Regulating Facial Recognition Technology in India

For Prelims: **Facial Recognition Technology**, **Right to Information,** Biometric Technology, **Artificial Intelligence**

For Mains: Facial Recognition Technology, Need for Governance of FRT in India, Its Implication and Uses, Challenges in FRT.

Source: ET

Why in News?

Recently, the **NITI Aayog,** the premier public policy think-tank of the Government of India, has called for **comprehensive policy and legal reforms** to **regulate the use of Facial Recognition Technology (FRT)** in the country.

- This step is considered a major development amid growing worries about **privacy, transparency,** and **accountability.**

What are the Proposals to Regulate the Use of FRT in India?

- **Status of Regulation in India:**
    - Currently, there is **absence** of any comprehensive legal framework present to regulate the use of Facial Recognition Technology (FRT) in India.
- **Need For Regulating FRT:**
    - **Multifaceted Challenges:** FRT presents distinct challenges compared to other technologies due to its **ability to capture and process sensitive biometric data remotely.** Existing regulations might not adequately address these specific concerns.
    - **Ensuring Responsible Development:** The objective is to create a comprehensive **governance framework that can ensure the responsible development and deployment of FRT in India.**
        - This is crucial to mitigate the risks and ethical concerns associated with the use of FRT, such as privacy violations, algorithmic bias, and abuse of surveillance powers.
    - **International Thought Leadership**: Proactive regulation will **allow India to emerge as a global thought leader on FRT governance,** shaping international discourse and policies.
    - **Promoting Public Trust:** Effective regulation will build public trust in the technology and facilitate its widespread adoption across various sectors.
    - **Balancing Innovation and Safeguards:** The reforms seek to strike a balance between **promoting FRT innovation and putting in place necessary safeguards** to protect individual rights and societal interests.
- **Key Proposals:**
    - **Standardising Liability:**
        - Establishing a **legal framework** that **imposes liability** and **defines the extent of damages** for harms caused by FRT malfunctions or misuse. This would

incentivise responsible development and deployment.
- **Ethical Oversight:**
  - Creating an **independent ethical committee** with diverse expertise to oversee FRT implementation. This committee would **address issues of transparency, accountability, and potential bias** within the algorithms.
- **Transparency in Deployment:**
  - Mandating **clear and transparent guidelines** on the **deployment of FRT** systems. This would include informing the public about the use of FRT in **specific areas** and obtaining consent where necessary.
- **Legal Compliance:**
  - Ensuring FRT systems comply with the Supreme Court's established legal principles in its judgment given in **_Justice K. S. Puttaswamy (Retd) Vs Union of India_** case.
  - These principles include **legality** (adherence to existing laws)**, reasonability** (proportionality to the objective), and **proportionality** (balancing the need for security with individual rights).

What is Facial Recognition Technology?

- **About:**
  - Facial recognition 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.
  - 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.
- **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.
- **Uses:**

  - **Verification:**

    - 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, it is used to **unlock phones.**
  - **Identification:**
    - 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. For example, law enforcement agencies usually procure FRT for identification.

[//](#)

Biometrics Face Recognition - How does it Work?

CAPTURING
EXTRACTING
COMPARING
MATCHING

Unique facial data
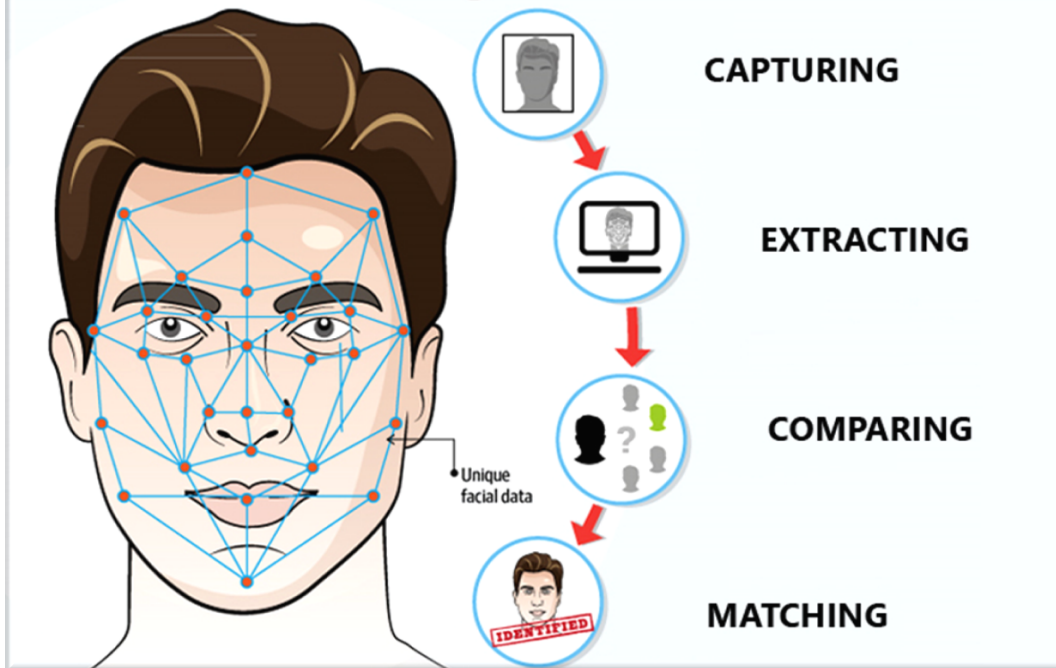
What are the Concerns Regarding the Use of FRT Technology?

- **Inaccuracy, Misuse and Privacy Concerns:** FRT's limitations include **misidentification**, particularly across racial and gender demographics. This can lead to **wrongful disqualification** of legitimate candidates.
  - The widespread use of FRT for **surveillance and data collection** can clash with the objectives of **data privacy and protection**, even in the presence of a legal framework.
- **Racial and Gender Biases: Studies reveal disparities in FRT accuracy based on race and gender, potentially excluding deserving candidates and reinforcing societal biases.**

- Exclusion from Essential Services: Failures in biometric authentication, such as under the Aadhaar system, have led to the exclusion of individuals from accessing essential government services.

- **Absence of Data Protection Laws:** The lack of comprehensive data protection laws makes FRT systems **vulnerable to misuse, with inadequate safeguards for the collection, storage, and use of biometric data.**
- **Ethical Concerns: It also raises ethical questions about the balance between public safety and individual rights, as well as the potential for misuse and abuse of the technology. There are concerns about the erosion of anonymity and the potential for FRT to be used for social control and suppression of dissent.**

FRT Regulation in Other Countries

- **European Union (EU): Apart from the General Data Protection Regulations (GDPR) and the Data Protection Directive, the EU has an AI Act which aims to create a risk-based compliance framework, categorising FRT systems as "high risk" and subjecting them to the strictest compliance requirements.**
- **UK, US, Canada, and Australia:** In these countries, the regulation of FRT is mainly governed by their **respective data protection and privacy laws.**

Way Forward

- **Robust Legal Framework:** Establish dedicated laws or regulations governing FRT deployment by both public and private actors. These laws should clearly define lawful purposes for FRT use, emphasise proportionality, and establish clear lines of accountability.
- **Ethical Oversight and Governance:** There is a need for creation of **independent ethical oversight committees** to assess the ethical implications of FRT deployments, prescribe codes of practice, and ensure compliance.
- **Transparency and Data Protection:** Make **public disclosure of FRT deployments mandatory** for both government and private entities and aligning FRT governance with India's upcoming data protection framework to ensure robust data protection safeguards.
- **Addressing Bias:** There is a need to develop clear guidelines **promoting fair and non-discriminatory use of FRT**, particularly in high-stakes applications.
- **Global Leadership:** Actively **participate in international discussions on FRT governance** to shape global standards. Leverage India's position as a technological leader to champion responsible AI development on the world stage.

Drishti Mains Question:

Discuss the major concerns associated with the deployment of Facial Recognition Technology (FRT) systems and suggest measures to ensure transparency, accountability and address potential biases.

UPSC Civil Services Examination, Previous Year Questions (PYQs)

Prelims

Q. With the present state of development, Artificial Intelligence can effectively do which of the following? (2020)

1. Bring down electricity consumption in industrial units
2. Create meaningful short stories and songs
3. Disease diagnosis
4. Text-to-Speech Conversion
5. Wireless transmission of electrical energy

Select the correct answer using the code given below:

(a) 1, 2, 3 and 5 only
(b) 1, 3 and 4 only
(c) 2, 4 and 5 only
(d) 1, 2, 3, 4 and 5

Ans: (b)

Q. The identity platform 'Aadhaar' provides open "Application Programming Interfaces (APIs)". What does it imply? (2018)

1. It can be integrated into any electronic device.
2. Online authentication using iris is possible.

Which of the statements given above is/are correct?

(a) 1 only
(b) 2 only
(c) Both 1 and 2
(d) Neither 1 nor 2

Ans: (c)

Mains

Q1. **"**The emergence of the Fourth Industrial Revolution (Digital Revolution) has initiated e-Governance as an integral part of government". Discuss. **(2020)**

Q2. What are the areas of prohibitive labour that can be sustainably managed by robots? Discuss the initiatives that can propel the research in premier research institutes for substantive and gainful innovation. **(2015)**

Q3. "Human beings should always be treated as 'ends' in themselves and never as merely 'means'." Explain the meaning and significance of this statement, giving it's implications in the modern techno-economic society. **(2014)**

PDF Refernece URL: https://www.drishtiias.com/printpdf/regulating-facial-recognition-technology-in-india