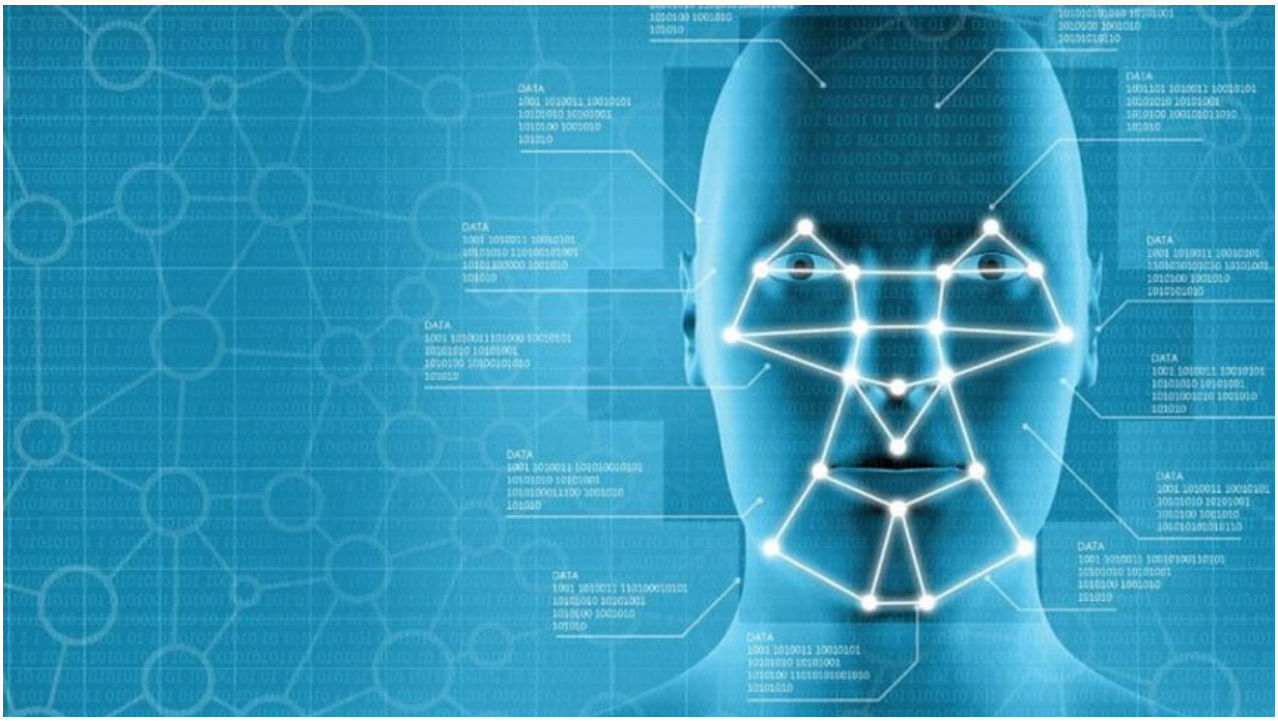
Not the Win We Were Rooting for

moneylife.in/article/automated-facial-recognition-systems-not-the-win-we-were-rooting-for/71164.html

Automated Facial Recognition Systems: Not the Win We Were Rooting for

Raushan Tara Jaswal (The Leaflet) 22 June 2023

0



Public Interest

The database breach of the government's digital platforms highlights the vacuum in legislation to adequately deal with such breaches. In the absence of legislation providing redress, attributing liability and adequate punishment— the fundamental right to privacy in India remains a toothless tiger. The author outlines the key shortcomings of automated facial recognition systems and proposes policy recommendations to address them effectively.

The recent breach of the CoWin database is yet another violation of the right to privacy on government-mandated technological platforms.
It highlights how technology used by the State machinery in India is prone to breaches, and is a timely reminder, if one was indeed needed, of the lack of robust data protection laws.

The growing concern is compounded by the fact that the State is operationalising more and more technology-driven solutions which collect and store sensitive personal data in the form of biometrics; and identification metrics such as phone, Aadhaar card and PAN

card numbers, and age, gender and health data.

An important issue that ought to be a cause of concern is the integration and use of an automated facial recognition system (AFRS) by the Delhi police, or even through the DigiYatra platform, which uses facial recognition technology (FRT) to authenticate and facilitate travel across airports and extends it to railways.
The State machinery in India is prone to breaches, and is a timely reminder, if one was indeed needed, of the lack of robust data protection laws.

What started as a bid to trace missing children in Delhi, is now being used to identify protestors in order to prosecute them under criminal law.
In identifying protestors in a criminal matter where the usual principle is 'beyond the pale of reasonable doubt', 80 percent accuracy was considered as "*positive identification*".

Moreover, such systems are being used without legislative backing or court-mandated processes, and with no mechanism to challenge such identification.

This has raised serious questions about the use of and reliance on such technology, especially in criminal proceedings.

In the absence of collection, storage, retention and publication policies, and the evidentiary value attributable in a criminal prosecution to such positive identification— the usage of FRT raises more concerns than it seeks to address.

In case of a breach which, given precedents, is inevitable— whom do we attribute blame and what remedies do we, as Indian citizens guaranteed the fundamental right to privacy, have?

The integration of an AFRS by the Delhi police through the city's closed-circuit television (CCTV) network raises important concerns pertaining specifically to constitutional principles of proportionality, privacy, lack of bias, *audi alteram partem*, and nexus to the objective sought to be achieved.

It is crucial to evaluate the use of this technology, particularly in cases involving criminal prosecution. Additionally, considerations of user consent, data retention, publication, storage, and the balancing of privacy rights within the limitations of 'public order' are vital.

The need for a clear legislative framework

The Delhi government has established a deep, pervasive network of CCTV cameras across public spaces in the city. The network seeps into even schools operated by the state government and the question of the right to privacy of students in light of such constant monitoring is currently sub-judice.
The conundrum that begs to be resolved through proactive legislation or judicial precedent is the fact that the Delhi police operate under the Central government while the CCTV system is managed by the city's state government.

In the absence of collection, storage, retention and publication policies, and the evidentiary value attributable in a criminal prosecution to such positive identification— the usage of FRT raises more concerns than it seeks to address.

It is imperative to establish clear legislation at both the Central and state levels, specifically outlining the use of CCTV systems by law enforcement agencies.

Presently, apart from the Information Technology Act, 2000 (ITA) and its subsequent Rules, no other legislation governs the AFRS and CCTVs. Therefore, in light of *K.S.Puttaswamy (Retd) and Anr versus Union of India and Ors*, 2017, specific legislation regulating the right to privacy in the context of public order should be introduced.
The usage of such technology, specifically in criminal proceedings, should also ideally be on a case-to-case basis with clear guidelines specifying what grounds can be evoked to use the evidence collected from the said technology.

Without legislative competence, the collection, processing, storage, publication, and transmission of biometric data without informed consent violate an individual's right to privacy.

Even if informed consent can be considered 'deemed' under the garb of public order, it cannot be in perpetuity or throughout the National Capital Territory (NCT) of Delhi, without violating the principle of proportionality.

Addressing accuracy and bias

Since the AFRS is a technology based on 'automation', there also lie substantial problems with 'accuracy' and 'bias'. Many such systems are based on 'self-learning' or 'machine-learning' and may substantiate the inherent biases of the creators, regulators and enforcement agencies. This defeats the principles of natural justice as law enforcement agencies may be relying on a system where there may be inherent biases in a self-perpetuating vicious cycle.
An AFRS can seek to counteract this bias by having an "*independent oversight board*" which would enable a human element to such technology checking for such inherent biases. Members of the board could be from the non-profit sector, judiciary and technical fields.

Regulating overreach by law enforcement agencies

Overreach by law enforcement agencies (such as the Delhi police, Central Bureau of Investigation (CBI), and Enforcement Directorate (ED) is a potential problem. This can be regulated if there is a specific legislation directing the kind of AFRS technology that can be employed and listing the circumstances in which AFRS can be used by such agencies.

This legislation can also be strengthened by providing for an independent oversight body to monitor, regulate and facilitate the use of pre-installed CCTVs.

What started as a bid to trace missing children in Delhi is being used to identify protestors in order to prosecute them under criminal law.

Ideally, there should be a regulatory mechanism to use or install new and updated technology to decrease dependence on existing CCTV technology prone to data breaches. Special cameras (and other relevant equipment) may be installed specifically for this purpose.

The oversight body can also evaluate the need on a case-by-case basis, rather than an infringement of everyone's right to privacy (through their bodily autonomy and biometric data collection).

Ensuring transparency, accountability and proportionality

Transparency in such systems remains a mystery. It also raises issues over accountability and proportionality to the objective AFRS seeks to achieve.

Ideally, the legislation(s) that are so enacted should also include (but should not remain limited to) mandatory disclosures of the use of AFRS, the data collected, the purpose for which such data is collected, storage mechanisms, retention policies and the scope (which should be extremely restricted and act as secondary or corroborative evidence, if at all) of reliance or efficacy of such data in criminal proceedings.

Safeguarding data security and privacy

Issues of data security, especially pertaining to the privacy of sensitive biometric data should be the most important thing that the proposed legislation must address. Apart from the legislation (which should make mechanisms for accountability and also penalise the person/agency for any breach), an attempt should be made to make the AFRS as robust as possible.

In the wake of repeated Aadhaar breaches, the Pegasus scandal, and the recent CoWin breach, it is shown that enforcement agencies may not be able to adequately protect an individual's privacy. However, regulatory mechanisms and technological innovations in tacit compliance through encryption, access controls and regular audits can be used to subvert some of the issues pertaining to data security.
To make the use of AFRS viable, a comprehensive understanding of the technology and its implications, along with restrictive legislation and usage guidelines is necessary at both the Central and state levels.

Defining objectives, functionality, and consent

If legislation is enacted to further the use of AFRS, it must clearly define the objectives, functionality and instances in which AFRS can be used. Ideally, its use should be limited to rare circumstances or determined on a case-by-case basis to adhere to the principles of proportionality and prevent arbitrary usage by law enforcement agencies.

The inclusion of a judicial check through an application to a judicial magistrate would provide an additional safeguard against potential misuse of this technology. Consideration should also be given to incorporating relevant provisions from the criminal procedure and the Digital Personal Data Protection (DPDP) Bill, 2022.

Respecting consent and personal autonomy

The consent and personal autonomy of an individual cannot be arbitrarily taken away or assumed by the State or its instrumentalities under the garb of 'public order' or to serve a 'public purpose'. It cannot be 'deemed' as it is proposed under the DPDP Bill.

This cannot be done *en-masse* for most of the population either, as the right to privacy has been affirmed by the Supreme Court to include these aspects as inherent in a person's enjoyment of privacy. To counteract this issue, a case-by-case basis needs to be determined by the legislation, judicial intervention (as and when required) and an independent oversight board.

Conclusion

While the AFRS system holds promise, it also raises numerous challenges that need to be addressed. The absence of regulation and legislation— biases, potential overreach, data security concerns, invasion of privacy, lack of transparency and accountability cannot be disregarded in light of the *Puttaswamy* judgment.

The use of 'automated' technology comes with inherent biases and risks, potentially targeting specific sections of the population disproportionately. To make the use of AFRS viable, a comprehensive understanding of the technology and its implications, along with restrictive legislation and usage guidelines is necessary at both the Central and state levels.

(Raushan Tara Jaswal is currently an Assistant Professor at O.P. Jindal Global University and a practising advocate at the Supreme Court of India. She has an LLM from the University of Cambridge as a Commonwealth Shared Cambridge Trust Scholar.)

Courtesy: TheLeaflet.in