WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Facial Recognition Technology and Fundamental Right to Privacy

Yash Gupta

Babasaheb Bhimrao Ambedkar University, Lucknow, India.

Introduction

The augmenting captivation in artificial intelligence has brought into the limelight a pivotal discourse on ethical and conscientious innovation. The most predominant contentious areas of concern swivel around the development and integration of AFRT which is the abbreviation for automated facial recognition technology, specifically in the context of policing and surveillance. This techno-modern tool has heightened global apprehensions due to predicaments pertaining to its configuration, technical limitations, and potential breach of constitutional freedoms and ethics.

In India, multiple state and national government agencies have been zealously pushing for the amalgamation of automated FRT into national law enforcement and policing practices under the umbrella of the National Automated Facial Recognition System.1 The apparent lack of information and transparency surrounding these cutting edge initiatives has instigated serious disquiet, which has impeded the indispensable public debate on these imperative quandaries. This dearth of open discourse has created an acute challenge grappling with the ethical and practical concerns connected with deployment of AI driven facial recognition technology. This has spurred discussions relating to the ethical considerations and governance of artificial intelligence. 2 Artificial intelligence, from a functional point of view, encompasses a range of technologies with computational and processing capabilities that can simulate certain aspects of human cognition. Nowadays in the technologically advanced era, the widespread implementation of AI largely centre around algorithms tailored for machine learning and deep learning, which pass through extensive training on large datasets.3 Automated Facial Recognition Technology, functions as an overarching umbrella term that comprises computer based algorithms that are fundamentally designed to facilitate the recognition and detection of individuals on the basis of their facial attributes and traits. These algorithms are proficient at extracting distinctive facial markers which include emotional expressions such as smiles or grimaces, and then carry out cross- evaluation with pre- extant visual datasets to foresee the likelihood of a person who is matching/ identical with individuals earlier existing in those datasets. The intensifying initiatives to incorporate AFRTs within law enforcement sectors have stirred turbulence among legal scholars and civil rights advocates, who are highly apprehensive about the possible encroachment upon a multitude of fundamental rights enshrined in the Indian Constitution primarily concerning on the fundamental right to privacy.4 The cornerstone of the right to privacy was firmly set up by the Supreme Court in the trailblazing Puttaswamy judgment that marked a crucial moment in the jurisprudential landscape.5

The reliance of the algorithms on computational Intelligence techniques (machine learning techniques and deep learning techniques) which involves extensive training datasets, inherently conflicts with the central axiom of data privacy, also known as informational privacy. In that case, the development of such algorithms are obliged to rigorously conform to the elevated benchmarks enumerated by the Supreme Court.6 A concomitant apprehension that is intricately intertwined with data privacy or informational privacy, pivots around the serious risk brought by AI driven FRTs in promoting and fostering widespread state surveillance, in consequence potentially transgressing upon the fundamental tenet of free speech. From a constitutional and legal frame of reference, a third paramount consideration is connected to the assurance of due process. The legal jurisprudence in India has indisputably established that the due process guarantees safeguarded by Article 21 subsume the dyad of substantive as well as procedural facets.7

Another chief apprehension associated with facial recognition technologies reside in its inherent imprecisions and errors. The desired outcome to gain absolute precision albeit under ideal laboratory conditions, persists as an elusive hard-to-attain goal. As a result, the real-world utilisation of this technology, where extraneous factors greatly influence image fidelity, instigate the peril of both false positives which refers to misidentification and false negatives meaning inability to identify. 8 Misidentification usually transpires when an individual is inaccurately matched with someone else, which potentially results in their unjustified and prejudiced implication in criminal investigations and this also reinforces existing biases targeting specific communities. On the contrary, a failure to accurately identify individuals might culminate in their exclusion from their workplace specifically when it is related to their attendance systems or could also block their access to government endeavours and benefits.

In the present landscape, it is imperative to deliberate upon that India has of late enacted the Digital Personal Data Protection (DPDP) Act of 2023. This leads to a fundamental inquiry regarding the extent to which this legislation proficiently tackles the persistent challenges connected with acquiring datasets for the construction of AFRT algorithms? Moreover, another question arises does the DPDP Act 2023 adequately safeguard the right to privacy of individuals, that can be imperilled and jeopardized by the utilization of Automated Facial Recognition Technologies (AFRTs)? It is also imperative to conduct a thorough analysis of the execution of NAFRS, assessing its ramifications on fundamental rights against the backdrop of four indispensable

The Privacy Paradox of FRT

The landmark Puttaswamy judgement laid down certain elements of right to privacy. The primary element being autonomy and control which is also an intrinsic element of an individual's dignity. The usage of FRT in an intrusive manner in the absence of informed consent sabotages the dignity of an individual, by placing them under constant surveillance. The utilisation of automated FRTs that possess an inherent opacity regarding the sources of training data is a blatant infringement of confidentiality. Facial data that is included under the gamut of personal information must be obtained only by the informed consent of the individuals to achieve and maintain autonomy as to how their facial data is utilised, further guaranteeing informational privacy. Privacy and freedom of thought and expression in my opinion are two facets of the same issue. Privacy is an imbedded spirit of free speech and individuals should be able to express themselves without the fear of surveillance. The other critical facet is the test of proportionality . The deployment of FRTs should only be utilised for specific legitimate purposes which should be proportional to the specific goal it seeks to accomplish, affirming that the intrusions on privacy are rational and legitimate. The balancing test is an inherent building block of right to privacy. It means that while implementing the FRTs, a balance must be struck between individual privacy and state interests.

The Digital Personal Data Protection Act, 2023 also referred as DPDP Act denotes a significant progression for India which incorporated holistic data privacy regulations. This legislation establishes well-defined guidelines for the entities who are accountable for digitally collecting and processing personal data (data fiduciaries), in their engagements with individuals to whom the data belongs (data principals).[10]

Camouflaged in the milieu of growing popularity of artificial intelligence applications that bank on copious quantities of personal data, the DPDP Act extends a reliable framework for affording data handling compliance. Nonetheless, it is crucial to acknowledge that while the legislation brings recourse, it also puts forth numerous issues and sparks a plethora of open ended issues. The development of FRTs is significantly impacted by the shortcomings in the current data protection framework. Firstly, the absence of clear guidelines in the framework governing acceptable uses for data collection, inclusive of face recognition indicates an uncontrolled and possibly unwarranted usage of this technology with undefined bounds. Secondly, there are uncertainties over the sufficiency and competency of security measures in protecting sensitive biometric data due to the lack of clear guidelines on "reasonable security precautions", which is an issue addressed under Section 8(5) of the DPDP Act. Furthermore, as a reflection of bigger issues with data privacy, the absence of required audits for compliance and proactive harm mitigation strategies renders FRTs vulnerable to potential abuse and unanticipated repercussions without providing any means for correction. The Act involves a number of exemptions for government agencies that enables them to process personal data of individuals bereft of the requirement to adhere to necessary
safeguards including obtaining consent or disclosing these operations to the data subject. Adding to this, Section 17(1)(c) of the Act bestows exemptions for agencies involved in processing personal data for the purposes of preventing, detecting, investigating, or prosecuting violations, which exempts them from specific critical legal mandates. [11] According to a TOI report, the Railways Department is kick-starting a major initiative to improve public area surveillance by installing a facial recognition system at major stations on the East Central Railway network. However, the boundless deployment of FRT integrated initiatives is becoming a casualty to unreasonable infringements upon personal privacy. The department by planning to combine the FRS data collection with other crime databases is incurring concerns about technology-induced discrimination and the possibility of mass surveillance and profiling.[12]

The privacy fiasco worsens when private sectors design and develop FRTs for police. Access to huge databases by private companies and the lack of accountability concerning the source of their data are grounds for concern. Problems are raised by the private sector's unfettered access to individual's biometric information, especially facial scans, for national security needs. Engaging private companies in FRT development further obfuscates the lines between state and non-state functions, specifically in the critical field of surveillance. It is unclear if they have an active involvement with assisting law enforcement deploy these tools or if their function is limited to procurement. Another issue is the lack of transparency and documentation in the procurement process, which deviates from accepted public scrutiny procedures and undermines confidence while raising potential legal and due process concerns. Article 21 of the Indian Constitution upholds the "procedure established by law" which mandates that any legal process must not only entail formal acceptance but should be also ethical and reasonable. This tenet is necessary in monitoring modern technologies like predictive policing, where the existing dilemma is the absence of a legal framework to govern the use of AFRT in the law enforcement agencies.

The AFRTs fail the legitimacy test since the usage of the technology is done in a legal vacuum and individual privacy is vitiated by the unregulated use of AFRTs. The result of this technology is not unerringly accurate thereby generates false positives and false negatives. Especially concerning the different communities, there is a constant apprehension that there are high chances where the AFRT systems can produce biased results. There is a lack of oversight and regulation that is necessary to ensure its legitimate use, further giving rise to "function creep" when a system progressively widens it's domain beyond its original motive to fulfil more broader functions.

The deployment of AI models for real-time biometric authentication in civic locales for law enforcement profoundly infringes individual rights, instituting a constant surveillance atmosphere. The FRS which is developed for crime prevention and identification of suspects, involves mass surveillance constricting privacy in public areas and is more intrusive in nature. This excessive surveillance is disproportionate and triggers qualms about its repercussions on democracy. Thus it stumbles in the test of proportionality.

"India is rapidly digitising. There are good things and bad, speed-bumps on the way and caveats to be mindful of".[13]

Conclusion and Last Thought

In my view, automated facial recognition technology is a trade-off, wherein gains materialize at the cost of fundamental rights, specifically the right to privacy. This paper mainly assesses the dimension of FRT deployed by law enforcement agencies, accepting that FRT transcends this purview, demonstrating some user-friendly accessibility like "Digiyatra". In India, FRT remains in a legal void and there has to be a dedicated framework that is tailored to this evolving technology. In order to recognise the ethical quandary, less intrusive alternatives like voice recognition, iris scanning, fingerprint recognition technology or deployment of surveillance cameras that have privacy enhancing features can be adopted. Like other countries in EU have established a moratorium on the use of FRTs, India should also adopt such moratorium until an exclusive legislation governing the technology

is put in place. FRT like any other technology is a cutting edge tool, so its final fruition entirely depends how, by whom and for what purposes it is used.

REFERENCE :

1. Ameen Jauhar, 'Indian Law Enforcement's Ongoing Usage of Automated Facial Recognition Tech – Ethical Risks and Legal Challenges' (2021) Vidhi Centre for Legal Policy <https://vidhilegalpolicy.in/research/indian-law- enforcements-ongoing-usage-of-automated-facial-recognition-technology-ethical-risks-and-legal-challenges/> accessed 25 October 2023
2. ibid
3. Faizan Mustafa and Utkarsh Leo, 'On Facial Recognition and Fundamental Rights in India: A Law and Technology
4. Perspective' (2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3995958> accessed 25 October 2023 4 ibid
5. Justice K.S. Puttaswamy v. Union Of India (2017) 10 SCC 1
6. Elonnai Hickok and others, 'Facial Recognition Technology in India' (2021) The Human Rights, Big Data and Technology Project, University of Essex, UK <https://cis-india.org/internet-governance/blog/hrbdt-and-cis-august- 31-2021-facial-recognition-technology-in-india> accessed 25 October 2023 Jauhar (n 1) 8
7. Vera Lúcia Raposo, 'When facial recognition does not 'recognise': erroneous identifications and resulting liabilities' (2023) AI & SOCIETY Journal of Knowledge, Culture and Communication <https://link.springer.com/article/10.1007/s00146-023-01634-z> accessed 25 October 2023
8. prerequisites, precisely: (i) test of legitimacy; (ii) the test of proportionality; and (iii) the existence of requisite procedural safeguards (due process)
9. Hickok and others (n 6) 18
10. Digital Personal Data Protection Act 2023 (India)
11. Digital Personal Data Protection Act 2023 (India)
12. Kumod Verma, 'Rlys set to install facial recognitionsystem at all major stations in ECR' (TOI, 28 August 2023) <https://timesofindia.indiatimes.com/city/patna/rlys-set-to-install-facial-recognitionsystem-at-all-major-stations- in-ecr/articleshow/103113914.cms> accessed 25 October 2023
13. Srinivas Kodali, 'Indians' Personal Data Breached Yet Again, but No Sign That Gaps Will Be Plugged' (The Wire, 30 October 2023) <https://m.thewire.in/article/tech/indians-personal-data-breached-yet-again-but-no-sign-that-gaps-will-be-plugged> accessed 30 October 2023