The Big Picture: Facial Recognition - Uses & Concerns

Facial recognition nowadays has become a cause for concern for the western democracies. European Commission is considering imposing a **five-year moratorium** on the use of facial recognition technologies in the European Union (EU). The United States municipalities are also passing rules for its prohibition.

However, India is keen to adopt public facial recognition techniques. Facial recognition systems have been made active at several major Indian airports, including Delhi airport, installed under **DigiYatra Initiative.** Also, **Telangana's Election Commission** recently piloted a facial recognition app in its civic elections to address the issue of voter impersonation.

Facial Recognition

- It is a **biometric technology** that uses distinctive features of the face to **identify and distinguish** an individual. Over a period of almost 6 decades, it has evolved in many ways- from looking at 3D contours of a face to recognizing skin patterns.
- **Working:**
    - The facial recognition system works primarily by capturing the face & its features through the camera and then using various kinds of software to reconstruct those features.
    - The captured face along with its features is stored into a database, which can be integrated with any kind of software that may be used for security purposes, banking services, etc.
- In the **Automated Facial Recognition System (AFRS)**, the large database (containing photos and videos of peoples' faces) is used to **match and identify** the person. Image of an unidentified person, taken from CCTV footage, is compared to the existing database using **Artificial Intelligence** technology, for pattern-finding and matching.

Uses

- **Authentication:** It is used for **identification and authentication** purposes with a success rate of almost 75%.
    - For instance, the **NCRB's Crime and Criminal Tracking Network & Systems (CCTNS)** managing crime data for police, uses automated facial recognition to identify criminals, missing people, and unidentified dead bodies, as well as for "crime prevention".
    - The project is aimed at being compatible with other biometrics such as iris and fingerprints. The integration of fingerprint database, face recognition software and iris scans will massively boost the police department's crime investigation capabilities.
- **Force Multiplier:** In India, where there are just 144 constables per 1 lakh citizens, this can act as a force multiplier. It neither requires too much manpower nor regular upgradation. Hence, this technology coupled with the present manpower in place can act as a game-changer.
- It is increasingly being used for everything from unlocking of mobile phones to validating the identity, from auto-tagging of digital photos to finding missing persons, and from targeted advertising to law enforcement.
    - However, China's reported use of facial recognition technologies for surveillance in the

Xinjiang province opens the possibility of its abuse which becomes problematic in the absence of privacy and data security laws.

Challenges

- **Infrastructural Costs:** Technologies like Artificial Intelligence and **Big Data** are **costly** to implement. The size of stored information is extremely large and requires huge **network & data storage facilities,** which are currently not available in India. Currently, to store the government data from the National Informatics Centre (NIC) and other agencies, international cloud servers are used.
- **Image Collection:** The sources from which images will be collected to create a repository/database needs to be known. Certain questions also need to be answered:
    - Will the information be collected from social media profiles like- Twitter, Facebook, Instagram, etc.?
    - What kind of relationship would it have with the private entities and security agencies?
    - How would that relationship reflect in the terms and conditions, to be fairly transparent, as these images would be made available to enforcement agencies?
- **Security of the Database:** In today's world of cybercrime, there is a dire need to put appropriate safeguards in place in order to ensure the **integrity** of the repository/database, so that it doesn't leak out the information and is not privatized or monetized.
    - Also, International & domestic **accessibility interests** need to be properly addressed.
- **Required Expertise:** The collected data from social media profiles where anybody can put anybody's image, puts to risk the authenticity of the data. Hence, experts are needed to verify such details before storing them who should be provided proper training to protect & avoid abuse and misuse of the collected data & database.
- **Reliability & Authenticity:** As the data collected may be used in the court of law during the course of a criminal trial, the **reliability and the admissibility** of the data along with standards and procedure followed would be taken into consideration. Hence, the **authenticity** of the data is crucial.
- **Right to Privacy:** Government although plans to address the **question of privacy** through the legal framework like **data privacy regime,** but keeping in mind the objectives it aims to achieve with the use of such technology, it comes into conflict with one another.
    - In the absence of data protection laws, Indian citizens become more vulnerable to privacy abuses. As it is sensitive data, it has tremendous potential of being misused.
    - Hence, the constitutional mandate of right to privacy needs to be safeguarded along with the nature of technology, addressing the fears of invasion & surveillance.
- **Inherent Challenges:** Over the time, the face may have different-different facets, for example, somebody has grown a beard, or the age has changed from the last taken photo, or somebody might have covered the face so as to escape from getting captured in the CCTVs. This becomes one of the challenging tasks to overcome.
    - However, it is claimed that such things are taken care of by the software, making it one of the best ways to recognize a person.

Way Forward

- This is a **compare and contrast tool** meant for identification based on existing information. The **process of identification can be accelerated** by its use. For example, there is a CCTV camera at a certain place where crime has been committed. As people spend time in trying to identify the captured image of the persons, the software can perform this without human intervention, thereby **reducing human error.**
- With proper safeguards, this technology is much needed for India. Having the **biggest IT workforce in the world,** the state-of-the-art technology can act as a game-changer for India.
- The notion that sophisticated technology means greater efficiency needs to be critically analysed. A **deliberative approach** will benefit Indian law enforcement agencies, as police departments around the world are currently learning that the technology is not as useful in practice as it seems

in theory.

- Police departments in **London** are under pressure to put a complete end to use of facial recognition systems following evidence of discrimination and inefficiency.
- **San Francisco** also recently implemented a complete ban on police use of facial recognition.
- Hence, it is necessary to make use of such technology, but it cannot act as the silver bullet for all the police reforms that we need.

Every country has its own challenges which are uncomparable. Given the size of India’s population and comparatively understaffed administration, the well-planned use of such nascent technology is a probable solution, provided there are sufficient safeguards to address its inherent concerns including the issue of privacy.