Educational Administration: Theory and Practice
2024, 30(4), 11210-11216
ISSN: 2148-2403
https://kuey.net/

Educational Administration Theory and Practice

Research Article

A Critical Study of Biometric Surveillance Laws in India and the Implications of the Criminal Identification Act 2022 In the Age of Digital Governance

Aakanksha Mishra[1*] and Dr. Pradip Kumar Kashyap[2]

[1*]Research Scholar, School of Law, Raffles University, Neemrana
[2]Assistant Professor of Law, School of Law, Raffles University, Neemrana

Citation: Aakanksha Mishra et al, (2024). A Critical Study of Biometric Surveillance Laws in India and the Implications of the Criminal Identification Act 2022 In the Age of Digital Governance, *Educational Administration: Theory and Practice*, 30(4), *11210-11216*
Doi: 10.53555/kuey.v30i4.9894

ARTICLE INFO	ABSTRACT

The increasing integration of biometric technologies into public administration has transformed the landscape of governance and surveillance in India. This study critically explores the legal, ethical, and policy implications of biometric surveillance laws, with particular focus on the Criminal Identification Act, 2022. Positioned within the broader context of digital governance, the research seeks to understand how the collection, storage, and use of biometric data by law enforcement agencies intersect with constitutional rights, data privacy principles, and emerging technological risks. The study begins by examining the historical evolution of biometric surveillance and its relevance in contemporary digital governance frameworks. It explores how biometric systems—such as facial recognition, iris scans, and fingerprinting—have been increasingly deployed for crime control, public safety, and identity verification.

The analysis further delves into the existing legal and regulatory structures governing biometric data in India, including the Aadhaar framework, the Information Technology Act, and draft data protection legislations. A comparative review of global standards is also undertaken to assess India's alignment with international human rights norms. A major component of the research is a detailed critique of the Criminal Identification Act, 2022, including its expanded scope for collecting physical and biological samples, the absence of robust data protection mechanisms, and its compatibility with the right to privacy as laid down in the Puttaswamy judgment. The study also addresses ethical concerns surrounding consent, potential misuse of surveillance technologies, and the lack of accountability in data handling. This includes recommendations for a more transparent, accountable, and rights-based approach to biometric governance in India. The study concludes that while biometric systems can enhance efficiency, they must be balanced with adequate legal safeguards to protect individual freedoms in a democratic society.

Keywords: Biometrics, Surveillance, Governance, Legislation, Privacy.

INTRODUCTION TO BIOMETRIC SURVEILLANCE AND DIGITAL GOVERNANCE

The global proliferation of biometric surveillance technologies represents one of the most profound developments in modern governance. From iris scans and facial recognition to voiceprints and gait analysis, biometric technologies have revolutionized identity verification and control mechanisms in both public and private domains.

In India, this transformation has been marked by a strong governmental push toward digital governance—most notably through initiatives like *Digital India* and the *Aadhaar* biometric identification system. With over 1.3 billion citizens enrolled in Aadhaar as of 2022, India operates the world's largest biometric database.[1] This

[1] "Aadhaar Identification Program: Providing Proof of Identity to a Billion," *The Reach Alliance available at*: https://reachalliance.org/case-study/aadhaar-identification-program-providing-proof-of-identity-to-a-billion/ (last visited April 04, 2024).

unprecedented scale brings with it immense potential for administrative efficiency, but also substantial legal, ethical, and human rights challenges.

The biometric technology, initially developed for secure access and criminal identification, has evolved into a multifaceted surveillance tool. While earlier uses were largely confined to forensic applications—such as fingerprint analysis in criminal cases—the integration of biometric systems into civil registration, social welfare, law enforcement, and public health has rapidly expanded. The COVID-19 pandemic further accelerated the adoption of contactless biometric systems, including facial recognition and thermal imaging, as a public health surveillance measure.[2]

In the Indian context, biometrics play a central role in governance and law enforcement. Police departments across states increasingly rely on facial recognition software, such as the National AFRS, for tracking suspects and locating missing persons. However, there is a critical gap in data protection. A IFF report 2022 revealed that out of 42 facial recognition systems deployed or being developed in India, only a few had privacy policies or legal oversight mechanisms.[3] This raises concerns under Art. 21 of the Indian Constitution, which guarantees the right to life and personal liberty—including the right to privacy, as affirmed in *Justice K.S. Puttaswamy v. Union of India*.[4]

The Act, 2022 marked a turning point in India's biometric surveillance regime. It expanded the scope of biometric data collection far beyond what was permitted under the Identification of Prisoners Act, 1920. The Act 2022 authorizes police to collect biological samples, retina and iris scans, and behavioral attributes from individuals—including those under preventive detention and even from those not yet formally charged with an offense. The absence of judicial oversight and limitations on data retention, combined with ambiguous language, has raised constitutional red flags.[5] The law also lacks a clear consent mechanism and contravenes global standards such as the EU's GDPR, which mandates explicit, informed consent for data collection and usage.

In contrast, countries like the UK and Germany have established strong legal frameworks that limit the scope of biometric surveillance. For instance, in *S. and Marper v. United Kingdom*[6], the ECHR ruled that the indefinite retention of biometric data of individuals not convicted of crimes violates ECHR.[7] India's digital governance trajectory is thus marked by a paradox: while embracing cutting-edge technologies for efficiency and modernization, it lacks robust legal frameworks to regulate them. As biometric surveillance becomes more embedded in governance, a rights-based, transparent, and accountable system is urgently required.

LEGAL AND REGULATORY FRAMEWORK GOVERNING BIOMETRIC SURVEILLANCE IN INDIA

The legal and regulatory framework governing biometric surveillance in India is currently at a critical crossroads. While biometric data collection has become a cornerstone of digital governance, particularly through projects like Aadhaar, the legal safeguards regulating its use remain fragmented, underdeveloped, and often outdated. The absence of a comprehensive data protection regime further amplifies concerns regarding the potential misuse of biometric information, posing risks to individual privacy, bodily autonomy, and fundamental rights.

At the national level, the primary legal instrument facilitating biometric data collection is the Aadhaar Act, 2016. The Aadhaar system assigns a unique 12-digit identification number to residents of India, based on their biometric and demographic data. As of March 2022, over 1.32 billion Aadhaar numbers had been issued, covering approximately 99% of India's adult population.[8] However, despite the system's scale, the Aadhaar Act does not provide detailed guidelines on data retention, third-party access, or grievance redressal mechanisms. Moreover, the Supreme Court in *Justice K.S. Puttaswamy v. Union of India*[9] upheld the constitutional validity

[2] F. L. Cabanillas et al., "Do biometric payment systems work during the COVID-19 pandemic? Insights from the Spanish users' viewpoint," 8 *Financial Innovation* 22 (2022).

[3] "Privacy marked absent? IFF writes to government departments against their use of Aadhaar biometric and facial recognition enabled attendance systems," *Internet Freedom Foundation*, 2024 *available at*: https://internetfreedom.in/privacy-marked-absent/ (last visited April 04, 2024).

[4] (2017) 10 SCC 1.

[5] B. E. S. Matthew C., "The Incompatibility of Substantive Canons and Textualism" *Harvard Law Review*, 2023 *available at*: https://harvardlawreview.org/print/vol-137/the-incompatibility-of-substantive-canons-and-textualism/ (last visited April 04, 2024).

[6] [2008] ECHR 1581.

[7] ECHR 1953, art. 8.

[8] "Approximately 99 pc adult population has been enrolled in Aadhaar: UIDAI CEO," *Unique Identification Authority of India | Government of India available at*: https://uidai.gov.in/en/media-resources/media/aadhaar-telecast/13708-approximately-99-pc-adult-population-has-been-enrolled-in-aadhaar-uidai-ceo.html (last visited April 04, 2024).

[9] *Id.* at 4.

of Aadhaar but struck down provisions allowing private entities to access Aadhaar data, reinforcing the need for proportionality and purpose limitation in biometric data usage.

The IT Act, 2000, and its associated rules, such as the IT Rules, 2011, provide some level of protection. These rules categorize biometric data as "*sensitive personal data*" and prescribe consent and data protection requirements. However, enforcement remains weak, and the provisions do not apply to government entities, creating a significant regulatory blind spot.

The Act, 2022, represents a significant shift in India's surveillance architecture. Replacing the colonial-era Identification of Prisoners Act, 1920, the new law authorizes law enforcement agencies to collect, store, and analyze biometric and behavioral data—including fingerprints, palm prints, iris and retina scans, and even handwriting and voice samples—of convicted, arrested, and even preventive detainees. Notably, the Act lacks explicit provisions for consent, oversight, or data minimization. It permits retention of data for up to 75 years and leaves the door open for integration with national and global criminal databases. The civil liberties groups have raised alarms over its potential to violate Art. 14, 19, and 21 of the Constitution, particularly in the absence of a data protection law.[10]

In contrast, international legal frameworks offer more robust safeguards. The EU's GDPR is widely considered the gold standard in data privacy law. It mandates explicit consent for biometric data processing, grants individuals the right to be forgotten, and imposes heavy penalties for violations. The GDPR recognizes biometric data as a special category requiring heightened protection.[11] Similarly, Canada's PIPEDA and Australia's Privacy Act 1988 include biometric data under the definition of sensitive personal information and impose strict conditions on its collection and use. India's lack of a comprehensive personal data protection law, despite the publication of the DPDP Act, 2023, leaves biometric governance in a legal vacuum. While the new Act introduces principles of consent, purpose limitation, and data fiduciary accountability, it still excludes national security and law enforcement agencies from many of its purview—further deepening the challenge of creating an equitable regulatory ecosystem.

THE CRIMINAL IDENTIFICATION ACT 2022 AND ITS LEGAL IMPLICATIONS

The *Act, 2022*, enacted by the Indian Parliament, signifies a watershed moment in India's biometric surveillance regime, replacing the archaic *Identification of Prisoners Act, 1920*. With its expansive scope, this law has sparked widespread legal and constitutional debates. It empowers police and prison authorities to collect, store, and analyze a wide array of biometric and behavioral data from individuals, including those arrested, detained, or even merely accused of a crime, and not necessarily convicted.[12] The Act's core objective is to enhance the identification process and support criminal investigations through the integration of advanced biometric technologies, but it has also raised deep concerns regarding privacy, proportionality, and potential abuse of state surveillance powers.

The Act notably broadens the definition of "*measurements*" to include fingerprints, palm prints, footprint impressions, iris and retina scans, photographs, physical and biological samples, and behavioral attributes such as handwriting and signatures. It permits the NCRB to store the data for up to 75 years, a significant extension from previous norms. Additionally, it allows the use of this information for criminal profiling and database matching across states and central agencies. However, the Act lacks clarity on procedural safeguards, oversight mechanisms, and consent-based collection, particularly for those not yet convicted.[13] The term "persons detained under any preventive detention law" is especially problematic, as it can cover individuals who have not committed any offense.

The judicial scrutiny has intensified since the enactment of this legislation. The critics argue that the Act contravenes Art. 21 of the Indian Constitution, which guarantees the right to life and personal liberty, including the right to privacy as upheld in the landmark *Justice K.S. Puttaswamy v. Union of India*[14] judgment. In that decision, a nine-judge bench of the Supreme Court unanimously affirmed that privacy is a fundamental right, and any limitation must pass the test of legality, necessity, and proportionality. The Act, 2022, arguably fails this test, as it lacks a strong legal justification and is overly broad in its applicability.

According to legal scholars and civil society organizations have highlighted the disproportionate impact the Act may have on marginalized and vulnerable communities, including individuals in preventive custody, political dissidents, and protestors. According to data published by the *IFF* and *Project Panoptic*, facial recognition and biometric profiling have already been disproportionately deployed in areas with high protest activity, such as

[10] "Draft Digital Personal Data Protection Bill, 2022," *PRS Legislative Research available at*: https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022 (last visited April 04, 2024).

[11] GDPR 2016, art. 9.

[12] Z. Mateen and M. Sebastian, "CPC: Criminal Procedure Identification Bill raises fears of surveillance in India," *BBC* 13 Apr. 2022.

[13] V. Singh, "How does the new Criminal Procedure (Identification) Bill, 2022 propose to collect sensitive data?" *The Hindu* (2022).

[14] *Id.* at 4.

Delhi and Uttar Pradesh.[15] The extension of such powers under this Act, without adequate safeguards, only heightens the risk of surveillance-led discrimination.

Comparatively, countries like the United Kingdom and Canada have implemented stronger checks on biometric data collection. The UK's *Protection of Freedoms Act, 2012* mandates judicial authorization for the retention of biometric information beyond a certain period and explicitly bars indefinite retention of data of individuals not charged or convicted. Similarly, Canada's *Privacy Act 1983* and *PIPEDA* provide individuals the right to access, correct, or delete their biometric data, ensuring transparency and accountability. As per India's recently passed *DPDP Act, 2023*, while promising, currently exempts data processing for the purposes of "sovereignty, security, and public order," creating a loophole for unrestricted law enforcement access. In the absence of an independent data protection authority with powers to oversee such state surveillance, the Act 2022 may significantly shift the balance of power in favor of the state, at the cost of civil liberties.

ETHICAL AND HUMAN RIGHTS CONCERNS IN BIOMETRIC SURVEILLANCE

The biometric surveillance, while instrumental in streamlining governance and enhancing national security, has sparked a global ethical debate concerning individual rights, consent, and civil liberties. In India, the implementation of large-scale biometric systems such as Aadhaar, and legislations like the Act, 2022, have brought these concerns to the forefront. The major ethical discourse are questions about privacy, data protection, informed consent, and the disproportionate impact on marginalized populations.

Biometric data is intrinsically personal and unique to each individual—once compromised, it cannot be changed like a password. The right to privacy, upheld as a fundamental right by the Supreme Court in *Justice K.S. Puttaswamy v. Union of India*[16], necessitates that any intrusion by the state must be lawful, necessary, and proportionate. However, most biometric surveillance in India occurs without explicit consent, and individuals often have limited knowledge or control over how their data is used. For example, a study by the IFF in 2022 revealed that 80% of respondents in Delhi were unaware that facial recognition systems were being used in public spaces, indicating a serious lapse in consent and transparency protocols.[17]

The Aadhaar system, despite its benefits for welfare delivery, has been criticized for creating a digital divide and excluding millions. As per the *ESI 2017-18*, an estimated 27% of people in rural areas faced authentication failures due to poor fingerprint quality or network issues.[18] These failures often resulted in the denial of essential services like food rationing, pensions, and healthcare, raising ethical alarms over data reliability and the consequences of a biometric mismatch.

The Act, 2022, allows for the collection of biometric and behavioral data from individuals even before conviction and extends data retention to 75 years. Without adequate legal safeguards or judicial oversight, this law opens the door for potential abuse and profiling.[19] The vague language of the Act, particularly its application to those detained preventively or under suspicion, erodes the presumption of innocence—a cornerstone of criminal jurisprudence. Moreover, the lack of independent redress mechanisms for wrongful data collection or breaches further aggravates the ethical implications.

Internationally, legal frameworks attempt to strike a more balanced approach. The European Union's GDPR enshrines principles like explicit consent, the right to be forgotten, and data minimization. The biometric data as a special category requiring explicit consent, except in cases of substantial public interest, and ensures independent data protection authorities can intervene in case of overreach.[20] The studies also show that countries like Germany and Sweden have outlawed the deployment of facial recognition in public surveillance unless it meets stringent legal thresholds. In contrast, India lacks a central data protection authority with sufficient autonomy to oversee government surveillance projects, despite the passage of the *DPDP Act, 2023*, which still exempts state agencies under broad national security grounds. The ethical stakes in biometric surveillance extend beyond privacy—they affect dignity, autonomy, and the trust citizens place in democratic institutions. Without robust legal frameworks, consent mechanisms, and oversight, biometric governance in

[15] "The Increasing Use of Facial Recognition Technology in India #ProjectPanoptic," *Internet Freedom Foundation*, 2021 *available at*: https://internetfreedom.in/the-increasing-use-of-facial-recognition-technology-in-india/ (last visited April 04, 2024).

[16] *Id.* at 4.

[17] A. Jain, "Delhi Police's claims that FRT is accurate at 80% are 100% scary," *Internet Freedom Foundation*, 2022 *available at*: https://internetfreedom.in/delhi-polices-frt-use-is-80-accurate-and-100-scary/ (last visited April 04, 2024).

[18] R. Khera, "Aadhaar Failures: A Tragedy of Errors", EPW 2019 *available at*: https://www.epw.in/engage/article/aadhaar-failures-food-services-welfare (last visited April 04, 2024).

[19] G. Mobilio, "Your face is not new to me – Regulating the surveillance power of facial recognition technologies," 2023 *available at*: https://policyreview.info/articles/analysis/your-face-is-not-new-to-me (last visited April 04, 2024).

[20] GDPR 2016, art. 9.

India risks becoming an intrusive tool of control rather than an enabler of digital empowerment.[21] Addressing these challenges is critical to ensure that technological advancement does not come at the cost of fundamental human rights.

TECHNOLOGICAL ADVANCEMENTS AND THEIR INFLUENCE ON BIOMETRIC REGULATIONS

The integration of cutting-edge technologies such as AI, FRS, and machine learning (ML) into surveillance mechanisms has significantly reshaped the regulatory landscape surrounding biometric data. These innovations, while enabling swift identification, predictive policing, and real-time monitoring, have also introduced complex legal, ethical, and cybersecurity challenges. In India and across the globe, the lack of a robust and adaptive legal framework for biometric regulation has created a precarious balance between national security and civil liberties.

The FRT has emerged as a major biometric surveillance tool used in law enforcement, airport security, and smart city programs. As of 2021, India had installed over 124 facial recognition systems across police departments, with New Delhi alone deploying the AFRS developed by the NCRB. These systems scan faces captured in CCTV footage and match them against databases containing photos of criminals, suspects, and even protestors, with real-time tracking capabilities. While touted as an efficiency tool, their accuracy and bias have been questioned. According to a 2020 report by the IFF's Project Panoptic, the Delhi Police's facial recognition system showed an accuracy rate of less than 1% in identifying suspects in the 2020 Delhi riots.[22] Yet, the system was used to justify arrests and surveillance operations without external audits or transparency.

AI-powered biometric surveillance is rapidly advancing to include gait recognition, iris scanning, emotion detection, and behavioral biometrics. These tools are often used in predictive policing and crowd behavior analysis.[23] For instance, in China, systems like Skynet integrate AI to monitor public behavior and maintain social credit scores. In India, there are ongoing efforts to integrate AI with Aadhaar-linked services, including attendance tracking in schools and offices and verifying users for government welfare schemes.[24] However, these integrations are often launched without comprehensive data protection assessments or robust encryption protocols, leaving room for misuse.

The cybersecurity risks associated with biometric databases are among the most serious concerns raised by civil society and legal scholars. Unlike passwords or ID cards, biometric data is immutable. Once stolen, it cannot be reissued. In 2018, Aadhaar—the world's largest biometric ID program—suffered a massive breach where personal data of over 1.1 billion users was allegedly sold online for as little as ₹500 via unauthorized access.[25] The investigations revealed that access was often granted to unauthorized agents of enrollment centers without layered cybersecurity protocols or audit trails.[26] This not only violated privacy rights but also highlighted glaring lapses in state-led data protection strategies.

Moreover, there is no uniform or sector-specific law governing biometric security in India. While the *IT Act, 2000* and the accompanying IT Rules, 2011, offer some protections for "*sensitive personal data*," they lack the granularity and enforceability required in the age of advanced AI surveillance. The newly enacted *DPDP Act, 2023* does introduce a consent-based framework and mandates purpose limitation, but it also contains broad exemptions for state surveillance under "*sovereignty*" and "*public order*" clauses. These carve-outs weaken accountability and limit the jurisdiction of any independent data protection authority.

There are countries like the United States and members of the European Union have adopted more nuanced approaches to biometric regulation. In the U.S., several cities including San Francisco, Boston, and Portland have banned the use of facial recognition technology by government entities, citing racial bias and violation of civil liberties. A 2019 landmark report by the NIST found that Asian and African American individuals were 10 to 100 times more likely to be misidentified by commercial facial recognition systems than white males, exposing racial and ethnic disparities in algorithmic outcomes.[27]

The EU's GDPR provides comprehensive protections for biometric data under Article 9, categorizing it as a "*special category of personal data*." The EU's upcoming AIA, expected to be enforced by 2025, includes

[21] L. Kisselburgh and J. Beever, "The Ethics of Privacy in Research and Design: Principles, Practices, and Potential," in B. P. Knijnenburg, X. Page, *et al.* (eds.), *Modern Socio-Technical Perspectives on Privacy* 395–426 (Springer International Publishing, Cham, 2022).

[22] *Id.* at 12.

[23] I. P. Basheer, "Bias in the Algorithm: Issues Raised Due to Use of Facial Recognition in India," 10 *JDPP* 61–79 (2024).

[24] R. Jayanth, "AI-enabled facial recognition system to monitor student attendance in Karnataka govt schools" *The Hindu*, 19 Mar. 2024.

[25] PTI. "Aadhaar: 'Leak' in world's biggest database worries Indians" *BBC* (2018).

[26] L. Golightly et al., "Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN," 1 *CSA* 100015 (2023).

[27] N. Singer and C. Metz, "Many Facial-Recognition Systems Are Biased, Says U.S. Study" *The New York Times* (2019).

prohibitions on real-time biometric identification in public spaces, except under strict circumstances such as counter-terrorism. The AIA mandates transparency, human oversight, and detailed risk assessments before deploying AI-based surveillance tools—principles notably absent in India's regulatory landscape.[28]
India's continued expansion of biometric technologies—especially in policing and public service delivery—necessitates a calibrated regulatory response.[29] The Act, 2022, which allows biometric data collection from a wide range of individuals including those detained or arrested for preventive purposes, offers little recourse for redressal or deletion of data. There is no mandatory periodic audit of stored biometric data, nor is there an independent review board to examine the necessity and proportionality of surveillance. Further compounding the issue is the interlinking of multiple databases—Aadhaar, voter ID, health IDs, and financial records—without clear legal oversight. This interconnectivity enables centralized biometric profiling, raising concerns about mass surveillance and state overreach. An Amnesty International report in 2023 warned that India's use of facial recognition during peaceful protests, such as those against the CAA, had a chilling effect on freedom of expression and assembly.[30]

To safeguard civil liberties while leveraging technological progress, India must adopt a layered regulatory framework. This would include:

1. *introducing an independent biometric data oversight authority,*
2. *implementing end-to-end encryption and anonymization techniques,*
3. *restricting the use of biometric surveillance to strictly necessary cases under judicial review, and*
4. *creating transparency dashboards for public accountability.*

Additionally, mandatory algorithmic audits and human-in-the-loop requirements can prevent biased outcomes in AI-powered systems. The technological advancements in AI and biometric surveillance present both a promise and a peril. While they can revolutionize law enforcement, public service delivery, and national security, their unregulated and opaque deployment can severely compromise constitutional rights. India's legislative and regulatory efforts must rise to the challenge, ensuring a people-centric digital governance model that respects privacy, guarantees security, and fosters trust in institutions.

POLICY RECOMMENDATIONS AND THE FUTURE OF BIOMETRIC SURVEILLANCE IN INDIA

To ensure that biometric surveillance in India aligns with constitutional values, international standards, and public trust, the following policy interventions are recommended:

- Move beyond the limited scope of the *DPDP Act, 2023* by introducing a robust data protection framework that guarantees the right to privacy, minimizes state exemptions, and enforces transparency in biometric data collection.
- Empower a truly autonomous regulatory body to monitor, audit, and penalize misuse of biometric data. The DPA should have the authority to review surveillance practices, enforce compliance, and protect individual rights.
- Enforce strict legal limitations on the purposes for which biometric data can be collected and retained. Limit retention periods, especially under the Act, 2022 and ensure that data is deleted once its purpose is served.
- Introduce legally binding requirements for free, informed, and revocable consent before biometric data is collected. Public bodies must publish transparency reports on the deployment and impact of biometric systems.
- All large-scale biometric surveillance projects—particularly those involving facial recognition—must require prior judicial authorization, periodic review, and public accountability.
- Mandate that facial recognition and other AI-based biometric tools be subject to regular algorithmic audits to detect and mitigate bias, discrimination, and erroneous profiling.
- Introduce safeguards to prevent over-surveillance of marginalized communities, such as Dalits, Adivasis, religious minorities, and political dissenters, who are disproportionately targeted by law enforcement surveillance.
- Align India's biometric regulations with global best practices such as the *EU GDPR* and proposed *EU AI Act*, ensuring interoperability and adherence to rights-based frameworks.
- Develop accessible and efficient redressal mechanisms for individuals to contest wrongful inclusion in biometric databases or surveillance systems.

[28] A. Mohanty and S. Sahu, "India's Advance on AI Regulation," *Carnegie Endowment for International Peace*.
[29] *Id.* at 16.
[30] "Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance," *Amnesty International*, 2020 *available at*: https://www.amnesty.org/en/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance/ (last visited April 04, 2024).

The rise of biometric surveillance in India, catalyzed by the Act, 2022 and rapid digital governance initiatives, presents a paradox of innovation and intrusion. Without a sound legal and policy architecture, these systems risk becoming instruments of unchecked state power rather than tools for public safety. By implementing the above recommendations, India can create a governance model that balances national security interests with democratic accountability and individual rights. A forward-looking framework must not only accommodate technological progress but must also enshrine the constitutional promise of dignity, autonomy, and justice for all citizens. Aligning domestic laws with international standards and embedding ethical safeguards will be key to ensuring that India's biometric future is secure, equitable, and rights-respecting.