The Big Picture: Facial Recognition - Uses & Concerns

Anchor: Frank Rausan Pereira

Guests: J Sai Deepak, Advocate, Supreme Court; Anuj Agarwal ,Chairman ,Centre for Research on Cyber Crime and Cyber Law; Dr. Vikram Singh, Former DGP, Uttar Pradesh.

What's in the News?

- Facial recognition has become a cause for concern in Western democracies. The European Commission is considering imposing a five-year moratorium on the use of facial recognition technologies in the European Union (EU).
- Municipalities have passed, or are considering passing prohibitions in the US, however, India is going around the opposite road and is rushing to adopt public facial recognition.

What is the Facial recognition system and how is it integrated in the larger system?

- Facial recognition is a biometric technology that uses distinctive features on the face to identify and distinguish an individual.
- Facial recognition has evolved in many ways, from the first cameras that could recognise faces in the mid-1960s up to now.
- It has evolved from looking at 3D contours of a face to recognising skin patterns.
- The facial recognition technology has been introduced primarily for two purposes:
  o As a compare and contrast tool meant for identification based on existing information or,
  o To create a repository on the basis of which the process of identification can be enhanced.
- The technology has become capable of sorting out types of faces with machine learning. This data is most often stored in a database.
  o The database often raises questions regarding personal security, even though it has been deemed as one of the best upcoming technologies.

How can the technology be used by the police force? What kind of impact does it have on their duties and responsibilities?

- The technology has been utilized primarily for either recognition or authentication or for both purposes, and has been successful.
- India is a country which has a large population and is heavily understaffed. There are 144 policemen to manage 1 lakh citizens, on an average and the ratio indicates how much responsibility each police officer would be undertaking. Thus, the intervention of technologies such as Artificial Intelligence (AI) and Facial recognition is very much welcome.
- When looked at from the perspective of a force multiplier, it is a success story. It could compensate for the understaffed police force. Many within the police force feel that any intervention of technology which would ensure a fair distribution of responsibility and make their work more efficient should be adopted and implemented.
- Besides the fact that would act as a force multiplier in the police department, precaution must be exercised, as similar to any other technology, the facial recognition technology and the AI technologies are still infallible.
- The usage of technology would also enable identification of persons, despite people trying to manipulate, conceal or camouflage their physical features through plastic surgery, scarring and heavy makeup.

- The police utilization of the technology would be allowed after the intelligence operations and after the investigative work is over. There have been multiple cases wherein the criminals have been nabbed with a combination of the face recognition system and human intelligence.
  - o In the event of a crime being committed, as opposed to people spending time, trying to identify a certain person in the absence of a database, the intervention of the technology would provide a back-end on the basis of which the software can perform the task of identification, thereby limiting human intervention, and consequently human error.
  - o This will also eliminate the intervention of motivated humans during the process.
- The technology however, isn't quite affordable and its upgradation also is quite expensive. Hence keeping in mind the cost factor, the technology must be implemented only in sectors and areas wherein its use is compulsory.
- Thus, it cannot be considered as the only solution to the problems being faced by the police force in a country like India. However, it could be considered along with a human element as a solution to the most of the major problems.
- No single technology would be the answer to all the problems, however AI could be adopted while on the lookout for other alternate solutions.

Are there sufficient regulations present to regulate the technology?

- The question of regulations calls one's attention to the following speculations:
  - o What would be the source for collection of the images to create a database?
  - o What kind of relationship would the private entities (such as Twitter, Facebook) have with the security agencies and how would it be reflected in the terms and conditions?
  - o Would the terms and conditions be transparent enough to record that the images and the database would be shared with a law enforcement agency in case of a need?, and
  - o Would the data be sought under a specific arrangement or just sourced from the publically available profiles?
- There's no sufficient information regarding the type of security that would be employed to ensure the integrity of the repository of the database such that it is not privatized or monetized.
- The level of reliability or admissibility standards that would apply to such data being presented as evidence during legal proceedings cannot be determined.
- The Government is yet to address the questions regarding privacy, and legal framework..
  - o The 172 page document released by the **National Crime Records Bureau (NCRB)** does not shed enough light on the regulations to which this technology would be subjected to. However, the document was meant to inform the providers of the technology rather than to throw light on the regulatory protocols.
- The Government would definitely address these issues as the government has a legitimate state interest in the introduction of these technologies because it falls within the broad police powers of the state.

What is the current utilization of the technology in the country?

- Facial recognition systems have been active at several major Indian airports, including the Delhi airport. These systems at airports have been installed under the DigiYatra initiative.
- Telangana's election commission piloted a facial recognition app in its civic elections in January 2020, and claimed that it could address the issue of voter impersonation.

Could the technology be used for mass surveillance purposes?

- The possibility that the technology could be used for mass surveillance is an issue of contention. However, there already is a form of mass surveillance that the public is subjected to, as a result of the CCTV cameras.
- Therefore, the facial recognition system isn't necessarily introducing the element of mass surveillance.

What impact would it have on an Individual's right to privacy?

- There is always a certain amount of compromise on the societal interest and the level of encroachment of individual rights that is involved while using such forms of technology.
- It is necessary to question if the technology is warranted and if there is proportionality between the extent of concession made, to the kind of benefit received.
- However, the country must first start to use the technology for its needs before trying to downplay it.

What are the issues associated with the Facial recognition system?

- The pace at which technology, which could have a bearing on privacy, is being incorporated exceeds the pace at which a regulating mechanism to protect privacy is being established.
- The government would have to find a balance between the introduction of technology and protection of privacy, as **Right to Privacy** is a fundamental right for Indian citizens under the Constitution of India (under Article 21).
- The Government of India would have to inform the public as to what the policy could be like on the question of privacy, as it would otherwise result in a spread of misinformation causing fear and panic amongst the public.
- Infrastructure is one of the major problems in the current situation.
  - The facilities to store such a vast amount of data is not available in India. Thus India is currently taking help from the cloud service providers.
  - Security of the data being stored is also a question to be answered, as there have been many breaches in the recent history, which immediately puts the privacy of the individuals involved into a compromised situation.
- India still relies on foreign countries and its suppliers for this technology. Thus it also raises concerns on the protection of the Indian interest on national and individual levels.

Way Forward:

- Training of the personnel to understand and interpret the data to be able to handle it and ensure its security has to be worked upon, as the data of such significance has the potential to be misused for nefarious activities including blackmail if passed into the wrong hands.
- The government would have to bring in regulations to control the collection, storage and utilization of the data by private companies.
- The technology must be customized according to the needs of the country. Thus, the technology must be customised according to the purpose and the manner of utilization by India. India must try to utilize the technology with specific targeting before permitting its usage in a public area.
- The technology must be implemented on a small scale, with a focus on the sensitive areas initially, rather than implementing it on a larger scale and running a high risk of investments and technical glitches.
  - India should initiate the adoption of the technology with targeted implementation, check whether it can handle a controlled flow of population, run multiple tests on its ability to identify and identify its errors before extending the scope of the technology to other sectors. Until then, the technology must be handled with caution.
- India must prepare a proper roadmap while keeping in mind that there will be both advantages and disadvantages to the implementation of the technology, and must analyze if the advantages outweigh the disadvantages.
- India has the biggest IT workforce in the world, yet it lags behind in terms of technological advancement in the country. Thus it is the right time for India to start experimenting with the face recognition technology to determine if it would be supportive of the country's needs.

Conclusion:

Although it is still a nascent technology, with proper safeguards, it could be a useful technology for India and its current needs. However, India must embark on the process of indigenization when it comes to critical technologies which have a bearing on privacy and thus it is time the government takes the R&D of this particular technology seriously as seen in the case of Israel and China, such that India's reliance on the foreign technology is reduced. Considering that India also has the largest IT workforce, it is time that it starts delivering goods by coming out with products more than just services.