INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

AN ANALYTICAL EXAMINATION OF BIOMETRIC SURVEILLANCE LEGISLATION IN INDIA AND THE CONSEQUENCES OF THE CRIMINAL IDENTIFICATION ACT 2022 WITHIN THE CONTEXT OF DIGITAL GOVERNANCE

AUTHORED BY - AAKANKSHA MISHRA
(Research Scholar, School of Law, Raffles University, Neemrana)
CO-AUTHOR - DR. PRADIP KUMAR KASHYAP
(Assistant Professor of Law, School of Law, Raffles University, Neemrana)

Abstract

The growing incorporation of biometric technology into public administration has altered the framework of governance and surveillance in India. This paper rigorously examines the legal, ethical, and policy ramifications of biometric monitoring legislation, namely the Criminal Identification Act of 2022. This research aims to examine the intersection of biometric data collection, storage, and usage by law enforcement agencies with constitutional rights, data privacy principles, and emerging technological risks within the framework of digital governance. The paper initiates by analyzing the historical development of biometric monitoring and its significance in modern digital governance structures. It examines the escalating use of biometric technology, including face recognition, iris scans, and fingerprinting, for crime prevention, public safety, and identity authentication. The report examines the current legal and regulatory frameworks regulating biometric data in India, including the Aadhaar system, the Information Technology Act, and proposed data protection laws. A comparative analysis of global standards is conducted to evaluate India's conformity with international human rights rules. A principal element of the research is a comprehensive analysis of the Criminal Identification Act, 2022, encompassing its broadened provisions for the acquisition of physical and biological samples, the lack of stringent data protection measures, and its alignment with the right to privacy as established in the Puttaswamy ruling. The research also examines ethical issues related to permission, the possible exploitation of surveillance technology, and the absence of accountability in data management. This includes suggestions for a more transparent, responsible, and rights-oriented framework for biometric governance in India. The research indicates that while biometric technologies may improve

ISSN: 2582-6433

efficiency, they must be accompanied by sufficient legal protections to guarantee individual liberties in a democratic society.

Keywords: Biometrics, Surveillance, Governance, Legislation, Privacy

Introduction

The worldwide expansion of biometric surveillance technology signifies one of the most significant advancements in contemporary administration. Biometric technology, including iris scans, face recognition, voiceprints, and gait analysis, have transformed identity verification and control systems in public and commercial sectors. In India, this change has been characterized by a strong state impetus towards digital governance, particularly via projects such as Digital India and the Aadhaar biometric identity system. As of 2022, India maintains the biggest biometric database globally, with over 1.3 billion persons registered in Aadhaar. This unparalleled magnitude presents significant opportunities for administrative efficiency, but also considerable legal, ethical, and human rights dilemmas.[1] The biometric technology, originally designed for safe access and criminal identification, has transformed into a versatile surveillance instrument. Initially, applications were mostly restricted to forensic usage, such as fingerprint analysis in criminal investigations; however, the incorporation of biometric systems into civil registration, social welfare, law enforcement, and public health has swiftly broadened. The COVID-19 pandemic expedited the use of contactless biometric technology, such as face recognition and infrared imaging, as a public health monitoring strategy. In India, biometrics are integral to government and law enforcement. Law enforcement agencies throughout are progressively using face recognition technology, including the National AFRS, for the identification of suspects and the recovery of missing individuals. Nonetheless, a significant deficiency exists in data protection. An IFF research from 2022 revealed that of 42 face recognition systems implemented or under development in India, only a limited number have privacy rules or regulatory monitoring frameworks. Three this invokes issues pertaining to Article 21 of the Indian Constitution, which ensures the right to life and personal liberty, including the right to privacy, as established in Justice *K.S. Puttaswamy* v. *Union of India*. The Act of 2022 signified a pivotal moment in India's biometric surveillance framework. It broadened the parameters of biometric data collecting much beyond those authorized by the

[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, 2025).

ISSN: 2582-6433

Identification of Prisoners Act, 1920. The Act of 2022 permits law enforcement to gather biological samples, retinal and iris scans, and behavioral characteristics from persons, including those in preventative custody and those not yet officially accused of a crime. The lack of judicial monitoring and restrictions on data keeping, coupled with vague terminology, has prompted constitutional concerns. The legislation also lacks a definitive consent procedure and violates international norms, including the EU's GDPR, which requires express, informed permission for data collection and use. Conversely, nations such as the UK and Germany have implemented robust legislative frameworks that restrict the use of biometric monitoring. In S. and Marper v. United Kingdom, the ECHR determined that the perpetual preservation of biometric data from persons not convicted of crimes contravenes ECHR standards. India's digital governance trajectory is characterized by a paradox: it adopts advanced technology for efficiency and modernization but lacks comprehensive legal structures for their regulation. As biometric monitoring becomes more integrated into government, there is an urgent need for a rights-based, open, and accountable framework.[2]

Legal and Regulatory Framework Regulating Biometric Surveillance in India

The legal and regulatory framework regulating biometric monitoring in India is now at a pivotal juncture. Although biometric data collecting has emerged as a fundamental aspect of digital governance, especially via initiatives such as Aadhaar, the legal protections governing its use are scattered, insufficiently developed, and sometimes antiquated. The lack of a robust data protection framework exacerbates worries about the possible exploitation of biometric information, threatening individual privacy, physical autonomy, and basic rights. The principal legal framework for biometric data gathering at the national level is the Aadhaar Act of 2016. The Aadhaar system provides a distinctive 12-digit identification number to Indian people, derived on their biometric and demographic information. As of March 2022, more than 1.32 billion Aadhaar numbers have been issued, including about 99% of India's adult population. Eight Nonetheless, despite the system's magnitude, the Aadhaar Act lacks comprehensive directives for data retention, third-party access, or grievance redressal procedures. Furthermore, the Supreme Court in Justice K.S. Puttaswamy v. Union of India affirmed the constitutional legitimacy of Aadhaar while invalidating clauses that let private companies to

[2] F. L. Cabanillas et al., "Do biometric payment systems work during the COVID-19 pandemic? Insights from the Spanish users' viewpoint," 8Financial Innovation22 (2022).

ISSN: 2582-6433

access Aadhaar data, therefore emphasizing the need for proportionality and purpose restriction in the utilization of biometric data. The IT Act of 2000 and its corresponding regulations, including the IT Rules of 2011, provide a degree of protection. These regulations classify biometric data as "sensitive personal data" and stipulate permission and data protection obligations. Nonetheless, enforcement is inadequate, and the restrictions exclude government institutions, resulting in a considerable regulatory oversight. The Act of 2022 signifies a substantial transformation in India's surveillance framework. The new legislation supersedes the colonial-era Identification of Prisoners Act, 1920,[3] empowering law enforcement agencies to gather, retain, and analyze biometric and behavioral data, including fingerprints, palm prints, iris and retina scans, as well as handwriting and voice samples of convicted individuals, arrestees, and preventive detainees. The Act notably lacks clear measures for permission, supervision, or data minimization. It allows for data retention for a duration of up to 75 years and facilitates potential integration with national and international criminal databases. Civil liberties organizations have expressed concerns over the possible infringement of Articles 14, 19, and 21 of the Constitution, especially in the lack of a data protection statute.[4] Ten conversely, international legal systems provide more substantial protections. The EU's GDPR is regarded as the benchmark in data privacy legislation. It requires express agreement for the processing of biometric data, confers the right to erasure onto persons, and enforces stringent penalties for noncompliance. The GDPR classifies biometric data as a unique category necessitating enhanced security. Likewise, Canada's PIPEDA and Australia's Privacy Act 1988 categorize biometric data as sensitive personal information and enforce stringent regulations on its collection and use. The absence of a comprehensive personal data protection legislation in India, although the release of the DPDP Act, 2023, results in a legal void regarding biometric governance. The new Act establishes concepts of consent, purpose restriction, and data fiduciary responsibility; nevertheless, it continues to exclude national security and law enforcement agencies from most of its scope, so exacerbating the difficulty of developing a fair regulatory framework.[5]

[3] "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).

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

[5] "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, 2025)

ISSN: 2582-6433

The Criminal Identification Act 2022 and Its Legal Ramifications

The Act of 2022, approved by the Indian Parliament, is a pivotal point in India's biometric monitoring framework, replacing the outdated Identification of Prisoners Act of 1920. This law's extensive breadth has ignited significant legal and constitutional debates. It authorizes law enforcement and correctional institutions to gather, retain, and examine a broad spectrum of biometric and behavioral information on people,[6] including those arrested, detained, or just suspected of a crime, regardless of conviction status. The primary aim of the Act is to improve the identification process and facilitate criminal investigations by the incorporation of sophisticated biometric technology; nonetheless, it has also elicited significant apprehensions about privacy, proportionality, and the possible misuse of governmental surveillance authority.[7] The Act significantly expands the definition of "measurements" to include fingerprints, palm prints, footprint imprints, iris and retina scans, pictures, physical and biological samples, as well as behavioral characteristics like handwriting and signatures. It allows the NCRB to retain data for a duration of up to 75 years, representing a considerable expansion over prior regulations. Furthermore, it permits the use of this information for criminal profiling and database comparison across states and central authorities. Nevertheless, the Act is ambiguous about procedural protections, supervision procedures, and consent-based data gathering, especially for those who have not yet been convicted. The phrase “persons detained under any preventive detention law” is particularly contentious, since it may include people who have not committed any crime. Judicial scrutiny has strengthened after the introduction of this Act.[8] Critics contend that the Act violates Article 21 of the Indian Constitution, which ensures the right to life and personal liberty, including the right to privacy as affirmed in the seminal Justice *K.S. Puttaswamy* v. *Union of India* ruling. A nine-judge bench of the Supreme Court unanimously determined that privacy is a basic right, and any restrictions must satisfy the criteria of legality, necessity, and proportionality. The Act of 2022 ostensibly fails to meet this criterion, since it lacks robust legal foundation and is very wide in its scope. Legal academics and civil society groups have emphasized the disproportionate effects the Act may have on disadvantaged and vulnerable people, including persons in preventive detention, political dissidents, and protesters. Data from the IFF and Project

[6] L. Golightly et al., “Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN,” 1CSA100015 (2023)
[7] A. Mohanty and S. Sahu, “India’s Advance on AI Regulation,”Carnegie Endowment for International Peace.
[8] 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, 2025).

ISSN: 2582-6433

Panoptic indicates that face recognition and biometric profiling have been disproportionately used in regions with significant protest activity, like Delhi and Uttar Pradesh. The expansion of such authorities under this Act, devoid of sufficient safeguards, exacerbates the possibility of surveillance-induced prejudice.[9] In comparison, nations such as the United Kingdom and Canada have instituted more rigorous regulations on biometric data gathering. The UK's Protection of Freedoms Act, 2012 requires court approval for the preservation of biometric data beyond a certain duration and clearly prohibits the indefinite retention of information pertaining to persons who have not been accused or convicted. Likewise, Canada's Privacy Act of 1983 and PIPEDA provide people the right to view, amend, or erase their biometric data, so promoting openness and accountability. The newly enacted DPDP Act, 2023 in India, while promising, presently exempts data processing for "sovereignty, security, and public order," so leaving a backdoor for uncontrolled access by law enforcement. Without an autonomous data protection body endowed with the capacity to supervise state surveillance, the Act 2022 may considerably alter the power dynamics in favor of the state, undermining civil rights.

Ethical and Human Rights Issues in Biometric Monitoring

Biometric monitoring, while crucial in optimizing governance and bolstering national security, has ignited a worldwide ethical discourse over individual rights, consent, and civil liberties. The deployment of extensive biometric systems, such as Aadhaar, together with legislations like the Act of 2022, has elevated these concerns in India.[10] The principal ethical considerations are to privacy, data protection, informed consent, and the unequal effects on underprivileged groups. Biometric data is inherently personal and unique to each individual; once hacked, it cannot be altered like a password. The right to privacy, recognized as a basic right by the Supreme Court in Justice K.S. Puttaswamy v. Union of India, requires that any governmental intrusion be legitimate, necessary, and reasonable.[11] Nonetheless, the majority of biometric monitoring in India transpires without express authorization, and people often possess minimal awareness or authority regarding the utilization of their data. A 2022 research by the IFF indicated that 80% of respondents in Delhi were oblivious of the use of face recognition

[9] R. Jayanth, “AI-enabled facial recognition system to monitor student attendance in Karnataka govt schools”The Hindu, 19 Mar. 2024.
[10] I. P. Basheer, “Bias in the Algorithm: Issues Raised Due to Use of Facial Recognition in India,” 10JDPP61–79 (2024).
[11] “Approximately 99 pc adult population has been enrolled in Aadhaar: UIDAI CEO,”Unique Identification Authority of India | Government of Indiaavailable 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, 2025)

ISSN: 2582-6433

technologies in public areas, highlighting a significant deficiency in consent and transparency measures. The Aadhaar system, although advantageous for welfare distribution, has faced criticism for fostering a digital divide and marginalizing millions. According to the ESI2017-18, around 27% of individuals in rural regions had authentication problems owing to substandard fingerprint quality or network complications. These shortcomings often led to the denial of vital services like as food rationing, pensions, and healthcare, prompting ethical concerns around data dependability and the repercussions of biometric discrepancies. The Act of 2022 permits the acquisition of biometric and behavioral data from persons prior to conviction and increases the duration of data retention to 75 years. This statute, without sufficient legal protections or judicial scrutiny, facilitates potential misuse and profiling. The ambiguous wording of the Act,[12] especially regarding its applicability to those arrested preventively or on suspicion, undermines the presumption of innocence, a fundamental principle of criminal law. Furthermore, the absence of independent redress procedures for erroneous data acquisition or breaches exacerbates the ethical ramifications. Globally, legal structures endeavor to achieve a more equitable approach. The European Union's GDPR establishes concepts such as express permission, the right to erasure, and data minimization. Biometric data is classified as a distinct category requiring specific authorization, except in instances of significant public interest, and guarantees that independent data protection authorities may intervene in circumstances of overreach. Research indicates that nations such as Germany and Sweden have prohibited the use of face recognition in public monitoring unless it satisfies rigorous legal criteria. Conversely, India does not possess a central data protection body with enough power to supervise government surveillance initiatives, despite the enactment of the DPDP Act, 2023, which continues to exclude state agencies under expansive national security provisions. The ethical implications of biometric monitoring transcend privacy; they impact dignity, autonomy, and the faith individuals have in democratic institutions. In the absence of strong legal frameworks, consent processes, and monitoring, biometric governance in India may transform into a repressive instrument of control instead of facilitating digital empowerment. Confronting these difficulties is essential to guarantee that technology progress does not infringe upon basic human rights.[13]

[12] 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 Privacy395–426 (Springer International Publishing, Cham, 2022).

[13] "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, 2025).

ISSN: 2582-6433

Technological advancements and their impact on biometric regulations

The incorporation of advanced technologies like AI, FRS, and machine learning (ML) into surveillance systems has profoundly altered the legislative framework governing biometric data. These developments, while facilitating rapid identification, predictive policing, and real-time surveillance, have also presented intricate legal, ethical, and cybersecurity issues.[14] The absence of a comprehensive and flexible legislative framework for biometric control in India and elsewhere has established a tenuous equilibrium between national security and civil rights. The FRT has become a significant biometric surveillance instrument used in law enforcement, airport security, and smart city initiatives. By 2021, India has implemented more than 124 face recognition systems across police agencies, with New Delhi specifically using the AFRS created by the NCRB. These systems analyze faces recorded in CCTV video and compare them to databases of images of criminals, suspects, and even demonstrators, including real-time tracking functionalities. Although promoted as a tool for efficiency, their precision and impartiality have been scrutinized. A 2020 study from IFF's Project Panoptic indicated that the Delhi Police's face recognition technology had an accuracy rate of under 1% in identifying suspects during the 2020 Delhi riots. Nevertheless, the method was used to rationalize arrests and monitoring activities devoid of external audits or transparency. AI-driven biometric surveillance is swiftly evolving to include gait recognition, iris scanning, mood detection, and behavioral biometrics. These instruments are often used in predictive policing and crowd behavior analysis. In China, systems such as Skynet use AI to surveil public conduct and uphold social credit ratings. In India, there are continuous initiatives to include AI with Aadhaar-linked services, such as attendance monitoring in educational institutions and workplaces, as well as user verification for government assistance programs. Nonetheless, these interfaces are often implemented without thorough data protection evaluations or stringent encryption measures, creating opportunities for exploitation. The cybersecurity threats linked to biometric databases are among the most significant issues highlighted by civil society and legal academics. In contrast to passwords or identification cards, biometric data is unchangeable. Once pilfered, it cannot be reprinted. In 2018, Aadhaar, the world's biggest biometric identification program, had a significant breach in which the personal data of over

[14] 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, 2025).

ISSN: 2582-6433

1.1 billion individuals was reportedly sold online for as low as ₹500 via illegal access. [15] The investigations showed that access was often permitted to unauthorized personnel at enrollment centers without robust cybersecurity measures or audit records. This not only infringed upon private rights but also highlighted significant deficiencies in state-sponsored data protection policies.[16] Furthermore, there is an absence of a standardized or industry-specific legislation regulating biometric security in India. The IT Act of 2000 and the associated IT Rules of 2011 provide some safeguards for "sensitive personal data," although they lack the specificity and enforcement necessary in the era of powerful AI monitoring.[17] The recently implemented DPDP Act, 2023 establishes a consent-based framework and enforces purpose restriction; nevertheless, it also includes extensive exemptions for state monitoring under the "sovereignty" and "public order" provisions. These exemptions undermine accountability and restrict the jurisdiction of any autonomous data protection body. Countries like as the United States and European Union members have implemented more sophisticated strategies for biometric control. In the United States, several towns such as San Francisco, Boston, and Portland have prohibited the use of face recognition technology by governmental agencies, claiming concerns of racial prejudice and infringement of civil rights. A 2019 pivotal research by the NIST revealed that Asian and African American persons were 10 to 100 times more likely to be misdiagnosed by commercial face recognition systems compared to white men, highlighting racial and ethnic discrepancies in algorithmic results. The EU's GDPR offers extensive safeguards for biometric data as delineated in Article 9, classifying it as a "special category of personal data." The forthcoming AIA of the EU, anticipated to be implemented by 2025, including bans on real-time biometric identification in public areas, unless under stringent conditions such as counter-terrorism efforts. The AIA requires openness, human supervision, and comprehensive risk assessments prior to the deployment of AI-based surveillance systems, aspects that are conspicuously lacking in India's legislative framework. The ongoing proliferation of biometric technology in India, particularly in law enforcement and public service delivery, requires a measured legislative response. The Act of 2022 permits the collecting of biometric data from a broad spectrum of persons, including those detained or

[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, 2025).
[16] 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, 2025).
[17] Z. Mateen and M. Sebastian, "CPC: Criminal Procedure Identification Bill raises fears of surveillance in India," BBC13 Apr. 2022.

ISSN: 2582-6433

arrested for preventative reasons, however provides little avenues for appeal or data deletion. No obligatory periodic audit of stored biometric data exists, nor is there an independent review body to assess the need and appropriateness of monitoring. The problem is exacerbated by the interconnection of several databases, including Aadhaar, voter ID, health IDs, and financial information, without explicit legislative control. This interconnectedness facilitates centralized biometric profiling, prompting apprehensions over mass monitoring and governmental overreach. A 2023 Amnesty International research said that India's use of face recognition technology during peaceful rallies, including those against the CAA, had a detrimental impact on freedom of speech and assembly. Furthermore, obligatory algorithmic audits and human-in-the-loop stipulations might avert biased results in AI-driven systems. The technical breakthroughs in artificial intelligence and biometric surveillance offer both potential benefits and significant risks. Although they have the potential to transform law enforcement, public service delivery, and national security, their uncontrolled and opaque implementation may significantly undermine fundamental rights. India's legislative and regulatory initiatives must meet the challenge by establishing a people-centric digital governance framework that upholds privacy, ensures security, and cultivates confidence in institutions.[18]

Recommendations for Policy 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:

(a) Move beyond the limited scope of the DPDP Act, 2023by introducing a robust data protection framework that guarantees the right to privacy, minimizes state exemptions, and enforces transparency in biometric data collection.

(b) 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.

(c) 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.

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

ISSN: 2582-6433

(d) 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.

(e) All large-scale biometric surveillance projects particularly those involving facial recognition must require prior judicial authorization, periodic review, and public accountability.

(f) 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.

(g) 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.

(h) 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.

(i) Develop accessible and efficient redressal mechanisms for individuals to contest wrongful inclusion in biometric databases or surveillance systems.