Journal of Contemporary Law and Society, *Volume 2, Issue 2, June 2025, pp. 98-102*

TECHNICAL ARTICLE
Online ISSN: 3139-1079
Doi: 10.18311/JCLS/2025/V2i2/51406

Online ISSN : XXXX-XXXX

Journal of Contemporary Law and Society

Contents available at: *www.informaticsjournals.co.in/index.php/jcls*

JCLS

Legal Implications of Facial Recognition Technology in India

Ronita Halder

L.L.M. (Criminal and Security Laws), West Bengal National University of Juridical Sciences, Kolkata - 700010, West Bengal, India; roneta.halder@gmail.com

Abstract

This article discusses the recent development of facial recognition technology and its value in security, convenience, and efficiency, as opposed to a major concern about privacy. Airport, law enforcement, banking, and retail applications of facial recognition technology increase security; however, they have the problem of unauthorised data gathering, misuse, bias, and dictatorial possibilities. Even though the lack of particular legislation in this regard still prevails, the issue was first addressed by the judiciary when the Supreme Court held that privacy is a Fundamental Right. This article also analyses the enactment of the Digital Personal Data Protection Act, 2023, as a significant milestone in the regulation of biometric data by informed consent, data minimisation, security, and accountability. However, India needs strong legal frameworks, robust data protection, transparency, and public awareness to responsibly leverage facial recognition technology with a focus on explicit consent, secure storage, correction rights, and penalties against misuse. This article supports the idea of moderation, which should encourage technology innovation and maintain privacy and human rights through responsible governance, continuous improvement, and extensive regulation. It further suggests that a balanced approach requires government, industry, and the citizens to work together to develop clear policies to provide security and avoid abuse so that India can enjoy the benefits of facial recognition technology without jeopardising the basic freedoms. Thus, facial recognition technology can turn into an instrument of social improvement instead of a source of social menace.

Keywords: *Biometrics, Facial Recognition Technology, Informed Consent, Privacy, Transparency*

1. Introduction

The world we live in today is evolving at an extremely rapid pace due to the advent of modern technology. Facial recognition is one of these new technologies. The technology assists computers and cameras in identifying and recognising the faces of people. One can enter an airport, and a camera scans his face to determine whether he is on the list or not. Or consider a person's phone unlocking at the sight of his face. These are some of the ways that facial recognition assists us in life. It can simplify, accelerate and protect. However, despite all the positive applications of facial recognition, it raises concerns. Some fear that their personal data, such as their face, may be misused.

Privacy is the ability to keep your personal information confidential. When the government or businesses gather facial data without consent or without reasonable cause, then it can be an issue (Smith and Miller, 2021). This information may be used by them to spy on or manipulate anyone, which is wrong. Therefore, despite the numerous advantages of facial recognition, it is highly significant to consider the impact that this technology has on our privacy. The government and the people in India are deliberating on the ways of utilising this technology wisely. They would like to ensure that it is utilised in a manner that is safe and equitable to all. This article will provide insights into facial recognition, its conflict with privacy and the stance of Indian jurisprudence to defend the rights of its citizens while enjoying the benefits of new technology.

2. Facial Recognition

Facial recognition is a special computer program that scans the face of an individual and attempts to identify who the individual is. The computer examines some features when an image of the face is captured or when someone is seen on camera. These characteristics are the form of the face, the gap between the eyes, the nose, the mouth, and other parts of the face. These features are then compared by the computer to a huge database of faces. When the computer detects the same features in the database, it can say, this is the person. It is a very quick process that may occur within a matter of seconds. Facial recognition is everywhere. It is used to locate criminals by police through the matching of faces captured on security cameras. In some instances, facial recognition may also be used to locate missing children by matching their images taken in various locations.

It is a convenient device that can simplify our lives and help us stay safe. It assists travellers in passing through security in airports (Khan & Efthymiou, 2021). An individual's face can be scanned within seconds instead of standing in long queues and presenting documents. This saves time, and it is easier to travel. They can match a picture of a suspect to any camera footage they have of the street or any other location to locate the individual. It is even applied in shopping malls and banks to avoid theft and fraud. These applications demonstrate how facial recognition technology can be useful in our daily lives and how it can make our communities safer. But, as with any potent instrument, there are issues with facial recognition technology, as well. Therefore, despite all the advantages of facial recognition, it is highly essential to learn how it operates and how it can be used responsibly.

3. Concerns Regarding Facial Recognition Technology

Facial recognition is also subject to concern. Though facial recognition technology may be quite helpful, there are several issues that are of concern to many people. One of the main concerns is privacy. People are not comfortable with the fact that they are having their faces scanned and stored without their consent. If a camera in a public place takes photos of everyone, they may feel that they are being spied on, which might not be the case. The other concern is regarding errors. The facial recognition system might identify a person in some cases. It may be assumed that someone is a criminal even when he or she is not. This may subject the innocent to unjustified misery. Besides, facial recognition is biased (Chandran 2023). It may suit one person and not the other. It may not be able to identify the faces of dark-skinned people or those of different appearance (Basheer, 2024). This may result in discrimination.

Another concern is misuse. Facial recognition could be used by people motivated by malicious intentions or illegal organisations to spy on others or invade their privacy. They would be able to monitor the movements of people, their activities, as well as who they interact with, without their consent. This would be applied to control or frighten people. The collection of facial data by governments or companies may have unclear and unfair reasons. People also fear that such information may be stolen or given to other individuals, and this may lead to issues pertaining to cybercrime. The issue of the duration of storing facial data is also a matter of concern. When companies or the government retain this information over a long period, they become more likely to abuse it or be hacked (Guleria, Krishan, Sharma & Kanchan, 2024). Therefore, at present, people are interested in understanding the protection and use of their facial information.

4. Privacy Laws in India

In India, since there exists no direct legislation on these issues, and until the enactment of the Facial Recognition Technology (Regulation of Police Powers) Bill, 2023, the judiciary has stepped up in times of necessity. The right to privacy in India is a Fundamental Right enshrined in Article 21 under Part III of the Constitution. Through purposive interpretation of the right to life and personal liberty, the courts have time and again enumerated that each individual is entitled to privacy. This implies that individuals can decide the privacy of their personal information and its usage. This right is, however, not absolute. In some cases, the government has to access personal information due to safety or security concerns. They can be required to check who enters a country or locate criminals. However, they have to do it fairly and reasonably. In 2017, the Supreme Court, through the case of Justice K.S. Puttaswamy (Retd.) v. Union of India, elaborated, the right to privacy falls under the right to life

and liberty enjoyed by every individual. It stated that the government cannot invade privacy unless it is following due process of law.

Since this ruling, India enacted the Digital Personal Data Protection Act, 2023 (DPDP Act, 2023). It offers an important legal framework for processing personal data, and its terms directly apply to the implementation and application of facial recognition systems. According to the DPDP Act, 2023, personal data is determined as any data through which one can be identified. The physical and biological features of any face are unique and therefore fall under this Act. This means that anyone dealing with or acquiring any kind of biometric data is required to comply with the Act. The most important of these is the need to seek direct consent of the person before processing their personal data, including facial images. This consent should be free, specific, informed, and unambiguous, meaning the data principal should agree with the processing. Moreover, the Act underlines the principle of data minimisation and states that only the data required by a given purpose must be gathered and processed (Parsheera, 2019). In facial recognition, this means that some justification has to be provided as to why such sensitive biometric information is collected, and that alternative, less invasive means are not possible to reach the desired goal. The reason why the facial information is gathered should be made known to the person, and the information should be utilised according to the intended purpose only. Any other subsequent purpose would probably need new consent.

Another new concept under the DPDP Act, 2023, is that of a Data Protection Board of India that will carry out the regulations of the Act and penalise those who violate them. Companies implementing facial recognition technology should, therefore, be careful in their operations, and their security solutions should be robust to avoid the risk of data breach. Under the Act, the personal data is also to be secured against unauthorised access, disclosure, editing and destruction. In the case of facial data, one of the most sensitive kinds of data, this requires high-level encryption, access checks, and frequent security audits. This has significant consequences for law enforcement agencies and other private organisations that use facial recognition to control access, surveillance, or identification of individuals. They should also put definite policies and procedures that meet the DPDP Act, 2023. This refers to performing Data Protection Impact Assessment to high-risk processing operations, frequent of which is facial recognition (Gupta & George, 2024). These tests can be used to detect and reduce privacy threats posed by the facial recognition system. Further, any kind of use of facial recognition technology has to now conform to the rigorous provisions of the DPDP Act, 2023. This regulatory change requires a more responsible and privacy-conscious method of processing biometric data, including transparency, consent, and safety as a means of protecting the rights of individuals within the digital age. The purpose of the Act is to balance the right to technological innovation and the right to privacy of citizens, so it is an important point of focus among all interested parties operating with facial recognition technology.

5. Balancing Benefits and Challenges of Facial Recognition

Facial recognition technology is definitely among the most revolutionary technologies of our era, and it has a lot of advantages that can improve the level of safety, efficiency, and convenience in our lives to a great extent. The fact that it can be used to identify and authenticate people faster opens potentially useful applications in many fields, both in law enforcement and security and in banking and healthcare. But with these benefits, some serious challenges and issues cannot be overlooked. Morally speaking, the use of facial recognition technology also brings up the issue of consent and autonomy. Individuals must be in control of their biometric information, but in most cases, they are not aware of when and where their faces are being scanned. Respect for individual rights requires transparency of policies and informed consent (Mehta & Jain, 2021). In addition, there is a danger of authoritarian abuse, which is a threat to democracy itself. Countries need to be clear, enforce laws that regulate facial recognition and ensure that fundamental rights are not violated. However, it should be noted that the technology itself is not harmful in nature. Its effects are determined by its use and control. Facial recognition can also be used to benefit the populace with responsible governance, including managing disasters, health emergencies, or safeguarding the vulnerable. In particular, in case of emergencies, it can assist in finding people in distress or

finding victims promptly. It can also help to provide safety in public without physical inspections.

The answer to responsibly using facial recognition technology is to develop an extensive legal framework, where the primary concerns are privacy and human rights (Jauhar, 2020). Governments need to put in place stringent data protection legislation, based on transparency, accountability, and informed consent (Choudary, 2025). Audits and independent control should become a regular practice to ensure that it is not abused (Sahoo, 2025). Furthermore, there is a need to keep on improving the technologies to eliminate the biases and errors in the systems to make the systems fair towards all groups of people. Citizens can also be informed about what to expect and their rights regarding facial recognition through public awareness campaigns. Facial recognition technology has immense potential, but it is also extremely dangerous. It has both sides of a coin. Its effects are determined by the standards of ethics and law which we have established. It needs to be a moderate stance with a focus on responsible consumption, strong regulation, and individual rights. This way, we will be able to reap the benefits of this innovative technology, and at the same time protect our privacy, dignity, and freedoms. Facial recognition can be used as an instrument of improvement instead of being an instrument of damage, but only with a careful approach.

6. The Way Forward

The government must develop effective and strict laws to make the facial recognition technology in India responsible. To start with, it must mandate individuals to provide express consent before their facial information is gathered. This will involve educating them on why their information is required, how they will use it and who will access it. Second, the data should be stored in a safe place where it cannot be stolen by hackers. There should be good security measures. Third, people should be able to make corrections and request their data to be deleted easily and quickly. Fourth, it is highly important to be transparent. People should be made aware when and how their facial data is being used by the government and companies. Fifth, there should be severe penalties against the wrongdoer who abuses or mishandles personal data. Sixth, the technology itself must be enhanced to reduce mistakes and bias, so that it is fair to all people, no matter their skin colour, age, or gender. Finally, a separate control is necessary to check the application of facial recognition and the adherence to the privacy legislation. Such measures will ensure that the privacy rights of all people are not compromised and that society enjoys the fruits of new technology. The collaboration of the government, companies, and citizens to develop just rules and abide by them is very important. That is when India can reap the rewards of facial recognition technology without the loss of personal privacy and rights.

7. Conclusion

Facial recognition is a significant principle that can assist us in numerous different aspects, including locating lost individuals, apprehending criminals, and making our lives easier day by day. However, it carries with it some risks, particularly to our privacy. Privacy is a natural right in India, and it is guaranteed by the Constitution and secured by the courts. Courts are currently insisting that facial recognition should be used under very stringent regulations and protection in order to promote the right to privacy. India is also still in the process of developing legislation to regulate the use of facial images. These are some of the steps to ensure a balance between technological advancement and constitutional rights. We should have regulations that seek permission first before collecting information, storing it securely and having the authority to access or erase their information. Going forward, India should devise a means of enjoying the benefits of new technology without invading the privacy of all. Such a moderate position will see India become a technological leader that does not violate privacy rights.

8. References

Basheer, I. P. (2024). Bias in the algorithm: Issues raised due to use of facial recognition in India. Journal of Development Policy and Practice, 10(1), 61–79. https://doi.org/10.1177/24551333241283992.

Chandran R. (2023). India's scaling up of AI could reproduce casteist bias, discrimination against women and minorities. Scroll.in. https://scroll.in/article/1055846/indias-scaling-up-of-ai-could-reproduce-casteist-bias-discrimination-against-women-and-minorities.

Choudary, K.R. (2025). Facial recognition and the right to privacy: legal and ethical concerns in India. IJLLR Journal. 7(3). https://www.ijllr.com/post/

facial-recognition-and-the-right-to-privacy-legal-and-ethical-concerns-in-india.

Guleria, A., Krishan, K., Sharma, V., & Kanchan, T. (2024). Global adoption of facial recognition technology with special reference to India—Present status and future recommendations. Medicine Science and the Law, 64(3), 236–244. https://doi.org/10.1177/00258024241227717.

Gupta, N., & George, A. (2024). Digital Personal Data Protection Act 2023. In Routledge eBooks, (pp.34-53). https://doi.org/10.4324/9781003505723-3.

Jauhar, A. (2020). Facing up to the Risks of Automated Facial-Recognition Technologies in Indian Law Enforcement. Indian Journal of Law and Technology, 16(1). https://repository.nls.ac.in/ijlt/vol16/iss1/1.

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

Khan, N., & Efthymiou, M. (2021). The use of biometric technology at airports: The case of customs and border protection (CBP). International Journal of Information Management Data Insights, 1(2), 100049. https://doi.org/10.1016/j.jjimei.2021.100049.

Mehta, N., & Jain, N. (2021). Rise in Facial Recognition Surveillance and its Implications for India in Coming Decades; Violation of Privacy and Human Right. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3877325.

Parsheera, S. (2019). Adoption and regulation of facial recognition technologies in India: why and why not? SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3525324.

Sahoo, P. (2025). Facial Recognition Technology and Privacy: A Legal and Ethical inquiry. International Journal of Law Management & Humanities. 8(2) 4513 - 4529. https://doij.org/10.10000/IJLMH.119497.

Smith, M., & Miller, S. (2021). Facial Recognition and Privacy rights. Biometric Identification, Law, and Ethics. In SpringerBriefs in Ethics, (pp. 21-38). https://doi.org/10.1007/978-3-030-90256-8_2.

The Digital Personal Data Protection Act, No. 22 of 2023 (India).