://www.nludelhi.ac.in (last visited on 15/12/2025).
[5] *Narendra Singh v. State of M.P., (2004) 10 SCC 699*.

II. Oversight and Accountability in Criminal Procedure: Constitutional Foundations

The concept of oversight occupies a central position in constitutional governance, particularly in areas where the State exercises coercive or intrusive powers. In criminal procedure, oversight functions as a safeguard against arbitrariness, excess, and misuse of authority. The Constitution of India, while not explicitly mandating oversight bodies in every context, embeds the principle of accountability within its guarantees of equality, personal liberty, and due process.[6] The expansion of biometric identification under the Criminal Procedure (Identification) Act, 2022 must therefore be examined against this constitutional backdrop.

Article 14 of the Constitution prohibits arbitrary State action and requires that discretionary powers be exercised in a non-discriminatory and reasonable manner. The Supreme Court has consistently held that uncanalised or unchecked discretion is antithetical to the rule of law.[7] When criminal procedure confers broad powers upon investigating agencies—particularly powers involving bodily intrusion and data collection—the absence of external oversight heightens the risk of arbitrary application. Biometric governance, by its very nature, involves discretion at multiple stages: selection of individuals for data collection, choice of measurements, duration of retention, and access or sharing of data. Without independent supervision, such discretion remains largely invisible and insulated from meaningful review.

Article 21 further reinforces the need for accountability by requiring that any procedure affecting life or personal liberty be "just, fair, and reasonable."[8] Judicial interpretation has clarified that fairness under Article 21 is not confined to the text of the law but extends to its implementation. Procedural safeguards must operate in practice, not merely on paper. Oversight mechanisms serve precisely this function: they translate abstract constitutional guarantees into enforceable standards by monitoring compliance, addressing grievances, and correcting institutional failures.

The judiciary has repeatedly underscored the importance of independent oversight in contexts involving surveillance, custodial power, and deprivation of liberty. In *People's Union for Civil Liberties v. Union of India*, the Supreme Court recognised that unchecked surveillance powers threaten democratic freedoms and emphasised the need for procedural safeguards to prevent

[6] Dicey, *supra* note 3, at 188–193.
[7] *E.P. Royappa v. State of Tamil Nadu*, (1974) 4 SCC 3.
[8] *Maneka Gandhi v. Union of India,* AIR 1978 SC 597.

abuse.[9] Similarly, in *D.K. Basu v. State of West Bengal*, the Court laid down detailed guidelines to curb custodial excesses, effectively creating an oversight framework through judicial intervention.[10] These cases illustrate a broader constitutional principle: where the potential for abuse is high, independent checks become constitutionally necessary.

Biometric data collection under the 2022 Act presents analogous risks. The extraction and retention of biometric data implicate bodily integrity, informational privacy, and dignity. Yet, the Act largely relies on internal administrative control exercised by the same agencies responsible for investigation. Such internal oversight lacks the independence required to inspire public confidence or ensure impartial accountability. As comparative experience demonstrates, self-regulation by enforcement agencies is often inadequate to prevent misuse, particularly in data-intensive systems.[11]

From a constitutional perspective, oversight is not merely a corrective mechanism but a legitimacy-enhancing institution. Independent supervisory bodies reduce the likelihood of rights violations while simultaneously strengthening the credibility of enforcement practices. By providing avenues for audit, complaint redressal, and transparency, oversight institutions help reconcile efficiency with constitutional restraint. The absence of such mechanisms under the Criminal Procedure (Identification) Act thus creates a structural imbalance between power and accountability.

Scholarly commentary has increasingly emphasised that data-driven governance requires regulatory architectures distinct from traditional command-and-control models.[12] In the absence of an independent authority to oversee biometric practices, individuals affected by data collection are left with limited remedies, often requiring them to approach courts—a process that is costly, time-consuming, and inaccessible for many. Oversight bodies, by contrast, offer preventive and remedial functions that operate continuously rather than episodically.

Therefore, the constitutional foundations of criminal procedure strongly support the establishment of independent oversight mechanisms in biometric governance. Articles 14 and 21, read together, demand not only lawful authority but accountable exercise of power. In a legal regime that permits extensive biometric collection and long-term data retention, oversight

[9] *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.
[10] *D.K. Basu v. State of West Bengal*, (1997) 1 SCC 416.
[11] Christopher Slobogin, *Privacy at Risk* (University of Chicago Press, 2007) 142–148.
[12] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books, 2019) 94–101.

is not a discretionary policy choice but a constitutional necessity. Without it, the promise of fairness and dignity risks being subordinated to administrative convenience and technological efficiency.

III. The Criminal Procedure (Identification) Act, 2022 and the Oversight Deficit

The Criminal Procedure (Identification) Act, 2022 constitutes a comprehensive legislative framework governing the collection, storage, and use of biometric and biological data in the criminal justice system. Enacted with the stated objective of modernising investigation and enhancing forensic capacity, the Act significantly expands the scope of permissible "measurements" and the categories of individuals from whom such data may be collected.[13] While the legislation provides statutory authority for biometric practices, it reveals a conspicuous deficit in independent oversight mechanisms—an omission with serious constitutional and institutional implications.

At the structural level, the Act centralises biometric data management under the National Crime Records Bureau (NCRB), which is empowered to collect, store, preserve, and share data with law-enforcement agencies.[14] The Rules framed under the Act further elaborate procedural aspects but do not create any independent supervisory body to regulate data practices. Oversight functions—such as determining necessity, monitoring retention, authorising sharing, or ensuring deletion—are largely entrusted to executive authorities themselves. This design effectively collapses the distinction between the collector, custodian, and regulator of biometric data.

Such an arrangement raises concerns about conflict of interest and accountability. Oversight that remains internal to the enforcement apparatus lacks the independence required to ensure impartial scrutiny. In administrative law, it is well recognised that effective oversight must be structurally separated from the entity being regulated.[15] The absence of this separation under the Act means that grievances relating to misuse, over-collection, or wrongful retention of biometric data have no specialised institutional forum for redress.

The breadth of discretion conferred by the Act exacerbates this problem. Section 3 authorises

[13] Statement of Objects and Reasons, Criminal Procedure (Identification) Bill, 2022.
[14] The Criminal Procedure (Identification) Act, 2022, ss. 2(1)(j), 4; Criminal Procedure (Identification) Rules, 2022.
[15] Wade & Forsyth, *Administrative Law* (Oxford University Press, 11th ed., 2014) 258–262.

the collection of biometric data from a wide range of individuals, including undertrials and persons detained under preventive laws.[16] Section 4 permits long-term retention of such data, subject to limited exceptions. The Act does not mandate periodic review of retained data, nor does it require automatic deletion upon acquittal or discharge. In the absence of an independent authority to oversee these processes, discretion operates largely unchecked.

Parliamentary debates surrounding the enactment of the legislation reflect concerns regarding privacy, misuse, and lack of safeguards. Several Members of Parliament expressed apprehension about the concentration of biometric data and the potential for abuse in the absence of independent oversight.[17] Despite these concerns, the final legislative framework did not incorporate an oversight body analogous to data protection authorities or surveillance review boards found in other jurisdictions. The omission appears particularly striking given the contemporaneous recognition of privacy as a fundamental right by the Supreme Court.

From a comparative standpoint, biometric governance frameworks in democratic jurisdictions frequently incorporate independent supervisory institutions. In the United Kingdom, for instance, the retention and use of biometric data are subject to oversight by designated commissioners and review bodies.[18] At the European Union level, data protection authorities function as independent regulators with powers to audit, investigate, and sanction misuse.[19] These institutions serve not merely as remedial bodies but as preventive mechanisms that ensure compliance before rights violations occur.

The Indian framework, by contrast, relies primarily on post facto judicial remedies. While courts undoubtedly play a crucial role in constitutional enforcement, judicial review is episodic and reactive. It is ill-suited to address routine administrative practices involving large-scale data processing. Expecting individuals to approach constitutional courts for every instance of biometric misuse places an unrealistic burden on access to justice and undermines the effectiveness of rights protection.[20]

The oversight deficit is further aggravated by the opacity surrounding biometric data practices.

[16] The Criminal Procedure (Identification) Act, 2022, s. 3.
[17] Rajya Sabha Debates, Criminal Procedure (Identification) Bill, 2022.
[18] Protection of Freedoms Act 2012 (UK); Biometrics Commissioner, *available at* https://www.legislation.gov.uk/ukpga/2012/9/contents (last visited on 09/01/2026).
[19] General Data Protection Regulation (EU) 2016/679, arts. 51–59.
[20] Marc Galanter, "Why the Haves Come Out Ahead", (1974) 9 *Law & Society Review* 95.

Individuals whose data is collected often lack clear information regarding retention periods, sharing protocols, or avenues for complaint. The Act and Rules do not impose robust transparency obligations on data custodians, nor do they provide individuals with enforceable rights to access, correct, or delete their data. In the absence of an independent authority to enforce such rights, informational asymmetry becomes entrenched.

Importantly, the absence of independent oversight also undermines the legitimacy of the biometric regime itself. Public trust in criminal justice institutions depends not only on effectiveness but on perceived fairness and accountability. Oversight bodies enhance legitimacy by signalling that State power is subject to continuous scrutiny. Their absence risks fostering suspicion and resistance, potentially weakening cooperation with law-enforcement efforts.

In sum, the Criminal Procedure (Identification) Act, 2022 establishes an expansive biometric governance framework without a corresponding accountability architecture. This imbalance between power and oversight represents a structural flaw rather than a mere procedural gap. Addressing this deficit is essential not only for safeguarding fundamental rights but for ensuring that biometric technologies operate within a constitutionally sustainable and democratically legitimate framework.

IV. Comparative Models of Independent Oversight in Biometric Governance

Comparative constitutional practice demonstrates that democratic legal systems addressing biometric identification and surveillance have increasingly recognised the necessity of independent oversight institutions. These mechanisms do not merely regulate data processing in the abstract but function as specialised bodies that supervise the collection, retention, sharing, and deletion of biometric data. Examining such models provides valuable insight into how accountability can be structurally embedded within biometric governance frameworks without undermining investigative effectiveness.

A. United Kingdom: Specialised Commissioners and Statutory Oversight

The United Kingdom offers a prominent example of institutionalised oversight in biometric governance. Following judicial scrutiny of biometric retention practices, particularly in *S. and Marper v. United Kingdom*, Parliament enacted the Protection of Freedoms Act 2012, which

introduced comprehensive safeguards governing biometric data.[21] Central to this framework is the office of the Biometrics Commissioner, an independent statutory authority tasked with overseeing the retention and use of fingerprints and DNA profiles by law-enforcement agencies.

The Biometrics Commissioner exercises powers to review police decisions, issue guidance, and require justification for continued retention of biometric material. Importantly, the Commissioner operates independently of investigative agencies and reports directly to Parliament, ensuring transparency and democratic accountability.[22] This model reflects an understanding that oversight must be external to enforcement structures to be effective. By providing an accessible institutional forum for review, the UK framework reduces reliance on courts as the sole avenue for redress.[23]

B. European Union: Data Protection Authorities as Rights Guardians

At the European Union level, biometric governance is regulated through a robust data protection framework under the General Data Protection Regulation (GDPR). While the GDPR applies broadly to personal data, it contains specific provisions governing biometric data as a "special category" requiring heightened protection.[24] Oversight is entrusted to independent Data Protection Authorities (DPAs) established in each Member State, vested with powers to monitor compliance, investigate violations, impose penalties, and provide remedies to individuals.

The independence of DPAs is constitutionally and legally safeguarded, reflecting the EU's recognition that effective data governance requires regulators insulated from political or executive influence.[25] In the context of law enforcement, supplementary instruments such as the Law Enforcement Directive further reinforce oversight obligations. The presence of dedicated supervisory authorities ensures continuous regulation of biometric practices rather than ad hoc intervention after violations occur.

[21] *S. and Marper v. United Kingdom*, (2008) 48 EHRR 50.
[22] Protection of Freedoms Act 2012 (UK); Office of the Biometrics Commissioner, "Home Page", *available at* https://www.legislation.gov.uk/ukpga/2012/9/contents (last visited on 15/12/2025).
[23] UK Information Commissioner's Office, "Biometrics and Data Protection", available at https://ico.org.uk (last visited on 11/12/2025).
[24] GDPR, *supra* note 19, art. 9.
[25] Regulation (EU) 2016/679 (General Data Protection Regulation), arts. 51–54; European Data Protection Board, *available at* https://edpb.europa.eu, (last visited on 19/12/2025).

C. Judicial Oversight and Hybrid Models

Some jurisdictions adopt hybrid oversight models combining administrative supervision with judicial authorisation. For example, certain biometric measures—particularly those involving intrusive data collection or extended retention—require prior approval from judicial or quasi-judicial bodies.[26] This layered approach recognises that different stages of biometric governance may warrant different forms of scrutiny.[27] Judicial oversight acts as a gatekeeping mechanism, while administrative bodies provide ongoing supervision and enforcement.

Such hybrid models underscore an important principle: oversight need not be monolithic. What matters is the presence of independent checks that constrain discretion, ensure proportionality, and provide remedies. These models also demonstrate that oversight can coexist with efficient investigation, countering arguments that external supervision necessarily hampers law-enforcement effectiveness.

D. Lessons for the Indian Context

The comparative experience reveals several lessons relevant to India's biometric governance under the Criminal Procedure (Identification) Act, 2022. First, oversight institutions enhance legitimacy by making data practices visible and contestable. Second, independence is essential; internal administrative control lacks the credibility and impartiality required to protect rights effectively. Third, oversight bodies perform preventive functions by guiding practice and correcting deviations before they escalate into systemic abuses.

In contrast to these models, the Indian framework lacks a dedicated authority empowered to supervise biometric practices in criminal procedure. While constitutional courts remain available as forums for challenge, comparative experience suggests that reliance on judicial review alone is insufficient in data-intensive regimes. Oversight institutions serve as intermediaries between individuals and the State, translating constitutional principles into operational standards.

Importantly, comparative models also demonstrate that oversight need not undermine sovereignty or investigative autonomy. Rather, it strengthens governance by aligning

[26] Council of Europe, "Biometrics and Human Rights", *available at* https://www.coe.int (last visited on 29/12/2025).
[27] Slobogin, *supra* note 11, at 155–162.

technological power with constitutional restraint. Adapting such institutional mechanisms to the Indian context would not require wholesale transplantation but contextual design informed by constitutional values and administrative realities.

V. The Case for an Independent Oversight Authority in India: Design, Functions, and Safeguards

The preceding analysis demonstrates that the absence of independent oversight under the Criminal Procedure (Identification) Act, 2022 is not an incidental omission but a structural weakness with significant constitutional implications.[28] This section argues that the establishment of an independent oversight authority is both normatively justified and institutionally feasible within the Indian constitutional framework. Such an authority would not displace investigative agencies or judicial review; rather, it would complement existing mechanisms by providing continuous, specialised supervision over biometric governance.

A. Constitutional Justification for an Oversight Authority

The constitutional basis for an independent oversight authority can be traced to Articles 14 and 21 of the Constitution of India. Article 14 requires that discretionary State power be exercised in a non-arbitrary manner, while Article 21 mandates that procedures affecting personal liberty be fair, just, and reasonable.[29] Where a statutory framework confers wide discretion to collect, retain, and share biometric data, constitutional fidelity demands the presence of institutional checks capable of preventing abuse and correcting error.

Judicial precedent supports this understanding. In *Maneka Gandhi v. Union of India*, the Supreme Court clarified that fairness under Article 21 extends to the manner in which power is exercised, not merely to the existence of legal authority.[30] Similarly, in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Court emphasised the need for safeguards, oversight, and accountability when State action intrudes upon privacy.[31] These principles apply with equal force to biometric data practices under criminal procedure.

[28] Internet Freedom Foundation, "Explainer: Criminal Procedure (Identification) Act, 2022", *available at* https://internetfreedom.in (last visited on 15/12/2025).
[29] *Royappa*, *supra* note 7; Constitution of India, arts. 14, 21.
[30] *Maneka Gandhi*, *supra* note 8.
[31] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

B. Core Functions of an Oversight Authority

An independent oversight authority in the context of biometric governance would perform several interrelated functions. First, it would exercise supervisory oversight by monitoring compliance with statutory and procedural requirements governing biometric collection and retention. This includes reviewing whether data collection is necessary and proportionate in specific categories of cases.

Second, the authority would serve a grievance redressal function, providing individuals with an accessible forum to challenge misuse, over-collection, or unlawful retention of biometric data. Such a mechanism would reduce the burden on constitutional courts and enhance access to justice, particularly for individuals lacking the resources to pursue prolonged litigation.[32]

Third, the authority would undertake audit and advisory functions, issuing periodic reports, guidelines, and recommendations to improve compliance and transparency. These preventive functions are essential in data-intensive systems, where harms often arise from systemic practices rather than isolated violations.

C. Institutional Design and Independence

For oversight to be meaningful, institutional independence is paramount. The authority must be structurally insulated from investigative agencies and executive influence. Comparative experience suggests that independence can be ensured through statutory guarantees relating to appointment procedures, tenure security, and functional autonomy.[33] Reporting obligations to Parliament, rather than to executive departments, further enhance democratic accountability.

Importantly, independence does not imply hostility towards law enforcement. Oversight bodies function most effectively when they engage constructively with enforcement agencies, offering guidance and corrective feedback rather than punitive control. This cooperative model preserves investigative efficiency while embedding constitutional restraint.

D. Scope of Authority and Safeguards

The oversight authority's jurisdiction should extend to all stages of biometric governance,

[32] Galanter, *supra* note 20.
[33] Protection of Freedoms Act 2012 (UK), *supra* note 22.

including collection, storage, sharing, and deletion of data. However, its powers must be carefully calibrated to avoid overreach. Judicial authorisation may remain appropriate for particularly intrusive measures, while routine oversight functions can be discharged administratively.

Safeguards against misuse of oversight power are equally important. Transparency requirements, reasoned decision-making, and judicial review of the authority's actions would ensure that oversight itself remains accountable.[34] This layered approach aligns with constitutional principles and mitigates concerns about bureaucratic overregulation.

E. Alignment with Emerging Data Protection Norms

The case for independent oversight is further strengthened by India's evolving data protection landscape. Committee reports and policy documents have consistently emphasised the need for independent regulators to govern data practices.[35] While criminal procedure presents unique considerations, these broader norms underscore a growing consensus that data-intensive governance requires specialised institutional supervision.

F. Normative Assessment

Establishing an independent oversight authority would recalibrate the balance between investigative efficiency and individual rights under the Criminal Procedure (Identification) Act, 2022. Rather than impeding law enforcement, such an authority would enhance legitimacy, reduce litigation, and foster public trust. In a constitutional democracy committed to the rule of law, oversight is not a concession but a constitutional imperative.

VI. Conclusion: Oversight as a Constitutional Necessity in Biometric Governance

The integration of biometric technologies into criminal procedure represents a profound shift in the architecture of State power. The Criminal Procedure (Identification) Act, 2022 reflects the State's attempt to modernise investigative practices by leveraging scientific and technological tools. While such modernisation may serve legitimate objectives of efficiency

[34] Wade & Forsyth, *supra* note 15, at 274–280.
[35] Justice B.N. Srikrishna Committee, "Report on Data Protection Framework for India" (2018), *available at* https://www.meity.gov.in; https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy (last visited on 15/12/2025).

and accuracy, its constitutional legitimacy ultimately depends on the presence of effective accountability mechanisms capable of restraining excess and preventing misuse.[36]

This article has argued that the absence of an independent oversight authority under the 2022 Act constitutes a critical institutional deficiency. By concentrating powers of collection, retention, and dissemination of biometric data within executive agencies, the existing framework creates an imbalance between technological capability and constitutional control. In a system where biometric data is enduring, reusable, and informationally rich, internal administrative supervision is insufficient to safeguard fundamental rights.

Constitutional principles embedded in Articles 14 and 21 demand that intrusive State powers be exercised within a framework that is fair, reasonable, and non-arbitrary. Judicial precedent has consistently recognised that unchecked discretion undermines the rule of law, particularly in domains involving surveillance, bodily intrusion, and deprivation of liberty.[37] Biometric governance under criminal procedure squarely implicates these concerns, making independent oversight not merely desirable but constitutionally necessary.[38]

Comparative experience reinforces this conclusion. Democratic jurisdictions confronting similar challenges have responded by establishing specialised oversight bodies tasked with supervising biometric practices, auditing compliance, and providing remedies to affected individuals. These institutions enhance legitimacy without compromising investigative effectiveness, demonstrating that oversight and efficiency are not mutually exclusive but mutually reinforcing.[39]

The establishment of an independent oversight authority in India would serve multiple constitutional functions. It would operationalise the safeguards mandated by privacy and dignity jurisprudence, provide accessible grievance redressal, reduce the burden on constitutional courts, and foster public trust in biometric systems.[40] Equally important, it would signal a commitment to rights-based governance in an era of rapidly expanding technological power.

Ultimately, the challenge posed by biometric identification is not technological but

[36] *Maneka Gandhi*, *supra* note 8.
[37] *Puttaswamy*, *supra* note 31.
[38] *PUCL*, *supra* note 9.
[39] Protection of Freedoms Act 2012 (UK), *supra* note 22.
[40] Srikrishna Committee, *supra* note 35, at 13.

constitutional. The question is not whether the State may use modern tools to investigate crime, but how such tools are governed within a constitutional democracy.[41] Independent oversight offers a principled and practical answer. By embedding accountability into biometric governance, the criminal justice system can harness technological innovation while remaining faithful to the Constitution's enduring commitment to liberty, dignity, and the rule of law.

[41] Wade & Forsyth, *supra* note 15, at 258–280.