USE OF FACIAL RECOGNITION TECHNIQUE IN CRIMINAL INVESTIGATIONS IN INDIA

Dr. Renu Pal Sood, Associate Professor, Shoolini University, Solan (Himachal Pradesh)

Modern social relations are characterized by the widespread use of electronic means of information processing. Taking into account the intensive development of computer technologies, they are already demonstrating readiness to perform complex functions involving comprehensive solution to both technical and creative problems. Technologies named "Artificial Intelligence" are currently successfully used in various spheres of human life: from face recognition on a Smartphone screen to creating art and musical works "from scratch". Given these circumstances, in legal science more and more judgments are made about the need to use high-tech means in criminal proceedings, including for determining criminal punishment and other forms of criminal law influence against persons who have committed a socially dangerous act.[1]

At present, there is no official definition of the concept of "artificial intelligence" at the legislative level. In the legal literature, various judgments have been made on this matter. So, in accordance with one of them, the defining difference between artificial intelligence and an ordinary robot is the presence of thinking or lack of it. The concepts of thinking and mental activity are disclosed in paragraphs 3.23 and 3.24 of GOST R 43.0.5-2009. In particular, thinking is the psychophysiological processes of the operator's brain, including those related to internal speech, memory, functional mental sensory states, ensuring implementation of mental activity with initiation of naturally intellectualized, hybrid-intellectualized, artificially intellectualized human-information interactions that affect the emergence and functioning of information and exchange processes, carrying out the corresponding information and intellectual activities. Thus, artificial intelligence should be understood as the direction of information technology, which deals with the study and development of systems (machines), endowed with the capabilities of human intelligence.[2]

What is facial Recognition Technique

Facial recognition technique (FRT) is an algorithm-based technology which creates a digital map of the face by identifying and mapping an individual's facial features, which it then matches against the database to which it has access.

It can be used for two purposes:

(A) Verification of identity

- Here the facial map is obtained for the purpose of matching it against the person's photograph on a database to authenticate their identity. For example, 1:1 verification is used to unlock phones.

- Increasingly it is being used to provide access to any benefits or government schemes.

(B) One-to-many identification

- There is the one-to-many identification of identity wherein the facial map is obtained from a photograph or video and then matched against the entire database to identify the person in the photograph or video.

---

[1] V F Lapshin et al 2020 IOP Conf. Ser.: Mater. Sci. Eng. 1001 012144 available at
https://iopscience.iop.org/article/10.1088/1757-899X/1001/1/012144/pdf
[2] Ibid

- Law enforcement agencies such as the Delhi Police usually procure FRT for 1:n identification.

- It generates a probability or a match score between the suspect who is to be identified and the available database of identified criminals.

- A list of possible matches are generated on the basis of their likelihood to be the correct match with corresponding match scores.

- However, ultimately it is a human analyst who selects the final probable match from the list of matches generated by FRT.

According to Internet Freedom Foundation's Project Panoptic, which tracks the spread of FRT in India, there are at least 124 government authorised FRT projects in the country.[3]

India has seen the rapid deployment of facial recognition technology (FRT) in recent years, both by the Union and State governments, without putting in place any law to regulate their use.

Use of FRT in Criminal Investigations

On the investigative front, FRTs carry potential in terms of their evidentiary value. India's Automatic Facial Recognition System envisages facilitating the investigation of crime and detection of criminals, missing children/persons, unidentified dead bodies and unknown traced children/persons (NCRB, 2020). In 2017, 75 percent of the First Information Reports (FIRs) that were closed without investigation were due to insufficient or untraceable evidence. Quality of investigation, particularly given high vacancies in policing and case pendency, can benefit immensely from the use of technology. Presently, investigations are based mostly on oral testimonies and therefore, if witnesses turn hostile, the cases often cannot be pursued due to insufficient evidence .[4]

Better forensic evidence, along with inputs in the form of visual feeds from CCTVs/FRT, can go a long way in addressing not just the issue of quality of evidence but also pendency. According to the data the Delhi police were able to locate 3,000 missing children using FRTs. [5] In April 2018, news items reported that the trial of a facial recognition system commissioned by the Delhi High Court helped correctly identify approximately 3000 missing children. [6]The Delhi High Court had in Sadhan Haldar v The State NCT of Delhi (2019) issued the use of Automated Facial Recognition System (AFRS) for the purpose of tracking and re-uniting children. The system had matched 10,617 children with missing cases from across the country - however, only 3202 of those children's identities have been verified.[7]

FRTs also have merit in terms of their potential influence on policing processes—specifically custodial ones due to better evidence. Use of force by the police against those in custody is well documented. The main

---

[3]Anushka Jain Gyan Prakash Tripath, Delhi Police's use of facial recognition technology, The Gist, The Hindu, 16 Aug, 2022

[4] Bothra. 2019. Why is our conviction rate so low? Available at: https://www.newindianexpress.com /opinions/2019/feb/21/why-is-our-conviction-rate-so-low-1941680.html

[5] Priya Vedavalli et al, Facial Recognition Technology in Law Enforcement in India: Concerns and Solutions, IDFC Institute Report, April 2021 available at

https://www.idfcinstitute.org/site/assets/files/16530/facial_recognition_technology_in_law_enforcement_in_india.pdf

[6] The Delhi Police is matching the photographs/videos against photographs collected under Section three and four of the Identification of Prisoners Act, 1920. This provision has now been replaced by the Criminal Procedure (Identification) Act, 2022. This Act allows for wider categories of data to be collected from a wider section of people, i.e., "convicts and other persons for the purposes of identification and investigation of criminal matters".

[7] *Supra*, Note no. 3

reason behind the use of 'third-degree' methods in India is the short duration of custody. The police are supposed to bring the suspect in front of the magistrate in under 24 hours which limits the time available for investigation. This is compounded by the fact that confessions made to them do not have evidentiary value, instilling systemic distrust in the police. However, Section 27 of the Indian Evidence Act allows material discovered as a result of a confession admissible in the court. FRT may, subject to acceptance of evidence, play a role addressing the need for quality evidence.

These technologies can also serve as deterrents to crime. The Institute for Economics and Peace estimated the cost of violence in India in 2017 as 9% of its GDP. While we don't have estimates on the direct impact of FRTs on the economic cost of violence, media reports suggest that these technologies have served as crime deterrents and reduced the incidence of crime. For example, in Surat, the city police credit their FRT system with a 27% reduction in crime.[89]

Limitations

The accuracy of the results depends on a number of factors, such as the quality of the photograph uploaded or captured (in the case of live automatic facial recognition technology), use of makeup, quality of the lighting, distance/angle from which the picture was captured. Variations in pose, illumination, and expression, among other factors, adversely impact the accuracy of automated facial analysis.[10]

Though FRT can potentially be a useful tool in assisting with the identification of individuals, it can also be misused depending on who uses the technology, for what purposes, in what configuration, and in the absence of a requisite legal and regulatory framework for governing its use. Poorly designed and trained FRT systems can result in inaccurate, discriminatory, and biased decisions.

- The use of FRT presents two issues:

1. Issues related to misidentification due to inaccuracy of the technology and

2. Issues related to mass surveillance due to misuse of the technology

- Extensive research into the technology has revealed that its accuracy rates fall starkly based on race and gender.

- This can result in a false positive rate, where a person is misidentified as someone else, or a false negative where a person is not verified as themselves.

- Cases of a false positive result can lead to bias against the individual who has been misidentified.

- On the other hand, cases of false negative results can lead to exclusion of the individual from accessing essential schemes. Ex. Failure of biometric based authentication under Aadhaar for and 90 YO person.[11]

At present, India does not have a data protection law or a FRT specific regulation to protect against misuse. In such a legal vacuum, there are no safeguards to ensure that authorities use FRT only for the purposes that

[8] Gershgorn, D., 2020. NEC Is The Most Important Facial Recognition Company You'Ve Never Heard Of. Available at: <https://onezero.medium.com/nec-is-the-most-important-facialrecognition-company-youve-never-heard-of-12381d530510>..
[9] *Supra*, Note no. 5
[10] Aayush Rathi and Ambika Tandon, ―The Digital Identification Parade,‖ The Indian Express (blog), July 29, 2019, available at https://indianexpress.com/article/opinion/columns/digital-identificationfacial-recognition-system-ncrb-5859072/.
[11]Delhi Police's use of Facial Recognition Technology, https://www.civilsdaily.com/news/delhifacial-recognition-technology-frt/

they have been authorised to, as is the case with the Delhi Police.FRT can enable the constant surveillance of an individual resulting in the violation of their fundamental right to privacy.Yet again the nation-security narrative comes into picture which cannot be ignored.It is feared that the Act will lead to overbroad collection of personal data in violation of internationally recognised best practices for the collection and processing of data.This revelation raises multiple concerns as the use of facial recognition can lead to wrongful arrests and mass surveillance resulting in privacy violations (if used for propaganda politics).[12]

Concluding Remarks

The use of facial recognition technology in India by law enforcement and the state is nascent but growing. Based on publicly available information about the use of FRT in India, the following observations can be made:

Need for a legal and regulatory framework Presently there are no legal or regulatory frameworks governing the use of FRT in India and existing legal frameworks for surveillance in India do not clearly extend to the use of FRT technology. In the Puttaswamy judgement (2017),[13] the Supreme Court held the right to privacy to be a fundamental right, and like other fundamental rights, held it to not be an absolute right. The right is subject to reasonable restrictions and the restrictions have to comply with a three fold test; (i) legality; (ii) legitimate state aim; and (iii) proportionality. The existing laws and regulations were formulated for regulating targeted surveillance and not bulk surveillance. When these laws and regulations were formulated, the technology for bulk surveillance was in its nascent stage and the discourse around privacy and surveillance was not as well developed as today.The existing laws governing surveillance in India do not incorporate the necessary privacy principles of purpose limitation, collection limitation, data quality, oversight and accountability and the rights of the persons who are under surveillance. In the absence of a data protection law, it is critical that surveillance laws incorporate these principles. Deployment of FRT is a means of bulk surveillance and it is not clear that it conforms with the principle of proportionality which subsequent to the Puttaswamy judgement has become one of the standards to test restrictions on the right to privacy. Further, as noted earlier, the Home Ministry has in response to a legal notice sent by the Internet Freedom Foundation stated that the basis of the FRT system such as the AFRS is a 2009 cabinet note, however a cabinet note is not a statutory enactment and cannot be used as a legal basis for deploying facial recognition technology. In the Aadhar judgement, the Supreme Court had struck down the use of Aadhar as a means for mandatory verification of SIM cards as there was no legislative backing for the same and held that it was a disproportionate and unreasonable state compulsion. It is also unclear what policies and procedures are being put in place when the technology is adopted at the state and city level. This raises serious concerns with respect to oversight, accountability, redress for the use of FRT and the consistent implementation of safeguards to protect against misuse. Hence, there is a need for a clear regulatory framework that defines the acceptable uses of FRT, the methods involved in its use, and safeguards to protect against the use of FRT for mass surveillance.

---

[12] *Supra*, Note no. 3
[13] Justice K.S Puttaswamy and Anr v. Union of India, AIR 2017 SC 4161