LEX GAZETTE
International Multidisciplinary Research Journal

ISSN: 3049-3536 (O)

VOLUME: II, ISSUE: I
JANUARY (2026)

Lex Gazette International Multidisciplinary Research Journal

DOUBLE BLIND PEER REVIEWED

OPEN ACCESS

EU AI ACT BANS AND BIOMETRIC PRIVACY: LESSONS FOR INDIA

Gayatri Rathi
Research Scholar at the Faculty of Law, Swami Vivekanand Subharti University, Meerut
Contact at: gayatrirathi950@gmail.com

Dr. Sarika Tyagi
Associate Professor at the Faculty of Law, Swami Vivekanand Subharti University, Meerut
Contact at: tyagisarika21@gmail.com

ABSTRACT

The Artificial Intelligence Act of the European Union, officially adopted as Regulation (EU) 2024/1689, considers biometric AI as an area where some uses are so rights-infringing that even a risk-management label would not suffice, therefore, it draws legally binding red lines through Article 5 of Regulation (EU) 2024/1689. The forbidden practices most relevant to biometrics comprise the use of "real-time" remote biometric identification in publicly accessible spaces for law enforcement purposes, which is subject only to tightly conditioned exceptions that are linked to specific objectives such as the search for missing persons, the prevention of imminent threats, and the identification of suspects of serious crimes, which must be supported by the prior authorization, registration, and deletion obligations. Furthermore, the Act disallows the creation or enlargement of facial recognition databases by indiscriminate scraping from the internet or CCTV, which is a depiction of the explicit legal decision that mass face capture destroys anonymity and scares public life. It bans biometric straightforwardness that is used to guess sensitive traits and prohibits emotion recognition in workplaces and educational institutions unless it is for the narrow purposes of medical or safety cases. These prohibitions are relevant for India because the Indian constitutional privacy doctrine, based on Article 21 of the Constitution of India and interpreted in K. S. Puttaswamy v. Union of India, requires State intrusions to be legal, necessary and proportionate, whereas Indias very recent data protection statute, the Digital Personal Data Protection Act, 2023, imposes cross-sector duties without biometric-specific per se bans. The takeaway from the comparison is that India can implement EU-style bright lines for high-chill biometric uses while fitting the safeguards to Indian welfare delivery, policing capacity, and oversight institutions through pinpointed statutory amendments, procurement conditions, and audit-ready authorization processes. A practical roadmap would be to enact biometric-specific prohibitions and narrow exceptions, harmonize legitimate grounds and retention limits between Section 29 of the Aadhaar Act, 2016, and the DPDP framework, and develop binding authorization, logging, and independent review provisions for any biometrics-based public space surveillance.

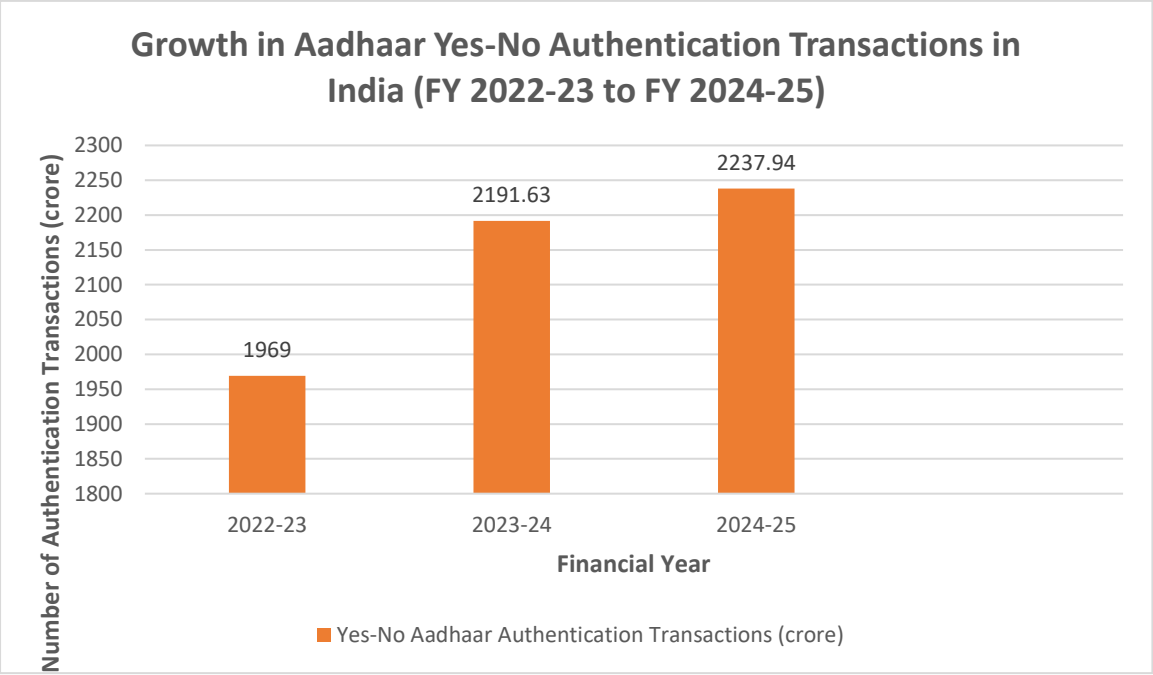
KEYWORDS

EU AI Act, Article 5 Bans, Biometric Privacy, Facial Recognition, Emotion Recognition, Predictive Policing, INDIA DPDP Act

1. INTRODUCTION

AI-driven biometrics moved beyond border control and high-security campuses into routine governance, private compliance, and everyday policing as identification at scale reduces transaction costs and provides administrative certainty. Meanwhile, this shift also changes the problem of privacy: biometric systems do not just capture attributes, they turn bodies into persistent identifiers that can be used to track a person across databases, locations, and time, including situations where the person has never really consented to participate. India's welfare distribution has been closely intertwined with identity infrastructure, and the Aadhaar system, together with e-KYC and authentication, clearly demonstrates how quickly identification becomes the default layer for service access, employment verification, and private-sector onboarding, even though the law's main focus is really on targeted delivery. The enactment of Aadhaar has several provisions addressing confidentiality, one of which is Section 29 of the Aadhaar Act, 2016, which prohibits the sharing of core biometric information by any means and restricts the use of identity information beyond the purposes notified; however, the wider governance environment continues to facilitate growth of function through new use-cases and integrated databases [1]. Alongside this, India's general surveillance agencies under "Section 5(2) of the Indian Telegraph Act, 1885" and "Section 69 of the Information Technology Act, 2000" show that the powers of interception can, in fact, be extended in practical terms without always generating biometric-specific standards of law, rules of retention, and independent transparency that would be consistent with the high level of intrusiveness of biometric tracking [2].

For this study, Biometric AI refers to an artificial intelligence system that uses biological, physical, or behavioural traits to infer an individual's identity or attributes. It uses systems or programs that perform facial recognition, fingerprint or iris recognition, voice recognition, gait analysis, or perform emotional analysis or general behavioral categorization of individuals in order to create, store, or transform informational signals into data that can be used in biometric systems. The concern extends further to the creation and storage of biometric data, to the identification of individual traits and the placement of individuals in a database classification system, and to subsequent judgments and decisions that may be made based on this information. The individual, once identified, thereby loses some of the integrity of their physical rights and may not be able to effectively exercise their rights fully in a meaningful way. [12], [65]



[3]

Figure 1. Year-wise Aadhaar Yes-No authentication transactions in India (crore), FY 2022-23 to FY 2024-25.

The reason the EU's move in "Regulation (EU) 2024/1689" is significant is that it considers biometric AI as a central issue of fundamental rights and develops a legal framework that combines risk levels with total bans, especially in "Article 5 of Regulation (EU) 2024/1689", where certain practices are prohibited in and of themselves rather than being permitted subject to general safeguards. For India, the constitutional basis is "Article 21 of the Constitution of India" as interpreted in *K. S. Puttaswamy v. Union of India[4]*, whereas the statutory basis is the "Digital Personal Data Protection Act, 2023", which establishes duties, rights, and an enforcement board but does not, in itself, delineate biometric bright lines that would be comparable to the EU bans [5]. The doctrinal chore, therefore, is to interpret the EU's bans as a list of legally cognizable biometric harms, and to wonder what India needs to do in law and governance to bring biometric deployments under clear legality, limited purposes, and real accountability [6].

1.1 RESEARCH QUESTIONS

The research questions for the study are as follows:-

1. Whether India’s existing constitutional privacy doctrine and statutory structure under the “Digital Personal Data Protection Act, 2023” can be interpreted to produce enforceable prohibitions equivalent to the EU’s “Article 5 of Regulation (EU) 2024/1689” for public-space biometric identification, untargeted facial scraping,

emotion recognition in asymmetrical settings, and sensitive-trait biometric categorisation?

2. Whether a dedicated Indian legislative design for biometric AI, combining bright-line bans, narrowly framed exceptions, prior authorisation, logging, independent review, and deletion duties, can better satisfy legality, necessity, and proportionality than a system that relies primarily on executive circulars, vendor assurances, and post-facto grievance processes?

1.2 PROBLEM STATEMENT

India does not have any sector-specific biometric statutory red lines that function as per se prohibitions, though the use of both the public and private sectors is expanding in welfare, education, workplaces, and policing. The Digital Personal Data Protection Act, 2023, establishes general grounds for processing and fiduciary responsibilities; however, it does not specifically target biometrics for higher consent thresholds, total bans, or narrowly defined exceptions requiring prior authorisation. This omission keeps legality and proportionality at the mercy of fragmentary rules, terms of procurement, and uneven oversight, thereby making the situation quite risky in the areas of function expansion, mass collection, indefinite retention, and low transparency effectiveness.

1.3 OBJECTIVES OF THE STUDY

The objectives of the study are as follows:-

1. To map the biometric-related prohibitions and limited exceptions under “Article 5 of Regulation (EU) 2024/1689” and connect them to the rights logic that animates EU fundamental-rights protection and data protection law.
2. To assess India’s constitutional and statutory adequacy under the “Digital Personal Data Protection Act, 2023” and the Aadhaar regime, and to argue for specific, enforceable reforms that can operate in welfare delivery and law-enforcement contexts without normalising mass biometric surveillance.

1.4 Research Methodology

This study adopts a doctrinal and comparative methodology. It analyses the text, structure, and logic behind the rights of Regulation (EU) 2024/1689, especially in relation to Articles 2, 5, 99, and 113. It then assesses how these Articles connect to the Indian constitutional privacy doctrine, the Aadhaar Act, and the Digital Personal Data Protection Act, 2023. This analysis primarily relies on first-order legal sources (e.g., statutes, regulations, decisions, and

government publications) and resorts to secondary legal literature only for doctrinal support. The study assesses the possibility of India embedding proportionality in legislative bans, prior authorisation, auditing, erasure, and establishing default remedies for the use of Biometric AI in the public and private sectors [12], [34], [36], [66].

2. EU "RED LINES" ON BIOMETRIC AI

Regulation (EU) 2024/1689 considers certain uses of biometric AI as prohibited practices because the infringement upon rights occurs at the design and implementation phase of the systems, rather than after an individual has been demonstrably harmed. Article 5 establishes a legal perimeter on practices that include the identification and the creation of non-consensual databases within public spaces, the creation of sensitive trait inferencing and emotion scoring systems in dependent and potentially harmful environments, and systems that assess and score criminality based on profiling and other forms of automated assessment and scoring. The importance of this design is that it does not support the view that notice, contract, or internal policy can redeem every biometric harm. A few limited exceptions exist only where the Act establishes strict goals together with prior authorisation, registration, and time/place/purpose limitations, as well as deletion duties. The design operationalises the compliance mechanism within the framework of fundamental rights [7], [8].

2.1 REAL-TIME REMOTE BIOMETRIC IDENTIFICATION IN PUBLIC SPACES

The EU's most visible and biometric line in the sand is about live identification of people in public. According to "Article 5(1)(h) Regulation (EU) 2024/1689", the use of "real-time" biometric identification systems that are remote and in publicly accessible spaces, for law enforcement purposes, is prohibited, subject only to strict necessity for specific objectives that the law itself enumerates. The permitted objectives are deliberately very limited: targeted searches for victims of abduction, trafficking, or sexual exploitation and searches for missing persons; prevention of a specific, substantial, and imminent threat to life or safety, or a genuine terrorist threat; and localization or identification of a suspect of serious crime for investigation, prosecution, or execution of a penalty, the latter being tied to serious offences and sentencing thresholds. The situation is not a general permission with safeguards; it is a general prohibition with exception gates. Governance conditions are then hard-wired by the Act: each use must be limited in time, geography, and persons; the authority must carry out a fundamental rights impact assessment and register the system in an EU database; each use must get prior authorisation from a judicial or independent authority, with only a short emergency window

and deletion duties if authorisation fails. The design here sees live public-space identification as a practice that changes the very concept of public anonymity, so it requires evidence of strict necessity rather than simple usefulness [9].

2.2 UNTARGETED SCRAPING OF FACIAL IMAGES

Under Article 5(1)(e) of Regulation (EU) 2024/1689, AI systems that scrape images from the internet and CCTV to create or increase the number of facial recognition databases will be banned from both national and international markets. The issue of concern here is that a person in a public or semi-public space will be unknowingly enrolled in a searchable identification system. The practice is identified in Recital 43 of the regulation, in conjunction with substantial interference with privacy, because it ignores the principles of notice and choice and circumvents the limitation of purpose and the right to contest at a later date. Therefore, the regulation acts against the method of building databases before it becomes commonplace, cheap, and difficult to trace to identify users.

2.3 BIOMETRIC CATEGORISATION FOR SENSITIVE TRAITS

The European Union's (EU's) ban on sensitive-trait inference equates the risk of discrimination with biometric profiling in such a way that they cannot be considered separately. "Article 5(1)(g) of Regulation (EU) 2024/1689" prohibits the use of biometric categorisation technologies that, through the analysis of biometric data, identify or imply race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation. "Recital 30 of Regulation (EU) 2024/1689" goes even further in that direction by characterising such systems as prohibited if they use face or fingerprint-style identifiers to obtain protected traits that are historically connected with persecution and structural exclusion [11]. The prohibition also draws the lines: on one hand, it is not intended to cover all labelling or filtering of biometric datasets that have been obtained lawfully, and, on the other hand, it allows certain categorisation of biometric data in a law-enforcement context, revealing that the EU sees trait inference as different from dataset management and from narrower operational processing. Even without certain exemptions, the main point is that sensitive-trait inference should not be considered a neutral technical characteristic; it is a legal harm multiplier because it creates an environment conducive to selective policing, employment discrimination, political targeting, and social sorting, frequently under circumstances in which the person who is the subject of these actions cannot even see or challenge the inference [12].

The issue of algorithmic bias is not only a technical problem, but a concern of rights, as erroneous rates and thresholds may create uneven distribution of suspicion among different groups. Facial recognition and biometric systems may demonstrate disparity and uneven performance based on different demographic and physical conditions, while the training data sets may be reflections of historical discriminatory policing and other forms of social underrepresentation. Within law enforcement, a false positive may result in a person being interrogated, or even detained and placed on a watchlist, while in social welfare and education, a false negative may lead to the exclusion of a person. Reforms in India, thus, should mandate the prohibition of any negative action that is based solely on a biometric match, along with local field validation, pre-deployment testing, and disclosure of demographic-related mistakes.

2.4 EMOTION RECOGNITION AT WORK AND IN EDUCATION

Article 5(1)(f) of Regulation (EU) 2024/1689 restricts the use of AI systems that recognize emotions of natural persons in the workplace and in educational environments. Specifically, the regulation argues that, for medical or safety purposes, the use of these systems may be justified. The reasoning behind the regulation is that there is often little choice in the workplace or educational environments to refuse to participate in mechanisms that are designed to monitor. Interviewers and teachers are able to determine assessments, and are able to manage classroom behaviors, and maintain classroom discipline, and these factors are able to be monitored for purposes of management and control. Performance management, classroom discipline, and educational assessments are therefore not within the regulation [13].

In educational environments, the regulation considers the rights of the child. The ability for children to give consent is eroded as a result of attendance, discipline, and grading structures built into the educational system. The Digital Personal Data Protection Act, 2023, acknowledges children's rights and incorporates a protection mechanism against tracking, behavioral controls, and advertising systems. Monitoring attendance, tracking behaviors, and control systems directed at children are used to justify school administration and do little to protect children's rights. A monitoring and measuring system should therefore be avoided outside of a proven safety and medical need [29], [66].

2.5 PREDICTIVE POLICING BASED SOLELY ON PROFILING OR TRAITS

The prohibition of predictive policing by the AI Act targets the move from evidence of acts to speculation about persons. "Article 5(1)(d) of Regulation (EU) 2024/1689" prohibits AI systems used for making risk assessments of natural persons to evaluate or predict the risk of

a person committing a criminal offence if the assessment is solely based on profiling or on assessing personality traits and characteristics. The provision also delineates a narrow boundary: it does not exclude AI systems used for supporting human judgment of the involvement in criminal activity, as the decision is already based on objective and verifiable facts directly linked to a criminal activity. The rationale behind the legislation is that a State may use tools to organize evidence, but it cannot replace evidence with suspicion of individuals coming from opaque correlations. This is important for biometric governance because the same biometric infrastructure that is used to identify people can be combined with risk scoring, so a face in a camera feed becomes a signal for heightened attention based on past associations, neighborhood patterns, or inferred traits. The EU's ban tries to prevent such a combination if it is based on profiling alone rather than crime-linked facts, thus drawing a rights line against automated suspecthood [14].

2.6 TIMELINES AND PENALTIES

The EU AI Act lays out a sequence of obligations whereby the most important "red lines" come into effect early and carry substantial financial risks. The Regulation will be applicable from 2 August 2026, according to Article 113 of Regulation (EU) 2024/1689, whereas Chapters I and II, which comprise the definitions and the prohibited practices, will be effective from 2 February 2025. The penalty structure is thus used to give the bans a real deterrent effect: Article 99 of Regulation (EU) 2024/1689 stipulates that failure to comply with the prohibitions in Article 5 of Regulation (EU) 2024/1689 shall be punished by administrative fines of up to EUR 35,000,000 or, in the case of an undertaking, up to 7 percent of the total worldwide annual turnover for the preceding financial year, whichever amount is higher. Hence, this equates to biometric prohibitions being able to attract a "board-level" exposure, whereby a prohibited biometric deployment cannot be considered as just a minor compliance gap, but rather it has to be seen as an enforcement event having quantified upper limits. Biometric bans are presented by the sequencing as a matter of urgency and are treated as such by the EU, which requires them to be binding on both the State and private actors even before the wider high-risk controls become fully mature; for instance, these can be seen as the guardrails that should limit both State and private actors in advance [15].

3. EU BIOMETRIC PRIVACY CONTEXT AND ENFORCEMENT

The EU biometric prohibitions are embodied in most of the relevant legal texts, where privacy, data protection, and non-discrimination appear as interdependent constraints on the exercise of

identification power. The EU AI Act considers the design and deployment of systems, while the data protection framework governs the processing of personal data situated in and around such systems. Biometric identifiers are permanent and malleable; the law must encompass the creation of databases, the construction of templates, the comparison of watchlists, the inference of sensitive traits, and the retention and subsequent access for searches. Where enforcement practices are concerned, regulators view indiscriminate facial scraping as an infringement, and not as a technical error. Thus, for India, the lesson is that a statutory prohibition is of great importance when the regulator can investigate, order the cessation of the activity, mandate the removal, and enforce sanctions that are greater than the perceived benefits of the illegal processing activity.

The GDPR and the AI Act have both a complementary and a distinct relationship with one another. The GDPR is applicable in the context of personal data, including, in defined circumstances, biometric data that is used for unique identification. Biometric data is considered high-risk data under Article 9. The AI Act is applicable beyond the bioethical bottleneck, in the design, deployment, and use of AI systems. Even in the absence of a specific case to make a data protection complaint, the GDPR provides a legal basis in the context of processing personal data, and in respect of the purpose limitation, security, transparency, and compliance with the rights of data subjects. In respect of certain high-risk activities, the AI Act provides legal provisions that remove the balancing of interests doctrine, and either provide bans or tightly defined exemptions. The Indian legal system adopts the first of these models in a limited sense and fails to adopt the second model beyond biometrics.

3.1 ECHR: S AND MARPER VS UNITED KINGDOM (BIOMETRIC RETENTION)

In the case of S. and Marper v. The UK (The European Court of Human Rights, 2008) [8] [9], the Grand Chamber ruled that the longstanding practice of law enforcement retaining fingerprints, DNA samples, and profiles, for persons who had never been convicted of an offence, was a violation of Article 8 of the ECHR. The Court recognized the considerable adverse impact of such a practice of law enforcement retaining fingerprints and DNA evidence for future use and policing purposes. The Court provided provisions for the retention of biometric evidence, which included retaining such evidence for a specific purpose, for a set period of time, and in a manner that would provide the evidence for a right to review and remove the evidence, in the specific circumstances for persons who had not been convicted of any criminal offence.

3.2 DPA ENFORCEMENT AGAINST SCRAPED FACIAL DATABASES

The collection of scraped facial recognition databases has been regarded by EU supervisory authorities as one of the most serious infractions of the GDPR. This is because the typical requirements for lawful processing are completely stripped away. From the decisions made, the theory of enforcement is largely the same: just because something is visible on the internet does not mean that consent is given for the inclusion of someone's biometric data, and the collection of images and the creation of a database of them in a searchable, electronic format is a continual intrusion. This allows us to understand the reasoning why Article 5(1)(e) of Regulation (EU) 2024/1689 is in place to prohibit the practice. The AI Act does not remove GDPR restrictions. Rather, it places a priori restrictions on a specific category of scraping that has been the most dangerous and has raised the most supervisory concerns, while the enforcement of the GDPR, with the removal and/or cessation of data, transparency orders, and fines, will still be applicable.

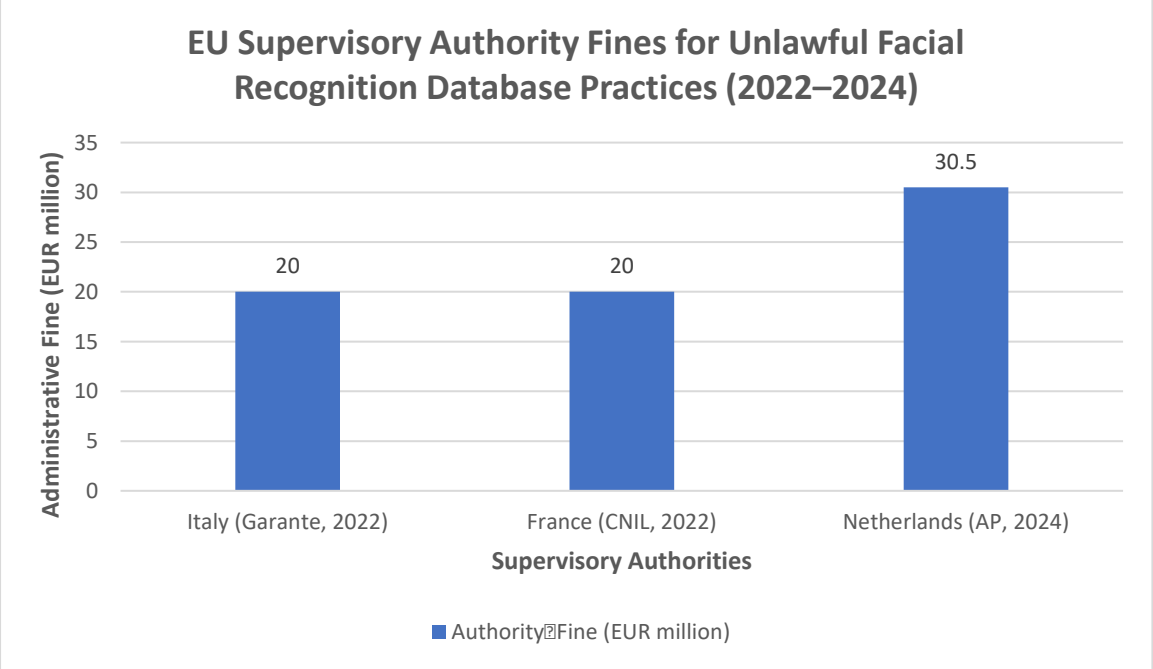


Figure 2

The Clearview AI Enforcement Line illustrates the application of the GDPR-AI Act. The French CNIL imposed a penalty of €20 million on October 20, 2022, for the capture of images published online, conversion of those images to biometric templates, and the provision of a facial recognition search service based on a lack of legal basis and inadequate transparency [22], [23]. On March 9, 2022, the Italian Garante imposed a strict penalty of €20 million and

ordered the immediate halting of the processing and deletion of illicitly processed biometric data of persons located in Italy [24]. The Dutch Autoriteit Persoonsgegevens imposed a penalty of €30.5 million on September 3, 2024, for the continued availability of the database, which was deemed ongoing unlawful processing [25], [26], [27]. These rulings support the notion that deletion and cessation, rather than client restrictions, are the minimum acceptable remedies for biometrically scraped data.

3.3 SCHOOL FRT UNDER GDPR

Facial recognition technology in schools presents the dilemma of the efficient automation of attendance being counterbalanced against coercion, the young age of users, the users' forced dependency on the system, and the gradual normalizing of biometric checks for identity. School systems are not like a free market, where students have the choice to opt out of the system and have to incur no social or academic costs in finding a substitute. The AI Act forbids emotion recognition in classrooms for the same reason that behavioral and affective observation in the classroom may result in the automation of teaching and the reinforcement of classroom control and assessment systems, with no justification. Therefore, the initial position should be non-use, allow narrowly justified use only, where the application can be shown to be safe or for the benefit of health, and only after all other options that are less intrusive have been considered. [28], [29].

With regards to the Swedish Data Protection Authority's decision regarding facial recognition technology used to track student attendance, the authority issued a 200,000 SEK fine to a municipal educational district after a three-week pilot, which used 22 students. The authority classified facial recognition as special-category biometric processing and deemed student consent as a weak legal foundation due to an unequal power dynamic within the compulsory school system and pressure to comply. The authority also determined that the use of biometric technologies was unnecessary, as it could give the same administrative outcome with less interference. The decision is important for India because it shows that even limited scope and temporary use fall short of the principle of proportionality when it comes to the use of biometric systems for the management of school administration.

4. INDIA'S LEGAL FRAMEWORK ON BIOMETRICS AND AI

India's biometric and artificial intelligence governance frameworks depend on constitutional privacy protections, the Aadhaar framework, the Digital Personal Data Protection Act of 2023, and customer-based police or welfare services. Article 21 interpreted alongside Articles 14 and

19 of the Constitution of India calls for a lawful authority, a legitimate purpose, necessity, proportionality, and safeguards when the State either collects or integrates biometric data. The Aadhaar verdicts placed biometric verification within a welfare framework but also cautioned against private gatekeeping and overbroad identity linking. The DPDP Act provides some general obligations about notice, consent, security, and accuracy, as well as data fiduciary assessments of significant data, and potential content neutrality. However, it does not issue a framework for public-facing facial recognition technologies and related biometric artificial intelligence systems.

4.1 RIGHT TO PRIVACY: PUTTASWAMY (2017)

The 2017 privacy ruling is important to biometric AI because it identifies the intersection of dignity, autonomy, equality, and privacy-related access control as the elements of informational privacy. When a biometric system allows the State or a private entity to identify, link, or profile individuals across welfare, education, employment, policing, and movement, it is no longer a neutral administrative system. The proportionality framework of the judgment requires a valid law, a legitimate State aim, necessity, proportionality, and safeguards. In the case of biometric AI, the framework goes further than consent and procurement; it goes to the decisions of the legislature to set constraints of purpose, retention, interlinking of databases, independent accountability mechanisms, and rights to remediation, across a continuum of governance to prevent the normalization of intrusive systems of public governance. [32], [33]

In Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (Supreme Court of India), a nine-judge bench held that privacy is a fundamental right protected through Article 14, Article 19, and Article 21 of the Constitution of India [34]. The Court recognized spatial, decisional, and informational privacy and acknowledged modern databases, identifiers, and analytics increase the risk of surveillance and profiling. The ruling did not determine the validity of Aadhaar, but it provided the test for biometric authentication and data linkage. Its main impact is methodological: the justification of law, necessity, proportionality, and safeguards, rather than administrative convenience, is required for all large-scale biometric systems.

4.2 AADHAAR JUDGMENT (2018)

As the first case to analyze a national identity system against the post-2017 privacy framework, Aadhaar's constitutional analysis is the most substantial Indian case, as it concerns the proportionality of biometric systems. The decision placed constitutional significance on

purpose limitation, exclusion risk, data protection, and constraints on the private use of the system, alongside security and data protection. This case is important in the context of artificial intelligence systems that use biometric data, in that the Court has said the use of biometric data systems in the context of a defined public good may be justified in such systems. However, the Court has said, the same data may not be used to justify systems that carry out private data collection or surveillance systems that are used on the general public. As a result, the decision endorses the need for law to set strict boundaries on the use of facial recognition systems and biometric data in the absence of measures that control the purpose and the scope of the systems [35].

In K. S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1 (Supreme Court of India), the majority affirmed the use of Aadhaar for targeted subsidies, benefits, and services under Section 7 of the Aadhaar Act, 2016, while restricting expansion into the private sector [36]. The Court narrowed the broader use of Section 57 of the Aadhaar Act, 2016, and emphasized purpose control and security, acknowledging the risk of exclusion due to authentication failure. The ruling sustains the welfare essence of Aadhaar, while unrestricted linkages of identity are viewed as constitutionally questionable. From the perspective of biometric artificial intelligence, the ruling promotes opting for alternatives to authentication, limited retention, and grievance rights, as well as the prohibition of using biometric identity as the primary means of imposing adverse civil consequences [37].

4.3 DPDP ACT 2023 AND DPDP RULES 2025

The Digital Personal Data Protection Act, 2023, formulates a more general model for regulating digital personal data, as opposed to a separate category for sensitive personal data. Thus, biometric data linked to an identifiable person is included in the Act when processed digitally. Nevertheless, the Act does not create biometric-specific exceptions equivalent to bans in Article 5 of Regulation (EU) 2024/1689. Section 8 creates obligations for accuracy, security, breach notification, and erasure, and Section 10 allows the classification of Significant Data Fiduciaries by considering the volume and sensitivity of data, and the risks related to the exercise of rights, public order, and State security. Section 9 creates a presumption of sensitivity for the data of minors and bans data tracking and data-driven behavioral analysis without the verifiable consent of a parent or guardian. The Digital Personal Data Protection Rules, 2025, which were issued on November 14, 2025, operationalize different components of the Act by specifying certain procedures, although they do not offer a warrant-like framework for public

facial recognition and data collection via the internet without specific targets, data collection for inferring emotions, and data collection for the purpose of categorizing biometric traits deemed sensitive.

4.4 LAW-ENFORCEMENT FRT IN INDIA

Rather than a comprehensive legislative act, the Indian law enforcement's use of facial recognition technology (FRT) has evolved through several avenues, namely, awarding of contracts, pilot projects, court-ordered experiments, and practices in investigative work. The National Crime Records Bureau (NCRB) described a project to create an Automated Facial Recognition System (AFRS) as a step toward a deeper integration of the technology and an imagined national system of searching images against databases of criminal records, missing persons, and unidentified corpses [41]. Reports show use at the state and city levels for policing, controlling public gatherings, searches for missing children, and securing events. The issue is not the existence of a public-safety intent. The problem is inadequate laws surrounding the technology to define the parameters of watchlists, control accuracy, define retention and logging periods, establish mandatory human review and public accountability reports, or provide recourse for erroneous matches. In the absence of such laws, procurement contracts serve as a substitute for legitimate control [40], [42], [43].

In S. Q. Masood v. State of Telangana, LAWS(SC)-2022-4-111, the Supreme Court of India examined facial recognition and surveillance practices. Its analysis makes a case about the unresolved constitutional space of public biometric identification in India [44]. It is reported that the petition asked about the facial recognition databases and identification practices carried out in the field in the absence of consent, limits on data retention, independent oversight, or a provision in law [45], [46]. This case is important because it conceptualizes facial recognition as a form of data collection that is much more advanced. The case demonstrates that a face is a persistent identifier that can link a person to a location, can associate a person, and can track a person in a given space, with given people, over time. The case also demonstrates the dangers of relying on the judiciary to review the case ex post facto to check if the case is in compliance with the constitution, when the practice continues to be deployed by the executive without any clear and settled standards [47].

Sadhan Haldar v. State (NCT of Delhi) & Ors. demonstrates [48] that while facial recognition technology has protective purposes in the context of missing children, [45] usability (i.e., capability to deliver an adequate result), the quality of matches, and the technical

impenetrability of the system have been and continue to be valid points of criticism [49]. The legal lesson is not that protective uses of biometric technologies must be entirely prohibited. The lesson is that even uses of biometric technologies that have a protective purpose must be deployed after establishing the legal framework, the dataset must be audited, a legal framework must be established to define the thresholds and limits of data retention, and adverse action must not be taken based solely on an algorithmic match.

EU ban and legal cite	**Scope and exceptions**	**Current Indian law/practice**	**Gap**	**Proposed Indian action**
Article 5 ban on real-time RBI in public spaces for law enforcement, with strict exceptions and prior authorisation	Allowed only for defined objectives such as missing persons and serious crime, with authorisation, limits, and deletion duties	No dedicated statute; deployments occur via policing practice and pilots, sometimes under court supervision	No statutory warrant-like scheme; weak transparency	Enact a default ban with narrow, time-bound exceptions requiring prior judicial or independent authorisation and logging
Article 5: Prohibition on untargeted scraping to develop facial recognition databases	Categorical ban	No explicit statutory bar; DPDP relies on purpose, consent, and exemptions	Dataset creation can outrun oversight.	Create an express statutory prohibition on untargeted scraping for biometric databases across public and private actors.
Article 5 ban on biometric categorisation for sensitive traits	Categorical ban	DPDP contains no sensitive-data category; constitutional equality exists,	No clear red line for inference systems	Enact a ban on biometric inference that categorises by protected or sensitive traits,

		but lacks an operational rule		with narrow, audited research exceptions if any.
Article 5 ban on emotion recognition in workplaces and schools	Categorical ban in those contexts	No sectoral ban; DPDP child protections can be engaged, yet do not directly prohibit emotion inference	Consent becomes coerced; monitoring normalised.	Adopt a bright-line prohibition through statute, supported by labour and education regulators.
Article 5 prohibition on certain criminal risk prediction based solely on profiling	Ban on prediction based solely on profiling/traits	No explicit prohibition; smart policing narratives and analytics projects proceed without a unified legal frame	Risk of biased enforcement loops	Statutory bar on predictive policing solely from profiling, with strict oversight for any permitted analytic use

Table 1: *Comparative Table of EU Artificial Intelligence Act Article 5 Bans and Corresponding Indian Legal Position under the Constitution, Digital Personal Data Protection Act, 2023, and Sectoral Practices, Highlighting Gaps and Proposed Statutory Actions for Harmonised Biometric Governance*

5. LESSONS FOR INDIA

The EU AI Act provides an opportunity for India to engage in constitutionally informed proportionality. An important consideration is that proportionality can be more than post-litigation balancing. It provides scope for statutory prohibitions where the infringement of rights is probable, severe, and irreparable. Litigation on Aadhaar and the Indian FRT an illustration of how a restrictive public good approach to ID can easily morph into routine verification, policing, and private sector compliance. The DPDP Act does provide some level of data protection and duty. However, the risks and threats posed by AI and biometrics call for

additional protections in the form of banned practices with limited exceptions, advance permission, audit log retention, duty to delete, independent oversight, and a right to redress for the harmed and impacted persons.

5.1 COUNTER-ARGUMENTS SUPPORTING LIMITED BIOMETRIC USE

Totally dismissing biometrics is not a proper representation of proportionality. It is not unreasonable to consider the use of biometric matching in finding lost minors, identifying unconscious or recently deceased individuals, deterring identity fraud for the delivery of social services, securing sensitive locations, and investigating severe crimes for which other means of ID do not suffice. The state has a duty to fulfill. Proportionality should not be equated with uncontrolled/absolute. The limited use of biometrics should be justified under a formally approved and clear purpose statute, and be supplemented by independent prior approval, adequate technical means, and a human referee should be employed to ensure that matches made are endorsed.

Lessons for India	Codify Bright-Line Bans in a Sector-Neutral Statute	Ban untargeted scraping, biometric categorization, emotion recognition, and predictive policing.
		Base bans on Articles 14 and 21 of the Constitution as inherently disproportionate. [50]
		DPDP Act provides the framework; biometric law defines offences and penalties.
	Narrow, Time-Bound Exceptions with Prior Authorization	Allow real-time identification only with judicial or independent authorization.
		Restrict to time-limited, purpose-specific uses such as locating missing persons or serious crimes.
		Maintain real-time logs and delete data post-use. [51]
	Independent Oversight and Remedies	Create a biometric licensing unit with power to suspend or refuse high-risk uses.
		Ensure complaint channels for victims of misidentification with enforceable deletion orders.
		Reduce constitutional litigation by offering quicker administrative redress. [52]
	DPIA and Transparency by Default	Mandate Data Protection Impact Assessments (DPIA) for all biometric uses.
		Publish DPIA summaries with details on dataset origin, retention, and error rates. [53]
		Transparency ensures legality and accountability in biometric governance. [54]
	Deterrent Penalties Harmonised with Turnover	Link fines to company turnover or vendor revenue share.
		Enforce personal accountability for senior officials in deliberate breaches. [5]
		Prevent large firms from treating penalties as routine costs. [56]
	Public Procurement and Standards	Include enforceable clauses in tenders for bans, deletion, and audit access.
		Require disclosure of testing data and suspend poorly performing systems.
		Ensure public procurement supports lawful and transparent biometric use. [57]

Figure 3: Legislative and Compliance Lessons for India Derived from the EU Artificial Intelligence Act

6. EXTRATERRITORIALITY AND COMPLIANCE FOR INDIAN COMPANIES

Employing a market-and-output model, Regulation (EU) 2024/1689 may capture Indian providers and deployers as non-EU participants. Article 2 expands coverage to providers who place AI systems and general-purpose AI models in the EU, deployers based in the EU, and third-country providers or deployers if the AI system's output is used in the EU. Thus, Indian biometric vendors will be subject to EU requirements if they provide facial recognition, emotion-based, and biometric classification and risk-assessment scoring systems to clients in the EU or if such systems generate outputs used in EU workflows. Since Article 5 bans apply

at the level of the activity, contractual language cannot circumvent the ban on certain functionalities. Products directed to the EU market must have features that are legally used, meet documented use cases, and have audit logs, retention controls, and the ability to enforce restrictions on use by customers [58].

The table below attempts to analyze the compliance ramifications of various standard business practices of Indian firms in the EU context, following the AI Act roles. The role analysis should take place during the initial stages of product design and again at the contracting stage. Because of where the system is deployed, a provider, deployer, subcontractor, or service supplier may fall within the scope of EU obligations. The outputs may also be used in the EU. Given Article 5, wherein certain products are completely banned from the market, biometric tools are especially risky. The Indian DPDP may help with compliance and privacy governance; however, they cannot fill the void of the EU's bans on facial scraping, workplace emotion assessment, biometric categorization of sensitive traits, and profiling for the criminal justice system [59].

Business scenario	**Triggered role under AI Act**	**Applicable bans or duties**	**Practical steps**
Indian vendor sells facial recognition software to an EU police or security buyer.	Provider placing an AI system on the EU market.	"Article 5" constraints on real-time RBI in public spaces and other prohibited practices	Remove banned functions by design, enforce strict configuration controls, document lawful use scope, build audit logging and deletion defaults.
An Indian firm provides a cloud API for emotion recognition used by an EU employer.	Provider; output used in the Union	"Article 5" ban on emotion recognition in workplaces	Disable EU access for the feature, block workplace use cases through contract and technical controls, redesign the product for non-banned analytics
Indian analytics company delivers "risk scores" for EU-	Provider or deployer whose output	"Article 5" prohibition where risk prediction relies	Rebuild model governance to require offence-linked, verifiable

facing policing workflows.	is used in the Union	solely on profiling/traits	inputs, prevent sole-profiling outputs, document oversight, and review gates.
An Indian contractor runs biometric categorisation on images supplied by an EU client.	Deployer or processor whose output is used in the Union	"Article 5" ban on biometric categorisation for sensitive traits	Stop the service for EU use, redesign to remove sensitive-trait inference, and adopt strict dataset provenance controls
An Indian platform builds a facial database via untargeted scraping then licenses it to EU customers.	Provider placing system on the EU market	"Article 5" ban on untargeted scraping for facial databases	Terminate scraping pipeline, purge unlawful datasets, adopt documented lawful collection pathways, and add compliance attestation in procurement

Table 2: Common Indian Business Scenarios Mapped to Roles and Compliance Obligations About the EU Artificial Intelligence Act (Regulation (EU) 2024/1689) – Focus on Article 2 Scope and Article 5 Bans

To begin a compliance checklist for Indian providers and deployers, role classification as per Article 2 of Regulation (EU) 2024/1689 must be done, followed by a review of prohibitions as per Article 5. The company must make sure that no product option allows customers' unconsented data to be scraped for facial recognition databases, for sensitive traits biometric categorization, for emotional recognition in workplaces/schools, or for criminal profiling (and subsequently likely to be classified as criminal case risk) identification. Uncontrolled remote recognition of biometrics in a public space must be assumed to be enabled, unless the exception, as per the European Union law, is evident. Among the many technical safeguards, customers must be prevented from enabling forbidden functions on the system, as per the terms of the contract. The contracts should provide for audit rights, provisions relating to deletion, and termination for misuse. Nevertheless, technical safeguards must take precedence.

6.1 LIMITATIONS OF THE STUDY

There are multiple constraints to consider. This analysis is limited to legal texts, reported judgments, official enforcement materials, and publicly available accounts of biometric

deployments; it does not study FRT accuracy, vendor datasets, or police workflows in the field. Indian litigation on facial recognition is uneven, and not all deployments disclose tenders, audits, or court documentation. For this reason, the comparison with the EU AI Act is more about what is normative and structural than saying India can blindly adapt the EU model. Federal policing, procurement leaks, and DFDP Board interventions will also impact the direction of reform in the practical realm.

7. CONCLUSION

Article 5 of the EU AI Act proposes a minimum rights floor for biometric AI and establishes certain practices as incompatible with the standard of governance in cases of operational imbalances of power, scale, identity linkage, and opaqueness, with the provision of subsequent remedies. The Indian provisions on proportionality in Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (Supreme Court of India), and K. S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1 (Supreme Court of India) include the necessary balancing tools, yet lack sufficiency with respect to public space facial recognition, facial recognition databases, and the inference of emotions and traits [60], [61]. This balancing exercise should recognize the legitimate interests of the State in the protection of the integrity of welfare and in searches for missing persons and the detection of serious crimes, as well as a legal presumption that would require the use of less intrusive practices if available to achieve the same effect. A rights-preserving Indian model would, therefore, combine clear and strict prohibitions, narrow frameworks of permission, independent oversight, obligations to ensure technical accuracy, deletion policies, public accountability, and deterrent penalties. The DPDP Act and the DPDP Rules establish a solid foundation for the governance of data, yet the integration of biometric AI in deployment practices requires a truly cross-sectional legislative framework, the goal of which would be to operationalize legitimacy and accountability ex ante [62], [66].

8. SUGGESTIONS

The subsequent reforms derive enforceable statutory, regulatory, and procurement measures from the framework of proportionality outlined in the constitutions of the member states, following a comparative analysis of the EU's biometric prohibitions and India's privacy framework.

1. Enact a sector-neutral "Biometric Uses and Safeguards Act". The statute should define and prohibit: (a) creating or extending facial-recognition databases through indiscriminate facial recognition; (b) implementing workplace and school systems for recognition of emotions; (c) revealing sensitive traits through biometric classification; and (d) conducting predictive policing through trait or personality profiling. The DPDP Act may establish baseline data duties; however, these prohibitions should only be removed through a specific statutory exception. The consequences should encompass turnover-related civil liability and individual civil liability for intentional breaches.
2. Warrant-style Pre-Authorization A warrant-style framework is used for real-time remote biometric identification in public spaces to request authorization for a specific use case with various constraints, including a geo-fence, confidence threshold, duration, prioritized watchlist, retention period, and duty to delete. Outside of the required framework, use is allowed for emergencies, but only for a short duration. Independent approval must be requested within 24 hours. If approval is denied, all non-hit data, the probe images, and watchlist-related requests must be immediately deleted. A public after-action summary and a rights impact assessment of the framework must be provided.
3. Facial datasets that have been scraped and are not targeted cannot be acquired, leased, or purchased. All vendors must provide documentation and attestations on provenance, consent, and demonstrated sources, gaps in data, and audits. If the provenance requirement is not met, contracts must be canceled, vendors must be blacklisted, and data must be deleted with the return of public funds. Data that has been scraped lawfully must be retained according to a schedule and accompanied by a datasheet. No agency may integrate or combine datasets without a new legal authorization.
4. For all high-risk biometric systems, a Data Protection Impact Assessment (DPIA) and public transparency will be required. A DPIA summary will be made available to the public, detailing the purpose and legal standing, the alternatives and anticipated accuracy and error rates, how long data will be kept, the level of human review, and the plans for red-team testing, with only narrow security redactions. This summary will be revised at least once a year and whenever there is a substantial change to the model, dataset, thresholds, or watchlist. Until this summary is made publicly available and reviewed by the Oversight Authority, no procurement, pilot deployment, or funding will be allowed.

5. Compulsory accuracy, bias, and field testing will be required. Biometric systems will be validated before and after deployment to control the rates of false positives and false negatives at an acceptably low level across demographics and image quality. Biometric systems must be tested by an independent 3rd party laboratory, and must be validated on field testing data rather than vendor-provided data. Systems that fail to meet these requirements will be decommissioned until the required changes have been made, validation testing has been performed, and independent certification has been granted.
6. Impose rigid logging, retention, and deletion policies sustained with verified evidence. Each search should be logged with the requesting officer, legal authority, version of the watchlist, threshold, probe image, match outcome, review, and result in logs that are tamper-proof. Unless retained for audit or litigation, probe images and non-matches should be deleted within 24 hours. Deletions of hits are required unless they are linked to a case. Transparency reports issued every quarter should include compliance with deletions and cryptographic or other evidence of deletion.
7. Establish a Biometric Oversight Unit. It will oversee the registration of deployments, approval of high-risk use, inspections of models and documents, requests for raw logs, and requests for use suspensions, as well as publishing annual reports. It may be a part of or the adjacent unit to the Data Protection Board; however, it must have its own dedicated experts in technology, law, and human rights. Complaint resolution will have set deadlines, and it will have the power to rapidly suspend the use of a system to protect human rights in case of high threats. The Unit will be funded by charging a licensing fee to the entities that deploy high-risk biometric systems.
8. Due process and safeguards will be enhanced for remedies and evidence. No detention, denial of service, disciplinary action, or punishment shall be based solely on the result of an algorithmic biometric match. Independent evidence must be available to support adverse action. Minimum damages and fee-shifting will apply when rights are proven in cases of misidentification, unlawful enrolment, excessive retention, and unauthorised disclosure for which a direct and statutory civil remedy will be applicable. Evidence obtained through unauthorised biometric surveillance will be liable to be dismissed, and affected persons will be formally and legally assisted.
9. Make it non-negotiable that public procurement safeguards rights. Tender papers should stipulate the inclusion of model cards, system cards, dataset sheets, audit hooks, security documentation, threshold disclosure, bias test results, deletion controls, and

termination rights risk clauses. Contracts should have model and configuration escrow for audit, vendor cooperation, and interoperability obligations to avoid lock-in. Milestone payments should be linked to independent testing, in the field, for accuracy and bias, under the most realistic scenarios.

10. Create capacity and limit sandboxes to opt-in, controlled settings. Police officers, prosecutors, judges, data protection officers, school administrators, and procurement officials should be trained on match thresholds, interpretation of errors, and on human corroboration and rights preserving workflows. Annual transparency reports should document the category of deployment, governance of watchlists, complaints, suspensions and their outcomes. Sandboxes should be allowed only with direct opt-in, independent ethics approval, a specific timeframe, a clear public interest goal, deletion requirements, and automatic expiration, unless the oversight authority posts a measurable public benefit and approves of the rights risk.

BIBLIOGRAPHY

[1] India Code. (n.d.). *Section 29: Restriction on sharing information*. Retrieved January 7, 2026, from https://www.indiacode.nic.in/show-data?actid=AC_CEN_37_85_00001_201618_1517807328460&orderno=32&sectionId=3607&sectionno=29

[2] Bhatia, G. (2014). State surveillance and the right to privacy in India: A constitutional biography. *National Law School of India Review, 26*, 127–152.

[3] Singh, S. S. (2011). Privacy and data protection in India: A critical assessment. *Journal of the Indian Law Institute, 53*, 663–677.

[4] *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*, (2019) 1 SCC 1 (Supreme Court of India).

[5] Rudschies, C., & Schneider, I. (2025). The long and winding road to bans for artificial intelligence: From public pressure and regulatory initiatives to the EU AI Act. *Digital Society, 4*, 57.

[6] van Kolfschooten, H., & van Oirschot, J. (2024). The EU Artificial Intelligence Act (2024): Implications for healthcare. *Health Policy, 149*, 105152.

[7] Artificial Intelligence Act. (n.d.). *High-level summary of the AI Act*. Retrieved January 8, 2026, from https://artificialintelligenceact.eu/high-level-summary/

[8] European Commission. (n.d.). *Regulatory framework for artificial intelligence*. Retrieved January 9, 2026, from https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

[9] Voigt, P., & von dem Bussche, A. (2024). *The EU AI Act: Regulation of artificial intelligence* (1st ed.). Springer.

[10] Kuru, T. (2024). Lawfulness of the mass processing of publicly accessible online data to train large language models. *International Data Privacy Law, 14*, 326. https://doi.org/10.1093/idpl/ipae013

[11] European Commission. (n.d.). *Recital 30*. AI Act Service Desk. Retrieved January 5, 2026, from https://ai-act-service-desk.ec.europa.eu/en/ai-act/recital-30

[12] Artificial Intelligence Act. (n.d.). *Article 5: Prohibited artificial intelligence practices*. Retrieved January 7, 2026, from https://artificialintelligenceact.eu/article/5/

[13] Matulionyte, R., Zalnieriute, M., et al. (Eds.). (2024). *The Cambridge handbook of the law, ethics and policy of artificial intelligence* (1st ed.). Cambridge University Press.

[14] Neuwirth, R. J. (2023). Prohibited artificial intelligence practices in the proposed EU Artificial Intelligence Act (AIA). *Computer Law & Security Review, 48*, 105795.

[15] European Parliament. (2025, February 19). *EU AI Act: First regulation on artificial intelligence*. Retrieved January 5, 2026, from https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

[16] Voigt, P., & von dem Bussche, A. (2024). *The EU AI Act: Regulation of artificial intelligence* (1st ed.). Springer.

[17] *S. and Marper v. the United Kingdom*, Applications Nos. 30562/04 & 30566/04 (European Court of Human Rights, December 4, 2008).

[18] European Court of Human Rights. (2008, December 4). *S. and Marper v. the United Kingdom* (Applications Nos. 30562/04 & 30566/04) [Judgment]. HUDOC. Retrieved January 4, 2026, from https://hudoc.echr.coe.int/fre?i=001-90051

[19] European Court of Human Rights. (2008, December 4). *Grand Chamber judgment: S. and Marper v. United Kingdom* [Press release]. HUDOC. Retrieved January 3, 2026, from https://hudoc.echr.coe.int/eng-press?i=003-2571936-2784147

[20] Kuru, T. (2024). *Lawfulness of the mass processing of publicly accessible online data to train large language models* [PDF]. Retrieved January 2, 2026, from https://academic.oup.com/idpl/advance-article-pdf/doi/10.1093/idpl/ipae013/59696479/ipae013.pdf

[21] Reuters. (2025, October 28). *Clearview AI faces a criminal complaint in Austria for suspected privacy violations*. Retrieved January 3, 2026, from https://www.reuters.com/sustainability/society-equity/clearview-ai-faces-criminal-complaint-austria-suspected-privacy-violations-2025-10-28/

[22] European Data Protection Board. (2022, October 20). *The French SA fines Clearview AI EUR 20 million*. Retrieved January 2, 2026, from https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en

[23] European Data Protection Board. (2023, May 11). *Facial recognition: The French SA imposes a penalty payment on CLEARVIEW AI*. Retrieved January 1, 2026, from https://www.edpb.europa.eu/news/national-news/2023/facial-recognition-french-sa-imposes-penalty-payment-clearview-ai_en

[24] European Data Protection Board. (2022, March 10). *Facial recognition: Italian SA fines Clearview AI EUR 20 million*. Retrieved December 31, 2025, from https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

[25] European Data Protection Board. (2024, September 3). *Dutch Supervisory Authority imposes a fine on Clearview because of illegal data collection for facial recognition*. Retrieved January 9, 2026, from https://www.edpb.europa.eu/news/national-news/2024/dutch-supervisory-authority-imposes-fine-clearview-because-illegal-data_en

[26] Autoriteit Persoonsgegevens. (2024, September 3). *Decision fine Clearview AI*. Retrieved January 8, 2026, from https://www.autoriteitpersoonsgegevens.nl/en/documents/decision-fine-clearview-ai

[27] Autoriteit Persoonsgegevens. (2024, September 3). *Decision fines and orders subject to a penalty: Clearview* [PDF]. Retrieved January 7, 2026, from https://www.autoriteitpersoonsgegevens.nl/en/system/files?file=2024-09%2FDecision+fines+and+orders+subject+to+a+penalty+Clearview.pdf

[28] Matulionyte, R., Zalnieriute, M., et al. (Eds.). (2024). *The Cambridge handbook of the law, ethics and policy of artificial intelligence* (1st ed.). Cambridge University Press.

[29] Swedish Data Protection Authority. (2019, August 20). *Supervision pursuant to the General Data Protection Regulation (EU) 2016/679 – facial recognition used to monitor the attendance of students* [Decision]. Retrieved January 6, 2026, from https://www.imy.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf

[30] Bhandari, V., & Sane, R. (2019). A critique of the Aadhaar legal framework. *National Law School of India Review, 31*(1), 72–97.

[31] Panigrahi, P., & Mehta, A. (2022). The impact of the Puttaswamy judgement on data protection regimes in India. *NUJS Law Review, 15*(1). Retrieved January 10, 2026, from https://nujslawreview.org/wp-content/uploads/2022/07/15.1-Panigrahi-Mehta-2.pdf

[32] Supreme Court of India. (2017). *Right to privacy: Puttaswamy judgment (Chandrachud, J.)* [PDF]. Retrieved December 31, 2025, from https://www.scobserver.in/wp-content/uploads/2021/10/1-266Right_to_Privacy__Puttaswamy_Judgment-Chandrachud.pdf

[33] Supreme Court of India. (2017, August 24). *Justice K.S. Puttaswamy (Retd) and Another v. Union of India and Others*. Indian Kanoon. Retrieved January 1, 2026, from https://indiankanoon.org/doc/91938676/

[34] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (Supreme Court of India).

[35] Ramnath, N. S., & Assisi, C. (2018). *The Aadhaar effect: Tracking the impact of India's biggest ID project* (1st ed.). Oxford University Press.

[36] *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*, (2019) 1 SCC 1 (Supreme Court of India).

[37] Matthan, R. (2023). *The third way: India's revolutionary approach to data governance* (1st ed.). Juggernaut Books.

[38] Saurabh, S. (2024). The Digital Personal Data Protection Act of 2023: Strengthening privacy in the digital age. *Indian Journal of Integrated Research in Law, 4*, 1183–1198.

[39] Katkuri, S. (2025). A critical analysis of the Digital Personal Data Protection Act, 2023. *International Journal of Law, 11*(10), 22–24.

[40] Bansal, V. (2022, August 21). *The low threshold for face recognition in New Delhi*. Wired. Retrieved January 5, 2026, from https://www.wired.com/story/delhi-police-facial-recognition/

[41] Government of India. (2020, June 22). *eProcurement System Government of India* [Tender notice]. Retrieved January 4, 2026, from https://eprocure.gov.in/eprocure/app?component=%24DirectLink&page=FrontEndViewTender&service=direct&sp=S%2B6yRhk%2BPBLNDUmlDZkD8DQ%3D%3D

[42] Jain, A. (2020, October 7). *Watch the Watchmen series part 4: The National Automated Facial Recognition System*. Internet Freedom Foundation. Retrieved January 3, 2026, from https://internetfreedom.in/watch-the-watchmen-series-part-4-the-national-automated-facial-recognition-system/

[43] Government of India. (2020, June 22). *Request for proposal to procure National Automated Facial Recognition System (AFRS)* [Tender notice]. Retrieved January 8, 2026, from https://eprocure.gov.in/eprocure/app?component=%24DirectLink&page=FrontEndViewTender&service=direct&sp=S%2B6yRhk%2BPBLNDUmlDZkD8DQ%3D%3D

[44] *S. Q. Masood v. State of Telangana*, LAWS(SC)-2022-4-111 (Supreme Court of India, April 27, 2022).

[45] Thomson Reuters Foundation. (2022, January 20). *Facial recognition taken to court in India's surveillance hotspot*. Al Jazeera. Retrieved January 2, 2026, from https://www.aljazeera.com/news/2022/1/20/india-surveillance-hotspot-telangana-facial-recognition-court-lawsuit-privacy

[46] The Times of India. (2022, January 4). *PIL says Telangana illegally using facial recognition tech, HC issues notice*. Retrieved January 1, 2026, from https://timesofindia.indiatimes.com/india/pil-says-telangana-illegally-using-facial-recognition-tech-hc-issues-notice/articleshow/88676854.cms

[47] Jain, A. (2020, April 22). *We wrote to NCRB and MHA requesting them to halt their ongoing National Automated Facial Recognition System (AFRS) project #SaveOurPrivacy*. Internet Freedom Foundation. Retrieved January 6, 2026, from https://internetfreedom.in/we-wrote-to-ncrb-and-mha-requesting-them-to-halt-their-ongoing-national-automated-facial-recognition-system-afrs-project/

[48] *Sadhan Haldar v. State (NCT of Delhi) & Ors.*, W.P. (Crl.) 1560/2017 (Delhi High Court, January 10, 2020).

[49] Cuthbertson, A. (2018, April 23). *Indian police trace 3,000 missing children in just four days using facial recognition technology*. The Independent. Retrieved December 31, 2025, from https://www.independent.co.uk/tech/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html

[50] Neuwirth, R. J. (2023). Prohibited artificial intelligence practices in the proposed EU Artificial Intelligence Act (AIA). *Computer Law & Security Review, 48*, 105795.

[51] Artificial Intelligence Act. (n.d.). *Article 5: Prohibited artificial intelligence practices*. Retrieved January 7, 2026, from https://artificialintelligenceact.eu/article/5/

[52] Voigt, P., & von dem Bussche, A. (2024). *The EU AI Act: Regulation of artificial intelligence* (1st ed.). Springer.

[53] Kuru, T. (2024). Lawfulness of the mass processing of publicly accessible online data to train large language models. *International Data Privacy Law, 14*, 326. https://doi.org/10.1093/idpl/ipae013

[54] van Bekkum, M. (2025). Using sensitive data to de-bias AI systems: Article 10(5) of the EU AI Act. *Computer Law & Security Review, 56*, 106115.

[55] Artificial Intelligence Act. (n.d.). *Article 99: Penalties*. Retrieved January 3, 2026, from https://artificialintelligenceact.eu/article/99/

[56] European Commission. (n.d.). *Article 99: Penalties*. AI Act Service Desk. Retrieved January 4, 2026, from https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-99

[57] Matthan, R. (2023). *The third way: India's revolutionary approach to data governance* (1st ed.). Juggernaut Books.

[58] Kuru, T. (2024). Lawfulness of the mass processing of publicly accessible online data to train large language models. *International Data Privacy Law, 14*, 326. https://doi.org/10.1093/idpl/ipae013

[59] Neuwirth, R. J. (2023). Prohibited artificial intelligence practices in the proposed EU Artificial Intelligence Act (AIA). *Computer Law & Security Review, 48*, 105795.

[60] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (Supreme Court of India).

[61] *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*, (2019) 1 SCC 1 (Supreme Court of India).

[62] Press Information Bureau, Government of India. (2025, November 17). *DPDP Rules, 2025 notified* [PDF]. Retrieved January 2, 2026, from https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251117695301.pdf

[63] Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (1st ed.). PublicAffairs.

[64] O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy* (1st ed.). Crown.

[65] European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, General Data Protection Regulation. EUR-Lex. Retrieved May 17, 2026, from https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[66] India Code. (2023). The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). Retrieved May 17, 2026, from https://www.indiacode.nic.in/handle/123456789/22037?view_type=browse