IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Facial Identity: An Access Card Or A Private Right?

[1]Meghna R

[1]LLB Student, Symbiosis Law School, Pune, India.

ABSTRACT: The Facial Recognition Technology is growing to be a new method of AI Surveillance to capture the threats posed to a nation, but the real question is doesn't it also capture a persons identity and restricts him from living a private and liberal life? The paper herein, speaks on the crux of this issue questioning the constitutional viability of governmental actions using this technology and the safe storage and usage of the identity of its citizen. Discussing its regulatory measures in India and its global counterparts at large. The paper sets to analyse this issue in various ways of factual, statistical, comparative and expert, as its metrics. The substantial use of our facial identities affecting the realms of our private lives. Moreover setting to analyse if the FRT, is properly developed, to deploy for serious applications such as evidence to crime.

Index Terms: *FRT, Right to Privacy, Right to Know, Government, Technology.*

I. INTRODUCTION

At the face of expansion of technology, life as we know it has had a sea of change from what was a decade back to what is present now.[1] Life has been made more simpler and more exposed both at the same time, quite ironically. The technology we use requires immense amount of data to function smoothly: Human are its 'Data Mines' and endless source of experiments can be run by the way of our behaviour, our needs and our identities. It is also a thrilling fact how we have let technology invade our homes, our lives and our privacy. Focusing on current problem, the misuse of such prime information. In a world which has AI enhancements that keeps track of our lives by feeding it information ourselves or even if we opt out by government surveillance, in the name of security, it is difficult to ensure such sensitive information doesn't fall in wrong hands. This paper concentrates on one such AI surveillance method of Facial Recognition Technology[2], how its use by the

[1] McPheat, David. "Technology and Life-Quality." Social Indicators Research, vol. 37, no. 3, 1996, pp. 281–301. JSTOR, http://www.jstor.org/stable/27522907.

[2] Feldstein, Steven. "Types of AI Surveillance." The Global Expansion of AI Surveillance, Carnegie Endowment for International Peace, 2019, pp. 16–21. JSTOR, http://www.jstor.org/stable/resrep20995.8.

government in the name of national security or even security of the public can be infringing the Right to Privacy, ensured under **Article 21**[3]. It is a fact that government has a duty to protect its people but it is also a war strained by the people's Right to know how their data is being used, ensured under **Article 19(1)(a)**[4]. The constitutional dilemma arises when facial identity which is being used to track every movement of the citizens encroaches on the fundamental rights to remain at peace and to live with liberty. The widespread usage of such recognition technology of tapping into people's lives for multiple purposes showed be based on strong principles in statutes.

II. Issue at Hand

The Facial Recognition Technology has extensive usage starting from face locks in our phones, facial mapping via CCTV cameras, facial identification to solve crimes, face tracking to notify the movements of a person. These are the few uses of FRT, these can be wrongly interpretated as the technology is still yet to develop its potential to the finest and the major threat is its consequence in case if its use is not done for just and fair purposes. It doesn't hold good for a democratic government to track its citizen and is in fact a breach to the essentials of constitutionalism set by the fathers of our current developed country. The issue of whether there are properly regulatory bodies surveilling the surveillance of our government and if all the information is transparent regarding tracking of individuals, if it is used for discriminatory purposes. Also, another major issue of theft of such sensitive from the storage facilities, is there is adequate rules protecting the citizens.

2.1 Research Objective

The objective of the paper is to analyse the depths and constitutional repercussions occurring due to FRT. To analyse the regulations set in India in furtherance of allowing the development of FRT whether adequate in comparison to the its global counterparts. The paper focuses on the usage of FRT if it poses serious threats to the Privacy and if the citizens are given enough information regarding their identities being used or if they have been swept aside in the name of Security. The paper elucidates with the factual, statistical and expert as metrics to deduce the objectives.

2.2 Research Question

- ***If Government's use of FRT poses a constitutional violation to the citizens of India?***
- ***Whether adequate regulations and statutes are present to normalize the use of FRT without infringing the Fundamental Rights?***
- ***How FRT is used globally and how people are protected worldwide?***
- ***Finally, if usage of FRT a necessity to secure a nation or is it just a tool to keep eyes on its citizens?***

[3] INDIA CONST. art. 21.
[4] INDIA CONST. art. 19, § 1, cl. a.

2.3 RESEARCH METHODOLOGY

All the information present in the research paper is descriptive, analytical and in doctrinal manner. The research was gathered from books, journals, case reviews, legal databases, legislation analysis and interpretation, and other peer-reviewed journals and research papers, among others, as mentioned below. The statistical information is obtained from well-established websites.

- Heinonline
- Jstor
- Lexis Nexis
- Newspaper: The Hindu, Economic Times,etc.

III. RESEARCH

3.1 WHAT IS FRT ?

Face Recognition Technology (FRT) is an Artificially Intelligent system which encompasses the system to on its own to recognise or map any given face to its ideal match.[5] This is established by software compressed in computer vision which helps in identifying the right match. There are various basic steps to achieve FRT at its finest:

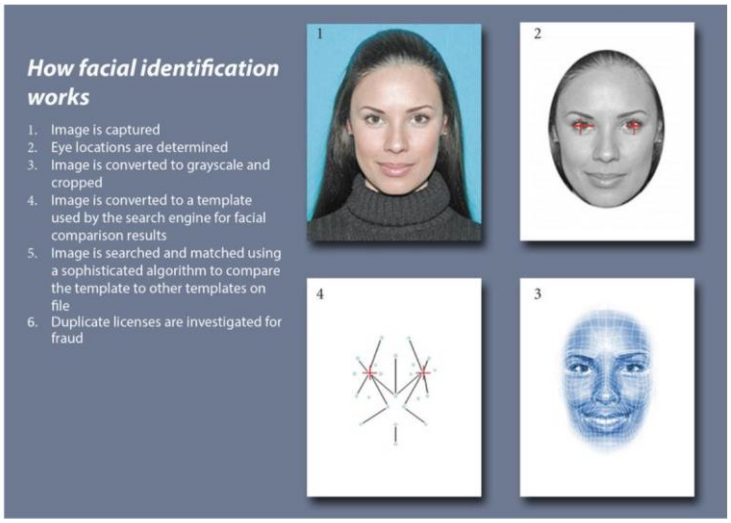
- Face Detection: The target face should be correctly captured and detected.
- Face Characterization[6]: The target face is then analysed with computer algorithm, there are different ways in which the face is analysed.
    1. Holistic Method
    2. Classical Method
    3. Multimodal Method
    4. Feature-Based Method

  The characterization is recently, is done by detecting the eyes and taking the width between the eyes or the shape of a chin.
- Face Verification[7]: Verification happens in 3 ways:
    1. Identifying an unknown person
    2. Verifying the identity of a known person
    3. Looking for multiple specific previously identified face

After the following 3 steps of detection, characterisation and verification, the system successfully produces a match. Now this can, also, be a false positive or false negative match, meaning that the system might falsely

[5] Lehr, Amy K., and William Crumpler. "What Is Facial Recognition?" Facing the Risk: Part 2: Mapping the Human Rights Risks in the Deployment of Facial Recognition Technology, Center for Strategic and International Studies (CSIS), 2021, pp. 2–3. JSTOR
[6] Sikender Mohsienuddin Mohammad, Facial Recognition Technology, June 2020,SSRN Electronic Journal, https://www.researchgate.net/publication/342067011_Facial_Recognition_Technology.
[7] Jennifer Lynch, "Face Off: Law Enforcement Use of Face Recognition Technology", Electronic Frontier Foundation, 2018., https://www.eff.org/files/2018/02/15/face-off-report-1b.pdf.

show a match similar to each other or it might show that there is 'no match' even though match is present, respectively.[8]



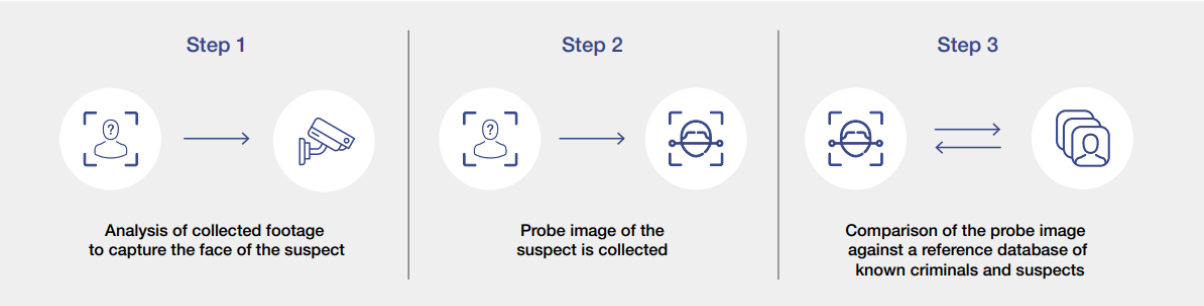
Source: Iowa Department of Transportation [9]

3.2 USAGE OF FRT

There is various usage for the FR technology as listed below:

- Private security: For example, the FRT is used to unlock the phones and entry to their houses.
- Identity verification: In the professional environment, for the sake of attendance and entry and exit of the employees.
- Live monitoring: In this system, the FRT is set in places that require live monitoring in common places, stores and roads for traffic control.
- Border control: FRT used for national security and borders to check on infiltration of people of any enemy State.[10]
- Retroactive Identification: FRT is used in places to identify any known person in a targeted place, example as the identification of the criminals.
- Access Management: entry to any particular restricted area.[11]

[8] Street Level Surveillance: Face Recognition, Electronic Frontier Foundation, https://www.eff.org/pages/face-recognition.
[9] Jennifer Lynch, "Face Off: Law Enforcement Use of Face Recognition Technology", Electronic Frontier Foundation, 2018., https://www.eff.org/files/2018/02/15/face-off-report-1b.pdf.
[10] Ünver, H. Akın. Politics of Digital Surveillance, National Security and Privacy. Centre for Economics and Foreign Policy Studies, 2018. JSTOR, http://www.jstor.org/stable/resrep17009. Accessed 16 Apr. 2023.
[11] Lehr, Amy K., and William Crumpler. "How Is Facial Recognition Being Used?" Facing the Risk: Part 2: Mapping the Human Rights Risks in the Deployment of Facial Recognition Technology, Center for Strategic and International Studies (CSIS), 2021, pp. 4–9. JSTOR, http://www.jstor.org/stable/resrep33749.6. Accessed 16 Apr. 2023.



Source: World Economic Forum on Facial Recognition for Law Enforcement Investigations 2022[12]

3.3 PROBLEM ARISING OUT OF FRT

There are many issues arising when in possession of FRT:

- Improper data storage: In case the biometric data is not stored with stringent security and multiple layer guard checks the breach of a person's identity may take place. In recent times, famous Cloud storage is used, but there is always means to hack leading to cybercrimes.
- Misuse and Misrepresentation of data: Any form of biometric data can be encrypted but the facial identity cannot be done, the misuse or misrepresentation of such data can be made easily.[13]
- Infringement of Right to Privacy: This provision though not an absolute right it is given provision under Article 21, ensuring it to be a fundamental right and in this case, when movement of the citizens are tracked by government leads to distrust between the government and its people.
- Infringement of freedom of speech and association: The minute-to-minute monitoring of the citizens and tracking especially of some specified organisation leads to infringing the fundamental rights enforced by the Article 19 of constitution.
- Lack of transparency: It is the citizens right to know the usage of their identity , the safety such that the information is not sold and the companies maintained such sensitive information are bound by the regulations and agreements.[14]
- Advancement of the FRT: The advancement of such technology in Open Access through lite versions present in Apps might normalise to the extent that they can be used by anyone to exploit someone else.[15]

3.4 USAGE OF FRT IN INDIA:

India has been growing and enhancing its abilities to be at par of its global counterparts in bringing up new technical developments in formation of smart cities. India uses FRT as tool to identify categories of people

[12]A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations INSIGHT REPORT,REVISED NOVEMBER 2022, World Economic Forum. https://www3.weforum.org/docs/WEF_Facial_Recognition_for_Law_Enforcement_Investigations_2022.pdf.

[13] Davis, Wendy N. "Face Time: Facial Recognition Technology Helps Nab Criminals—and Raises Privacy Concerns." ABA Journal, vol. 103, no. 10, 2017, pp. 16–18. JSTOR, https://www.jstor.org/stable/26516097.

[14] "In the Face of Danger: Facial Recognition and the Limits of Privacy Law." Harvard Law Review, vol. 120, no. 7, 2007, pp. 1870–91. JSTOR, http://www.jstor.org/stable/40042639. Accessed 16 Apr. 2023.

[15] 7 Biggest Privacy Concerns Around Facial Recognition Technology,Liberties, Tech and Rights, October 25, 2022, https://www.liberties.eu/en/stories/facial-recognition-privacy-concerns/44518.

such as missing persons, surveillance and tracking, to solve a crime, and for national security. A list below elucidates India's journey in usage of FRT:

- **Digi-Yatra**: A policy launched in 2018, used as a facial biometric boarding system for automated processing of passengers at airports.[16] Here an Id is given to the passengers and with their consent their facial data is shared via the Digi-yatra platform. By 2019, passengers have access to use their face as a boarding pass.[17]
- **FRT usage in Aadhar**: UIDAI[18], incorporated FRT in process of application of Aadhar Id, here facial identity is used as multifactor authentication[19], for avail financial payments.[20]
- **Identifying Missing Children**: FRT was used to identify 3000 children in Delhi.[21]
- **Identifying Public Protests:** To keep an eye surveilling the protestors or an association of potential public protest for public order.[22]
- **National Automated Facial Recognition System (NAFRS):** This is a system which was started to emohasis the modern policing system and provision of processing live video footage and matching the suspects face. NCRB[23] hosted millions of images that is to processed.[24]
- **Usage of FRT for police operation is various states:** There are various schemes n different states as listed below:
    1. Punjab Artificial Intelligence system.
    2. Pehchaan App in Uttar Pradesh.
    3. Face Tagr App in Tamil Nadu
    4. Neoface Tech in Gujarat.
    5. e-beat book app by the Delhi Police

3.5 LEGAL PROVISION AVAILABLE TO REGULATE THE USAGE OF FRT

India has struck to regulate protection of data through a Personal Data Protection Bill, 2019, this classifies information from FRT as 'sensitive data' and there are a few provisions relating to FRT are:

1. Clauses 3(7): in this the term 'biometric data' comprises of 'facial images' as well.

---

[16] Digi Yatra‖- Reimagining Air Travel in India, August 9, 2018, http://civilaviation.gov.in/sites/default/files/Digi%20Yatra%20Policy%2009%20Aug%2018.pdf

[17] _Delhi Airport begins facial recognition tech trials for domestic vistara flyers', https://inc42.com/buzz/delhi-airport-to-enable-facial-recognition-tech-under-digiyatra/

[18] Unique Identification Authority of India.

[19] Authentication Ecosystem, Unique Identification Authority of India | Government of India, accessed November 30, 2020, https://uidai.gov.in/aadhaar-eco-system/authentication-ecosystem.html.

[20] ―Aadhaar Enabled Payment System (AePS) – Aadhaar Pay | NPCI,‖ accessed January 4, 2021, https://www.npci.org.in/what-we-do/aeps/product-overview.

[21] Richa Banka,Delhi HC Seeks Ministry Officials' Reply on Plea Regarding Difficulty in Tracing Missing Kids, Hindustan Times, May 1, 2019, https://www.hindustantimes.com/delhinews/delhi-hc-seeks-ministry-officials-reply-on-plea-regarding-difficulty-in-tracing-missingkids/story-PAVLYqgD3YJSiqpzj99igM.html.

[22] Jay Mazoomdar, ― Delhi Police film protest, run its images through face recognition software to screen crowd‖, Indian Express, December 28, 2019, available at https://indianexpress.com/article/india/police-film-protests-run-its-images-through-face-recognitionsoftware-to-screen-crowd-6188246/.

[23] National Crime Records Bureau

[24] Faizan Mustafa and Utkarsh Leo, "On Facial Recognition and Fundamental Rights in India: A Law and Technology Perspective", December 29, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3995958.

2. Clause 3(36): This categorizes 'biometric data' as 'sensitive personal data'.
3. Clause 33 and 34: Clause 33 states that such 'sensitive data' may be transferred outside India subject to conditions laid down in Clause 34, but should always remain in India.

Addition in the IT Act, 2000 of Section 43A which holds Computer resource owners, controllers and operators liable to compensate to the affected party in case of loss of any data that was meant to be protected and maintained and handled negligent.[25]

Ministry of Electronics and Information Technology prepared a draft Bill, named the Digital Personal Data Protection Bill, 2022 and has invited feedback from the public for public consultation.

3.6 Does FRT affect the Fundamental rights of Indian Citizens?

The question of Constitutionalism of FRT can be identified in two parts, whether the usage of FRT in India infringes the Right to Privacy of its citizen. Whether the conscious consent is given by the citizen and if they are aware of the usage of their facial identity. Indian Constitution enables every citizen with Right to know expressed within the definition of Article 19(1)(a), where disclosure of document affecting the citizens must be available to the free eye of the citizens. In case such opinions are allowed then the usage of the identities of the citizens must also be disclosed.

Article 21, in recent times, enables various forms of Right to Privacy, as an essential ingredient of personal liberty, if the current right includes telephonic conversations, then the movement of any citizen of genuine relations showed also be held private.

IV. Analysis

4.1 Comparative Analysis

Analysing the usage and provisions provided by different countries as shown below:

- In the **US**, FRT has growing usages in its Federal agencies as well as private companies. An effluent company of ClearViewAI has placed itself in agreements with the US government as it majorly process such facial data and trains its system in large. Due to the political organistaion of US, different states in US are approaching the usage and banning of FRT, based on their convenience and Their respect towards the privacy of citizens. In states suich as the New Hampshire, it is even banned to take images of driving license without warrant. But in all the states FRT is majorly used for the Policing purposes.[26]
- In **Canada**, ClearViewAI conducted many tests with regards to solving crime and after analysis of the algorithms that the company required to process such an output, they considered this is a human rights' violation and has not allowed the diffusion of FRT at a faster pace, as it is meant to be.

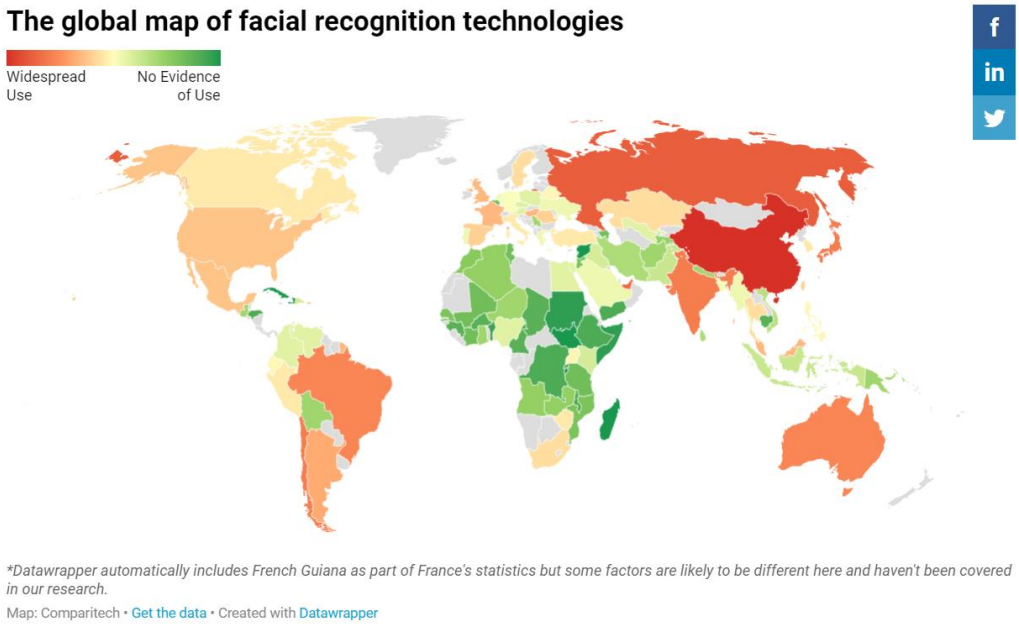
[25] Facial Recognition Technology, 23 DEC 2022 1:59PM by PIB Delhi, https://pib.gov.in/PressReleasePage.aspx?PRID=1885963.
[26] Lewis, James A., and William Crumpler. Facial Recognition Technology: Responsible Use Principles and the Legislative Landscape. Center for Strategic and International Studies (CSIS), 2021. JSTOR, http://www.jstor.org/stable/resrep36913.

- In **Australia**, like in the US are using only for policing purposes subjected to many restrictions, such that the sharing of images of driving license, passports and other sources remain within the jurisdiction of only a handful of governmental agencies.[27]
- In **China,** it can be seen that there is majority of diffusion of FRT in the lives of all their citizens. The Chinese are paying the price of losing their privacy in order to speed up their payment process. There are several technologies developed in China where FRT is used as GPS tracking and movement tracking systems and it provides these technologies for various other countries as well. [28]
- In **Russia**, FRT is actively used and set as an example of the city of Moscow =, as one of the world's largest video surveillance urban area. The social filter in Russia is much weaker, as there are siting of usage of FRT, in black markets, for commercial purposes as well.[29]
- In **EU countries**, GDPR[30] holds as a checkpoint to any data being violated or misused, the strongest of all regulatory works have been provided under GDPR. FRT is done but they have introduced certification schemes to ensure that not only human rights are violated but also to regulate it such that its usage happens in a Non-discriminatory manner.[31]

4.2 Analytic Analysis

From the above a statistical data can be observed with respect to the behaviours of countries with regards to FRT and their minimal usage such the it doesn't infringe the rights of its citizens.

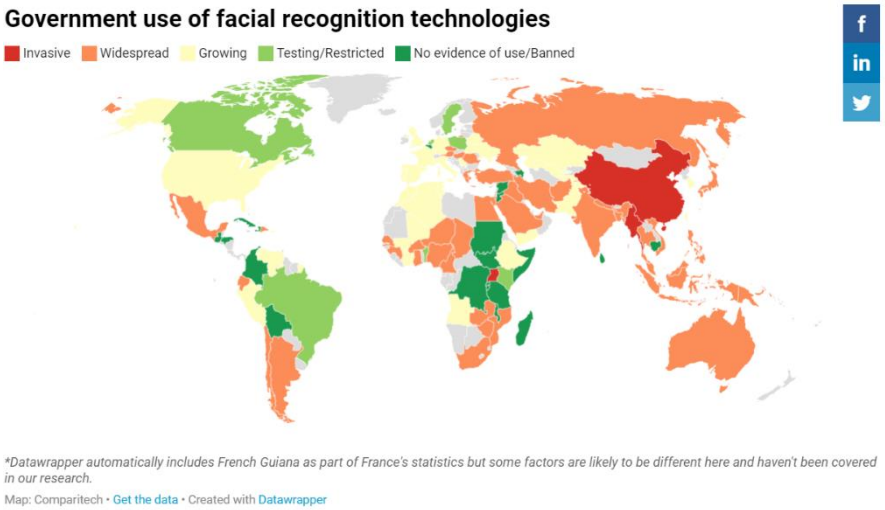
Looking into data of countries that use FRT:



[27] Smith, M., Miller, S. (2021). Facial Recognition and Privacy Rights. In: Biometric Identification, Law and Ethics. SpringerBriefs in Ethics. Springer, Cham. https://doi.org/10.1007/978-3-030-90256-8_2
[28] Kosals, Leonid. "Legitimation of Innovation: The Case of AI Technology for Facial Recognition." The Ambivalence of Power in the Twenty-First Century Economy: Cases from Russia and Beyond, edited by Vadim Radaev and Zoya Kotelnikova, UCL Press, 2022, pp. 80–99. JSTOR, https://doi.org/10.2307/j.ctv280b65x.13.
[29] Ibid.
[30] General Data Protection Regulation 2016/679
[31] Kindt, Els J. Transparency and Accountability Mechanisms for Facial Recognition. German Marshall Fund of the United States, 2021. JSTOR, http://www.jstor.org/stable/resrep28527.

Source: Facial Recognition Technology around the world by ComapriTech[32]

Looking into countries which lead in government usage:



Source: Facial Recognition Technology around the world by ComapriTech[33]

4.3 Analysis with Case Laws

The right to privacy after the leading case of Puttaswamy[34] was read in different light of incorporating the right in the ambits of privacy into the liberty of a person. The right is subject to reasonable restriction and the courts have a 3-fold way to represent the same:

1. Existence of law.
2. Legitimate reason of State.
3. Propotionality of the usage.

In case of Mohd. Arif v Registrar, Supreme Court of India[35], it was held that Article 21 , should be read with other fundamental rights, where the procedure established by law has to be just, fair and reasonable, even the law is to be reasonable.

Sadhan Haldar v The State NCT of Delhi[36] : In the case, it was issued that the use of Automated Facial Recognition System (AFRS) to track and re-unit children.

4.4 Critical Analysis

The state has adequate reasons to enforce FRT usage in governmental practices as it is mainly shown as to stop crime rate in India and for the protection of national security. The purpose of usage of FRT is in fact legitimate and just if it is only used for the purpose to safeguard and catch hold of criminals, but the violation of privacy comes into play when there is over emphasis in the usage of FRT in tracking the movements of certain groups and certain people, this is equivalent to listening into the private conversation of the individuals.

[32] Facial recognition technology (FRT): 100 countries analyzed, Paul Biscoff, https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/.
[33] Ibid.
[34] K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1
[35] Mohd. Arif v Registrar, Supreme Court of India (2014) 9 SCC 737
[36] Sadhan Haldar v The State NCT of Delhi , (W.P. (CRL) 1560/2017.

Upholding of Article 21 in this case is closely linked to the aspects of transparency given by the government by respecting the ambits of Right to know established in Article 19(1)(a). In this present scenario government keeping track of people involved in public protests or certain groups of people is infringing their private to move freely and form association , again protected in the Article19 of our constitution.

V. Conclusion and Suggestion

The play between Government and its citizen with respect to the usage of FRT extensively , is based on the amount of transparency government gives to its citizen. The question of Constitutionalism is also depended on the same, since FRT is used for good purposes as well, by identifying and bringing back several thousand missing children. For such rescue operation and policing purposes government has used the technology in fair and just manner. This was subjected to the preview of the Courts, where the courts had decided if the usage of FRT in a widespread manner was held justified. It can be observed how well served are the regulatory measures of foreign countries are subjected with the use of FRT. In India, for such widespread use there is no proper legislative framework to ensure safe transaction storage of such sensitive facial data. In the modern world of Cyber crime at rise it is quite difficult to ensure unencrypted data such as the facial data, to be preserved. An example of infringement of private organisation Pegasus in hidden form of spyware did try to get hold of our sensitive data[37], and once data is lose in widespread manner recording the movements of every citizen it becomes difficult to protect the citizens from harms way. Hence India is in grave need of more regulatory and legislative measures before the full-fledged usage of the Facial Recognition Technology.

VI. Bibliography

- McPheat, David. “Technology and Life-Quality.” Social Indicators Research, vol. 37, no. 3, 1996, pp. 281–301. JSTOR, http://www.jstor.org/stable/27522907.
- Feldstein, Steven. “Types of AI Surveillance.” The Global Expansion of AI Surveillance, Carnegie Endowment for International Peace, 2019, pp. 16–21. JSTOR, http://www.jstor.org/stable/resrep20995.8.
- Lehr, Amy K., and William Crumpler. “What Is Facial Recognition?” Facing the Risk: Part 2: Mapping the Human Rights Risks in the Deployment of Facial Recognition Technology, Center for Strategic and International Studies (CSIS), 2021, pp. 2–3. JSTOR
- Jennifer Lynch, “Face Off: Law Enforcement Use of Face Recognition Technology”, Electronic Frontier Foundation, 2018., https://www.eff.org/files/2018/02/15/face-off-report-1b.pdf.
- Sikender Mohsienuddin Mohammad, Facial Recognition Technology, June 2020,SSRNElectronicJournal,https://www.researchgate.net/publication/342067011_Facial_Recognition_Technology.

[37] Explained: The findings of the Pegasus committee, and what we know about the use of the Israeli malware,Explained desk , August 26, 2022 07:40 IST, https://indianexpress.com/article/explained/explained-sci-tech/supreme-court-verdict-pegasus-spyware-case-explained-8110710/.

- Ünver, H. Akın. Politics of Digital Surveillance, National Security and Privacy. Centre for Economics and Foreign Policy Studies, 2018. JSTOR, http://www.jstor.org/stable/resrep17009. Accessed 16 Apr. 2023.
- Lehr, Amy K., and William Crumpler. "How Is Facial Recognition Being Used?" Facing the Risk: Part 2: Mapping the Human Rights Risks in the Deployment of Facial Recognition Technology, Center for Strategic and International Studies (CSIS), 2021, pp. 4–9. JSTOR, http://www.jstor.org/stable/resrep33749.6. Accessed 16 Apr. 2023.
- A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations INSIGHT REPORT,REVISED NOVEMBER 2022,World EconomicForum.https://www3.weforum.org/docs/WEF_Facial_Recognition_for_Law_Enforcement_Investigations_2022.pdf.
- "In the Face of Danger: Facial Recognition and the Limits of Privacy Law." Harvard Law Review, vol. 120, no. 7, 2007, pp. 1870–91. JSTOR, http://www.jstor.org/stable/40042639.
- Davis, Wendy N. "Face Time: Facial Recognition Technology Helps Nab Criminals—and Raises Privacy Concerns." ABA Journal, vol. 103, no. 10, 2017, pp. 16–18. JSTOR, https://www.jstor.org/stable/26516097.
- Faizan Mustafa and Utkarsh Leo, "On Facial Recognition and Fundamental Rights in India: A Law and Technology Perspective", December 29, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3995958.
- Lewis, James A., and William Crumpler. Facial Recognition Technology: Responsible Use Principles and the Legislative Landscape. Center for Strategic and International Studies (CSIS), 2021. JSTOR, http://www.jstor.org/stable/resrep36913.
- Smith, M., Miller, S. (2021). Facial Recognition and Privacy Rights. In: Biometric Identification, Law and Ethics. SpringerBriefs in Ethics. Springer, Cham. https://doi.org/10.1007/978-3-030-90256-8_2
- Kosals, Leonid. "Legitimation of Innovation: The Case of AI Technology for Facial Recognition." The Ambivalence of Power in the Twenty-First Century Economy: Cases from Russia and Beyond, edited by Vadim Radaev and Zoya Kotelnikova, UCL Press, 2022, pp. 80–99. JSTOR, https://doi.org/10.2307/j.ctv280b65x.13.
- Kindt, Els J. Transparency and Accountability Mechanisms for Facial Recognition. German Marshall Fund of the United States, 2021. JSTOR, http://www.jstor.org/stable/resrep28527.