INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA).*

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

USE OF AUTOMATED FACIAL RECOGNITION TECHNOLOGY-LEGALITY AND ITS IMPLICATIONS ON RIGHT TO PRIVACY

AUTHORED BY - MR.HANUMANTHAPPA G T
Research Scholor P.G Department of studies in Law Karnatak University Dharwad

ABSTRACT

Automated Facial Recognition Systems (AFRS) have become one of the most important technological advances of the contemporary world and revolutionized the areas of governance, security, surveillance, and online identification. These systems apply the artificial intelligence, biometric analysis, and machine learning algorithms in tracking or confirming people based on their faces. Facial recognition technology is becoming more commonly used in crime prevention, border security, airport control, attendance, banking authentication and administration of populations around the world. AFRS implementation in India has been growing quickly by a number of governmental programs such as the suggested National Automated Facial Recognition System (NAFRS). Although it may have some benefits, the implementation of the facial recognition technology has grave legal, constitutional, and ethical issues. Facial data collection and storage entails sensitive biometric data, which presents the threat of invasion of privacy, mass surveillance, false identification, algorithms bias, and misuse by the government or individuals. Without a certain statutory framework governing AFRS in India, it is questionable whether there will be legality, accountability, transparency, and procedural safeguards. The seminal case of Justice K.S. Puttaswamy v. Union of India acknowledged privacy as a basic right under Article 21 of the Constitution, and thus all surveillance actions must meet the legality, necessity and proportionality requirements. This paper is a critical discussion of the concept, operation, use, and implications of Automated Facial Recognition Systems. It examines the legal system in place in India, applicable constitutional provisions, judicial decisions and international comparative practices. The paper contends that India is in dire need of a rights-based and committed regulatory framework of AFRS. This framework must guarantee transparency, judicial checks and balances, data reduction, responsibility, anti-discrimination protections and penalties against abuse. The article concludes that technological advancement and freedom of the press can only co-exist

ISSN: 2582-6433

when innovation is informed by rules of law and the constitution.

Keywords: Automated Facial Recognition Systems, AFRS, Privacy, Surveillance, Biometric Data, Artificial Intelligence, Fundamental Rights, Article 21, Puttaswamy Case, Data Protection, India, Constitutional Law, State Surveillance, And Regulatory Framework.

I. INTRODUCTION

The booming development of science and technology has dramatically changed nearly all aspects of human life, such as the government, law enforcement, business, education, and social life. In the present digital age, governments throughout the world are turning more to technological tools to enhance efficiency, security, and administrative operations. Facial recognition technology has become one of the most controversial and powerful innovations of these. It has attracted massive publicity due to its capability to detect people rapidly, automatically and sometimes even without actual physical contact. Facial recognition is a very potent tool in contemporary administration unlike conventional forms of identification like identity cards, passwords or fingerprints, which require one to be physically present in the presence of the administration to be identified.

Automated Facial Recognition Systems (AFRS) work by taking a snapshot of the face of an individual, processing distinctive facial features and comparing those features to a database to identify who they are or find possible matches. AFRS can analyze large data volumes in real time through artificial intelligence, machine learning, and biometric analysis. Some of the ways this technology has been marketed to be very useful include crime prevention, suspect identification, missing children, border control, airport security, attendance check, banking verification and access control systems. The numerous advocates claim that AFRS enhances the efficiency of operations, minimizes human errors, and enhances national security.

Facial recognition systems have become of great interest in India in recent years. Facial recognition technologies have been tested or implemented in multiple state agencies and governmental bodies in airports, railway stations, traffic management systems, police investigations, and other large public gatherings. The proposed National Automated Facial Recognition System (NAFRS) was seen as a centralized system, which would have been able to combine criminal databases and would help police agencies in locating the suspects and

ISSN: 2582-6433

missing persons. Facial recognition has also been adopted by different police departments in protests, elections and even during events in order to keep order and monitor crowds. But the increasing use of AFRS has also cast some grave legal, constitutional and ethical issues. India does not have a particular and detailed legislation that governs the facial recognition technology. Without any clear legal protection, there is uncertainty about the gathering, storing, distributing, and keeping of biometric information. Facial data unlike other personal information, is sensitive and non-retractable, as an individual cannot easily change his or her face, like a password or an identification number. The unauthorized access or abuse of such data can put individuals at risk of long-term privacy.

The main problem is how to reconcile both the safety of the people and constitutional rights. AFRS can be used to add to safety and administrative convenience, however, it also allows constant monitoring of citizens in open areas. This kind of surveillance may infringe on the right to privacy, discourage free speech and right of assembly, and instill fear in the people who will feel that they are under constant surveillance. It is also feared that women, minorities, or marginalized groups may be wrongly suspected or discriminated against by the face recognition systems since they could give an inaccurate identification.

Thus, the controversy about AFRS is not just about technology but is a profoundly constitutional and democratic issue. A contemporary legal framework should have in place a system that does not allow civil liberties to be eroded by technological innovation. That is why the existence of a strong regulatory framework is needed to ensure transparency, accountability, necessity, proportionality, and adequate remedies against abuse. It is only with a proper regulation that India can reap the rewards of the facial recognition technology without infringing on the dignity and the rights of its citizens.

2. RESEARCH PROBLEM

The main legal and policy issue related to Automated Facial Recognition Systems in India is that there is no particular legislative act that regulates the usage, implementation, data processing criteria, and the responsibility of such systems. Facial recognition technology is increasingly used by police authorities, transport agencies and administrative institutions despite the fact that there exists no special legislation that clearly spells out when and how the systems can be effectively used. This raises grave doubts as to legality, procedural protection,

ISSN: 2582-6433

and constitutionality.

Facial recognition technology deals with collecting and processing information of biometric type which is one of the most sensitive types of personal information. Biometric data, in contrast to normal personal information, is specific to each person and once lost, it cannot be readily altered. Without any clear legal regulation, citizens are left uninformed on the location of facial data collection, duration of storage, sharing of data with third parties, and the purpose of using such data. This cloudiness augments the threats of arbitrary state action and unauthorized surveillance.

The other significant issue is that it can be abused by the government or individuals. Not only can AFRS be applied to legitimate security purposes, it can also be employed to conduct mass surveillance, political profiling, protests monitoring and dissenting voices targeting. Without legal checks, technology that could be used to enhance security can be turned into a tool of overreaching state authority. This issue is more crucial in democratic countries where freedom of religion, movement, and assembly are guaranteed by the Constitution.

Moreover, facial recognition systems are not always that accurate. Mistakes in identification can lead to innocent people being interrogated, arrested or stigmatized. Research in different jurisdictions has revealed that not all facial recognition systems might work equally well with various age groups, gender groups, and ethnic groups. This begs issues in Article 14 of the Constitution that ensures equality before law and equal protection of laws.

Second, proportionality test established by the Supreme Court in Justice K.S. Puttaswamy v. Union of India continues to be core in determining the legality of facial recognition surveillance. In this constitutional standard, any limitation on privacy needs to meet the following requirements:

- **Presence of Law -** It has to have an existing law permitting action of the state.
- **Legitimate State Aim** -It should be an objective that is both legal and needed in the common good.
- **Rational Connection-** The measure should be rationally related to the objective. Necessity, No alternative demands of less intrusion should exist.

ISSN: 2582-6433

- **Proportionality -The** intrusion should be moderate amid the purpose of the populace.
- **Procedural Safeguards -** It should have control, auditing and a check on misuse.

Without a clear legislative framework, it is possible that usage of AFRS on a mass scale would not be subject to constitutional review within the privacy doctrine. Thus, the research problem is the question of whether the current legal framework in India can sufficiently govern facial recognition technology without violating the basic rights.

3. AUTOMATED FACIAL RECOGNITION SYSTEMS – HOW IT WORKS.

(a) Definition

Automated Facial Recognition Systems are technologically developed biometric systems that identify, verify or classify individuals based on the unique facial features. These systems are based on digital imaging, pattern recognition and artificial intelligence to compare facial features including eye spacing, jaw structure, cheekbone contours, nose shape, forehead dimensions, and other quantifiable features. Facial recognition is believed to be an effective tool in authentication of identity since each human face possesses a distinct blend of features.

(b) Nature of AFRS

Facial Recognition Systems are automated and have the following features:

- **Biometric Systems** -Biometric systems rely on the distinctive body features to identify individuals.
- **AI-based Technologies** -They are based on algorithms and machine learning models.
- **Data-Intensive Systems -** They work with lots of pictures and personal information.

Surveillance Tools - They are able to spy on people in open or closed areas.

- **Verification Mechanisms** -They authenticate an identity claimed to be genuine.
- **Identification Mechanisms** -They match unknown faces to databases.

Therefore, AFRS is a mixture of surveillance, data analytics, and biometric authentication.

(c) How It Works

The operation of AFRS typically consists of several technical steps:

- **Image Capture:** A facial image is captured by cameras, CCTV systems, mobile devices or scanners in real time or on existing footage.

ISSN: 2582-6433

- **Face Detection**: This software recognizes the human face in the image and separates the face out of the backdrop.
- **Mapping / Feature extraction:** The system determines such important facial features as eyes, nose, lips, jawline, and ratios among them. These are translated into mathematical template or biometric signature.
- **Database Matching:** The template created is matched against available databases of passport photographs, criminal databases, employee databases or other image databases.
- **Result Generation and Scoring.** The software is used to give confidence scores and present possible matches to be reviewed by humans or automatically acted upon.
- **Storage and Future Use.:** The data are stored in some systems to be later verified, analyzed, or monitored.

(d) Uses of AFRS

Facial Recognition Systems can be automated, and are deployed in a number of industries, including:

- **Criminal Investigation-** Recognition of suspects on CCTV images.
- **Airport and Border Security** -Verification and immigration of passengers.
- **Attendance Systems-** Attendant control of employees or students.

KYC: Banking and Financial KYC provides identity checks on online services.

- **Missing Person Tracing -** Find missing children or adults.
- **Access Control** -Restricted access to offices, laboratories or equipment.
- **Smart Cities** – Traffic and citizens safety surveillance.

5. INDIAN FACIAL RECOGNITION REGULATIONS.

India currently lacks a specific Facial Recognition Act that directly addresses the implementation and control of AFRS. The current laws are disjointed, indirect and do not adequately deal with the multidimensional problems of biometric surveillance.

4. EXISTING APPLICABLE RELEVANT LAWS

(a) Acts of Parliament, (a) Information Technology Act, 2000.

The Information Technology Act only offers few protections in regard to unauthorized access, hacking, and abuse of electronic data. Some of the rules that are framed under the Act are concerning sensitive personal data, yet they fail to regulate facial recognition systems by the

ISSN: 2582-6433

state exhaustively.

(b) Digital Personal Data Protection Act, 2023.

The law provides a framework to guard personal data and responsibilities to data fiduciaries. Nevertheless, it does not concern itself in particular with facial recognition surveillance or real-time monitoring, or independent authorization criteria of law enforcement application.

(c) Indian Telegraph Act and Surveillance Rules.

The law In the context of traditional surveillance, the main focus of the law is on interception of communications, like telephone conversations. They were adopted prior to the existence of modern biometric technologies and are thus not aimed at ruling the governance of facial recognition.

(d) Constitution of India.

- The Constitution is the best protection against abuse:
- Article 14 - Equality before law and non-arbitrariness.
- Article 19 - Freedom of speech, movement, and peaceful assembly.
- Article 21 -Right to life, dignity, and privacy.
- Therefore, although constitutional norms are applicable, the use of facial recognition, audits, and retention time, the standard of consent, and wrongful identification solutions are not regulated by any comprehensive statutory framework. This leaves a gap in the law.

5. INTERNATIONAL SCENARIO WITH USE OF FACIAL RECOGNITION SYSTEMS.

United States

The use of facial recognition by police has been the subject of a wide discussion in the United States. The city of San Francisco and Portland among others placed prohibitions or limitations on some of their governmental applications because of issues of privacy and civil liberties. Simultaneously, other security-related applications are still being investigated by federal agencies. The American system is still decentralized and has different regulations between states and cities.

ISSN: 2582-6433

European Union

The EU AI Act and data protection legislation like the GDPR have introduced a rights-based and risk-oriented approach by the European Union. Public remote biometric identification is considered high-risk and is a matter of strict conditions, requirements of transparency, and regulatory oversight. The model of EU focuses on human dignity, privacy, and accountability.

United Kingdom

In the United Kingdom, police forces have tested the live facial recognition in the public. Judges have questioned the use of such deployment in accordance with the human rights, legality, and proportionality. The question of efficiency of policing and the rights to privacy is the matter of public discussion.

China

China has used facial recognition massively in transport, city control, people security, and business. The technology is entrenched in day to day governance and business. Nevertheless, the world community tends to question the level of surveillance and restrictions in privacy.

Lessons for India

The practice of facial recognition cannot be left unregulated based on the experience of other countries around the world. Either the countries place restrictions, or establish risk-based frameworks, or are subject to intense judicial and popular scrutiny. India can emulate these experiences by implementing a moderate legal regime that ensures innovation and protection of constitutional rights.

6. JUDICIAL APPROACH ON THE RIGHT TO PRIVACY AND STATE SURVEILLANCE.

The Indian judiciary has been very instrumental in safeguarding civil liberties and keeping in check the powers of the State within the constitutional boundaries. With time, courts in India have come to appreciate the fact that privacy, dignity, liberty and autonomy are fundamental rights envisaged under the Constitution. Judicial interpretation has taken on a new significance especially in achieving a balance between national security and individual freedom in an era of digital governance and surveillance technologies. Application of Automated Facial Recognition Systems (AFRS) should therefore be looked into in terms of constitutional

ISSN: 2582-6433

principles that have been achieved via landmark court ruling.

The term privacy is not explicitly mentioned in the Indian Constitution as an independent basic right. Nonetheless, over time, courts have interpreted that privacy is intrinsic to the right to life and personal liberty in Article 21, and has a connection with the freedoms in Article 19 and equality in Article 14. This broad interpretation of constitutional rights directly applies to state surveillance technologies, such as facial recognition.

(a) Justice K.S. Puttaswamy v. Union of India (2017).

The landmark case on privacy in India has been the case of Justice K.S. Puttaswamy (Retd.) v. Union of India, concluded by a nine-judge bench of the Supreme Court in 2017. The Court in this historic case unanimously stated that right to privacy is fundamental right under Part III of the Constitution. The Court believed that privacy is inherent to life, liberty, dignity, bodily integrity, informational self-determination, and personal autonomy.

The ruling has extensive implications on technologies that deal with the collection of personal data, particularly biometric monitoring. The Court clarified that privacy is not a right that is absolute, and that in some circumstances, the State can make reasonable restrictions. But, any violation of privacy should meet the following constitutional criteria:

(b) PUCL vs Union of India.

People's Union of Civil Liberties (PUCL) v. Union of India is another case that is significant with regard to the surveillance powers. The Supreme Court looked into telephone tapping and interception of communications without authorization in this case. The Court realized that unregulated surveillance can pose a grave danger to privacy and freedom. It thus established procedural checks to guard against capricious executive action.

The Court pointed out that the powers of surveillance could not be utilized freely. There should be proper authorization, necessity, time constraints and review mechanisms. The reasoning of the case, though in the context of telephone interception, is very applicable to online surveillance equipment, including facial recognition systems. In the event that telephone monitoring needs security, then biometric surveillance that involves facial data needs even greater security measures since facial recognition may be used to track individuals anywhere and without their awareness.

ISSN: 2582-6433

(c) Other Judicial Principles (c).

The Indian courts have always believed that constitutional rights should change according to the times. The courts have acknowledged human dignity, informational privacy, freedom of movement, and freedom of expression as the key democratic values. Constant surveillance using facial detection can lead to people not protesting, taking part in political meetings or attending other gatherings, thus indirectly influencing Article 19 freedoms.

Moreover, when the AFRS systems have a bias or are inaccurate to cause wrongful suspicions of some groups that application can also be against Article 14 that ensures equality before the law and protection against arbitrary state action.

(d) Implications to AFRS.

All these judicial precedents indicate that the indiscriminate use of facial recognition systems without legal authorization, transparency, or regulation might be unconstitutional. Administrative convenience or security claims cannot be the only basis on which state authorities can be relied. They should show that the use of facial recognition is legal, justified, reasonable and provided with sufficient safeguards. Thus, the judiciary has created a constitutional basis that demands a strict control over AFRS in India.

7. SUITABLE REGULATORY FRAMEWORK IN INDIA SHOULD BE ADOPTED.

India is in dire need of a more detailed and specialized legislation on Automated Facial Recognition Systems. The swift growth of facial recognition in law enforcement, airports, trains, and government has led to the rapid advancement of legal protections behind it. Unless it is regulated, AFRS can be abused and lead to breach of privacy, discrimination and random surveillance.

A special framework is required due to the following reasons:

(a) Privacy.

Biometric templates and facial pictures are very sensitive personal information. Facial characteristics are permanent and cannot be easily changed as it is unlike passwords or identity numbers. The privacy of citizens may be put at risk in the long-run due to unauthorized collection or leakage of such data. Thus, legal regulations should establish the instances in

ISSN: 2582-6433

which the facial data can be gathered, by whom, and why.

(b) Transparency

The people in a democratic society have the right to be informed of the location of surveillance systems and the purposes of the surveillance. Facial recognition systems should not be deployed secretly because it causes fear and mistrust. There should be a regulation framework that mandates public notice, use case disclosure and policy publication.

(c) Accountability

The persons in charge of AFRS should be held accountable in case of abuse, laxity, or unlawful spying. Institutional responsibility and not anonymity or vagueness in decision-making should exist. Accountability has to be checked through independent audits, record-keeping and complaint mechanisms.

8. CONCLUSION

The Automated Facial Recognition Systems are one of the strongest technological advances of the modern age. Their capability to recognize people quickly, and process high volumes of visual information has seen them find application in governance, policing, border control, digital verification, and administration of the people. Such systems can be used to locate missing individuals, prevent crime, enhance security infrastructure, and enhance administrative efficiency, when applied responsibly. Nonetheless, there are also threats that are associated with the same technology. Facial recognition may turn into a tool of intrusive surveillance when used without any legal protections, democratic checks and balances, and considerations of basic rights. In contrast to traditional surveillance practices, AFRS allows identifying people remotely, monitoring the mobility of individuals across the locations, and establishing a set of permanent biometric databases. These powers, when unchecked, can pose a threat to privacy, autonomy, dignity, equality and a freedom of expression. In India, AFRS is becoming more used by governmental bodies and this has occurred without any specific statutory framework. This legal loophole leaves it unclear what can be used, how data is stored, how it is controlled and what can be done in the case of abuse. The right to privacy as established in constitutional right to privacy of Justice K.S.Puttaswamy v. Union of India, it is evident that any surveillance action should be legal, necessary, proportionate and backed by procedural protection.

ISSN: 2582-6433

Thus, India needs to shift to a more transparent, rights-based and future-oriented legal framework of the face recognition systems. Such a system must include transparency, accountability, judicial checks and balances, data minimization, anti-discrimination principles, and efficient redress to citizens. Regulation must not be considered a hindrance towards innovation but a requirement of authentic and reliable innovation.

After all, technological advancements and the freedom of democracy do not have to work against each other. India can achieve the advantages of the Automated Facial Recognition Systems and retain the freedoms and dignity of its citizens with a careful legal design and constitutional commitment.

REFERENCES

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
2. People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
3. Information Technology Act, 2000, No. 21 of 2000, India.
4. Digital Personal Data Protection Act, 2023, No. 22 of 2023, India.
5. Articles 14, 19 and 21.of Constitution of India
6. National Crime Records Bureau. (2020). Request for Proposal for National Automated Facial Recognition System (NAFRS). Government of India.
7. Basheer, I. P. (2025). Issues raised due to use of facial recognition in India. *Indian Journal of Public Administration*, 71(2), 210–225.
8. Ramaswamy, S. (2024). The evidence machine: Rethinking admissibility and privacy in India's AI surveillance state. *Indian Journal of Law and Technology*, 20(2), 1–24.
9. Singh, N. (2021). Privacy governance and facial recognition. In *Anthology on Law and Privacy* (pp. 1–9). INSC Publishers.
10. Gupta, K., & Bharadwaj, A. (2023). Facial recognition systems: Privacy and criminal justice implications. Bennett University Press.
11. Dixon, P. (2017). A failure to do no harm: India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S. *Health and Technology, 7*(4), 539–567.
12. Jauhar, A. (2020). Facing up to the risks of automated facial-recognition technology in India. *Indian Journal of Law and Technology*, 16, 55–78.

ISSN: 2582-6433

13. Uppal, V., Nagpal, P., Gera, H., Upadhay, K., & Mittal, K. (2026). Right to privacy under Article 21 versus AI surveillance: Constitutional validity of facial recognition technologies in India. *IJEDR Journal*, 14(1), 1–12.
14. Gupta, Y. (2025). Facial recognition technology and fundamental right to privacy in India. SSRN Electronic Journal.
15. Bhatia, S. (2025). AI-driven facial recognition: Human rights implications. *Panjab University Journal of Law*, 12(1), 44–61.
16. Abraham, M. M. (2025). AI-driven surveillance in India: Reconciling privacy and national security. *Journal of Data Protection Policy*, 8(2), 183–207.
17. Thorat, S. B. (2010). Facial recognition technology: An analysis with scope in India. *arXiv Preprint arXiv:1005.4263*.