Indian Law Enforcement's Ongoing Usage of Automated Facial Recognition Tech – Ethical Risks and Legal Challenges

Working Paper 1 | August 2021

V | D H | Centre for Legal Policy
Better laws | better governance

This working paper is an independent, non-commissioned piece of research undertaken by the Vidhi Centre for Legal Policy, an independent think tank doing legal research to help make better laws.

About the Author

Ameen Jauhar is a senior resident fellow at the Vidhi Centre for Legal Policy, leading its Centre for Applied Law & Tech Research. Ameen's focus areas include AI ethics and governance, and the use of AI in legal and justice systems.

The author would like to thank Alok Prasanna (Lead, Vidhi Karnataka), Neha Singhal (Lead, Criminal Justice at Vidhi), Jai Vipra (Senior Resident Fellow, Vidhi), Naseem Jauhar (PhD candidate, University of Toronto), and Dhruv Somayajula (Research Fellow, Vidhi), for their detailed and invaluable inputs which have led to this iteration of the working paper.

The author further acknowledges the excellent research assistance provided by Prerna Sengupta (NALSAR) and Aryan Dama (NLU Mumbai).

About the Centre for Applied Law & Tech Research

The Centre for Applied Law and Technology Research (ALTR) has been established within Vidhi to spearhead original, independent research on crucial issues emerging within the law and technology domain. The team was formally constituted in September 2020, comprising an interdisciplinary roster of researchers from both legal and social science backgrounds. The Centre's key objective is to conduct high quality research, as well as engaging with the main stakeholders to translate our academic work into actionable reforms. Our ongoing work focuses on three main areas: Internet and data governance; Digital economy; and AI ethics and governance of AI. In pursuit of its research and policy work, ALTR has forged crucial partnerships and collaborations, including those with the UN Resident Coordinator's office, IIIT Delhi, NITI Aayog, Dept. of Transport (Govt. of NCT of Delhi), etc., among other stakeholders.

Table of Contents

Executive Summary

With an increasing interest in the potential for AI, there are also concerns that have been highlighted, driven by ideas of responsible and ethical innovation. One of the most contentious use of intelligent algorithms is the development and deployment of automated facial recognition technology (AFRT), especially for law enforcement and surveillance purposes.

Across the globe, concerns have been flagged regarding the design and technical flaws in AFRTs, along with its potential chilling effect on constitutional freedoms and values. In India, across different states, as well as at a national level, different government agencies are pursuing AFRTs' integration into domestic law enforcement practices. Where this becomes particularly alarming is how most of this has happened without much information or transparency, thereby eluding a necessary public debate around the issues.

In this background, this paper, along with the subsequent working papers of this series, will bring to light certain facets which are crucial from the Indian standpoint, yet under discussed or completely ignored. This paper specifically, is a primer on how the issues around AFRTs in Indian law enforcement have currently been discussed, some of the key risks and challenges that have emerged therein. The challenges can broadly be classified into constitutional and legal challenges; ethical risk; and the exact value of AFRTs under Indian Evidence Act for their usage in the criminal justice system.

The paper concludes by stipulating why and how more elaborate discourses are needed around these issues of AFRTs, to achieve India's stated goal of "responsible AI for all".

Prefatory Remarks

> *"There should be a moratorium on the use of Facial Recognition technology in the context of peaceful protests, until States meet certain conditions including transparency, oversight and Human Rights due diligence before deploying it."*
>
> Michelle Bachelet, UN Human Rights Chief[1]

Background

Across the globe, and in India, there is a surge in *artificial intelligence* (AI) innovation, resulting in conversations around AI ethics and its governance.[2] In a functional sense, AI can be defined as a collective term for technologies that have computational capabilities that can mimic some aspects of human cognition.[3] Presently, the more commonly designed and deployed AI are *machine learning* or *deep learning* algorithms, that are trained on copious amounts of training datasets.

In India, a 2018 strategy paper published by NITI Aayog identified different sectors including agriculture, education and health as potential avenues for the application of AI technologies. However, even outside of these specifically identified sectors, the state has been deploying AI, in a relatively less transparent way. The use of *automated facial recognition technologies* (AFRT) by Indian law enforcement agencies, is arguably the prime example of the more contentious application of AI in a public sector, potentially impacting millions of citizens. AFRT is a catch-all terminology for computational algorithms primarily facilitating identification of individuals using facial maps and features. Such algorithms extract unique identification facial features, including emotional displays (like smiles, frowns, etc.) and cross analyse them with existing visual datasets to predict the percentage matchability of a person with existing individuals in such datasets.[4] Given its innately versatile nature, AFRT is fast gaining popularity for its commercial usage. For instance, many smartphones now have a common feature of using facial biometric information to unlock and access the content of such phones. Similarly, airports, including in India, have attempted to create digital check-in facilities using AFRTs at kiosks.[5]

---

[1] Dogantekin V. (2020) *UN raises concern about facial recognition technology*, AA, available at, https://www.aa.com.tr/en/science-technology/un-raises-concern-about-facial-recognition-technology/1890067, last accessed on August 1, 2021.

[2] Good overviews of global AI ethics' conversations can be found in Gupta A., *et al.* (2020) *The state of AI ethics June 2020*, Montreal AI Ethics Institute, available at https://montrealethics.ai/wp-content/uploads/2020/06/State-of-AI-Ethics-June-2020-report.pdf, last accessed on August 1, 2021; and Gupta A., *et al.* (2020) *The state of AI ethics October 2020*, available at https://www.researchgate.net/publication/345351765_The_State_of_AI_Ethics_Report_October_2020, last accessed on August 1, 2021.

[3] For a detailed discussion on how AI and other intelligent technologies mimic human cognitive activities, see Bostrom N. (2014) *Superintelligence: Paths, dangers, strategies*, Oxford University Press (26-61); and Husain A. (2017) *The sentient machine: The coming age of AI*, Scribner, (20-34).

[4] Krier S. (2020) *Facing affect recognition*, available at https://asiasociety.org/sites/default/files/inline-files/Affect%20Final.pdf, last accessed on August 1, 2021.

Unlike some of these innocuous applications, the use of AFRT in surveillance and law enforcement is far from a benign application and is laden with considerable risk. This conversation around its risks is not limited to India; across the globe concerted efforts have been made to identify and document the risks of AFRTs in law enforcement, and determine a fundamental question based on this risk assessment - should such technology even feature in policing and law enforcement in the first place?[6]

For India, where at present this technology is being designed and deployed in the absence of any legislative or regulatory oversight, it is also crucial to identify the practical implications of its use by police and law enforcement agencies, and consequently answer the same fundamental question - should AFRTs be banned, temporarily subjected to a moratorium, or continue to be developed and deployed with adequate regulation and checks and balances?

Research objective

Keeping this context in mind, the Centre for Applied Law & Technology Research (ALTR), aims to publish a series of working papers on the use of AFRT by Indian law enforcement agencies. Each of our papers will cover a distinct theme, developed through a mixed methodology of desk review of literature (with a focus on Indian scholarship), and where possible, conduct empirical research to develop new hypotheses and analyses. While recognising the gamut of issues that emanate from the discourse on the use of AFRTs in policing, for our current project, we have narrowed our immediate focus to three areas. This paper was the introductory document providing a primer on key issues for India's use of AFRT in law enforcement. Following from this, we have identified two more themes that we feel are currently lacking in the Indian discourse around AFRT usage.

a. First, there is a dearth of empirical research work on AI in general, and particularly regarding AFRTs in India. As such, our second paper will be examining some of the risks identified in this paper by undertaking a data driven study of AFRT usage by the Delhi Police. It will set out the broad implications of such technologies for predictive policing; and
b. Second, we will be examining the role that the private sector is playing in the current process of designing and deploying AFRTs for law enforcement, the risks involved in this, and recommendations to safeguard public interest.

---

[5] Tejaswi M. (2021) *Facility for face recognition planned*, The Hindu, April 1, 2021, available at https://www.thehindu.com/news/national/facial-recognition-tech-coming-up-for-some-airports/article34217449.ece, last accessed on August 1, 2021.

[6] For instance, see Louradour S. (2021) *What to know about the EU's facial recognition regulation – and how to comply*, available at https://www.weforum.org/agenda/2021/04/facial-recognition-regulation-eu-european-union-ec-ai-artificial-intelligence-machine-learning-risk-management-compliance-technology-providers/, last accessed on August 1, 2021. For a cross jurisdiction comparison between US, EU and India, see Jauhar A. (2021) *Facing up to the risks of automated facial recognition technologies in Indian law enforcement*, Indian Journal of Law & Technology Vol 16(1), pp. 1-15.

It is pertinent to mention here that whether AFRTs are actually effective in improving policing and law enforcement, is a question that requires immediate and rigorous data-driven research work. However, this is not a focus point for this paper, or for the remainder of this series, and must be undertaken separately.

Scope and Research Methodology

As more and more states are eager in their deployment of such tools to ease the burden of policing and establish newer technocratic models, this paper, the first in our three-part series, aims to do a deep dive into how such usage is likely to pan out in India. For this we have undertaken a desk-review of the existing gamut of published and grey literature, studying the use of AFRT within policing and law enforcement, and putting forth the risks that have featured in such literature, as well as our synthesis of the same. While we have relied on some public resources from other jurisdictions, it is pertinent to mention that the focus of this paper centres around challenges posed to Indian citizens by law enforcement's use of AFRTs.

Our desk review of existing literature was undertaken through the following steps:

a. A comprehensive web search was conducted of news reportage over the past three years, reviewing coverage of different states deploying facial recognition technology in their respective police forces;
b. Published articles in Indian law journals, available on platforms like HeinOnline and Westlaw, or on Google Scholar, were reviewed to examine key issues that have been identified around the use of AFRT in law enforcement in India;
c. Boolean search was conducted on Google's search engine and Google Scholar to examine any additional published and grey literature, focusing mostly on India-centric scholarship, examining the use of AFRT in law enforcement; and
d. For international documents, our review is limited to governmental and official publications from the EU and the United States, where the debate around AFRTs has expanded quite rapidly in the last few years.

Through our literature review, we have been able to glean the key issues that have featured either commonly across most of the scholarship, or in some cases, demonstrate the unique challenges that will be posed in India, using AFRT for law enforcement. Broadly, we will be dividing the challenges arising from this, into three broad categories:

a. Constitutional Issues, involving the right to privacy, freedom of speech and expression and prevention of mass state surveillance, and vitiation of due process afforded to every accused under Article 21 (**part I of this paper**); and
b. AI ethics' problems, including lack of transparency and accountability in the deployment of AFRTs by police forces and states, inaccuracies and biases being potentially reinforced, and the systemic targeting of vulnerable groups (**part II of this paper**).

c. A third category of issues that we will also be exploring, though it has not found much discussion in existing literature, is criminal justice related problems (**part III of this paper**). Specifically, we will be examining and discussing how evidence extracted from the use of AFRTs will be utilised in the current legislative framework governing criminal trials.

I. Constitutional Problems Arising from the Use of AFRTs

Across the globe, a key element of the AI ethics' discourse has been the preservation and safeguarding of basic human rights and values that form the foundation of modern societies.[7] For instance, the CEPEJ charter on the ethical use of AI in justice systems unequivocally espoused the need to guarantee its alignment with the core ethos of European democracies. This has further been reiterated by the European Union in its White Paper on AI,[8] and the recently released proposal for legislative regulation of AI.[9]

In the Indian context, the approach document published by NITI Aayog, the Indian government's think-tank, has categorically stipulated the need to adhere to our *constitutional morality* which "extends beyond the mere text of the Constitution to encompassing the values of a diverse and inclusive society while remaining faithful to other constitutional principles".[10] Fundamentally, constitutional rights and ethos must serve as the benchmark to adhere to, while designing and deploying AI in India, in any sector (including law enforcement).[11]

Having said this, the increasing interest in AFRTs by state police forces has certainly alarmed constitutional scholars and civil rights activists about its potential to trample several fundamental rights afforded by the Indian Constitution. Foremost amongst these is the potential infringement of a person's right to privacy, as was read into Article 21 by the Supreme Court in *Puttaswamy*.[12] As discussed in the introductory portion of this paper, the commonly prevalent AI are algorithms which rely on *machine* or *deep learning* techniques, requiring copious amounts of training datasets. Hence, the creation of such algorithms inherently conflicts with the idea of informational privacy, and must comply with the high threshold laid down by the Supreme Court.[13] Add to this, the fact that India presently does not have a well-defined data protection

---

[7] CEPEJ (2018) *European ethical charter on the use of AI in judicial systems and their environment*, European Commission for Efficiency of Justice, available at https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c, last accessed on August 1, 2021.

[8] European Commission (2020) *White Paper: On Artificial Intelligence – a European approach to excellence and trust*, available at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf, last accessed on August 1, 2021.

[9] European Commission (2021) *Regulation of the European Parliament and the Commission laying down harmonised rules on AI (AI Act) and amending certain Union legislative Acts*, COM(2021) 206 Final, 2021/0106 (COD), available at https://eur-lex.europa.eu/legal-content/EN/TXT/DOC/?uri=CELEX:52021PC0206&from=EN, last accessed on August 1, 2021.

[10] Roy A., *et al.* (2021) *Responsible AI: Approach document for India Part I – Principles for responsible AI*, NITI Aayog, available at https://indiaai.gov.in/research-reports/responsible-ai-part-1-principles-for-responsible-ai, last accessed on August 1, 2021.

[11] Id. at pp. 3, 38-39.

[12] *K.S. Puttaswamy v. Union of India*, W.P. 494 of 2012.

legislation, there will be a perpetual risk of sourcing datasets for the designing of AFRT algorithms.

Another concern, somewhat linked to informational privacy, has been against the high risk of AFRTs facilitating mass state surveillance and consequently impeding free speech.[14] There have been numerous instances across the globe where police forces have questionably deployed AFRTs to identify and single out protestors.[15] The legality of such tactics is currently moot, with many civil rights organizations criticising such a heavy-handed state surveillance mechanism. In India too, a recent example, which demonstrates a disconcerting alacrity of law enforcement to identify and prosecute protestors, emerged in 2020 when reportedly, the Delhi Police reportedly decided to deploy such technologies to potentially charge anti-CAA protestors.[16]

The third key consideration from a constitutional and legal standpoint is the guarantee of *due process*. Indian jurisprudence has categorically held that due process guarantees under Article 21 include both substantive and procedural processes. This means that the use of AFRT in law enforcement, and its potential usage, to charge and to incarcerate individuals must also satisfy these criteria.[17] All these issues will be discussed in more detail in this part.

a. Privacy risks posed by AFRTs

The increasing efforts to integrate AFRTs into law enforcement have raised alarm bells for privacy advocates, researchers and civil society activists, on the potential implications this may have on an individual's informational privacy. The collection, storage and usage of data lies at its heart even in the context of AFRTs. First, there appears to be a lack of clarity on what kind of data will be tapped into, for designing indigenous AFRT tools for Indian law enforcement. In the broadest possible sense, this can include facial scans, CCTV footage, archived databases of pictures (like Aadhaar), images available from identification documents (like drivers' licenses, passports, etc.). For instance, the National Crime Records Bureau (NCRB), in its original tender,

---

[13] Bhatia G. (2017) *The Supreme Court's Right to Privacy Judgment*, Economic & Political Weekly LII No. 44 (November 4, 2017): pp. 22–25

[14] Chandak S. (2020) *Artificial Intelligence and policing: A human rights perspective*, 7(1) NLUJ Law Rev. 43, pp. 44-69.

[15] See Vincent J (2020) *NYPD used facial recognition to track down Black Lives Matter activist*, The Verge, August 18, 2020, available at https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram, last accessed on August 1, 202. For more such examples from the UK and Hong Kong, see Sabbagh D. (2020) *South Wales police lose landmark facial recognition case*, The Guardian, August 11, 2020, available at https://www.theguardian.com/technology/2020/aug/11/south-wales-police-lose-landmark-facial-recognition-case, and Mazur P. (2019) *In Hong Kong protests, faces become weapons*, The New York Times, July 26, 2019, available at https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html, last accessed on August 1, 2021, respectively.

[16] "Anti-CAA" is a colloquial collective term used for diverse citizen groups and individuals who have been participating in large-scale demonstrations against the Citizenship Amendment Act, 2019, passed by the Indian Parliament, available at https://egazette.nic.in/WriteReadData/2019/214646.pdf, last accessed on August 1, 2021. See also, Mazoomdaar J. (2019) *Delhi police film protests, run its images through face recognition software to screen crowd*, The Indian Express, December 28, 2019, available at https://indianexpress.com/article/india/police-film-protests-run-its-images-through-face-recognition-software-to-screen-crowd-6188246/, last accessed on August 1, 2021.

[17] Jauhar, *supra* n. 6.

indicated that it will be integrated with "different systems & databases like ICJS, CCTNS, Immigration Visa Foreigner Registration Tracking (IVFRT), *khoya paya*, advanced state police integration software and other" which is apparently an all-inclusive list of data corpuses.[18] After a legal notice was issued challenging the legality of this tender, the same has been revised to include a more conservative list of datasets.[19] However, there are even more invasive data gathering processes which have been in existence. The starkest example is that of *Clearview AI* (Clearview), a corporation based out of New York (US), which has been front and center in the global discourse on privacy implications of AFRTs.[20] Clearview has gained international infamy for the expansiveness of its database for training its facial recognition algorithms. It taps into all available images of individuals across the globe, across social networks like Facebook, and other sources on the Internet.[21] Further fueling this already combustible issue is how Clearview over the past few years has contracted its AFRT to numerous governmental and private organizations, both within the United States and outside.[22] The *Clearview* scenario has triggered a serious consideration amongst policymakers of not only the implications of AFRT in law enforcement, but also the more fundamental issue - whether such invasion is permissible when weighed against the potential security benefits such predictive tools may yield.

In the Indian context, the right to privacy has arguably been the single most prominent talking point for tech policy professionals, both legal and otherwise. The genesis of this more recent revival of the privacy debate was the *Puttaswamy* judgment of the Supreme Court which reversed parts of existing jurisprudence on the issue, to unequivocally read the *right to privacy* within Part III of the Indian Constitution.[23] A significant element of the judgment was the acknowledgement of an individual's autonomy over her personal information.[24] In fact, the judgement determines this autonomy as the ability to determine what information is to be collected, how, and for what purpose.[25] It is this aspect of individual autonomy which is seemingly being vitiated through the design and deployment of AFRTs.

---

[18] NCRB (2019) *Request for proposal to procure National Automated Facial Recognition System (AFRS)*, Ministry of Home Affairs and NCRB, available at https://drive.google.com/file/d/1rZhDeH9a9E6T7zDTNZoyBdPakwwFFpBU/view, last accessed on August 1, 2021.

[19] NCRB (2020) *Request for proposal to procure National Automated Facial Recognition System (AFRS)*, Ministry of Home Affairs and NCRB, available at https://drive.google.com/file/d/1KgnURYsFLBqOhLidW28nrbugI--SnKx5/view, last accessed on August 1, 2021.

[20] Hill K. (2020) *The secretive company that might end privacy as we know it*, The New York Times, January 18, 2020, available at https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html, last accessed on August 1, 2021.

[21] Hill K. (2020) *Your face is not your own*, The New York Times, available at https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html, last accessed on August 1, 2021.

[22] Mac R., *et al.* (2020) *Clearview's facial recognition app has been used by the Justice Dept., ICE, Macy's, Walmart and the NBA.* BuzzFeed (Tech), February 27, 2020, available at https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement, last accessed on August 1, 2021.

[23] Puttaswamy *supra* n. 12.

[24] Puttaswamy *id.*, especially plurality opinion of Justice Chandrachud.

[25] Bhatia *supra* n. 13. See also, Bhandari, V., *et al.* (2017) An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict. IndraStra Global, 11, 1-5, available at https://nbn-resolving.org/urn:nbn:de:0168-ssoar-54766-2, last accessed on August 1, 2021.

Box 1: Lack of informational autonomy of individuals

In its landmark ruling of *Puttaswamy,* the Supreme Court has unequivocally hinged the right to privacy on the idea of an individual controlling access and usage of her personal information. With AFRTs, and the lack of clarity of how such algorithms are sourcing the training data corpuses, this autonomy is at risk. Lack of consent for allowing such one's visual data to be made available for developing AFRTs is a clear infringement of one's right to privacy and determining the use of her data. An example could include a person applying for passport renewal and consenting to her picture being taken for the same. However, that was not a consent to have the same picture be used for adding it to the data corpus for training a *facial recognition* algorithm. The person's consent is very specific for a limited scenario and unilateral expansion that is arbitrary and violative of the right to privacy. because any individual who submitted her facial image for a specific purpose did not consent to this extended use of the same.

Beyond the consent of a person, there is the concern on how FRT developed for a specific function is expanded into law enforcement without any oversight or regulatory framework. This became abundantly clear when the Delhi Police announced last year that it will be using its FRT hitherto used for locating missing children, to identify protestors in the Anti-CAA movement. This "creeping scope of usage" occurs in the absence of any procedural safeguards and is presently, seemingly left to the wisdom of the law enforcement agencies, who clearly have a bias to adopt such tools without giving adequate thought to due process.

The privacy conundrums surrounding AFRTs use in law enforcement will also not be checked by the draft PDP bill which was tabled in Parliament in 2019. The draft bill has crafted sweeping exemptions (under Ss. 35 and 36) which is likely to prevent any meaningful regulation of FRT in law enforcement to safeguard informational privacy.[26] That said, the fundamental right to privacy as established through *Puttaswamy* still remains and FRT in law enforcement must adhere with the *proportionality* test established therein.[27] The current design of AFRTs in law enforcement provides no understanding of how this burden is being met by the state or the police. This makes the use of such technology susceptible to a constitutional challenge, to effectuate checks and balances which are presently missing.

b. State surveillance and impeding free speech and expression

[26] See sections 35 & 36 of the PDP Bill, 2019 confer powers on the Central Government to exempt any governmental agency (s. 35) or certain data processors (s. 36). See the full text of the PDP Bill, 2019, available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf, last accessed on August 1, 2021.

[27] The *proportionality* test draw from the European standard – Justice Chandrachud's plurality opinion establishes three prongs for this test, namely, legality, legitimate goal, and proportionality by establishing nexus between the means and ends. For a more detailed discussion see Bhadari, *el al.*, *supra* n. 25.

Directly connected to the use of AFRTs in law enforcement, is the underlying risk of excessive surveillance to target opposition, vulnerable populations, or other anti-establishment elements. Even internationally, there is an increasing sense of discomfiture on the unbridled use of AFRTs to suppress legitimate protests or target specific opposition - a fact that becomes abundantly clear from the recent AI Global Surveillance Index.[28] This index showed more than 80 percent of the countries it examined relying on AFRTs for surveillance purposes.[29]

Perhaps, internationally, the most prominent specimen of this state surveillance emerged from the Hong Kong protests in 2019, wherein facial identification technology was being deployed to identify masked protestors.[30] Similar reports also emerged in last year's *Black Lives Matter* protests across the United States.[31] Closer home, in India, FRT has also been touted by police and other law enforcement to target protests, including the aforementioned announcement by the Delhi Police to target anti-CAA protestors last year.[32]

In the absence of a governing legal or regulatory framework, such unbridled and arbitrary exercising of surveillance measures can seriously impinge on the fundamental right of free speech and expression, which enshrines within itself the liberty to organise and protest.[33] Furthermore, given the current political climate, several non-state actors, both domestic and non-Indian, have repeatedly suspected the robustness of India's democratic credentials. While public order is carved out as a *reasonable* exception to free speech and expression, it is imperative that this reasonableness be demonstrated through legislative checks and balances. In the absence of such reasonable restraint, such technologies can further state sanctioned deprivation of the most basic and fundamental rights enshrined in the Indian Constitution.

c. Due process concerns regarding AFRTs in law enforcement

The Indian Constitution establishes the idea of "procedure established by law" under Article 21, as an exception to the *right to life and liberty* afforded therein. Over the years, constitutional jurisprudence has construed this phrase to include both *procedural* and *substantive* due process elements. Consequently, not only must a process or procedure be established by law (procedural due process), the same must also be fair, just and reasonable.[34] Therefore, no process(es) in law may be inherently arbitrary - a principle that needs to be cautiously safeguarded in new age

---

[28] Feldstein, S. (2019) *The global expansion of AI surveillance*, Carnegie Endowment for International Peace, available at https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847, last accessed on August 1, 2021.

[29] Parsheera, S. (2019) *Adoption and regulation of facial recognition technologies in India: Why and why not?*, Data Governance Network Working Paper 05, available at https://datagovernance.org/files/research/NIPFP_Smriti_FRT_-_Paper_5.pdf, last accessed on August 1, 2021.

[30] Mazur, *supra* n. 15.

[31] Vincent, *supra* n. 15.

[32] Mazoomdaar, *supra* n. 16.

[33] Parsheera , *supra* n. 29.

[34] *Maneka Gandhi v. UOI*, 1978 SCC (1) 248.

predictive policing efforts. A recent case study of the Delhi Police's predictive policing efforts, exposed how *arbitrariness* was inherently hardcoded into their respective frameworks.[35]

Arguably, arbitrariness is demonstrated in the current absence of any legislative, regulatory, or governance framework to govern AFRTs use in Indian law enforcement. At present, nothing in the statute books prescribes any limits, or checks and balances on the police's ability to design, deploy, and scale this technology.[36] Coupled with the opacity with which this entire process is happening, it is entirely plausible that police forces will risk due process norms to merely hasten their investigative processes.[37]

Therefore, AFRTs in law enforcement present due process challenges both from the procedural and substantive standpoints. Procedurally, the absence of any act or statute authorising their use, prescribing the methods and limits to their application, and establishing other statutory processes is a significant lacuna. Add to that, the aforementioned arbitrariness in its current application, a person can potentially be prosecuted based on evidence that is ungoverned or unauthorised in Indian law, at the discretion of the authorities who have a clear conflict of interest in promoting the use of AFRTs.

In light of this discussion, it can certainly be postulated that the use of AFRTs in India by the police and other law enforcement agencies is currently rife with legal and constitutional infringements. It certainly warrants a greater and more transparent deliberation on how the same need to be remedied, and the interim measures that need to be adopted to ensure compliance with the Constitution and law of the land. The final segment of this paper will delve more into these points.

---

[35] Vidushi Marda and Shivangi Narayan *'Data in New Delhi's predictive policing system'*, (2020), 317-324, DOI:10.1145/3351095.3372865.

[36] This has also been argued in a legal notice served to the NCRB seeking rescinding of its request for proposals for the nationwide AFRS. See Internet Freedom Foundation (2019) *Rejoinder to Reply dated November 5, 2019*, available at https://drive.google.com/file/d/1Cb9BtySI7Z7IM7tvAJGNRqQ96ypAGtbN/view, last accessed on August 1, 2021.

[37] Jauhar, *supra* n. 6.

II. Ethical Challenges in AFRTs' Adoption and Usage

Beyond the aforementioned constitutional and legal challenges, there are ethical concerns surrounding the very nature of AFRTs, which get aggravated when the same is used by law enforcement of individual identification and surveillance. These include issues of lack of transparency and accountability, technical flaws in design and deployment of AFRTs, and how these flaws arguably reinforce existing societal biases. These themes are also present in the larger discourse of AI ethics and have devolved into standards for examining the risks of most forms of present AI applications, and not just AFRTs.

The problem of lack of transparency has two facets. First, there is the technical facet, i.e., are AFRTs transparent and explainable algorithms? Second, there is the issue of administrative transparency and accountability in terms of how state police in India are currently setting up such systems in complete opaqueness, with little to no publicly available information. Such a scenario raises several red flags in terms of accountability, and who to hold responsible in the event of a harm being caused by the use of such technology. It also strikes at the root of democratic institutions and can foster distrust against public institutions like the police working in complete secrecy on the use of such systems.

The design and data flaws are the other set of challenges that have emerged from both Indian[38] and foreign[39] scholarship. For example, research shows that current models of facial recognition often yield inaccurate results, especially against darker complexioned people. Such false positives can prove particularly catastrophic when the outcome of such technologies can effectively result in the arrest and possible incarceration of an individual.[40] There is also the concern that such technology, especially in the Indian context, could be used to reinforce police's targeting of already vulnerable populations.[41] All these ethical issues are explored in a more detailed manner hereinafter.

a. Shortcomings in design and administrative transparency

[38] See Jauhar *supra* n.6; and Parsheera *supra* n. 29.

[39] Joy Buolamwini and Timnit Gebru (2018) *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Conference on Fairness, Accountability and Transparency, available at http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf, last accessed on June 23, 2021

[40] Burton-Harris V. & Mayor P. (2020) *Wrongfully arrested because face recognition can't tell black people apart*, ACLU, available at https://www.aclu.org/news/privacy-technology/wrongfully-arrested-because-face-recognition-cant-tell-black-people-apart/, last accessed on August 1, 2021.

[41] Bokil, A., *et al.* (2021) *Settled habits, new tricks: Casteist policing meets big tech in India*, TNI Longreads, available at https://longreads.tni.org/stateofpower/settled-habits-new-tricks-casteist-policing-meets-big-tech-in-india, last accessed on August 1, 2021. See also Marda & Narayan, *supra* n. 35.

One of the most prominent concerns around algorithmic decision making, and predictive tools, is how the underlying machine learning algorithms are inexorably opaque. These algorithms are trained to evolve the logic of arriving at an answer "on their own" by observing patterns in a large number of datasets.[42] As such, it is not always possible to explain even for the developer(s) of such algorithms to completely break down why an ML algorithm arrived at a particular output. ML algorithms tend to get opaquer as their predictive power increases.[43] There is some degree of opacity in the use of AI in law enforcement due to IP laws as well.[44] In the past, for instance, IBM refused to reveal the kind of data it has used for its facial recognition software, citing its own intellectual property rights.[45] This opacity has important implications for the transparency of decision-making that uses ML algorithms.

Box 2: Right to Explanation - Lessons from the GDPR

Even if the exact logic of how a decision was made cannot be explained, a minimum right to explainability of the contours of an algorithmic process can be enshrined in law. For example, the EU's GDPR includes such a "right to explanation" to "meaningful information about the logic involved" in algorithmic decision-making, in Recital 71. While this has been debated as a non-binding stipulation within the regulations, it presents the idea of affording a general legal right to any individual who may be subjected to algorithmic decision making, to have a clear understanding of such decisions and their outcomes. The objective is seemingly to improve transparency of algorithmic decision-making processes, for the common data subject. Enforcing similar standard of explainable AFRT could be one way to mitigate the algorithms' "black-box" problem.

With respect to the lack of design transparency, a more common idea being advocated by AI ethicists and researchers, is to ensure "human-in-the-loop".[46] This basically requires that a human be present in the decision-making loop for sensitive decisions involving algorithms; or that a certain process be following while developing and deploying an algorithm; or that algorithmic audits be carried out to ensure there is no error or discrimination. Facial recognition systems in law enforcement deal with sensitive issues of people's freedom. They should be subjected to certain standards of transparency and accountability. However, it must be pointed

[42] Husain, *supra* n. 3.

[43] Carabantes, M. (2019) *Black-box artificial intelligence: an epistemological and critical analysis*, AI & Society, DOI:10.1007/s00146-019-00888-w

[44] Chandak, *supra* n. 14.

[45] Solon O. (2019) *Facial recognition's 'dirty little secret': Millions of online photos scraped without consent*, NBC News, available at https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921, last accessed on August 1, 2021.

[46] A detailed discussion on how human-in-the-loop models can foster ethical AI, can be found in Guszcza J., *et al.* (2020) *Human values in the loop: Design principles for ethical AI*, Deloitte Insights, (especially the section on autonomy) available at https://www2.deloitte.com/content/dam/insights/us/articles/6452_human-values-in-the-loop/DI_DR26-Human-values-in-the-loop.pdf, last accessed on August 1, 2021.

out that this human interaction with AFRTs *per se* poses additional challenges, including automation biases and machine influenced decision making.

In addition to the lack of design transparency, specific to the ongoing integration of AFRT in different state police forces, there is an inherent lack of *administrative transparency and accountability* measures should something go wrong. In fact, the lack of public information is so disconcerting that the National Crime Records Bureau was served a legal notice in 2019/20 for furnishing more details than what were presented on its website.[47] Even for our own empirical research, we intended to investigate the use of AFRTs by four police forces namely Hyderabad, Delhi, Mumbai, and Punjab. One manifestation of the lack of publicly available information is the fact that we had to opt for these four police forces based on reportage in local and national media on their use of AFRTs for different police operations. We filed RTI applications (Annexure I) with these different departments, as part of our data gathering exercise for this project, during the months of November 2020 till March 2021. However, predictably, we received sparing information from three of the four states we tried to investigate. Simply put, questions around who is determining the use of AFRT by state police forces were left unanswered. When we inquired about official notifications, memos, or minutes of meetings to shed more light on internal deliberations on the use of AFRT, the most common response was that such documents do not exist. Some sample responses to our RTI applications are collectively appended to this paper as **Annexure-2**.

Box 3: Lack of administrative transparency

While design transparency and the black-box phenomenon is problematic in unraveling the functionality of AFRTs, lack of transparency in administrative processes, breeds arbitrariness in the use of these technologies by law enforcement. The absence of how states are deciding when to rely on these technologies effectively grants *carte blanche* to state police and law enforcement agencies, to deploy these tools without any scrutiny or oversight. For a democratic society, operating within the bounds of the rule of law, such unbridled and opaque *modus operandi* around AFRTs is a definite red flag.

To improve overall state accountability regarding the application of AFRTs in law enforcement, it is imperative that legislative mandates be put in place to address this vacuum. In other countries in the EU,[48] as well as some states in the US,[49] legislation has been enacted to either ban, put a moratorium on, or regulate the use of AFRTs in law enforcement. In India, however,

[47] Internet Freedom Foundation, *supra* n. 36.

[48] Jain A. (2021) *Facial recognition laws in Europe*, Project Panoptic, available online at https://panoptic.in/case-study/facial-recognition-laws-in-europe, last accessed on August 1, 2021.

[49] Jain A. (2021) *Facial recognition laws in the US*, Project Panoptic, available at https://panoptic.in/case-study/facial-recognition-laws-in-the-united-states, last accessed on August 1, 2021.

there is no legislative framework overseeing the implementation of AFRTs in law enforcement. As per a recent report, the NCRB has recorded a 2009 cabinet note as its primary source of legal mandate to call for bids for a nationwide facial recognition system.[50] However, this document is no substitute for legislative mandate, and more importantly, there is presumably no discussion of accountability measures prescribed therein. It is necessary to reiterate that parts of this argument are speculative, precisely because of the lack of transparency in this process.

The duality of this problem of lack of transparency is indeed of grave concern. From a purely legal standpoint, there is an overarching question of whether the use of AFRTs is even legally permissible, given the legal vacuum around it. Secondly, from an accountability perspective, it is impossible to impute liability against a particular state or private actor, which arguably sets up this entire mechanism of AFRTs in law enforcement as a patently arbitrary exercise of executive power. Therefore, these transparency and accountability issues certainly contravene the notions of ethical and responsible use of AI, as has been purported in the NITI Aayog's document.

b. Technical inaccuracies afflicting AFRTs

At present, the two dominant uses of AFRTs are *verification* (1:1 matching, where the software checks whether a face is the same as a certain face stored in its database, such as the technology used for unlocking a phone) and *identification* (1:many search, where the software checks whether a face matches any of the several faces stored in a database, such as the technology used to identify a suspect from a feed of passengers). In general, verification AFRT tends to be more accurate than identification AFRT.[51] One reason for this is the action of verifying involves a more precise and limited comparison with datasets, whereas for identification an algorithm essentially analyses the entire universe of a data corpus, thus, expanding the probability for errors.

It should be mentioned here that accuracy in AI which rely on current techniques of *machine learning*, or even *deep learning*, are only as accurate as the data corpuses which are used to train the underlying algorithm. In the case of AFRTs, it has been suspected for a while if their accuracy would falter if the image in question involved a darker complexion, or non-white, non-caucasian features.[52] This hypothesis was empirically corroborated in a 2018 seminal study conducted by two researchers at MIT, who demonstrated that three of the most prominent AFRT algorithms were statistically more likely to be inaccurate for racial minorities, especially those

[50] NCRB (2019) *NCRB's response on the legal notice*, IFF, available at https://drive.google.com/file/d/0B3J0iAyRzCGxRXViUWcya3RXS0hXb3cxeDJYQU5DWnZKZnhj/view?resourcekey=0-DY2SxktJLnw9EkC8rZsQ9A, last accessed on August 1, 2021, at pg. 1.

[51] Castelvecchi D. (2020) *Is facial recognition too biased to be let loose?*, Nature, available at https://www.nature.com/articles/d41586-020-03186-4, last accessed on August 1, 2021.

[52] Lohr S. (2018), *Facial recognition is accurate, if you're a white guy*, The New York Times, February 9, 2018, available at https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html, last accessed on August 1, 2021.

with darker skin tones.[53] One of the principal reasons attributed to these inaccurate outcomes was the idea that training datasets used for these algorithms were predominantly of white males.

In the Indian context, not only would non-Indian algorithms be susceptible to producing inaccurate results, but given the sheer diversity of the Indian population, it is likely even domestic AFRT might have challenges in accuracy if the training dataset was flawed or inadequate.[54] The potential for inaccuracy implies that police departments, in the interests of transparency, ought to be forthcoming about the inherent algorithmic accuracy, external conditions, and the accuracy threshold or confidence level chosen while using AFRT.

In addition to these data biases or limitations, there are also design limitations which can affect accuracy of AFRT predictions. For instance, more such algorithms are typically trained on high definition or sharp clarity images. However, in actual deployment, the clarity of the images, consistent lighting and positions, recency of identification pictures, and placement of cameras, can vitiate the image feed which is to be used for identification or verification.[55] There are variations in accuracy among different algorithms as well. Under the upper-bound of accuracy provided by the algorithm and external conditions, AFRT users can also adjust the level of accuracy desired from the technology, depending on their tolerance for false positives. A higher accuracy threshold would mean that some correct matches are rejected and a lower accuracy threshold would mean that more incorrect matches are accepted.[56] The US National Institute of Standards and Technology measures the accuracy of facial recognition software globally and has reported a sharp increase in accuracy since 2018, but significantly, large technology companies like Amazon, Facebook, Apple and Google have not participated in this measurement.[57]

Inaccuracy does not necessarily reduce surveillance concerns. On the contrary, the use of inaccurate AFRT in law enforcement systems can mean that innocent people pay the price for false positives that the technology throws up.[58] Inaccuracies in AFRT have been so significant that many companies have chosen to, or been pressured by their workers to, roll back the development and sale of AFRT.[59] In the Indian context, where there is a clear legislative vacuum

---

[53] Buolamwini & Gebru, *supra* n. 39.

[54] Parsheera, *supra* n. 29.

[55] Castelvecchi, *supra* n. 51.

[56] Crumpler W. (2020) *How Accurate Are Facial Recognition Systems - and Why Does It Matter?*, Center for Strategic and International Studies, available at https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter, last accessed on August 2, 2021.

[57] Castelvecchi, *supra* n. 51.

[58] Marda V. (2018) *Artificial Intelligence Policy in India: A Framework for Engaging the Limits of Data-Driven Decision-Making*, Philosophical Transactions, available at https://royalsocietypublishing.org/doi/pdf/10.1098/rsta.2018.0087, last accessed on August 2, 201.

[59] Vedavalli P., *et al.* (2021) *Facial recognition technology in law enforcement in India: Concerns and solutions*, Data Governance Network Working Paper 16, available at https://www.idfcinstitute.org/site/assets/files/16530/facial_recognition_technology_in_law_enforcement_in_india.pdf, last accessed on August 2, 2021.

and oversight, the problems posed by inaccurate predictions could be catastrophic, not only potentially resulting in false arrests or criminal prosecutions, but also leaving little to no recourse in terms of any form of restitution for such wrongly detained individuals.

c. Discriminatory treatment against vulnerable populations

Given that AFRT is largely contingent on the robustness of data corpuses created for training the underlying algorithm, there are implications of biases or discriminatory treatment being meted out to a specific section(s) of the population. Like other machine learning algorithms, FRT is often developed with the use of "training" datasets that help the algorithm learn how to discern between faces. If the training dataset contains a bias, i.e., if it underrepresents a certain type of face, the algorithm will be less accurate at recognising or classifying that type of face. It has been demonstrated that some FRT systems have higher levels of inaccuracy when trying to identify people of colour, young people, and women. The aforementioned study of three private sector AFRT algorithms by Buolamwini and Gebru, clearly establishes the high likelihood of such technologies to misclassify darker-skinned females, and least likely to misclassify lighter-skinned males.[60]

Literature on AFRT from India has pointed out that such technology can similarly perpetuate existing social biases in India, related to not only skin colour or gender, but also to caste and religion.[61] Two Indian researchers, Marda and Narayan, provide an ethnographic analysis of predictive policing in Delhi (not including FRT) and find that the technological systems used by the police have three kinds of bias: historical bias towards poor and vulnerable sections, representation bias in data like call data due to the under-use of policing services by marginalised people, and measurement bias due to the difficulty in mapping temporary settlements.[62] Additionally, there is also a paradox of inclusion: having a data footprint is a sign of privilege, but inclusion in an AFRT database increases the risk of profiling and surveillance.[63] The ideal policy response to bias in FRT should then not be one of inclusive datasets, but to examine the very basis of using FRT in policing.

The adding of algorithmic predictions can further exacerbate this human bias by furnishing a potential tool that may be interpreted or utilised to confirm existing predispositions. While AFRT will not include the same biases because the underlying data and uses of the technology are different, it is helpful to broadly examine how historical, representation and measurement bias manifest in AFRT. As policing can be a discriminatory activity in itself, the use of AFRT has the

---

[60] Buolamwini & Gebru, *supra* n. 39.

[61] Sylvester P. & Saini K. (2019) *'India is falling down the facial recognition rabbit hole*, The Centre for Internet & Society, available at https://cis-india.org/internet-governance/blog/india-is-falling-down-the-facial-recognition-rabbit-hole, last accessed on August 2, 2021.

[62] Marda & Narayan, *supra* n. 35.

[63] Marda, *supra* n. 58.

potential to exacerbate discrimination. This issue is something that we will be examining in a more nuanced manner, supported by empirical evidence, in our second paper of this series.

III. Evidentiary Value of AFRTs in Indian Law

The final element that we intend to discuss in this paper is the role AFRTs can play in gathering evidence for a criminal prosecution. The fundamental objective of the use of this technology is to aid in surveillance by locating or identifying potential suspects - however, once this has been accomplished, can the predictions be produced in a court of law to prosecute said accused? These are questions which remain fairly open-ended and unexplored in the Indian context. In fact, having undertaken our desk review of published and grey literature on the subject, we were unable to find any discussion of this pure question of evidence law. Nonetheless, being a primer document, it is imperative for this paper to present some of the fundamental challenges that will inevitably confront the use of AFRT as an evidentiary tool under the existing legal framework.

In 2000, the Indian Evidence Act, 1872 (Evidence Act), was amended to make it more contemporaneous with the rapidly evolving use of information technology in everyday life.[64] Two new provisions, sections 65A and 65B, were added to part V of the Evidence Act which discusses admissibility of electronic records. These provisions have since become pivotal in a slew of criminal law jurisprudence to determine where courts may rely on electronic databases, recordings, emails, etc. to further corroborate other evidence. In some cases, courts have also recognised electronic evidence as the dominant form of evidence which asserts the guilt of an accused.[65]

What has become indisputable is that electronic records, as long as they satisfy the conditions of Section 65B, will be deemed admissible in a court of law. However, the exposition of “electronic records" in Section 65B (1) is limited to construing electronic evidence as a proxy of physical documents to establish a fact. This provision, in its existing statement, arguably fails to cover AFRT, which is essentially a form of algorithmic prediction or decision-making process. More importantly, an algorithm is not merely documentation or record keeping in an electronic format; these are sophisticated and intelligent data processing technologies which improve and “learn” through usage. Such a dynamic technology is certainly not featuring within the concept of ‘electronic records’ under sections 65A and 65B. Furthermore, the current provisions are solely discussing the admissibility of electronic records, but do not cover the more fundamental issues about the accuracy or potential biases in the use of AFRT. As has been noted in several

[64] *Tomaso Bruno v. State of U.P.* (2015) 7 SCC 178; *Jisal Rasak vs The State Of Kerala* Crl.MC.No.4148 OF 2019(G) (Kerala HC).
[65] *Md.Ajmal Md.Amir Kasab vs State Of Maharashtra* (2012) 9 SCC 1.

judgments, the susceptibility of electronic evidence to potential tampering, is seen as a good ground to allow it as corroborative evidence, rather than the only piece of evidence.[66]

Box 4: Definitional lacunae in the Indian Evidence Act

Sections 65A and 65B only permit "electronic records" as evidence. The provisions were enacted to allow phone recordings, emails, and other means of electronic recordkeeping to be brought on the same pedestal as their physical counterparts. However, AFRT is a whole different ball game. It is a sophisticated, predictive algorithm that is significantly quite different from the aforementioned conventional electronic records. Therefore, at present, the Indian Evidence Act has a significant vacuum in terms of defining "predictive algorithms", and assigning them a clear evidentiary value, as has been done for electronic records.

The previous section particularly highlights the design and data flaws that typically affect most forms of AFRT algorithms. This being the case, its utility as evidence is certainly vitiated, and needs legislative mandate governing its usage preconditions. Specifically, the Evidence Act and the Criminal Procedure Code, 1973, must be suitably amended to incorporate and govern the use of AFRT and other predictive technologies.

[66] *Tukaram S. Dighole V. Maikrao Shivaji Kokate* CIVIL APPEAL NO.2928 OF 2008; see also, *Rasak*, *supra* n. 64.

Concluding Remarks

The debates surrounding the use of AFRTs in law enforcement, are both complex, and yet, as manifested in India, hardly being deliberated over. The biggest concern of Indian law enforcement's increasing affinity with this technology is not the risks it poses, but the fact that many in the citizenry are either unaware or lacking adequate knowledge to assess the risks for themselves and engage with the debate. Add to that how the technology is touted as sophisticated and efficient despite its actual risks. In fact, while AFRTs have been putatively deemed as efficient and better technologies for policing and law enforcement, there are no real data driven studies or research which demonstrates this improvement. Most of it is apparently anecdotal, and arguably at the risk of underplaying the risks involved in it.

The idea of responsible and ethical AI is intertwined with establishing infrastructure of trust; trust in turn, requires transparency and accountability, both of which are currently missing from the rampant efforts of integrating AFRTs in Indian policing and surveillance. There is of course the democratic argument that such large scale public policy interventions should be undertaken with much better public and stakeholder engagement. Furthermore, there is also the need to set out regulatory oversight and adequate checks and balances to ensure such activities of state sanctioned mass surveillance are not performed arbitrarily, at the discretion of the Executive alone.

This paper, by delving into the different ethical risks and legal challenges posed by AFRT's use in law enforcement, has sought to provide an accessible and comprehensible document to promote greater deliberations. There are unquestionably legislative, regulatory and overall governance loopholes that need to be addressed - however, while the policymaking goes on, the citizenry must recognise the apparatus that is being deployed by the state. Larger questions of whether such technologies need to be outrightly banned, temporarily suspended or effectively regulated, must be addressed through greater engagement with the people who are likely to be on the receiving end of such interventions. These must be balanced with the ideas of modernising and improving efficacy (not merely efficiency) of policing systems and practices. The use of AFRTs must be objectively studied and evaluated by policymakers and other stakeholders contributing to the policy process, to determine its actual merit in contributing towards efficacious, due-process oriented, policing. Furthermore, being one of the seminal and more contentious uses of AI in a public facing sector, the use must adhere to ethical principles established for India's responsible use of AI, both in letter and in spirit.