Facing up to the Risks of Automated Facial-Recognition Technologies in Indian Law Enforcement

Ameen Jauhar[*]

> "In addition to the admitted lack of precision of the technology, I find it difficult to see how the deployment of a technology that would potentially allow the identification of each single participant in a peaceful demonstration could possibly pass the test of necessity and proportionality."
>
> Joseph Cannataci, UN Special Rapporteur on Privacy

I. Prefatory Remarks

As the world increasingly witnesses numerous dystopian themes transform into reality, the risks posed by emerging technologies driven by *deep learning algorithms* and *artificial intelligence* ('AI') are arguably a prominent theme featuring in many of these conversations. There has been a spate of recent controversies where tech moguls like Facebook, Amazon, Apple, Alphabet,

[*] The author is a Senior Resident Fellow at the Vidhi Centre for Legal Policy, currently heading its Centre for Applied Law & Technology Research, and working on judicial reforms with the JALDI mission. The author would like to acknowledge the tremendous research assistance provided by Mr. Devansh Kaushik (National Law School of India University). The author also thanks Mr. Sebastien Krier (AI policy and ethics adviser) and Mr. Jonas Schuett (Legal Priorities Project), for their valuable inputs on the earlier drafts of this paper.

and Microsoft (infamously christened as the 'Frightful Five')[1] have been at the forefront. These have ranged from illegal data mining to covert development of technology that may evade the necessary regulatory and legal checks and balances in place.[2] These instances certainly warrant the question of how far humanity is prepared to deal with the fallout of deploying these emerging technologies ubiquitously. The answer to that question, for now, appears to be that our regulatory efforts are work in progress at best, and entirely inadequate at worst.

Within the larger discourse of risk mitigation of emerging technologies, the ever-expanding deployment of *automated facial recognition technology* ('AFRT') is garnering much skepticism amongst privacy advocates, and researchers and academics working on the intersection of law and technology. It is designed and trained on large corpuses of digital images of millions of humans, curated through CCTVs, media, social media, and other sources. Basic facial recognition tools use key features of the face and their respective distances from one another to morph a virtual facial map (something akin to sketches made by sketch artists in police stations).[3] The virtual facial map is then referenced to millions of digital images in databases to assess familiarity. However, AFRT is a more refined tool, allowing automatic referencing to occur from (say) CCTV footages that are being recorded in real time. This is what makes it more promising in preventing crime, since there is capacity for identifying a potential 'preparator' in real time, based on the large troves of digital images such technologies are trained on and have access to.[4] Given the sophistication and time efficiency of AFRT in *facial profiling*,[5] it is most commonly being utilised by law enforcement officials across the globe.

The frequently touted benefit of AFRT in law enforcement is its accuracy in discerning unique features, facial tics, potential disguises, and other facets

---

1 Farhaad Manjoo, 'Tech's Frightful Five: They've Got Us' (*The New York Times*, 10 May 2017) <> accessed 2 August 2020.

2 Paul Nemitz, 'Constitutional Democracy and Technology in the Age of AI' *International Review of Law, Computers & Technology* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3234336> accessed 30 April 2020 (forthcoming).

3 Nila Bala and Caleb Watney, 'What are the Proper Limits on Police Use of Facial Recognition?' (*Brookings Institution*, 2019) <> accessed 30 April 2020.

4 Christopher Rigano, 'Using Artificial Intelligence to Address Criminal Justice Needs' (*National Institute of Justice (US DoJ)*, 2018) <https://nij.ojp.gov/topics/articles/using-artificial-intelligence-address-criminal-justice-needs#sidebar-the-national> accessed April 30, 2020

5 Monique Mann and Marcus Smith, 'Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight' (2017) 40(1) *University of New South Wales Law Journal* 121.

of a human face.[6] Furthermore, unlike conventional security checks, AFRT allows the ability to simultaneously screen numerous individuals from a safe distance.[7] On the other hand, as aforementioned, its inaccurate results, and the dire impact it can cause on individual liberties and informational privacy, are massive risks that have generated a vocal debate against its rampant adoption.[8] In India too, there has been a reported rise of states and law enforcement officials enthusiastically resorting to the use of AFRT.[9] In fact, AFRT has become a pivotal cornerstone in the larger scheme of *predictive policing* in India. A recent empirical study, conducted by two Indian researchers on such practices in Delhi, reiterated the aforementioned risks that have regularly featured in Western literature.[10] Problems of bias, arbitrariness, opacity, and discrimination are hard-coded into the law enforcement officials' unbridled use of such technologies.[11]

In this background, this paper seeks to serve as a primer on the use of AFRT by law enforcement officials. It will initiate readers into some key discussions on the risks posed by AFRT and some proposals for their regulation (within the Indian context) through a doctrinal analysis of existing scholarship. It is pertinent to acknowledge how vast each theme touched upon in this paper is, encompassing an expanding and nuanced discourse. However, by aiming to be adequately referenced, this paper should provide a layperson with enough sources to garner a more meticulous understanding of these numerous debates.

---

6 ibid. See also Andy Adler and Michael E. Schuckers, 'Comparing Human and Automatic Face Recognition Performance' (2007) 37(5) *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)* 1248 <> accessed 20 May 2020.

7 Mann and Smith (n 6); Rigano (n 5).

8 Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research <> accessed 30 April 2020. See also Larry Hardesty, 'Study finds Gender and Skin-type Bias in Commercial Artificial-Intelligence Systems' (*MIT News Office*, 11 February 2018) <> accessed 30 April 2020; Arindrajit Basu and Siddharth Sonkar, 'Automated Facial Recognition Systems and the Mosaic Theory of Privacy: The Way Forward' (*The Centre for Internet and Society*, 2 February 2020) <https://cis-india.org/internet-governance/automated-facial-recognition-systems-and-the-mosaic-theory-of-privacy-the-way-forward> accessed 20 May 2020.

9 Smriti Parsheera, 'Adoption and Regulation of Facial Recognition Technologies in India: Why and Why Not?' (2019) Data Governance Network Working Paper 5 <tps://papers.ssrn.com/sol3/papers.cfm?abstract_id=3525324> accessed 2 August 2020. See also Vasudevan Sridharan, 'India Setting up World's Biggest Facial Recognition System' (*Deutsche Welle*, 7 November 2019) <-up-worlds-biggest-facial-recognition-system/a-51147243> accessed 20 April 2020.

10 Vidushi Marda and Shivangi Narayan, 'Data in New Delhi's Predictive Policing System' (2020) Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency 317 <DOI:10.1145/3351095.3372865>.

11 ibid 321-323.

The author will first delve into some of the controversial risks associated with AFRT, analysing them through the lens of Article 21 and the principle of *due process* under the Indian Constitution. The paper will then identify some of the regulatory solutions that are currently part of the discourse on minimising risks of AFRT and balancing their use with constitutional values, and fundamental and human rights. In particular, this discourse will examine an arguable temporary moratorium on AFRT, or alternatively, imposing statutory limitations on their prevalent use. For this, the paper will delve deeper into the governance and regulatory frameworks being deliberated and designed in the United States ('US') and the European Union ('EU'), which are two jurisdictions putatively leading this discourse. The final segment of this paper will propose a way-forward strategy for India, drawing from the international discourse.

II. AFRT and the Perils of Intelligent Surveillance – A Discursive Overview

While surveillance and intelligence gathering has been an inherent part of law enforcement, it has always required checks and balances in modern democracies, to fulfill the promise of individual freedoms and liberties unimpededly. Maintaining this balance has always been precarious – as states resort to increasingly sophisticated, surreptitious and technologically-enhanced methods for conducting surveillance, the law has largely played the unfortunate role of catching up with these trends of modernization.[12] AFRTs are perhaps the most discreet and arguably dangerous of these technologies. They present a high risk, high reward scenario (i.e. large-scale, cost-efficient surveillance *vis-à-vis* furthering the growth of a 'police state'), which as research and experience shows, has many takers in the conventional law enforcement establishments.

The main threats of AFRT's growing usage by the police and state apparatuses are three-fold. *First*, there are legitimate concerns about the accuracy of such tools, which *inter alia* demonstrate biases against certain vulnerable populations (including racial minorities and women).[13] *Second*, despite these evident inaccuracies, the fact that these tools are becoming an integral part of law enforcement, resulting in the potential indictment and incarceration

---

[12] Christopher S. Milligan, 'Facial Recognition Technology, Video Surveillance, and Privacy' (1999) 9 Southern California Interdisciplinary Law Journal 295, 297-298.

[13] Buolamwini and Gebru (n 9).

of an individual, raises concerns about violation of due process.[14] To make matters worse, there is a significant *automation bias* which is at play in the deployment of such technologies.[15] Automation bias creates a false 'trust' in algorithmic decision-making tools and processes. It stems from the lay-person notion that machine learning and sophistication of algorithms will always improve the quality of human decision-making, eventually resulting in a blind and uncritical favouring of any algorithmic decisions.[16] *Third*, in the absence of a robust data protection and privacy guaranteeing legal framework, AFRT-driven surveillance risks undermining civil liberties, and instead imposing the trappings of a 'police state' which is antithetical to the tenets of constitutional democracies. As aforementioned, this paper aims to delve deeper into how an unregulated, unbridled adoption of AFRT by law enforcement agencies in India can vitiate due process. Hence, the author will be limiting the discussion to the first two issues, as the implications of AFRTs on civil liberties are not germane to that discussion.

A. Questionable Accuracy and the Threat of Criminal Sanction

The accuracy of AFRT has been the central contention in most discourses. One of the seminal instances for this debate was when a group of researchers from MIT and Stanford University undertook a pioneering exercise to evaluate Amazon's *facial recognition tool* called Rekognition.[17] This research paper demonstrated how facial recognition algorithms, despite their inherent design sophistication, were still significantly inaccurate in their results. The problem was compounded by the fact that the error rate was significantly higher when women with a darker skin-tone were the subject of *facial profiling*.[18] Furthermore, since this technology was being deployed by law enforcement agencies in different states in the US, the conversation adopted a strong undertone of racial inequality and the vulnerability of African-Americans

[14] Abhinav Chandrachud, 'Due Process' in Sujit Choudhry, Madhav Khosla and Pratap Bhanu Mehta (eds), *The Oxford Handbook of the Indian Constitution* (OUP 2010).

[15] Mary Cummings, 'Automation Bias in Intelligent Time Critical Decision Support Systems' (2004) Collection of Technical Papers - AIAA 1st Intelligent Systems Technical Conference 2 <DOI: 10.2514/6.2004-6313>.

[16] ibid. See also Solon Barocas, Moritz Hardt and Arvind Narayanan, *Fairness in Machine Learning: Limitations and Opportunities* (2020) <s://fairmlbook.org/> accessed 2 August 2020 (Incomplete working draft).

[17] Buolamwini and Gebru (n 9).

[18] The research showed that Amazon's Rekognition tool was misidentifying darker-skinned women as men 31% of the times; lighter-skinned women were incorrectly identified 7% of the times, and darker-skinned men had an error rate of 1%. See Hardesty (n 9).

particularly from the use of such technologies.[19] Similar problems have also featured in other countries. For instance, there have been a rising number of protests against the London Metropolitan Police's use of AFRT.[20] In fact, this tool too has been criticised of severe inaccuracies in its results, in some cases, "*getting it wrong 81% of the time*".[21]

These results clearly puncture some erroneous notions lying at the heart of inducting AFRT and similar modern tech interventions into the criminal justice system. The first assumption is that such technologies will bolster human efficacy in monitoring and surveillance, to preemptively detect criminals and improve the overall law and security situation within a community.[22] The second assumption is about the speed and accuracy with which such technology conducts such crime detection, justifying its rapidly burgeoning adoption across the world.[23] However, given the high rate of errors in identifying individuals, the use of these machines poses serious risks and undermines their viability. It is pertinent here to reference how even the most impressive accuracy numbers in AFRT have usually been registered close to 70 to 80%.[24] In purely numerical values, this would translate into misidentifying two lakh to three lakh people for every one million people, even with the most accurate AFRTs. The implications of such large discrepancies are far-reaching, which are discussed hereinafter.

Despite its inaccuracies, AFRT is being used ubiquitously by law enforcement officials across the globe.[25] In India too, numerous state police forces have already started using different types of AFRT within their surveillance and monitoring functions.[26] This means that AFRT can become a decisive

---

[19] Natasha Singer, 'Amazon is Pushing Facial Recognition Technology that a Study says could be Biased' *(The New York Times*, 24 January 2019) <ps://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html> accessed 24 April 2020.

[20] Adam Satariano, 'Police Use of Facial Recognition is Accepted by British Court' (*The New York Times*, 4 September 2019) <https://www.nytimes.com/2019/09/04/business/facial-recognition-uk-court.html> accessed 20 May 2020.

[21] Charlotte Jee, 'London Police's Face Recognition System Gets it Wrong 81% of the Time' (*MIT Technology Review*, 4 July 2019) <296/london-polices-face-recognition-system-gets-it-wrong-81-of-the-time/> accessed 2 August 2020. See also Vikram Dodd, 'Met Police to Begin Using Live Facial Recognition Cameras in London' (*The Guardian*, 24 January 2020) <an.com/technology/2020/jan/24/met-police-begin-using-live-facial-recognition-cameras> accessed 2 August 2020.

[22] Rigano (n 5).

[23] ibid.

[24] Singer (n 20); Hardesty (n 9).

[25] Pamela Bump, 'Facial Recognition in Law Enforcement – 6 Current Applications' (*Emerj*, 2018) <> accessed 2 June 2020.

[26] These include the police forces of Delhi, Punjab, Andhra Pradesh, Tamil Nadu, and Gujarat, deploying these tools in different cities. See Anand Murali, 'The Big Eye: The Tech is all Ready for Mass Surveillance in India' (*Factor Daily*, 2018) <> accessed 24 July2020.

variable to determine an individual's guilt in a particular situation, resulting in her criminal prosecution and in some cases, arguably endangering such individual's liberty. This threat becomes particularly dangerous and could arguably add a new menace to the larger problem of malicious prosecution, which is well documented in Indian scholarship and jurisprudence.[27]

B. Is Due Process Vitiated?

While the language of Article 21 in the Indian Constitution uses the phrase "*process established by law*", this has been read as inclusive of both *procedural* and *substantive* due process elements, in numerous judgments.[28] Procedural due process mandates the deprivation of *individual life or liberty* only through "*fair, just and reasonable*" legal procedures.[29] It serves as judicial oversight on legislative or executive overreach in implementing arbitrary procedures, even if such procedures are provided through a legislation mandate. On the other hand, substantive due process evaluates even substantive provisions of the law, ensuring that any procedures do not vitiate the substantial legal and constitutional rights guaranteed to the citizens (and non-citizens in some cases).

Axiomatic to the Supreme Court's reading of *procedural* due process is the need for legal processes to prevent arbitrariness and abuse of power. Therefore, under Article 21, no process of law may arbitrarily result in the forfeiture of individual life or liberty. The present unregulated use of AFRT seemingly vitiates this very standard. As Marda and Narayan argue in their seminal empirical study of Delhi's predictive policing system, *arbitrariness* is being hard-coded into these frameworks.[30] This is visible in the inexplicable manner in which datasets for training machine learning tools (including AFRTs) are collated. Furthermore, the entire process operates in blatant opacity on how AFRTs are being deployed, devoid of any public scrutiny of such drastic interventions, and finding considerable exemptions even under the Right to Information Act.[31]

These patently questionable processes in the deployment of AFRTs specifically, and predictive policing in general, indicate our failure in recapitulating our lessons from the past. Indian law enforcement's experiments with modernisation in collection of evidence have a checkered history. The most

---

[27] N.C. Asthana, 'Malicious Prosecution: A Deep Dive into Abuse of Power by Police' (*The Wire*, 2020) <> accessed 30 August 2020.
[28] Chandrachud (n 15).
[29] *Maneka Gandhi v Union of India* (1978) 1 SCC 248.
[30] Marda and Narayan (n 11) 322-323.
[31] ibid. 323.

notorious of these instances was the growing dependence on *narco-analysis* which was used to place an accused into drug-induced stupor to answer questions, akin to a lie-detector test. Narco-testing was initially legitimized, after several judgments accepted its evidentiary value. However, there were numerous contentions raised against it, ranging from violation of the fundamental right against self-incrimination,[32] to how the statements induced through these tests were often unreliable and fictional.[33] These techniques were also considered involuntary, with a dangerous potential of police targeting innocents to expedite investigations, rather than resorting to more conventional but legal methods of interrogation. After numerous challenges, it was in the landmark decision of *Selvi* v. *State of Karnataka*[34] that the apex court held narco-tests and other involuntary mechanisms like brain-mapping techniques and polygraphs to be unconstitutional, unless the accused consented to them.

The problem with the use of AFRT overlaps in some ways with the challenges we confronted with narco-analysis. Like the latter, AFRT is presently unregulated and left to the absolute discretion of states and police forces to deploy them. These are institutions that have an inherent conflict of interest in overlooking (or bending) *due process* norms, to hasten investigative procedures. This bias is precisely the reason why the Constitution places careful checks and balances on the power of the Executive. Add to this the complete secrecy in which these tools are being designed and deployed, which fuels the apprehension of use of excessive force by law enforcement officials.

At present, in the conspicuous vacuum of any governing legislation, regulation, guidelines, or policy statement identifying the circumstances wherein AFRT can deployed, it is being used ubiquitously and arbitrarily. Such an unchecked system, allowing the police to undertake large-scale surveillance of innocent civilians and potential criminals alike, seems to be an overkill for maintaining law and order. Therefore, a warranted question occurs on how the use of AFRT can be regulated to ensure minimal risks and maximise its benefits.

---

[32] Constitution of India, art 20(3).
[33] *Selvi v State of Karnataka* (2010) 7 SCC 263 : AIR 2010 SC 1974.
[34] ibid.

III. Governance of AFRT – Statutory Regulation Versus Usage Moratorium

A growing debate on risk mitigation regarding the use of AFRT has featured prominently in two regions – the US[35] and the EU[36]. While the US has taken a more formal statutory route of regulation and governance of AFRT, the EU published its White Paper on AI, earlier this year, wherein it contemplated a wide-ranging deliberation to determine specific cases where AFRT could be utilized, without undermining human and fundamental rights of the citizens of EU member states.[37]

A. The Regulation of Facial Recognition Tools in the US

The US appears to have a relatively better regulatory framework in place to monitor the use of AFRT by law enforcement agencies. This comprises proposed legislation,[38] government oversight bodies,[39] and independent civil rights groups[40] working as the three pedestals upholding this oversight ecosystem.

As previously highlighted, the potential risks in use of AFRT by law enforcement agencies became a contentious issue after the uncovering of the high error rates in identifying people of colour, especially darker-skinned women, by Amazon's *Rekognition* tool.[41] In fact, there are further concerns

---

[35] Senator Roy Blunt (Chairman Senate RPC), 'Facial Recognition: Potential and Risk' (*Policy Papers Senate RPC*, 2019) <> accessed 28 August 2020.

[36] European Commission, *On Artificial Intelligence – A European Approach to Excellence and Trust* (White Paper, 2020) <ttps://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf> accessed 30 April 2020.

[37] ibid. See also Elena S. Nicolás, 'EU Backtracks on Plans to Ban Facial Recognition' (*EU Observer*, 2020) <euobserver.com/science/147500> accessed 30 April 2020.

[38] Khari Johnson, 'US Senators Propose Facial Recognition Moratorium for Federal Government' (*The Machine*, 12 February 2020) <ecognition-moratorium-for-federal-government/> accessed 24 June 2020.

[39] US Government Accountability Office, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy* (Report to the Ranking Member Subcommittee on Privacy, Technology, and the Law, Committee on the Judiciary, US Senate, 2016) <> accessed 24 June 2020. See also US Government Accountability Office, 'Face Recognition Technology: DOJ and FBI have Taken some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, but Additional Work Remains' (Testimony before the Committee on Oversight and Reform, House of Representatives 2019) <> accessed 24 June 2020.

[40] See e.g., *Carpenter v United States* 198 L Ed 2d 657 : 137 S Ct 2211 : 582 US ___ (2017); *City of Los Angeles v Naranjibhai Patel* 2015 SCC OnLine US SC 7 : 192 L Ed 2d 435 : 135 S Ct 2443 : 576 US ____(2015), *Riley v California* 2014 SCC OnLine US SC 71 : 180 L Ed 2d 285 : 573 US ___ (2014); *United States v Davis* 785 F 3d 498 (11th Cir 2015).

[41] Brief filed on behalf of the ACLU, *Willie Allen Lynch v State of Florida* Florida SC, No SC2019-0298 <https://www.aclu.org/lynch-v-state-amici-brief> accessed 24 June 2020.

about how the use of AFRT in the criminal justice system can further target different segments of the population, who are already arguably unjustly victimized through unfair arrests and police harassment.[42] In this background, two bills were tabled in the last year alone (i.e. 2019) to regulate the use of AFRT in law enforcement processes. The *Facial Recognition Technology Warrant Bill, 2019* ('FRT Bill') was tabled in the US Congress to provide judicial oversight.[43] This Bill mandates and establishes the procedure for securing a warrant to undertake surveillance by deploying AFRT.[44] Furthermore, the FRT Bill also includes a termination clause, ending any ongoing surveillance through AFRT if the petition for a warrant is denied, and imposes a limitation of thirty days on the duration of the surveillance (subject to extension).[45] With respect to reporting and oversight, there are detailed provisions setting out the requirement of governmental disclosures of the use of AFRT by federal agencies, which are to be tabled before the Judiciary Committees of the US Congress, thus, granting legislators the authority to audit and curtail the abuse of AFRT.[46] In quick succession to the FRT Bill, two Democratic legislators also introduced the *Ethical Use of Facial Recognition Bill, 2019* ('EFR Bill'). In contrast to the FRT Bill, this one proposes a complete moratorium on the use of AFRT, until adequate guidelines and regulations are put in place for its governance.[47]

While these legislative efforts are one part of the proposed regulation of AFRT, established government agencies within the US have already expanded their scope of jurisdiction to also monitor the use of AFRT. For instance, the US Government Accountability Office published two reports on how the use of AFRT by the Federal Bureau of Investigation ('FBI') was not concomitant to existing privacy laws and policies, and also questioned the accuracy of this technology.[48]

Lastly, through a gradually rising number of cases, civil rights groups are becoming more involved in independently taking stock of the actual and potential abuse of AFRT in the criminal justice system. Numerous *amici* briefs have been filed by renowned groups like the American Civil Liberties Union ('ACLU'), and even university research centres like Georgetown Law's Centre on Privacy & Technology.[49] These briefs have helped in the evolution

---

[42] Ethical Use of Facial Recognition Act (Bill), § 2.
[43] Facial Recognition Technology Warrant Act (Bill) 2019.
[44] ibid § 3 "Limitations on use of facial recognition technology".
[45] ibid.
[46] ibid., § 4 "Reports on government use of facial recognition technology".
[47] Ethical Use of Facial Recognition Act (Bill), perambulatory text.
[48] US Government Accountability Office (n 40).
[49] Brief filed on behalf of the ACLU (n 42).

of useful jurisprudence to the dangers of AFRT biases and how the same can have real-life ramifications for individuals subjected to them.[50]

The result of this trinitarian set up is the formation of a large ecosystem where decisions regarding the development, deployment, and scaling of AFRT are not limited to a privileged few (as aforementioned in the context of the '*Frightful Five*'). The regulation in such an ecosystem tends to be more bottom-up, instead of the reverse. It is by no means a foolproof set up for regulation, but unquestionably more inclusive and holistic, allowing room for a robust discourse to feed into the policy and law-making processes.

B. Ethically Compliant AI – The EU's Governance Framework for AFRT

The debate on regulation of AI in general, and more focused conversations on AFRT's usage, within the EU, have occurred more recently since the adoption of the *General Data Protection Regulation, 2016* ('GDPR').[51] In this background, the EU has vociferously favoured the idea of ethically-designed AI, resulting in the drafting and adoption of the *European Ethical Charter on the Use of AI in Judicial Systems and their Environment* in December 2018.[52]As per the European Commission for the Efficiency of Justice ('CEPEJ'), the body responsible for drafting this Charter, the EU member states will focus on harnessing the transformative potential of emerging technologies like AI to improve judicial efficiency but in a responsible manner.[53] This would entail compliance with the fundamental rights guaranteed by the European Convention on Human Rights and the GDPR.

Following from this Charter, the EU recently put out its white paper on AI.[54] A draft of this white paper, previously leaked, revealed that the EU was contemplating a three to five year moratorium on the use of AFRT.[55] However, the final text has revealed a less radical approach – instead of

---

[50] ibid 9-11.

[51] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 <europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> accessed 24 June 2020.

[52] Council of Europe, '*European Ethical Charter on the Use of AI in Judicial Systems and their Environment*' (*European Commission for Efficiency of Justice* (*CEPEJ*) 2018) <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c> accessed 20 May 2020.

[53] ibid.

[54] European Commission (n 37).

[55] Elena S. Nicolás, 'EU Keen to set Global Rules on Artificial Intelligence' (*EU Observer*, 21 January 2020) <https://euobserver.com/science/147198> accessed 2 August 2020.

banning its use, the EU will undertake large-scale stakeholder consultations to draft a set of rules and regulations regarding risks, safe use and regulations, and liability for AI fallouts.[56]

It becomes evident from this set of documents that while well-intentioned, the EU is currently straggling behind in developing a regulatory framework for AI in comparison to the US. This could also be attributed to the more rapid advancements that the latter has made in designing and deploying AI-driven technologies (including AFRT), thus, necessitating an urgent formulation of a robust regulatory framework. However, the *prima facie* advantage of the EU model is the stakeholder engagement and debate it is encouraging, making the whole process more democratic. Additionally, given its aforementioned Ethical Charter, the EU is seemingly increasingly committed to establishing the balance necessary for minimising risks and maximising benefits from the use of technologies like AFRT. How effectively it manages to translate its ambitious intent into actuality, and what will be the actual implementation gap between proposed policies and end products, are questions that can currently only be speculated at best.[57]

IV. AFRT in Indian Law Enforcement: Regulatory and Governance Lessons

The deployment of AFRT in India is no longer a theory – multiple state governments[58] and the National Crime Records Bureau ('NCRB') are at different stages of deploying such technologies.[59] In a country like India, with tremendous diversity in physical facial features,[60] and a massive population of 1.3 billion people, the idea of unbridled power of state surveillance is laden with risks. Additionally, the absence of a robust data protection law governing the collection of biometric information, and strict procedural law(s) establishing clarity of circumstances wherein AFRT can be deployed for monitoring and collection of evidence, makes the situation worse.

---

[56] Nicolás, 'EU Backtracks on Plans to Ban Facial Recognition' (n38).

[57] It is pertinent to mention here that there have been numerous criticisms of the EU's lack of concrete steps on regulating AI, particularly its failure to impose 'standards' which are arguably crucial for establishing a safe and ethical AI regime. The EU's promise for regulation is, therefore, not an end in itself; the promise must be effectively fulfilled to ensure trust and confidence in its governance of AI.

[58] Murali (n 27).

[59] Parsheera (n 10).

[60] ibid., 33.

Given the NCRB's proposal to establish the *National Automated Face Recognition System* as a nationwide AFRT platform,[61] it is imperative to press for adequate regulatory measures with great expediency. The discussion from the previous section demonstrates a two-pronged approach to regulation of AFRT. *First*, is a strong legislative framework which will provide a definitive and limited use of such technology; however, in the interregnum, a moratorium on AFRT usage is also propped as a solution. *Secondly*, in the absence of a strong legislative framework, it is left to the courts to enforce the balance between security necessities, and individual liberties and civil rights.

Drawing from these jurisdictions, such measures must address the following key areas.

A. Transparency and Accountability

A key concern surrounding the rampant and discretionary use of AFRT in law enforcement has been about how such actions are nebulously justified for security purposes. For instance, in India, the NCRB's aforementioned proposal for constructing a nationwide facial recognition tool has been shrouded in darkness. There are little to no publicly available details about how such decisions have been arrived upon, or what kind of ministerial processes have been followed to this end. Furthermore, there is also ambiguity about which datasets will be harnessed to train these technologies, and whether their usage will be subject to any independent technical and design audits, as well as impact evaluation exercises. All these elements are vital in building the confidence of the citizenry that will ultimately bear the brunt of these technological interventions. In the absence of such confidence building measures, numerous civil society activists and legal academics have criticised the seeming arbitrariness and haste in deploying AFRT in India.[62] It is necessary to put all relevant details about AFRT in the public domain. While the Right to Information Act, 2005 warrants such information to be readily accessible to any citizen, the clandestine manner in which these technologies are being adopted, leave little room for debate regarding the intent of the policymakers, or the machiavellian uses for AFRT. It is, therefore, imperative for the legislatures to enact laws to enforce transparency and accountability around the use of AFRT in law enforcement in their respective jurisdictions.

---

[61] NCRB, 'Request for Proposal to Procure National Automated Facial Recognition System (AFRS)' (National Crime Records Bureau and Ministry for Home Affairs, Government of India) <> accessed 24 July 2020.

[62] Parsheera (n 10) (and more papers cross cited in it).

B. Proportionality in Adoption and Usage

Both the EU and the US have been debating measures to limit the use for AFRT. Most recently, the city of San Francisco effectuated an ordinance wherein the city's departments must specify 'necessary circumstances' warranting the procurement and use of AFRT .[63] In India, the Supreme Court's *proportionality* test laid down in the *Puttaswamy* judgment[64] governs state interventions which may result in vitiation or violation of an individual's right to privacy. As per this test, such interventions must be established by law, in pursuit of a state interest, and must also prescribe checks and balances to prevent abuse of the state's surveillance powers. However, the current use of AFRT is arguably bereft of at least two of these yardsticks. This must be rectified through a prospective regulatory and statutory framework governing and limiting its use to necessary instances.

C. Stakeholder Engagement

It is also imperative to conduct large-scale engagements with numerous civil society activists, privacy advocates, academics, and members of the legal fraternity, to get a fair sense of the legal, constitutional, and regulatory challenges associated with AFRT. Presently, the deployment of these tools by state police forces, and the proposed all India facial recognition grid have inspired little or no confidence, sparking massive doubts around their actual end use (in furthering a surveillance state), given how these have been top-down decisions. A constitutional democracy like India is established on the idea of bottom-up building of policy interventions. *Suo motu* prescriptions like the AFRT are antithetical to the ideas of a participatory democracy.[65] In this background, any proposed legislation(s) must adhere to the tenets of participatory democracy, empowering and actively engaging its citizenry in the lawmaking and policy making processes.[66]

---

[63] Acquisition of Surveillance Technology, Ordinance No 190110. See also Kieren McCarthy, 'San Francisco Votes No to Facial-recognition Tech for Cops, Govt– while its Denizens Create it' (*The Register*, 14 May 2019) <https://www.theregister.com/2019/05/14/san_francisco_facial_recognition_ban/> accessed 2 August 2020.

[64] *K.S. Puttaswamy v Union of India* (2017) 10 SCC 1.

[65] For a larger discourse on how authoritarian states adopt sophisticated state surveillance methods and technologies, see Hannah Arendt, *The Origins of Totalitarianism* (Meridian Books 1958).

[66] Sherry R. Arnstein, 'A Ladder of Citizen Participation' (1969) 35(4) *Journal of the American Planning Association* 216.

V. Concluding Remarks

The deployment of AI in general, and AFRT specifically, seems to be already in motion in India. What is disconcerting is the hastiness with which these interventions are being scaled across states, disregarding constitutional morality and the fundamental tenets of procedural fairness. All this is being advocated on the tenuous premise of greater efficiency which flounders when one reviews the concerns regarding inaccuracies of AFRT across jurisdictions. Even if one was to assume the effectiveness, such radical and disruptive technologies cannot and should not be utilised in an unregulated and arbitrary manner. It is the need of the hour to accept these risks and find solutions to them – if not, like the popular adage, Indian law enforcement, and the criminal justice system, are doomed to repeat some of their ill-fated history.