DEEPFAKE TECHNOLOGY: A GLOBAL THREAT

What Are Deepfakes?

- Deepfakes are **AI-generated videos, images, and audio recordings** that convincingly **imitate real people**.

- Fraudsters are leveraging this technology to **manipulate legal processes**, impersonate **government officials**, and execute **financial crimes**—creating unprecedented challenges for corporate legal teams and regulatory bodies.

How Deepfake Technology is Misused?

- **Impersonate** government officials or corporate executives

- **Exploit deepfake voice and video calls** to extract confidential information, authorize unauthorized deals.

- AI-generated deepfakes **bypass biometric authentication** and **KYC checks**

- **Manipulate digital evidences** and surveillance footage.

W: yellow-stone.in
M : +91 90290 87532

REAL-LIFE CASES OF DEEPFAKE

- **Scammers Impersonate Hong Kong Firm's CFO on Video Call (2023)**

In a first-of-its-kind case, cybercriminals used deepfake video technology to impersonate a CFO on a virtual meeting, tricking employees into transferring a significant sum of money. The fraud was undetectable in real time due to the high accuracy of AI-generated visuals and speech.

- **Deepfake Videos Used to Undermine Political Leaders**

Governments worldwide are dealing with deepfake-generated misinformation campaigns. In 2024, AI-generated videos of U.S. President Joe Biden and Indian Prime Minister Narendra Modi surfaced online, spreading false messages to manipulate public perception ahead of elections.

- **$35 Million Bank Heist Using AI Voice Cloning (2020)**

A UAE-based bank fell victim to a deepfake voice scam where fraudsters cloned the voice of a company executive and convinced a bank manager to transfer $35 million to fraudulent accounts. The criminals even used deepfake emails to support their request, exploiting weak verification processes.

LAWS IMPLEMENTED GLOBALLY TO TACKLE DEEPFAKE TECHNOLOGY

Country	Law/Regulation	Key Provisions	Eff. Yr
United States	No AI FRAUD Act (Proposed), State-level laws (e.g., NY)	Criminalizes AI-generated depictions without consent, covers explicit content, growing focus on political deepfakes	Proposed (2024)
United Kingdom	Online Safety Act	Criminalizes non-consensual AI-generated intimate images, covers threats and harassment	2024
European Union	AI Act, GDPR	Requires clear disclosure of AI-generated content, GDPR covers misuse of personal data	2024
China	Regulations on the Administration of Deep Synthesis of Internet Information Services	Requires labeling of AI-generated content, mandates consent for altering an individual's likeness or voice	2023
India	IT Act 2000, IPC	No specific deepfake law yet, existing cybercrime laws apply, considering new regulations	Ongoing
Australia	Online Safety Act 2021	Grants power to eSafety Commissioner to take down harmful deepfake content, exploring stricter AI misinformation laws	2021

HOW TO COMBAT DEEPFAKE?

For Corporates and Institutions

- Use **deepfake detection software** like Deepware Scanner, Sentinel, and Microsoft's Video Authenticator to verify digital content.

- **Implement liveness detection in facial recognition systems** to prevent AI-generated fraud

- Set up **verification protocols** for video/audio-based directives from executives or clients.

- **Educate employees** about deepfake risks and how to identify manipulated media.

For Individuals

- **Cross-check official communications** through alternative verified sources before acting.

- **Avoid sharing excessive personal data online,** which fraudsters can exploit for AI cloning.

- Be cautious of **unsolicited video calls or messages** requesting financial transactions.