VOLUME 1 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

COMPROMISING FACIAL MATRICES – THE SURVEILLANCE CRISIS

- Sadhu Samba Kailash[1]

ABSTRACT

Technological advancements often come at a price of sacrificing sacramental human rights. More often than not significance is provided to the latter than the former, especially when it offers an enticing manner to control and retain power. Judiciary often considered harbinger of fundamental and natural rights, offers mild euphemism and oversight through its pro-active judgments that look far into the future. Yet we see the human suffer whenever law is seen playing catchup with technology. While it struggles to offer proper protection to its Aadhar database, India is considered boldly ambitious in issuing a Request for Proposal for an Automated Facial Recognition System. As questions arise regarding the applicability of laws or approachability to courts if the proposal comes to pass, ignorance cannot be feigned to the states that have turned almost autocratic by exploiting surveillance mechanisms to commit barbaric acts of racial segregation. While we observe big players like Google & Amazon failing to get it right, we also see the small players in India struggle to meet the criteria required for such proposal, yet again increasing the chances of leaving it to a foreign firm to come to the rescue. With doors locked every side, does the Personal Data Protection Bill 2019 show up as a panacea?

INTRODUCTION

The concept of state made proper sense in the state contract theory by John Locke. Where he purports that a group of individuals decide to sacrifice certain liberties of individuals in exchange for the protection granted by the state. Here the scales are starting to tip as India seeks to create a National Automated Facial Recognition Database. Though facial recognition is being

[1] Student of Hidayatullah National Law University, Raipur

offered as a security measure, the bigger question is whether the people are actually willing or comfortable to sacrifice the liberty at the cost of being watched 24/7?

It's like a trace of digital footprint that's left wherever you go and whatever you do. In essence you are always being watched. It's like having a person follow you every single minute. The argument that "if you do nothing wrong then there is no reason to be afraid" fails to apply to this scenario. When seen in a slightly similar perspective it is just as if the invigilator is breathing down your neck as you are writing your paper, it's that discomfort of being watched.

The second reason is that when something is invented, seen not only are its benefits but also its consequences as it falls into the wrong hands. Like the powers of emergency that were designed to make our country adept to changes by transferring the entire control to the Centrewere blatantly misused and have very well shown India what can be called as the darkest era it has experienced post-independence.

A very disturbing parallel can be drawn with the Orwellian state famously known as the Big Brother which watches you constantly 'for your own protection'. Although in the real world often the word is used to refer to Russia, increasingly it is also becoming a common term to China[2] followed closely by India that does not yet have a law to regulate the facial recognition software and its usage.

WHAT BROUGHT THIS INTO LIGHT RECENTLY?

Although this technology hasn't yet been recognized for official usage by the government, certain sectors are already putting it to use. One special case that comes to our notice during these hard times is the incident where the protesters against CAA in Delhi are video graphed by the police and later on run through the unofficial AFRS – Advanced Facial Recognition Software (developed by Innefu Labs) to recognize identified faces[3]. It is similar to an incident in china where a company got an email (best to say a warning) from the government stating that one of his employees is flouting the lockdown rules and was spotted by one of the cameras. Surprisingly he was also wearing a mask, which according to many of us still can stop facial recognition, but it cannot be further from truth[4].

[2] Keegan, M. (2019, December 02). Big Brother is watching: Chinese city with 2.6m cameras is world's most heavily surveilled. Retrieved from https://www.theguardian.com/cities/2019/dec/02/big-brother-is-watching-chinese-city-with-26m-cameras-is-worlds-most-heavily-surveilled

[3] Reuters. (2020, February 18). Delhi, UP Police use facial recognition tech at anti-CAA protests, others may soon catch up. Retrieved from https://www.indiatoday.in/india/story/delhi-up-police-use-facial-recognition-tech-at-anti-caa-protests-others-may-soon-catch-up-1647470-2020-02-18

[4]Knappily. (n.d.). In China, Big Brother is always watching you. Retrieved from https://knappily.com/technology/in-china-big-brother-is-always-watching-you-178

Reason justifies the usage of technology that is normally precepted to be a blatant invasion of privacy. China has used the facial recognition of software to contain people in their own houses and enforce better lockdown. Although it's not the usage that we must be afraid of, rather the potential to be subjected to misuse.

The advantages sure are many using this technology, especially for the law enforcement agencies and in this aspect comes a very fine example of Operation Smile by the state of Telangana that uses facial recognition technology to trace and locate missing children. This has been very successful and has helped the police locate missing children within weeks of being reported as missing.[5]

HOW DOES AFRS WORK?

The AFRS tries to match any given photograph with the existing database to identify individuals and benefit through the information ecosystem that exists on various databases regarding the same individual.[6]

Facial recognition software usually follow a similar pattern of recognition and it becomes extremely important for us to understand its workings as it gives a picture of the deep waters that we are currently headed into.

It follows four steps in brief [7] :

1. Detection: The basic features of a face are detected in any photo or video that includes either a single person or a group
2. Analysis: Each and every feature of the face is captured through a total of 80 nodal points such as the distance between your forehead and chin, the distance between your eyes. Such data is also termed as facial geometry.
3. Generating a signature: Such analysis of data generates a code that turns a face into mere numbers in a mathematical formula. This is called as a facial signature and is as unique as a fingerprint to each and every individual. The advantage of such analysis lies in the fact that even if a face partially changes, it can still be recognized as they measure 80 nodal points some of which cannot be subject to change.

[5] NewIndianXpress. (2020, February 02). Operation Smile: Telangana cops rescue 3,600 kids. Retrieved from https://www.newindianexpress.com/states/telangana/2020/feb/02/operation-smile-telangana-cops-rescue-3600-kids-2097943.html

[6] Banerjee, P. (2020, January 02). Success of facial recognition tech depends on data. Retrieved from https://www.livemint.com/technology/tech-news/success-of-facial-recognition-tech-depends-on-data-11577986675080.html

[7] Symanovich, S. (2020, July 06). How does facial recognition work? Retrieved from https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html

4. Recognition: Such facial signature is then used for comparison against the existing database.

Generally, the said database could range from police mugshots in criminal database to photo ids that have been collected by the government in the form of Drivers License. While this could help in curbing of crimes linked with the CCTV infrastructure all through the major roads and highways, a revised request for proposal stated that AFRS will neither involve installation of CCTV cameras nor will it connect to any existing CCTV camera anywhere. The biggest challenge lies here as our government recently undertook the world's largest biometric identification project i.e., Aadhar.[8] Adding to our concerns such a database has been leaked or subject to hacks multiple times. Hence,it's not only the government that we need to worry about but due to a weak security system the entire population of our country can become a database to any private party around the world.

HOW FAR ARE WE FROM NATIONAL AUTOMATED FACIAL RECOGNITION DATABASE?

A Tender was floated by National Crime Records Bureau run under the Ministry of Human Affairs titled "Open Bids for Automated Facial Recognition System" on 5th July 2019.[9] Quite recently, a revised Request for Proposals has been released which postponed the deadline to submit the bids for the 9th time to 6th August 2020.

Companies state that the qualification criteria is unpalpable i.e., A50 crore rupees turnover and the experience of floating three of such AFRS installations across the world.Also, the firm's algorithm is to be compliant with standards set by NIST USNIST – (US National Institute of Standards and Technology).[10]

Such qualifications and criteria put out most of the Indian players out of the play as a foreign firm is expected to win the national contract. Notable Indian players like Innefu & Staqu said they were not bidding as they lack the qualifications.[11]

---

[8] Financial Express. (2018, March 23). Aadhaar now world's largest biometric database: 5 facts from UIDAI CEO's presentation in Supreme Court you must know. Retrieved from https://www.financialexpress.com/aadhaar-card/aadhaar-now-worlds-largest-biometric-database-5-facts-from-uidai-ceos-presentation-in-supreme-court-you-must-know/1108622/

[9] Sircar, S. (2019, July 09). Govt Planning Facial Recognition System; Raises Privacy Concerns. Retrieved from https://www.thequint.com/news/india/ncrb-automated-facial-recognition-system-ministry-of-home-affairs-data-protection-bill-privacy-pending

[10] Sircar, S. (2019, July 26). Face Recognition Tender Harsh on Indian Bidders: Companies To NCRB. Retrieved from https://www.thequint.com/news/india/ncrb-facial-recognition-system-tender-harsh-on-indian-companies-bidders-say

[11] Reuters. (2020, February 18). Delhi, UP Police use facial recognition tech at anti-CAA protests, others may soon

QUESTIONS OF LEGALITY?

In an RTI reply to the Internet Freedom Foundation, the NCRB justified the project of AFRS using a cabinet note that dates back to 2009(a general record of the meetings proceedings that consist no legal bases whatsoever) where a similar system was being talked about.[12]

Without the Data Protection Bill being passed or any guidelines regarding the usage of facial recognition software, there exists no legal procedure for how to collect, store and use the data, thereby leading to very little legal avenues that are available to the citizen for law enforcement.

It would have been great if India adopted the EU Data Protection Drive which currently has the General Data Protection Regulation, rather the only act that comes to mind is the Information Technology Act 2000. It did not come with any Data Protection Mechanism and hence the amendment of 2008 which inserted S.43A[13] and 72A[14]. While these laws may act as a protection to an extent, The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 make it more interesting. It states certain guidelines regarding data collection that apply only to body corporates and persons located within India. Some important guidelines[15] in brief are:

1. To obtain consent before collection
2. Shall not be collected unless for lawful purpose
3. Awareness regarding the purpose of such collection of data
4. Retain information no longer than required
5. Take such permission from information provider before disclosing such information to a third party[16].

The clarifications issued on this act exclude the application of the above rules if a body

---

catch up. Retrieved from https://www.indiatoday.in/india/story/delhi-up-police-use-facial-recognition-tech-at-anti-caa-protests-others-may-soon-catch-up-1647470-2020-02-18

[12] Agrawal, A. (2019, July 23). IFF calls NCRB's automatic facial recognition system 'unfathomably detrimental to Indians'. Retrieved from https://www.medianama.com/2019/07/223-iff-calls-ncrbs-automatic-facial-recognition-system-unfathomably-detrimental-to-indians/

[13] **Section 43A** of the IT Act explicitly provides that whenever a corporate body possesses or deals with any sensitive personal data or information, and is negligent in maintaining a reasonable security to protect such data or information, which thereby causes wrongful loss or wrongful gain to any person, then such body corporate shall be liable to pay damages to the person(s) so affected.

[14] **Section 72A** provides for the punishment for disclosure of information in breach of lawful contract and any person may be punished with imprisonment for a term not exceeding three years, or with a fine not exceeding up to five lakh rupees, or with both in case disclosure of information is made in breach of lawful contract.

[15] Rule 5, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

[16] Rule 6, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

corporate is under contractual obligation with any legal entity within or outside India is not subject to the above rule. To be more specific, if the current National Facial Recognition Database is adopted and deployed by Indian government, none of these rules come to our rescue. Our only resort might be the broad category of fundamental rights as recognized by the constitution and the quest for right to privacy as recently recognized by the supreme court in the recent Kuppuswamy judgement which states that the same can only be exercised in accordance with the procedure established by law. Currently there exists no procedure for the same as the Information Technology Act is entirely silent on the issue of facial recognition. Moreover, the justification of NCRB being a cabinet note in 2009, it cannot justify its legality as it was approved prior judgment.[17]

PERSONAL DATA PROTECTION BILL, 2019

There is a dire necessity for data protection laws in India irrespective of the oncoming facial recognition database. The Personal Data Protection Bill 2019 has provided a basic framework and also tries to fit in Facial recognition issues. Assurance can be found in the definition of biometric data as adopted by the bill in Clause 3(7) which includes facial images, with Clause 3(34) classifying such biometric data as sensitive personal data. The term sensitive personal data has been offered a higher status of protections and has been distinguished from personal data in many clauses. as has been stated in:

Clause 11: - Obtaining explicit & separate consent in case of every single step of processing sensitive personal data.

Clause 15: - Provides the authority to the government to notify categories of personal data as sensitive personal data.

Clause 33(1): - Provides that sensitive personal data may be transferred outside India subject to clause 34(1) of the said act.

Clause 34(1): - It not only mandates explicit consent from the person to whom such data belongs to but also sets a number of other criteria for allowing such transfer as mentioned in clause 33(1)

CONCLUSION

It impacts you psychologically, to say in simple terms you become conscious of every single

[17] Barik, S. (2019, November 14). 'Automatic Facial Recognition System is made legal by a 2009 cabinet note,' says NCRB. Retrieved from https://www.medianama.com/2019/11/223-ncrb-afrs-legality/

thing you do. We often hear people unable to smile or simply becoming rigid citing camera consciousness as a reason, another instance can be where you carefully monitor yourself when you are told you are on loudspeaker or when you know that the call is being recorded. Courts would become avenues of right enforcement if the said AFRS is enacted without prior legal framework.

Irrespective of the General Data Protection Regulation, the EU was considering a ban on the usage of FRS for up to 5 years.[18] California has banned it as it is considered as a blatant violation of privacy.[19] It is also subject to misidentification of faces similar to what happened with an Facial Recognition Software developed by Google for sorting out photos identified 'two black people as Gorillas'[20].

FRS developed by Amazon known as Recognition was openly marketed to be useful to law enforcement purposes, only to find that it grossly misfired by identifying matches between members of congress and criminal mugshots. If companies with R&D like Google and Amazon are still struggling to ace this technology, it might not really be a good time to start placing reliance on Facial Recognition Technologies as of now yet.[21]

"*Take the most risky application of this technology, and chances are good someone is going to try it. If you make a technology that can classify people by an ethnicity, someone will use it to repress that ethnicity*." said Clare Garvie, an associate at the Center on Privacy and Technology at Georgetown Law.[22]It has been said in the context of racial profiling that was done by China using its surveillance integrated FRS to identify Uighurs (a largely Muslim minority).

Perhaps one of the best approaches that can be adopted towards facial recognition is to inherently presume that it violates the fundamental right of privacy of people, but start considering exceptions to its application as the advancement of technology is something that cannot be denied its place in law and society.

[18] BBC. (2020, January 17). Facial recognition: EU considers ban of up to five years. Retrieved from https://www.bbc.com/news/technology-51148501

[19] Metz, R. (2019, September 13). California lawmakers ban facial-recognition software from police body cams. Retrieved from https://edition.cnn.com/2019/09/12/tech/california-body-cam-facial-recognition-ban/index.html

[20] The Guardian. (2018, January 12). Google's solution to accidental algorithmic racism: Ban gorillas. Retrieved from https://www.theguardian.com/technology/2018/jan/12/google-racism-ban-gorilla-black-people

[21]Sky well, S. (2019, October 29). Top Artificial Intelligence Fails in Image and Facial Recognition. Retrieved from https://medium.com/swlh/top-artificial-intelligence-fails-in-image-and-facial-recognition-dfc1527b2295

[22] Mozur, P. (2019, April 14). One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority. Retrieved from https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html