Page 1238 - 1247 **DOI:** *https://doij.org/10.10000/IJLSI.11720*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 3 | Issue 3

2020

Adoption of AI Facial Recognition Technology: Challenges to Indian Legal Regime during Pandemic

LAVANYA G T[1] AND VIOLA RODRIGUES[2]

ABSTRACT

The Covid-19 pandemic and its sudden impact not only rattled the lives, but also led to the development of a variety of technologies. The conventional adoption of Contact biometric technologies has not only become obsolete but it is also extremely dangerous as it contains the risk of spreading the infection. Although, Indian Companies may be reluctant to adjust to changes, however by the pandemic, the companies are persuaded to reconsider their adoption to the new technologies such as AI facial recognition, the major biometric technology. Its competence to assess a person's face by mapping his or her facial characteristics with the aid of images and then evaluating the same with the related databases with no physical contact has made the technology inordinately popular amid Covid-19 pandemic. One of the major concerns for the said technology is its lack of regulation and without the proper backup of law regulating the same in Indian legal regime, the privacy and security of an individual is at stake and thus, this Paper emphasises on the same. In India, there is no specific law dealing with data and privacy, thereby this lacuna poses a major question as to how the AI facial recognition technology would be regulated and also at the same time how the issues of privacy and security would be resolved. Thus, this Paper analyses and makes a comparative study of laws regulating the AI Facial Recognition System in other countries. The Paper focuses on suggesting a suitable similarity metric in parlance with other countries which could be incorporated in Indian Legal scenario in regulating the AI Facial Recognition Technology.

Keywords: *AI Facial Recognition Technology, Covid-19 Pandemic, Indian Legal Regime, Regulation, Privacy and Security issue.*

[1] Author is a student at School of Law, CHRIST (Deemed to be University), Bengaluru, India.
[2] Author is a student at School of Law, CHRIST (Deemed to be University), Bengaluru, India.

 [ISSN 2581-9453]

I. INTRODUCTION

In today's digital infrastructure we have to interact with an increasing number of systems, both in the physical and the virtual worlds. Due to the outbreak of coronavirus, there is enhanced interaction in virtual worlds endangering an individual's security. This increased interaction has led to shift in the usage of technologies. For example, from use of fingerprints to AI-based Facial Recognition Technology (hereinafter referred as "FRT") for various purposes and means.

Biometrics, is defined as the automated recognition of humans based on biological or behavioural characteristics[3]. Biometric Recognition cannot be forgotten or misplaced because of the physiological or behavioural characteristics[4]. In government initiatives such as border protection and government-to-citizen services, along with consumer-facing applications in the health care and finance industries, biometrics are being widely used. Biometric technologies offer reliable and efficient recognition that is necessary as our real and virtual worlds are further enmeshed. As our real and virtual worlds are further enmeshed, biometric technologies deliver accurate and efficient identification that is essential.

As very said, technology is dynamic in nature and keeps evolving thereby posing many challenges. In lines of same, even the Facial Recognition adoption was indeed costlier as the usage of the same was not in demand because of other biometric identification techniques. Due to the situation posed by the occurrence of pandemic, the said technology has gained huge potential and the cost is going down dramatically[5].

Facial scan biometrics is an automated way of identifying a person by their distinct individual facial features[6]. Face recognition being one of the kinds of biometric recognition has several advantages over other biometric identification techniques, such as fingerprint and iris scans – *"besides being natural and nonintrusive, the most important advantage of face is that it can be captured at a distance and in a covert manner"*[7].

Recently, facial scans have become a growing concern in India as they are used to detect and identify someone as a potential threat. This is not, however, their only function; for many different purposes, they are used to classify and verify people. Facial scans are done via many

[3] Tavani, H.T & J.H. Moor, *Privacy Protection, Control of Information, and Privacy-enhancing technologies,* 31 Comput Soc 6-11 (2001).
[4] Shimon K. Modi, Biometrics in Identity Management 2 (1st ed. Artech House 2011).
[5] S.B. Thorat, S.K. Nayak & Jyothi P Dandale, *Facial Recognition Technology: An Analysis with Scope of India,* 8 IJCSIS, 325 (2010).
[6] John R Vacca, Biometric Technologies And Verification Systems 95 (Elsevier Science & Technology 2007).
[7] Stan Z. Li. & Anil K. Jain, Handbook of Face Recognition, (2nd ed. Springer-Verlag London 2011).

different techniques, and involve advanced software to analyse and break down specific details and features of each face[8].This is also, however, the precise explanation why biometric data, in general, and facial data, in particular, pose special and far-reaching privacy challenges for individuals and communities. Thus, it can be stated that along with knowledge and possession-based methods, biometric technologies also have their weaknesses.

With the increased acceptance, there is a rise in the standards expected from AI based FRT. *Biometrics is not a silver bullet; it cannot provide 100% security, nor can it provide a reliable solution for every problem*[9]. Thus, the Paper in the forthcoming chapters will elaborate on the Challenges put forth by this technology to the law enforcement agencies.

II. CORE FUNCTIONS OF FRTS: BUSINESS AND GOVERNMENT AGENCIES

The hit of Covid-19 has led to more reliance on usage of technology mainly from the health point of view. Apart from the security concerns that might bother the companies, the Covid-19 pandemic has enabled many business organisations to still maintain their productivity without face-to-face meetings leading to a greater work-at home flexibility. The reason for the same is adoption of enhanced technology and thus there is a creation of environment wherein employees work remotely from home. A study in the New England Journal of Medicine found that Covid-19 can live two to three days on plastic and stainless steel[10]. Paying systems, self-service kiosks and secured physical spaces also require authentication, and this allows us to connect with something we know, like a pin or something that we have, as an access card. Biometrics, like voice and face, are a contactless way to confirm the identification of an individual[11]. This technology will contribute to existing environment by preventing the risks of viruses across corporate offices, hospitals, airports and other safe locations, which often rely on fingerprint readers, card access and manual identification checks. The digital transformation not only helps the business and consumers to accept the reality put forth by covid-19 but also prepares to equip them to the usage of the future digital transformations, flexibility and growth. As there is more consciousness developed, there is an increase in concern for privacy and security.

FRT has been used in a wide variety of contexts. The tasks that are intended to be performed by this technology is one easy way of laying classifications of the usage functions of the said technology.

---

[8] *Id.*
[9] Shimon, *supra* note 2.
[10] Kim Martin, *ID R&D: How biometrics enable a new and improved normal*, Biometric Institute (Apr. 25, 2021, 9:29 AM) https://www.biometricsinstitute.org/?smd_process_download=1&download_id=6110
[11] *Id.*

The FRTs, *firstly* has a key feature to use the face of a person as a basis to authenticate his identity; it is a person that really appears to be and/or that tests if he or she has the right to access those systems. To better explain this feature, the instance of Unique Identification Authority of India (UIDAI) can be taken into consideration. The UIDAI announced to use FRT as the method of authentication under the Aadhar Act. In addition to this, mandatory imposition was done on telecom service by UIDAI to use the said technology for authentication of their subscribers. But all the aforesaid mandatory imposition of usage of facial recognition technology by government was not allowed by the subsequent verdict delivered in *Puttaswamy case*[12]. Under this case, distinction was drawn between the use of Aadhaar authentication for the delivery of government welfare benefits and other purposes such as KYC verifications.

Secondly, the AI FRT helps in performing the functions of security and surveillance which refers to increased security coverage including the functions of face identification to check whether a person is an authorised user for a specific purpose. For example, the verification of passengers and immigration checks at airports. Also, recently, the Indian government has approved the use of Automated Facial Recognition System (AFRS) wherein the facial biometrics can be extracted from video and CCTV which will be matched with the image of individuals whose photos and identity information are already being saved in a database maintained by the National Crime Records Bureau (NCRB) under the purview of the Minister of State for Home Affairs (MHA)[13].

Thirdly, in India, for the law enforcement, the said technology has been adopted. For example, CCTV footage. Here Cameras are placed in the midst of a crime scene and are regularly checked to identify and trace the movements of the suspect. Also, the traffic violations can be found out by placing the cameras at traffic signals. Other applications reported in the field may include the search for missing persons, the monitoring of trafficking in human beings and the identification of the use of false ID documents[14]. *Fourthly,* for increase of business competence like for instance, ability of retail and hospitality sectors to identify their customers or dynamically generating services and content suited for their profiles[15].

[12] Smriti Parsheera, *Adoption and Regulation of Facial Recognition Technologies in India: Why and Why Not?* SSRN (2020), http://dx.doi.org/10.2139/ssrn.3525324
[13] Anthony Kimery, *India set to stand up world's largest government facial recognition database for police use,* Biometric Update (Apr. 29, 2021, 8:23 pm), https://www.biometricupdate.com/202003/india-set-to-stand-up-worlds-largest-government-facial-recognition-database-for-police-use
[14] Smriti, *supra* note 11.
[15] *Id.*

Apart from the aforementioned usages and core functions of FRT, there lies another major usage. i.e use of Attendance Systems. The said technology is used for taking attendance of employees in companies and also of students in schools. For example, Delhi's Indian Institute of Technology has a home-grown solution called Timble that is used to mark student attendance[16]. Proposals are also underway to roll out similar systems to mark the attendance of young school going students in Tamil Nadu's government schools[17] and for all government teachers in the State of Gujarat[18].

There are many instances of FRTs being implemented in India by private and government organisations. To note, mainly in India, the implementation of the said technology is done in absence of strong data protection law. Thus, apart from the technological advantages, it is imperative to strike a balance between the benefits and concerns posed simultaneously with the usage of the said technology.

III. LEGAL REGIME OF FRTS IN INDIA

The speedy development of FRT without proper legal basis or frameworks poses numerous challenges. It can be the lack of transparency in facial recognition systems; their consequences for privacy and civil liberties; and evidence of bias and prejudice in their findings. Although all these issues hold true for the Government as well as private entities' regarding the use of FRT, the disparity of power between the individual and the state and the possible effects of the misuse of that power makes this an alarming issue in the context of the use of law enforcement.

Indian laws do not explicitly recognise the implementation of FRTs. It's the need of the hour for India to have a comprehensive law passed by the Parliament of India authorizing the implementation of the said technology. At present, in India there is no law which specifically deals with the deployment of these technologies[19]. The Information Technology Act, 2000 and its allied rules are completely silent on this aspect. This lacuna has an adverse effect on the governance and privacy. To note, there is no specific law dealing with data and privacy

[16] Press Trust of India, *Attendance woes? IIT Delhi resorts to beacons, smart phones*, India Today (Apr. 30, 2021, 4:25 pm) https://www.indiatoday.in/pti-feed/story/attendance-woes-iit-delhi-resorts-to-beacons-smart-phones-911199-2017-04-19

[17] India Today Web Desk, *Tamil Nadu Schools to Launch Facial Recognition app to replace attendance registers*, India Today (May 1, 2021, 7:00 pm) https://www.indiatoday.in/education-today/news/story/tamil-nadu-schools-facial-recognition-app-attendance-registers-artificial-intelligence-divd-1406813-2018-12-11

[18] Ritu Sharma, *Facial-recognition attendance system: It is fool-proof, has no scope for manipulation, says Gujarat's education secretary,* The Indian Express (May 2, 2021, 4:00 pm) https://indianexpress.com/article/education/facial-recognition-attendance-system-it-is-fool-proof-has-no-scope-for-manipulation-says-education-secretary-5925570/

[19] Pavan Duggal, *Facial Recognition in India- Some Legal Challenges*, Cyber Laws Net (May 2, 2021, 10:20 pm)http://cyberlaws.net/blog/facial-recognition-india-legal- challenges/

itself[20]. Amidst such lack of legal backup, the implantation of the FRTs will be a major challenge for Indian legal regime. In this chapter, the Paper shall put forth the current legal scenario pertaining to the FRT in India.

(A) Facial Recognition and the Data Protection Bill, 2019

The Personal Data Protection Bill, 2019 (hereinafter referred as "PDP Bill") mainly applies to processing of personal data of natural persons, of which sensitive personal data and critical personal data are subsets[21]. The PDP Bill, when enacted, will replace Section 43A of the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 which currently, in tandem with sectoral laws, provide for the data protection framework in India[22]. The passing of this bill has the ability of creating an impact on the usage of the said technology by the Government as well as Private entities.

Section 3 (7) of the PDP Bill defines "Biometric Data" as *"biometric data" means facial images, fingerprints, iris scans, or any other similar personal data resulting from measurements or technical processing operations carried out on physical, physiological, or behavioural characteristics of a data principal, which allow or confirm the unique identification of that natural person".* Thus, facial images form a part of biometric data. Further, Section 3 (36) of the said Bill categorizes 'biometric data' as 'sensitive personal data'. The Bill classifies the data into three categories namely critical, sensitive and general. Section 33 of the PDP Bill imposes a prohibition on processing sensitive personal data and critical personal data outside of India. Section 33 specifies that sensitive personal data may be transferred outside of India but must continue to be stored in India. In effect, a local copy of all sensitive personal data must remain within India at all times. But the said transfer of 'sensitive personal data' shall be subject to conditions laid out in Clause 34 of the Bill which therein outlines the circumstances in which sensitive personal data and critical personal data may be transferred outside of India. Thus, in the future if the said bill is being passed by the Parliament of India, both the Government and private entities must comply with the legal framework set out under the Act. To note, the bill lacks clarity in certain aspects of Data processing thereby staking individuals privacy which shall be addressed in Chapter IV of this Paper.

[20] Majid Durrani, *Facial Recognition Technology and its issues*, Tsg Sunday Guardian LIVE (May 2, 2021, 11:15 pm) https://www.sundayguardianlive.com/legally-speaking/facial-recognition-technology-issues

[21] *Analysis of The New Data Protection Law Proposed in India*, Nishith Desai (May 3, 2021, 10:00 am) http://www.nishithdesai.com/fileadmin/user_upload/pdfs/NDA%20Hotline/Analysis_of_the_new_Data_Protection_Law_Dec2419.pdf

[22] *Id.*

(B) Analysis of FRTs via Puttaswamy Judgement

In India, the State's interference in Citizen's privacy by means of any action put forth have to pass the tests laid down by the Supreme Court in the case of *K.S. Puttaswamy v. Union of India*[23]. The said case, affirms that privacy is a fundamental right of the citizen under Indian Constitution. The application of the aforesaid test was subsequent seen in the decision of Aadhaar Case. Moreover, there are a range of cases which are currently pending before the Supreme Court to the Constitutional validity of the surveillance architecture in India. Therefore, the way in which Courts in future will examine the validity of a mechanism like the proposed face recognition system of the NCRB is very likely to be affected in these relevant contexts by the application of the Puttaswamy tests[24]. The Supreme Court stated that although Right to Privacy is not explicitly recognised under our Constitution, it is one of the facets of Article 21 of Indian Constitution and also satisfies the golden triangle requirement laid down under *Maneka Gandhi Case*[25] i.e Right to equality (Article 14), Right to free speech and Expression (Article 19) and Right to life and personal Liberty (Article 21). Thus, State's intervention in citizen's privacy must be fair, just and reasonable.

The judges then went on to explain what it would mean to be fair, just and reasonable in the context of privacy, laying down the following tests: (i) legality – the intervention should be supported by a law; (ii) legitimate goal – it should pursue a legitimate state aim; and (iii) proportionality – there should be a rational nexus between the objects and the means adopted to achieve them. Further, it was also observed that there is a need of an appropriate procedural guarantee to check against the abuse of State power[26].

Thus, when the Supreme Court has created a path for the State to intervene in citizen's privacy subject to the conditions aforementioned, the implementation of the FRTs should be in parlance with the same. India being a democratic country, the ultimate objective of the State should become citizens welfare. Therfore any welfare measure brought through the usage of technology must not impinge on fundamental rights guaranteed by the Constitution. Thereby, balancing between these interest poses a real challenge to Indian Legal regime.

IV. MAJOR CONCERN AND ITS SUGGESTIVE MEASURE

The increased use of FRTs ignites many controversial issues. Right to privacy forms a major issue, thereby becoming a hurdle in successful regulation of FRT. The right to privacy is a

[23] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[24] Smriti, *supra* note 11.
[25] Maneka Gandhi v. Union of India, 1978 SCR (2) 621.
[26] Smriti, *supra* note 11.

Fundamental Human Right as described in Article 12 of the Universal Declaration of Human Rights.[27] Thus, Privacy becomes a major aspect in striking the balance of power between citizens and the Government or an individual and large business companies. A citizen's right to freedom of speech, freedom of religion, freedom of movement-all these are determined by privacy. The right to privacy has been significantly undermined in recent years by emerging technologies which are continuously threatening it.[28] For instance, the use of CCTV cameras involving the FRTs involves constant tracing of a person which is in fact an infringement of an individual's privacy. Also, the use of surveillance technology coupled with FRTs raises a concern in a situation such as an individual using face cover in a mass protest.[29]

In the United States, privacy has not been explicitly recognized, but several legal experts recognise that fundamental right to privacy exist amongst the Amendments.[30] In the US, Cities and States have been pioneers in governing facial recognition in the absence of any national legislation or policy.[31] The two states that have settled laws which concentrate on restricting the use of biometrics, are Texas and Illinois. Laws relating to the use of technology for facial recognition are not limited to the public sector. Several States have integrated biometric data into their current data privacy laws or have developed new laws expressly geared towards collecting biometric data.[32] The first State to tackle the processing of biometric data from private firms was Illinois. The Biometric Information Privacy Act (BIPA) 2008, puts major restrictions on how a person's biometric data can be obtained and used by private entities. The said Act forbids the use of biometric data, places a limitation on disclosing collected data, defines business data privacy obligations and provides write-up actions for individuals whose information has been collected or used in violation of law. This Statute benefits an individual in a situation wherein he/she is unable to prove that any violation in respect of collection or usage of data has directly affected him/her.

Texas laws provides the destruction of data after one year and prohibits the sale of biometric information and places restrictions on the way information must be stored. Other States such

[27] Udhr. art. 12.
[28] Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, The Guardian (May 2, 2021, 12:25 pm), http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy.
[29] Smriti, *supra* note 11.
[30] Griswold v. Connecticut, 381 U.S. 479, 483 (1965).
[31]Sam Dupont, *Without Legal Safeguards, this technology will undermine democratic values and fundamental rights*, Nextgov (May 3, 2021, 6:15 pm) https://www.nextgov.com/ideas/2020/07/facial-recognition-here-we-have-no-laws/166711/
[32]Benjamin Hodges & Kelly Mennemeier, *The varying laws governing Facial Recognition Technology*, IPWatchdog (May 3, 2021, 9:35 pm) https://www.ipwatchdog.com/2020/01/28/varying-laws-governing-facial-recognition-technology/id=118240

as Washington, California have also provided law in this regard.[33] Washington State law requires businesses, in limited conditions, to sell biometric information whereas Californian laws recognises the rights of the consumers by allowing them to obtain information about the collection and the sale of their personal information and by allowing consumers to opt out of the sale of their personal information.

Unlike the US, the right to privacy in India is not explicitly recognized by the Constitution, but it forms a facet of life and personal liberty which is enshrined under Article 21 of the Indian Constitution. However, it is enunciated that it has no active data privacy framework. In the absence of a legal framework, an ideal decision was taken to set up a Committee which was led by Justice BN Srikrishna and thereby the bill called "The Personal Data Protection Bill, 2019" becomes highly significant. Even though the said bill lays down the framework for regulation of data processing, the bill lacks clarity on the aspect of restrictions being placed on private entities in processing biometric Data. Section 92 of the Bill states that *"No data fiduciary shall process such biometric data as may be notified by the Central Government, unless such processing is permitted by law".* As per the Section 3(13) of the Bill, Data Fiduciary includes company and as per aforementioned provision, there is lack of clarity on restrictions placed on Companies unlike Biometric Information Privacy Act in Illinos. Also, Section 35 provides Government agencies a wide power with respect to processing citizens' personal data. It is suggested that when the law provides such a wide power to the Government on one hand, it becomes crucial on the other hand to provide wider law facilitating the citizens their right to get information about processing of their data by the Government.

V. CONCLUSION

With further advancements in the technology and the discovery of newer use-cases, the adoption of FRTs can only be expected to rise further. At the same time, increasing adoption will also exacerbate many of the concerns. The challenge therefore lies in being able to assess the tradeoffs between the drawbacks and advantages of adopting FRTs in different contexts. This sort of thinking is necessary for assessing whether, and under what circumstances, should this technology be adopted.

Thus, to conclude, it can be seen that, the outbreak of Coronavirus has intensively led to rise in the usage of FRTs. And this usage will not merely stop at this phase. Technology is

[33] Sam Castic, Shea G. Leitch, Aravind Swaminathan and Antony P. Kim, *Biometrics: A Fingerprint for Privacy Compliance*, Orrick Trust Anchor (May 3, 2021, 6:15 pm), http://blogs.orrick.com/trustanchor/2016/03/04/biometrics-a-fingerprint-for-privacy-compliance-part-i/

dynamic in nature and will keep evolving and gradually becomes part of a human life. In such a situation forecasting the technological future, it is necessary that the legal protection accord to the citizen of the country must also be developed. The Draft PDP bill along with suitable amendments must be strictly enforced to prevent any infringement on citizens Privacy as the said aspect is recognised as fundamental right. Thus, the state must ensure that the core values of democratic country is being preserved in presence of robust framework meant to tackle the challenges put forth by FRTs in present and future.

*****

 [ISSN 2581-9453]