Dealing with Deepfakes

For Prelims: Deepfake technology**,** deep synthesis technology, Artificial Intelligence technology**,** blockchain technology

For Mains: Impact of Deepfake Technology, India's stand on dealing with deepfakes, Ethical concerns associated with deepfakes

Why in News?

Recently, various news sources have focused on the **growing concern over deepfakes**, which are **fabricated media created using deep learning technology.**

- While deepfakes have the potential to distort reality and manipulate public perception, they also **hold promise in various fields.** The challenge lies in responsibly wielding this technology and addressing its impact on society.

What is Deepfake Technolgy?

- **About:**
  - **Deepfake technology** is a method for manipulating **videos, images, and audio** utilizing powerful computers and **deep learning.** Deep learning is a part of **Deep synthesis.**
    - **Deep synthesis** is defined as the use of technologies, including **deep learning** and **augmented reality, to generate text, images, audio** and **video to create virtual scenes.**
  - It is used to generate **fake news** and **commit financial fraud** among other wrongdoings.
  - It overlays a digital composite over an already-existing video, picture, or audio; cybercriminals use **Artificial Intelligence technology.**
  - Deepfakes **surpass traditional photo editing techniques** by leveraging **machine learning algorithms.**
  - Deepfakes have been used to create **manipulated content,** such as **fake videos of political figures and false disaster images.**
- **Redeeming Applications of Deep Learning:**
  - Deep learning technology has enabled positive advancements, such as **restoring lost voices and recreating historical figures.**
  - The ALS Association's voice cloning initiative and recreations of artists and celebrities showcase the potential benefits of deep learning.
  - Deep learning techniques have been applied in **comedy, cinema, music, and gaming to enhance artistic expression.**
- **Unsettling Consequences and Ethical Concerns:**
  - Deepfakes have been employed for **malicious purposes, including revenge porn and hacking facial recognition systems.**
  - They **undermine trust in the media** and **blur the lines between fact and fiction.**
  - Misinformation propagated by deepfakes can be mistaken as true, leading to potential social unrest.

What is India's Stand on Dealing with Deepfakes?

- India **does not have specific laws or regulations that ban or regulate the use of deepfake technology.**
- Existing laws such as **Sections 67 and 67A of the Information Technology Act (2000)** have provisions that may be applied to certain aspects of **deepfakes, such as defamation and publishing explicit material.**
- Section **500 of the Indian Penal Code (1860)** provides punishment for defamation.
- The **Personal Data Protection Bill (2022),** if passed, could provide some protection against the misuse of personal data, but it does not explicitly address deepfakes.
- India **needs to develop a comprehensive legal framework** specifically targeting deepfakes, considering the potential implications for privacy, social stability, national security, and democracy.

What are Other Countries doing to Combat Deepfakes?

- **European Union:**
  - In 2022, the **European Union** has updated **Code of Practice on Disinformation** that was introduced in 2018 to stop the spread of disinformation through deepfakes.
- **United States:**
  - The **U.S.** introduced the **bipartisan Deepfake Task Force Act** to assist the Department of Homeland Security (DHS) to **counter deepfake technology.**
- **China:**
  - China introduces **comprehensive regulation on deep synthesis**, effective from January 2023. Aimed at curbing disinformation, the regulation requires **clear labeling and traceability** of deep synthesis content. **Consent from individuals and adherence to laws and public morals** are mandated. Service providers must establish review mechanisms and cooperate with authorities.

Way Forward

- **AI-Powered Social Media Fact-Checking:** Engage social media platforms to invest in **AI-powered algorithms and tools** that can **automatically detect, and flag potentially manipulated** or **deepfake content.**
  - Collaborate with fact-checking organizations and utilize the power of public participation to quickly address and act against the spreading of false information through deepfakes.
- **Blockchain-based Deepfake Verification:** Use **blockchain technology** to create an **unchangeable record** of who created a piece of digital media and **ensure transparency** in verifying its **authenticity.**
  - This **decentralized approach allows individuals to trace the origin** and **modification history of media**, discouraging the creation and dissemination of malicious deepfakes.
- **Deepfake Impact Mitigation Policy:** Set up a **fund to help** individuals and organizations **affected by deepfakes.**
- **Deepfake Accountability Act (DAA):** DAA can be introduced aimed at addressing the challenges posed by deepfakes and ensuring accountability in their **creation and distribution and controlling.**
- **Punishments and Public Awareness Campaigns:** Laws should punish **bad-faith actors and protect individuals** from the **manipulation of their digital representations.**
  - **Public awareness and literacy in scientific and digital domains** are crucial to combat the spread of deepfakes.

Source: TH