

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

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.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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.

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.

DOCTRINAL RESEARCH ON THE SUBJECT OF AI FACIAL RECOGNITION AND FUNDAMENTAL RIGHTS

AUTHORED BY - VIBITHA.M

LL.M Final Year Student (Criminal Law) Crescent Law School,
B. S. Abdur Rahman Crescent Institute of Science & Technology, TN

ABSTRACT

The rapid development of Artificial Intelligence (AI) has led to the increased use of facial recognition technology to identify, verify, monitor and enforce the law. Facial recognition technology gives large technological and administrative advantages, but its broad use creates serious constitutional difficulties of privacy, equality, personal liberty and human autonomy. In the absence of an inclusive and specialised regulatory framework for facial recognition in India, questions regarding to the collection, processing, preservation and use of facial data have arisen. This article is a doctrinal analysis of the constitutional implications of AI based facial recognition in India and its impact on Articles 14, 19 and 21 of the Constitution and judicial admission of right to privacy. The paper explores the main constitutional principles, judicial rulings, statutory law and the present regulatory framework on personal and biometric data. It also touches on issues of mass surveillance, algorithmic bias, faulty identification and lack of transparency / accountability. The report points out the flaws in the present legal framework and offers the necessary safeguards to make sure that the development and use of face recognition technology is in conformity with constitutional rights and ideals.

INTRODUCTION

Artificial Intelligence (AI) has grown rapidly and has transformed many sectors of modern life like healthcare, banking, transportation, security and law enforcement. One of the most current, talked about uses of AI is facial recognition technology. This method uses the visual traits of a person to verify or identify that person. In general, facial recognition systems rely on the collection, processing and matching of facial photographs or biometric data to existing databases¹. The use of these technologies in surveillance and identification systems is emerging, consequently creating new prospects for crime prevention, public safety and

¹ National Institute of Standards and Technology, Face Recognition Technology Evaluation (FRTE): Demographic Effects, U.S. Dep't of Commerce (2025).

effective identification. ²The mass collecting and processing of biometric information of the face also throws up fundamental concerns of privacy, dignity, equality, liberty and human autonomy under law and constitution. Facial recognition technology is growing significant in India, especially in the areas of law enforcement, public security, surveillance and digital identification. Facial recognition technologies are able to identify a person from photos or video footage and this can assist authorities to identify perpetrators, find missing persons and improve security mechanisms. But the deployment of such technology also raises questions as to the level of identification and surveillance to which people may be subject without their knowledge or meaningful agreement. There are also issues of the protection of individual rights in relation to misidentification, algorithmic bias, over-collection of data and unlawful storage or use of biometric information. In the Indian context, the constitutional implications of AI-based facial recognition are particularly pertinent given the fact that the Constitution guarantees fundamental rights that might be directly damaged by the use of such technology. Article 14 provides for equality before law and equal protection of the laws. That's a problem when facial recognition technology produces biased or inconsistent results. People may change the way they act when they think they are being electronically watched. Article 19 safeguards crucial liberties such freedom of speech and expression and the right to peaceful assembly, which could be damaged. Article 21 guaranteeing right to life and personal liberty has been judicially interpreted to include right to privacy, dignity and personal autonomy. Because face recognition includes the collecting and analysis of data about an individual's physical traits, it should be addressed within the framework of constitutional protections of privacy and individual liberty.

TECHNOLOGICAL AND CONCEPTUAL FRAMEWORK FOR FACE RECOGNITION

Facial Recognition Meaning and Definition

It is a biometric technique for identification and verification.³ It is based on computational algorithms that analyse the unique features of the human face. This is the identification, measurement and comparison of facial features in an effort to identify whether a given face is that of an individual present in a database. The integration of machine learning and artificial intelligence has significantly enhanced the ability of facial recognition systems to process

² Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

³ Patrick Grother, Mei Ngan & Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280, Nat'l Inst. of Standards & Tech. (2019)

massive sets of facial photos and detect patterns at a much quicker rate and more efficiently. In AI-assisted facial recognition, a person's face is usually turned into a digital template that can be matched against other stored templates. The technology might look at factors like how the eyes are positioned relative to each other, to the nose, lips, jawline and other facial features. The resulting biometric representation is then ready to be used for matching against information stored in a database, for verification or identification purposes.

Artificial Intelligence and Machine Learning in Face Recognition

Artificial intelligence is defined as computer systems that can accomplish activities that generally need some element of human intelligence, such as pattern recognition, learning, classification and judgement. It is now a core feature of AI, giving computer systems the ability to spot patterns in data and to improve their performance when they are given the right data. Today's facial recognition systems employ machine learning and deep learning-based algorithms to process pictures of faces. These systems can be developed utilising algorithms based on big data sets like facial photos. Machine learning and artificial intelligence can accelerate and scale facial recognition. But the quality of the final identification depends on various aspects such as quality and diversity of training data, ambient conditions, quality of images, algorithmic design and the way the system is implemented. Thus, the technical efficiency does not exclude the case of faulty or biased outcomes.

Types of Facial Recognition Systems

Facial recognition systems can be broadly classified depending on their functionality and the way they operate. facial verification is the task of matching a person's facial information to a given identity to check if the claimed identity corresponds to the subject under examination. It's usually seen as a 1-to-1 comparison. Facial identification is the technique of identifying a person by comparing an unknown face with a number of face representations stored in a database. This is called one-to-many matching in comparison. Facial recognition can be divided into two categories: real-time facial recognition and retrospective facial recognition. Real-time systems assess images of faces of individuals walking in a specific place or in a surveillance environment. Retrospective systems are systems that look at video or photographs that have been recorded after an occurrence has occurred.

Biometric Technology – Facial Recognition

Facial recognition is a type of biometric technology, as it uses physical traits linked with an

individual to identify or authenticate them. Biometric information is unique from typical identifying information in that biological properties are inherently connected to the identity of the person and usually cannot be changed as a password or identification number may. Identification by face features has certain privacy and security issues. The unlawful acquisition, storage, disclosure or misuse of face information may impair an individual's capacity to govern personal information that may pertain to their identity. The relevant legal matter is therefore not only the capture of a picture, but the systematic processing of face features for identification, classification or surveillance.

Bias and discrimination in algorithms

Algorithmic bias is unfair and systematic discrimination in algorithm output.⁴ Bias exists in the training data for facial recognition, in the architecture of the algorithms, in the context in which the technology is deployed, or elsewhere. If the training data is not representative of some demographic groups or the system behaves differently for different groups, then divergent results may occur. Such challenges have constitutional repercussions in India as Article 14 guarantees equality before law and equal protection of laws. Facial recognition can potentially run into issues of arbitrariness and bias if it leads to systematic unequal treatment.⁵ Technology used by public organisations should thus be assessed not only for its technical correctness but also for its prospective impact on equality and fundamental rights.

FRAMEWORK OF FACE RECOGNITION IN CONSTITUTION OF INDIA

New Technologies and Constitutionalism

Constitutionalism is the notion that the constitution limits the power of the State.⁶ The fact that technology is new or quickly moving does not mean it is outside the constitutional framework. When state authorities deploy AI-based systems for the collection, processing or analysis of information on individuals, its use must be assessed in the light of fundamental rights, legality and procedural safeguards.⁷ Facial recognition technology poses a particular constitutional challenge since it can be used to identify persons en masse, even when the individuals may not have voluntarily provided information for a particular purpose. Such technology calls for, therefore, a constitutional review that accounts for the combination of technological

⁴ National Institute of Standards and Technology, Face Recognition Technology Evaluation: Demographic Effects, U.S. Dep't of Commerce.

⁵ E.P. Royappa v. State of Tamil Nadu, (1974) 4 SCC 3

⁶ Kesavananda Bharati v. State of Kerala, (1973) 4 SCC 225.

⁷ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

opportunity with limitations on state power. The use of facial recognition has to rely on an acceptable legal framework and has to comply with the constitutional standards for limitation of individual rights.

Article 14 and Facial Recognition

The State shall not deny to any person equality before the law or the equal protection of the laws, as is provided in Article 14 of the Constitution. The constitutional principle of equality is especially relevant to facial recognition, because systems based on artificial intelligence might produce different results depending on the quality of the data, the design of the algorithms and the demographic characteristics of the subjects. Algorithmic bias can cause some human groups to be more or less accurate. The use of facial recognition technology by public agencies may lead to incorrect or discriminating outcomes which may create issues of equality and non-arbitrariness. Hence, the interpretation of Article 14 requires an assessment of both the formal neutrality of a facial recognition system and its practical impact.

Article 19 and Face Recognition

Section 19 of the Constitution provides citizens with some rights such as freedom of speech and expression and right to assemble peaceably and without armaments. Facial recognition doesn't directly violate fundamental rights, but it can change how people exercise them through mass surveillance. The threat of monitoring may be experienced in terms of the danger of being identified en masse using facial recognition, especially in public assemblies, demonstrations or other forms of collective expression. People may change their behaviour if they fear that their involvement in legal activities can be tracked, detected and then associated with their identities.⁸ This raises fears that surveillance may have a chilling effect on constitutionally protected liberty.

Article 21 and Facial Recognition

No individual shall be deprived of his life or personal liberty save in accordance with procedure established by law. The pronouncements of the Court have brought about a dramatic change in the interpretation of Article 21 and have given rise to the acceptance of several rights which are fundamental for the protection of human dignity and liberty of the individual. Facial recognition may be problematic under Article 21 as it entails the collection, processing and

⁸ Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

retention of information directly linked to the identification of an individual. Constant or wide surveillance of individuals may threaten personal autonomy and control over information about oneself. Facial recognition use, therefore, should be assessed in the light of the constitutional guarantees of life, liberty, dignity and privacy.

Article 20 – Right not to incriminate oneself

Article 20(3) of the Constitution provides protection from being compelled to be a witness against oneself.⁹ The link between face recognition and Article 20(3) raises difficult legal questions about the relationship between testimonial evidence and biological or physical characteristics. Facial recognition is essentially a physical features query, not communicating personal knowledge. But as biometric technologies become more common, it will be vital to carefully evaluate the constitutional border between compelled testimonial communication and the collection of physical attributes. Legal concerns may rely on the method by which facial information is collected, processed and subsequently used.

Facial Recognition: Constitutional Protections

The constitutional framework must offer adequate safeguards where facial recognition technology could affect basic rights. Such safeguards may include explicit statutory authority, specific aims, limits on collecting, limits on retention and access, independent oversight, transparency requirements, accuracy testing, procedures for rectifying inaccurate identification, and appropriate remedies for unlawful usage. In the end, constitutional regulation of facial recognition should seek a balance between legitimate government interests and individual rights. Technological innovation does not justify unrestricted surveillance and processing of biometric data. In terms of the use of facial recognition, India must continue to be governed by constitutional principles of equality, liberty, privacy, dignity, proportionality, accountability and rule of law.

PRIVACY AND FACIAL RECOGNITION RIGHTS USING AI

Development of Right to Privacy in India

The right to privacy has undergone a lot of evolution in India through judicial interpretation. In *Kharak Singh v. State of Uttar Pradesh*, the Supreme Court had to consider the constitutional consequences of police surveillance and personal liberty.¹⁰ In *Gobind v. State of Madhya*

⁹ INDIA CONST. art. 20(3)

¹⁰ *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.

Pradesh, the Court accepted privacy as part of personal liberty but accepted that private may be subject to valid restrictions in some situations.¹¹ The evolution of privacy jurisprudence suggests that state surveillance and collection of personal information should be analysed in light of constitutional principles. This is especially relevant given the rising use of AI-enabled facial recognition technology by law enforcement organisations to identify and monitor persons by their facial traits.

Privacy as a Human Right

The Supreme Court has finally determined the constitutional status of privacy in Justice K.S. Puttaswamy (Retd.) v. Union of India. The nine-judge bench had held that the right to privacy is a fundamental right under the Constitution, notably under Article 21. The Court tied privacy to dignity, autonomy, liberty and the ability of people to control personal information. This principle is crucial in the case of facial recognition as the facial information can be collected and analysed without active participation of the user. Such use of technology by the State authority thus requires a constitutional scrutiny.

Facial Recognition, Information and Privacy

Facial recognition using AI is the collection, analysis, comparison and storing of facial data. Facial biometric data, unlike normal photos, may be used to identify a person and possibly associate their identity with other data such as location, movement or activities. The largescale collection of facial data has sparked concerns regarding privacy of information. Questions can be asked about who collects the data, for what purpose, how long it is stored, who may have access to it and whether it can be shared with other authorities. Without sufficient restrictions, such methods may cause unwarranted interference with individual privacy.

Personal Autonomy, Dignity and Privacy

The right to privacy is an inherent part of human dignity and personal autonomy. The management of information regarding one's identity and one's own conduct is a legitimate interest. The frequent or omnipresent use of facial recognition could provide a sense of being constantly monitored, of being constantly watched, of being constantly tracked. Such a level of surveillance may also have a chilling effect on individual activity, particularly if people worry that their involvement in public activities, demonstrations or other lawful activities may

¹¹ Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148

lead to identification and monitoring. This means that the use of facial recognition must be balanced not only with data protection, but also with dignity and personal liberty.

The need for strong privacy protections

“AI-based facial recognition should be used with adequate legal and institutional safeguards. These should include clear rules on the goal of data collecting, limit on data keeping, protection against unauthorised access, openness in the management of the system and independent oversight. Individuals should also be able to use appropriate processes to make complaints and seek redress if there has been misuse or mistaken identification. What is needed, therefore, is a rights-based regulatory framework that will ensure that facial recognition technology can be used for legitimate purposes and will not lead to undue interference with the fundamental right to privacy.

CIVIL LIBERTIES AND SURVEILLANCE FACIAL RECOGNITION

Facial Recognition and State Surveillance

AI-based facial recognition is gradually becoming a crucial tool for identification and surveillance. It is used by law enforcement authorities and can help to identify people using images or video evidence. However, the notion of continuous and extensive human identification also evokes fears of intrusive State surveillance. Facial recognition surveillance could affect people even if they have not been suspected of a crime. Such technology may only be used consequently when there is clear legal permission and the end is adequately described with precautions to prevent unnecessary monitoring.

The mass surveillance and privacy implications Facial recognition might be linked to CCTV networks and other databases allowing authorities to identify individuals in a variety of locations. Such a level and breadth of surveillance could infringe on the reasonable expectation of privacy and individual autonomy. The constitutional problem is even more serious when facial data is collected indiscriminately, without a stated goal and with appropriate limits. In theory, data collected for one purpose can be used for another purpose. There is the risk of function creep. It is therefore important that the collection and use of facial data is limited to defined and legally permitted purposes.¹²

¹² Digital Personal Data Protection Act, 2023

Real time and historical face recognition

There are two general uses of facial recognition, real-time identification and post-event identification. Real-time facial recognition attempts to recognise people as they are in a specific place at the time. Facial recognition in retrospect looks at pictures or video material that has previously been recorded. Real-time identification poses severe problems. Technology can enable persons to be tracked in public locations constantly.¹³ Retrospective identification may have privacy concerns if large databases of photographs are searched without adequate limitations. Both kinds therefore need appropriate legal and procedural safeguards.

Freedom of expression and peaceful assembly

The operation of facial recognition in public places may pose a threat to the preservation of liberty under Article 19 of the Constitution. People may be less willing to take part in lawful demonstrations, meetings or other forms of public communication if they believe their identities are routinely tracked and watched. This prospect may have a chilling effect on the exercise of constitutional liberty. Facial recognition, therefore, should not be used to hinder lawful expression or peaceful assembly needlessly.¹⁴

Misidentification and Inaccuracy

Another major difficulty is the danger of misidentification. Facial recognition technology are not always accurate and sometimes wrongly identify or fail to identify people. Law enforcement officials may be mistaken and subject someone to undue investigation, interrogation, monitoring or other adverse impacts. Do not automatically consider facial recognition results as identification confirmation. “Any material legal or coercive action based on an automated match is subject to human review and applicable procedural safeguards.

The need for accountability and oversight

Significant institutional accountability for the use of facial recognition technology. Authorities must retain precise records on the purpose of deployment, the collection of data, access to databases and storage of face information. Independent oversight, transparency and effective remedies are essential to protect against abuse. A constitutional approach would call for face recognition to be used only for legitimate purposes, and in a way consistent with privacy, dignity, equality and individual liberty.

¹³ People’s Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.

¹⁴ INDIA CONST. art. 19(1)(a)

LEGAL AND REGULATORY ENVIRONMENT IN INDIA

Information Technology Act, 2000

The Information Technology Act, 2000 is the primary law in India dealing with the protection of electronic information and data. Its provisions on protection of personal information and on unauthorised access are vital for digital processing and security of information. But the Act was not specifically designed to regulate modern AI face recognition technologies. This could mean that more specific legal safeguards may be needed for the issues associated with computerised facial identification, algorithmic decision-making and large-scale biometric surveillance.

Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 concerns with processing of digital personal data.¹⁵ It sets out principles on allowed processing, specified purposes, duties of data fiduciaries and protection of personal data. Facial recognition is an area where the Act is very important as facial information can be used to identify an individual and hence raises major data protection issues. However, the application of the data protection framework to the different governmental applications of facial recognition technology should take into account the legislative exemptions and other pertinent regulations.

Biometric Authentication and Aadhaar

The Aadhaar framework is one example of biometrics in use inside India's digital identity system. S. K. S. Supreme Court in K. The Puttaswamy (Aadhaar) v. Union of India case concerned issues of biometric data, privacy and usage of personal data by the State. The constitutional principles developed in the Aadhaar case are relevant to facial recognition, especially in terms of legitimate purpose, proportionality, data privacy and safeguards against misuse.

Criminal Investigations -Facial Recognition

Criminal investigation and identification may involve technical tools such as facial recognition. It can help authorities review CCTV footage and spot potential offenders. However, an automatic facial match should not be seen as solid evidence of guilt on its own. Without accuracy, reliability, adequate verification, and procedural protections, legal action cannot be

¹⁵ Digital Personal Data Protection Act, 2023, No. 22 of 2023

based on facial recognition results.

APPLICATION OF FACE RECOGNITION IN LAW ENFORCEMENT

Suspect Identification and Surveillance

All investigations begin with a hunch a blurry CCTV still or a distorted image shot on the phone of a passer-by. Advances turn these fragments into facial recognition. Authorities may even spot criminals in seconds across thousands of live feeds, matching gathered faces to criminal databases and watchlists. In large cities, integrated systems automatically identify persons in the camera footage and flag them as repeat offenders, wanted people or people on surveillance lists. This has shifted the focus of investigations from reactive review to proactive detection. Officers receive data-driven notifications, in real-time, not hours of tape. That means more leads generated, more accurate suspect matching and more cases solved.

Locating of missing people

There are few operations that are more time sensitive than the location of a missing person. Facial recognition is crucial to these missions, which scan social media clips, CCTV networks and live video streams to identify people who match registered photographs. The Delhi Police's facial recognition initiative in India became a landmark success story, helping trace over 3,000 missing children and adults within months with the help of Innefu's AI Vision. The system regularly scans footage from public places, transport hubs and surveillance systems to find matches with missing persons databases. This feature transforms search operations from a needle-in-a-haystack search around the metropolis into a pinpoint technology-based quest.

Security Crowd and Event Tracking

Management of public gatherings, whether protests, political rallies or sporting events, requires deep and immediate information. Facial recognition can scan crowds in real time and set off alarm systems. It may instantly identify persons of interest, known troublemakers or suspects being watched as they enter a monitored zone, in conjunction with city surveillance or drone feeds. By providing advance visibility, authorities can prevent security occurrences instead of responding to them after the fact. "These systems are an invisible safety net at high-profile events such as state visits or festivals, scanning crowds silently to keep citizens and officers safe.

Airport & Cross Border Security

Borders are often the front line of national security, and identity verification at scale is a huge challenge. Facial recognition is now fundamental to automated systems for immigration, customs and visa management. The faces of travellers are compared to passport, visa and criminal databases, allowing authorities to swiftly identify false documents, dual identities or persons on worldwide watchlists. Facial biometrics are being utilised more and more in countries such as the US, UK, Singapore and India to power automatic e-gates at airports, enhancing speed and security. It's handy, but it also helps ensure national borders are safeguarded from identity theft, infiltration activities and cross-border crime.

Digital Forensics and After-Incident Analysis

Facial recognition is a great investigative tool, even after a crime has been committed. Analysts overlay face scans to historical video material to reconstruct a suspect's activities, verify alibis or identify accomplices. This ability has proved important in tough cases to establish the position of the culprit at a given time, and so reinforce the chain of evidence in court. Facial recognition, combined with video timelines, GPS coordinates and communication data, transforms raw material into a forensic account that helps investigators get to the bottom of what really happened.

FINDINGS

Constitutional Privacy Protection

The use of facial recognition is directly connected to the fundamental right to privacy under Article 21. Collection and processing of facial biometric information might impair an individual's privacy, dignity and personal autonomy.

Algorithmic Bias and Equality

Facial recognition tech can generate misleading or biased findings. Such results may cause unequal treatment or false identification and, hence, create problems under Article 14 of the Constitution.

Effect on Fundamental Freedoms

Constant surveillance through the use of facial recognition may have an impact on the way people exercise their right to freedom of expression and peaceful assembly under article 19. The risk of being identified and watched may deter participation in authorised public activities.

Shortcomings of the Current Legal Framework

India's existing legal regulations and general data protection legislation are applicable to face recognition but there is a need for clearer and more specialised regulation that addresses the unique hazards of AI-based facial recognition.

Risk of Excess Surveillance

The extensive use of facial recognition, particularly in combination with CCTV networks and databases, could enable the extensive monitoring of individuals. These standards must define explicit boundaries around purpose, access and retention of facial data.

RECOMMENDATIONS

Particular Legal Framework

India needs a clear and comprehensive legislative framework focused on AI based facial recognition. The framework should include authorised purposes, authorised agencies and criteria for deployment.

Data Protection & Privacy

Facial biometric data may only be acquired for specified and legitimate purposes. Strict rules on storage, retention, sharing and erasure of facial data must be followed.

Auditing Algorithms

Facial recognition technologies should be subject to frequent testing and auditing for accuracy, bias and discriminatory consequences. Independent technical audits can discover and decrease problems.

Human in the Loop

Automated facial recognition results should not be used as the sole reason for arrest, investigation or other undesirable action. Legal action of a serious nature should be preceded by human verification.

Accountability and Transparency

Those that use face recognition technology should be transparent about what the technology is for and how it works, within real security concerns. Responsibility for misuse, unauthorised access or mistaken identification should be clearly assigned.

Independent Review

There has to be an impartial monitoring system to examine the deployment and usage of facial recognition by public bodies and to verify compliance with constitutional provisions.

CONCLUSIONS

Artificial intelligence-based facial recognition technology has developed as a significant tool for identification, investigation, surveillance and public security. The technology has clear advantages, but its growing use also raises important constitutional and legal challenges, especially in relation to privacy, equality, dignity, personal liberty and freedom of expression. The report notes that collection and processing of facial biometric information may have a direct impact on the fundamental right to privacy enshrined under Article 21 of the Constitution. Algorithmic prejudice, wrong identification, over-surveillance and abuse of personal data are additional matters of concern under Articles 14 and 19. Therefore, constitutional protection cannot be divorced from technological innovation. Current legal structure in India gives certain safeguards in the form of constitutional principles, data protection laws and judgements. However, the lack of a broad and explicit regulatory framework for face recognition results in an uncertainty in the collection, storage, retention, sharing and use of facial recognition. Hence the need for clear regulations and institutional safeguards. Use of facial recognition should be subject to legality, legitimate purpose, need and proportionality. Transparency, oversight by humans, independent monitoring, algorithmic auditing and effective remedies are equally crucial in preventing misuse and protecting persons from false identification. The purpose should be not to avoid technological growth, but to protect its appropriate and constitutional use. A balanced, rights-based legislative framework can enable India to benefit from AI-based facial recognition, while safeguarding the fundamental rights, dignity, privacy and liberty of individuals.