Legal Issues surrounding Deepfakes

What are Deep fakes and how are they made ?

A Deepfake is a type of modern media created using digital software, machine learning and face swapping.

They are a combination of artificial videos and images which show events, statements or actions that have not actually happened. They are often very hard to determine whether they are real or fake.

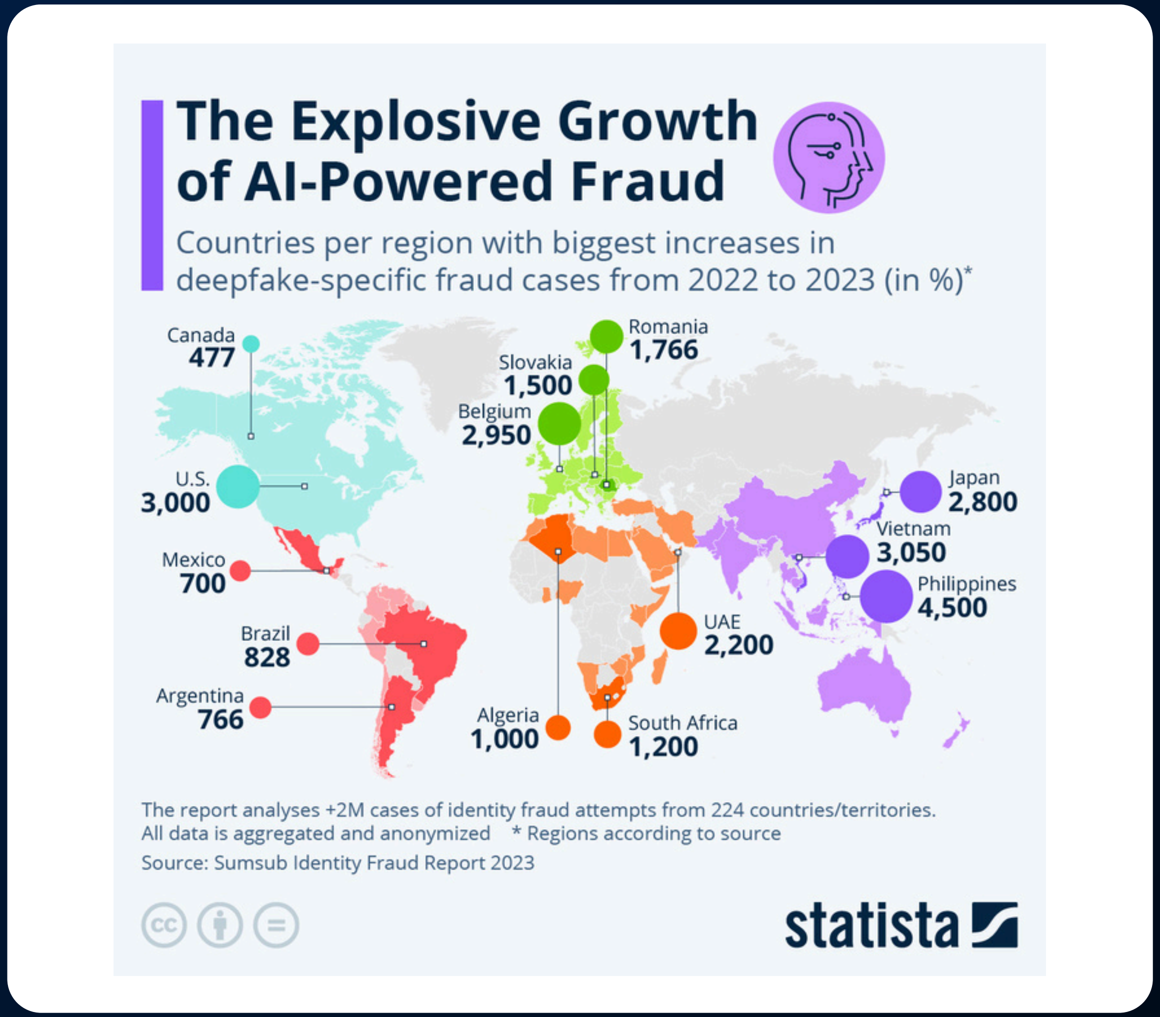
Real or Fake ?

Focus - Legal Issues

Rapid growth of deepfake technology has fuelled a surge in AI-powered fraud.

Increasing realism makes it harder for people and organisations to distinguish genuine content from fabricated media.

The expanding sophistication of deepfakes is creating new risks in trust, security, and information integrity.



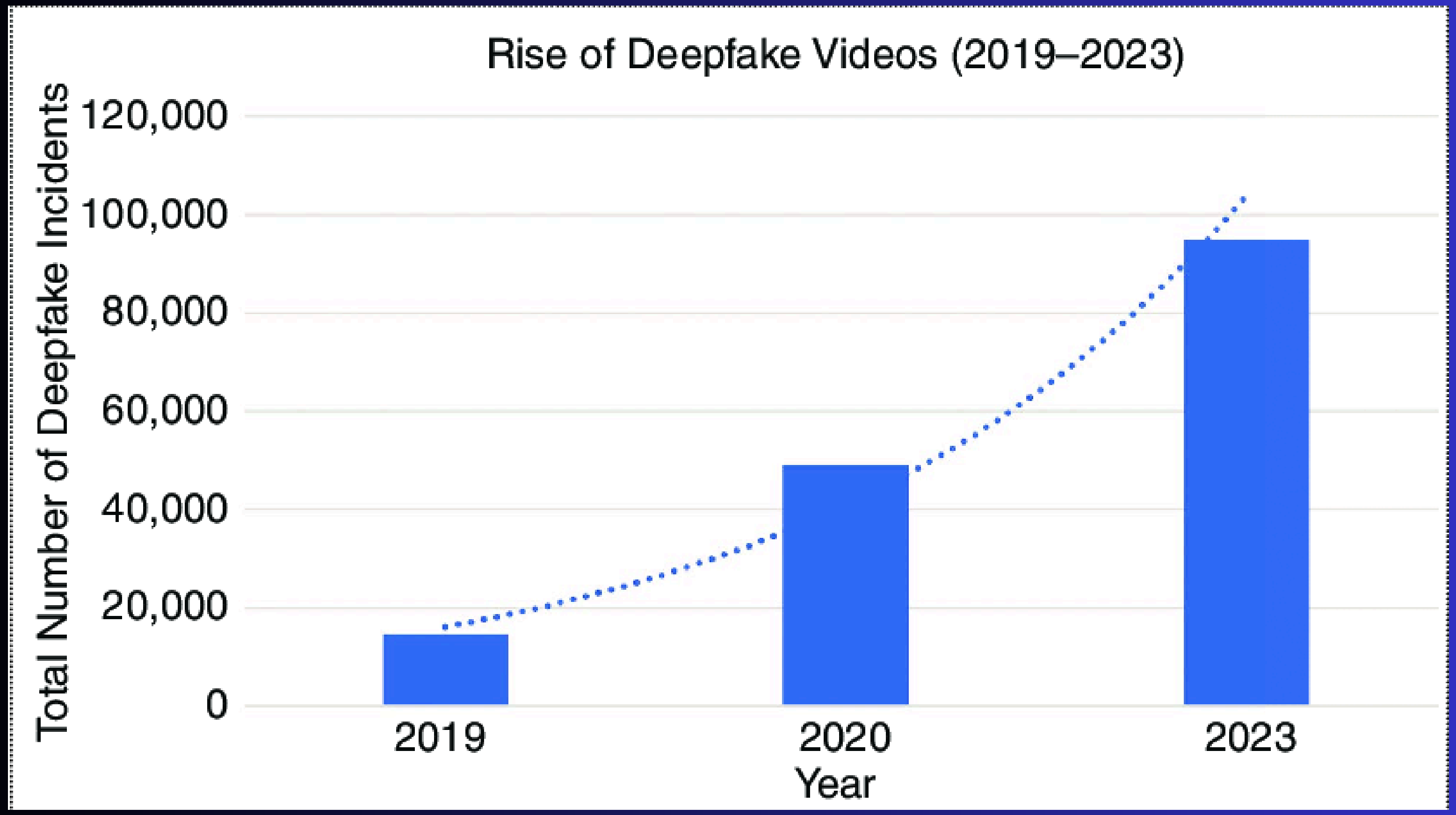
The Explosive Growth of AI-Powered Fraud

Countries per region with biggest increases in deepfake-specific fraud cases from 2022 to 2023 (in %)*

The report analyses +2M cases of identity fraud attempts from 224 countries/territories. All data is aggregated and anonymized * Regions according to source

Source: Sumsub Identity Fraud Report 2023

statista



Rise of Deepfake Videos (2019–2023)

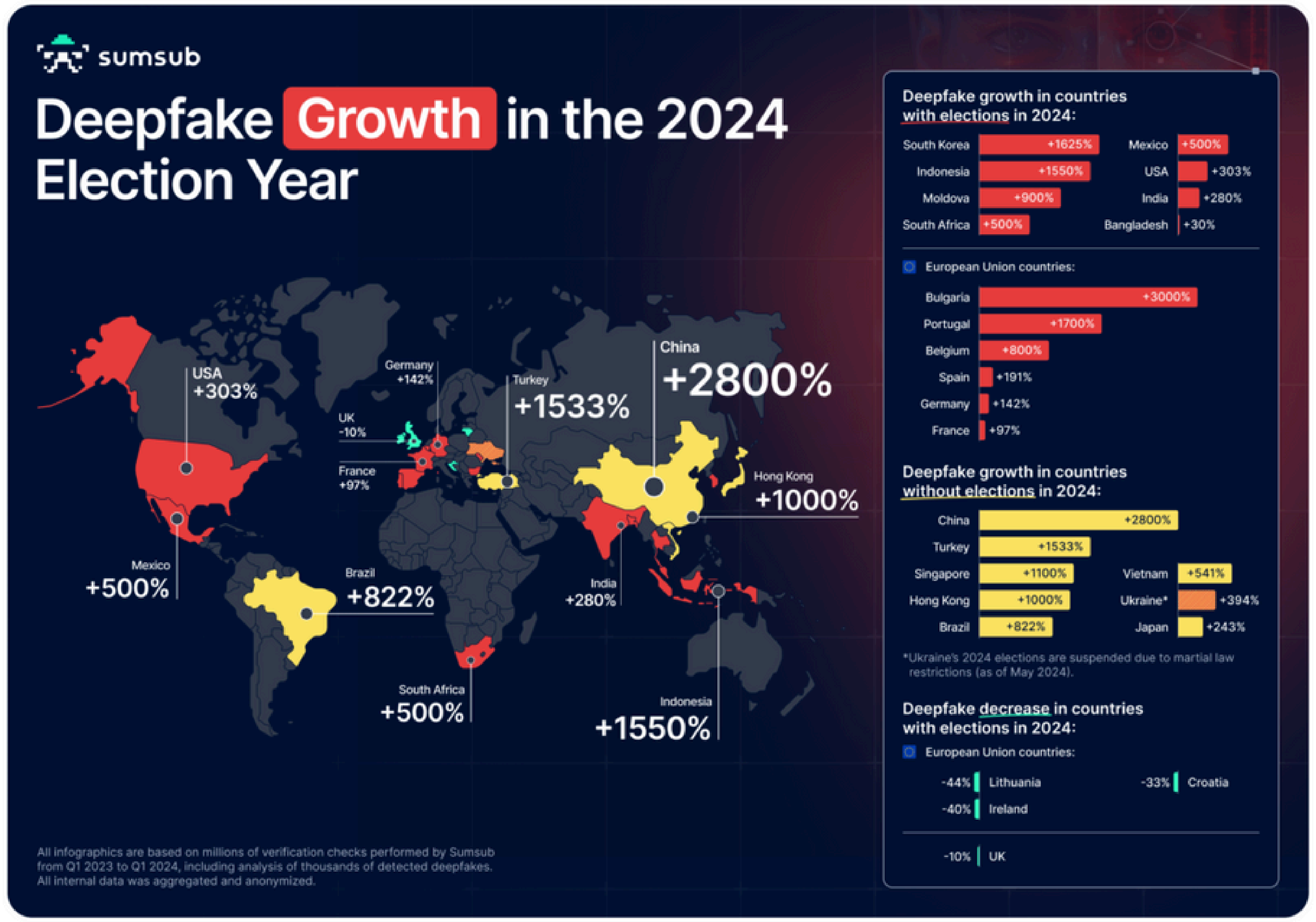
Deepfakes and Emerging Legal Issues

- Identity Fraud
  Deepfakes are increasingly used to impersonate individuals in video or audio, enabling scams, financial fraud, and unauthorised access to secure systems.

- Intimate Image Abuse
  AI-generated explicit content of real people—created or shared without consent—is now recognised as a serious form of digital sexual abuse and is being criminalised in many jurisdictions.

- Child Sexual Abuse Material (CSAM)
  Creating or distributing deepfake content involving minors is illegal everywhere, even when no real child was present, due to the clear harm and exploitation involved.

- Disinformation & Election Interference
  Deepfakes are being deployed to spread false narratives, manipulate public opinion, and undermine trust in democratic processes, prompting new regulatory and legal responses.



sumsub

Deepfake Growth in the 2024 Election Year

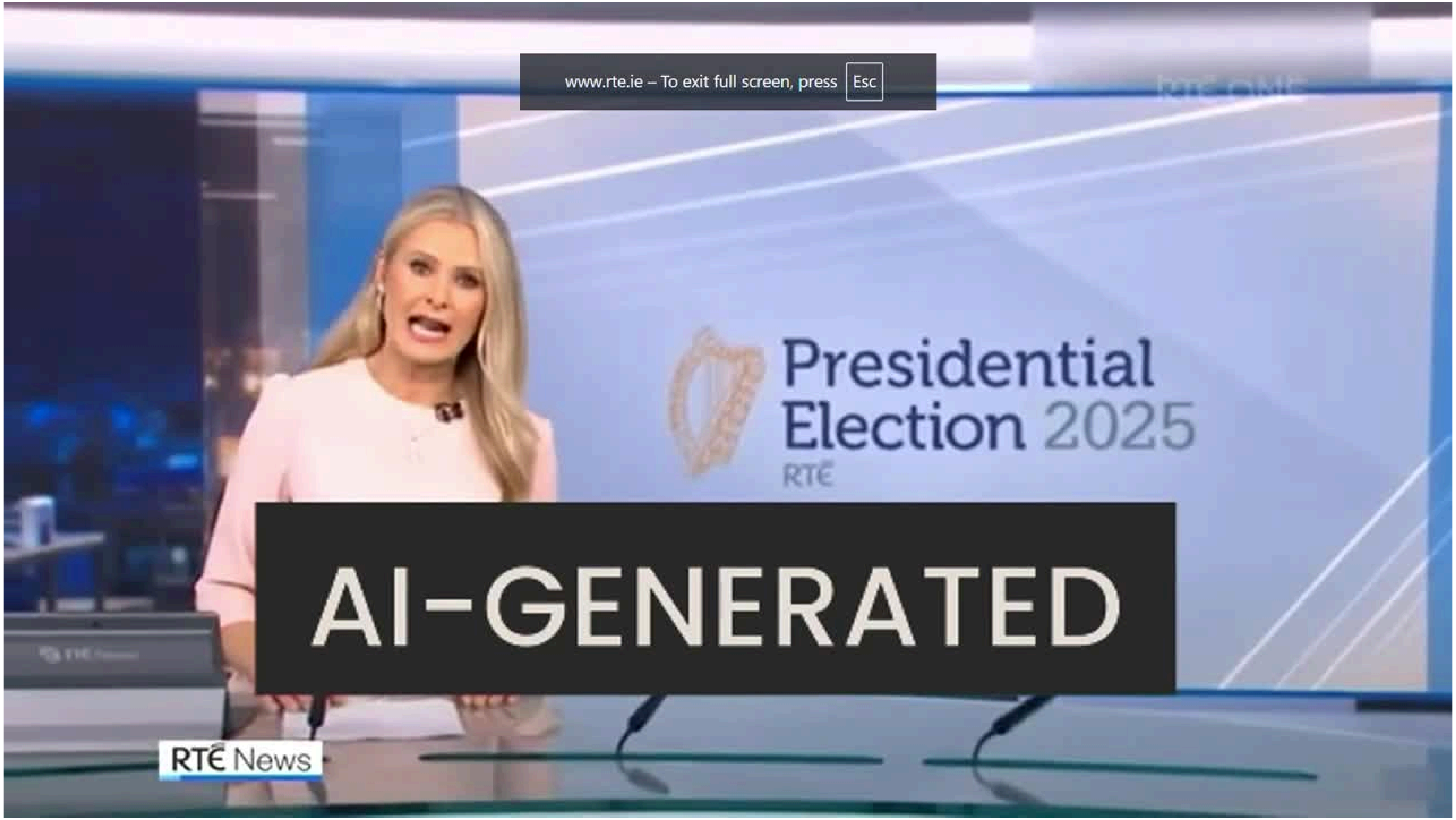
Deepfake growth in countries with elections in 2024:

Deepfake growth in countries without elections in 2024:

*Ukraine's 2024 elections are suspended due to martial law restrictions (as of May 2024).

Deepfake decrease in countries with elections in 2024:

All infographics are based on millions of verification checks performed by Sumsub from Q1 2023 to Q1 2024, including analysis of thousands of detected deepfakes. All internal data was aggregated and anonymized.


www.rte.ie – To exit full screen, press Esc
Presidential Election 2025
RTÉ
AI-GENERATED
RTÉ News

(Ryan, 2025)

Who Deepfakes affect

Political Leader – the individual being impersonated and potentially defamed.

Voters – people relying on accurate information to make informed decisions.

Election Authorities – responsible for maintaining trust and fairness in the electoral process.

Social Media Platforms – hosting and moderating the spread of the DeepFake.

News & Fact-Checking Organisations – working to verify authenticity and counter misinformation.

Opposing Political Groups – may be affected by shifts in public opinion caused by the fake content.

(Jacobson, 2024)

Real or Fake ?

Potential Harm

- Voter Manipulation - deepfake content may infulence opinions
- Damage to Reputation - target may suffer political harm
- Erosion of Public Trust - people may lose confidence in the democratic processes or information sources
- Social Division - false narratives can intensify conflict

How AI Contributes

- High Realism - AI generates high grade audio and video that appear real
- Rapid Production - DeepFakes can be created quickly with next to no skill
- Easy Amplifiaction - Spreads rapidly through the social media algorithms
- Difficulty Detecting Fakes - Due to AI advancement, it is harder for the public to distinguish real from fake media

Should Creating or sharing DeepFakes be Regulated

YES

- DeepFakes cause harm such as identity fraud, intimate image abuse and political manipulation
- Regulation can help protect a persons right, prevet exploitation, and even maintain trust in public information

Challenges for Law

- **AI advancement - technology is advancing faster than legislation**
- **Jurisdication - Laws differ between countries while DeepFakes spread globally**
- **Proof - It is difficult to identify who created and shared DeepFakes**
- **Rights - Laws must respect the legitimate uses of DeepFakes**

Indicators of DeepFake

1. Unnatural facial movements
2. Lighting or shadows that don’t match the environment
3. Distorted or blurred areas around the face or edges
4. Inconsistent audio - video synchronisation

(Swatton and Leblanc, 2024)

Arup Engineering DeepFake Fraud 2024
An employee in the Hong Kong office was tricked into transferring $25 million. Criminals used an AI generated video to impersonate an executive during a fake video call

(Milmo, 2024)

Why Public Awareness Matters

- People need to be aware of the warning signs
- Critical thinking will help a perosn question suspicious content before sharing it
- Awareness will help reduce the spread of misinformation

Counteracting DeepFake Misinformation

1. AI detection tools
2. Public education
3. Clear Legal Frameworks

Justifiaction

DeepFakes affect all levels of society meaning a multi-layered response is needed.
Having shared responsibility will ensure that there is accountability across all groups.
This reduces the risk of misinformation spreading.

Who Should Hold Responsibility ?

Shared responsibility:

- Tech Companies → Should develop tools to detect and label AI generated content
- Governments → Laws should be created, penalities enforces and public awareness should be supported.
- Users → Should verify the content before sharing it and report suspicious media.

Thanks

Oisin Gibson