

Umelá inteligencia v kybernetickej a informatickej bezpečnosti



**KONFERENCIA
O VEDE A TECHNIKE
NA SLOVENSKU**

doc. Ing. Peter Papcun, PhD.
Technická univerzita v Košiciach
Fakulta elektrotechniky a informatiky
Katedra kybernetiky a umelej inteligencie
6.11.2025

Umelá inteligencia

- 1946: ENIAC, 1951: UNIVAC
- Umelá inteligencia:
 - Turingov test 1949 (prekonaný 2012: Goostman)
 - definovanie pojmu 1956 (John McCarthy)
 - strojové učenie 1959 (regresia, klasifikácia, zhukovanie, asociácia)
- 1965: prvý chatbot (ELIZA)
- 1965: fuzzy logika (nie len 0 a 1)
- 1970: prvý osobný počítač
- 1980: expertné systémy (znanostné systémy: báza znalostí, báza dát, inferenčný mechanizmus)
- 1997: Deep Blue
- 2011 – 2014: Siri, Cortana, Google Now
- 2016: AlphaGo
- 2022: GPT 3.5

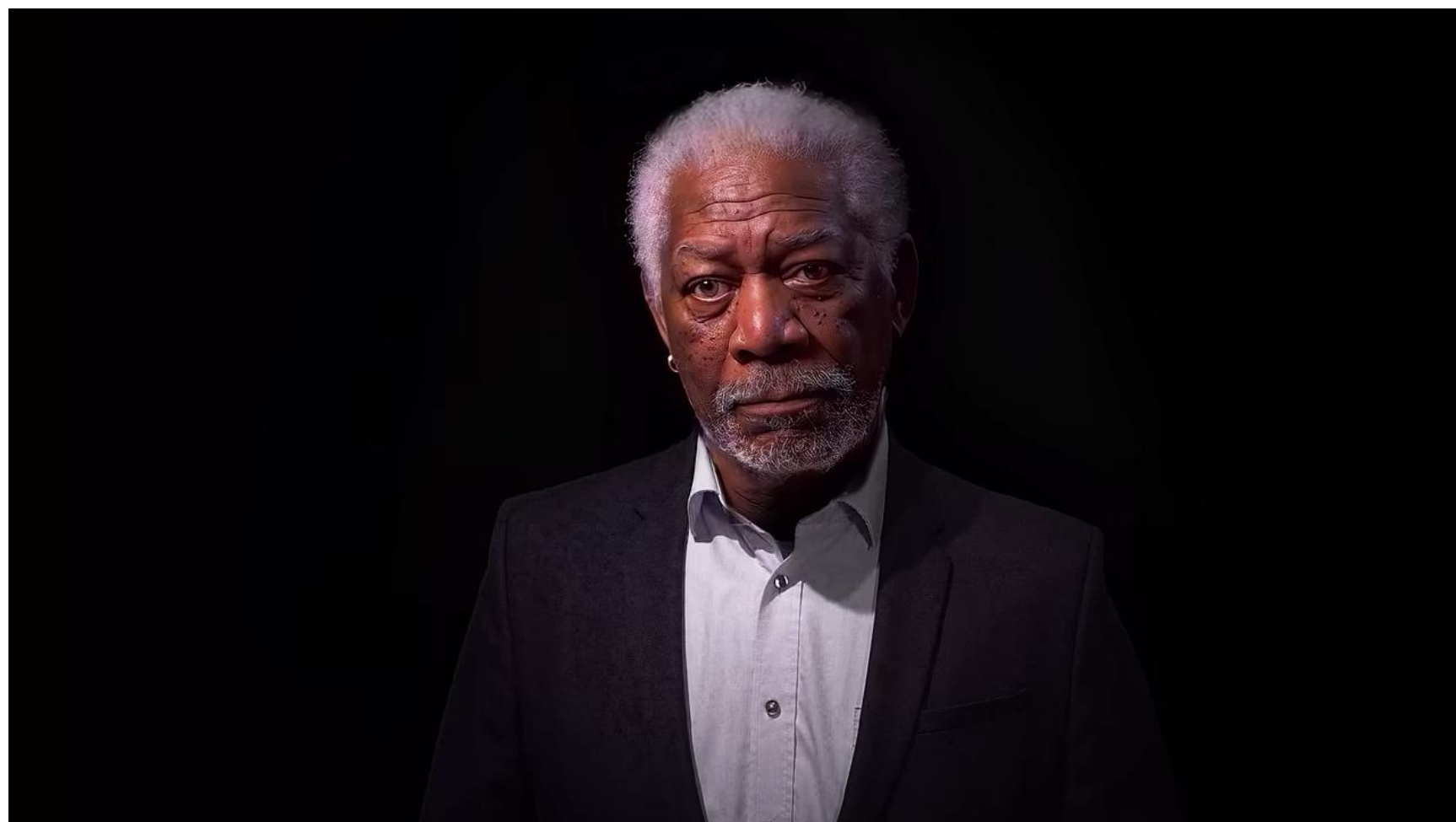
Deep Fake

- 2009: DNN
- 2014: GAN (Generatívne adverzné siete)
 - filmy (Indiana Jones, omladenie hercov, modeling, ...)
- 2017: definovanie pojmu
 - aplikácie: filtre, výmena tvári
- 2021: Dall-E (Open - AI)
- 05 / 2024: GPT 4o
- 12 / 2024: Sora (videá)
- 03 / 2025: update GPT 4o (obrazy)
- 08 / 2025: GPT 5
- 09 / 2025: Sora 2 (zvuk)



Sociálne siete a deep fake

- Dezinformácie
- Spočiatku potrebný herci, teraz len prompt

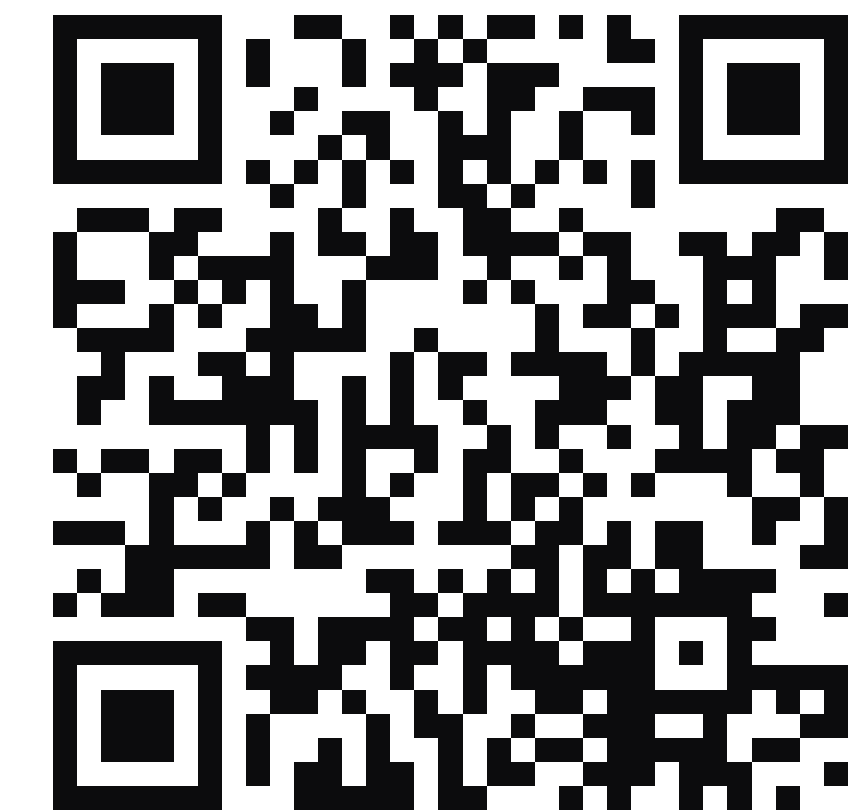
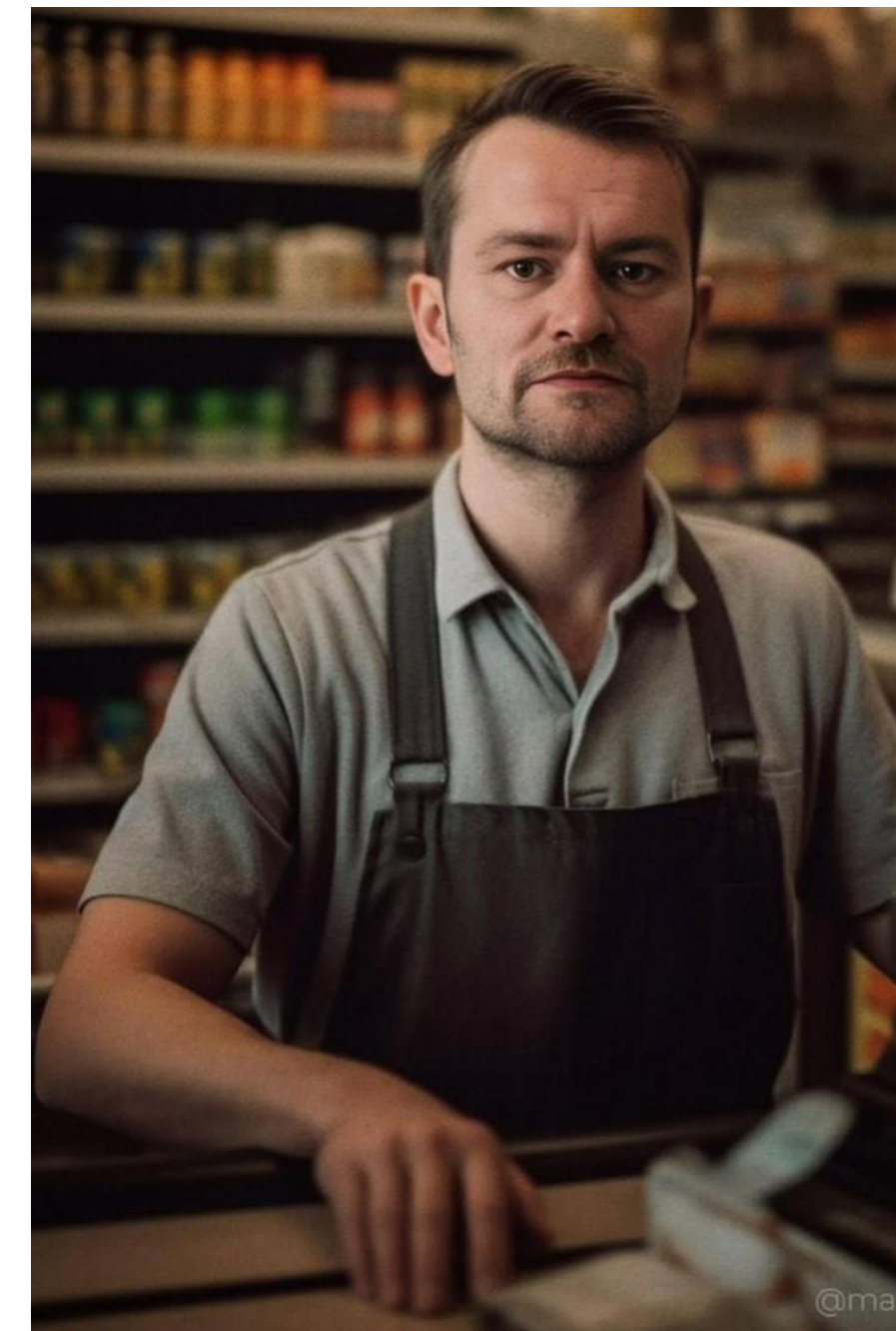


Sociálne siete a dezinformácie

- ilustračné fotografie
- podpora konšpiračných teórií
- diskreditácia
- a iné



https://www.instagram.com/vivat_slovakia/



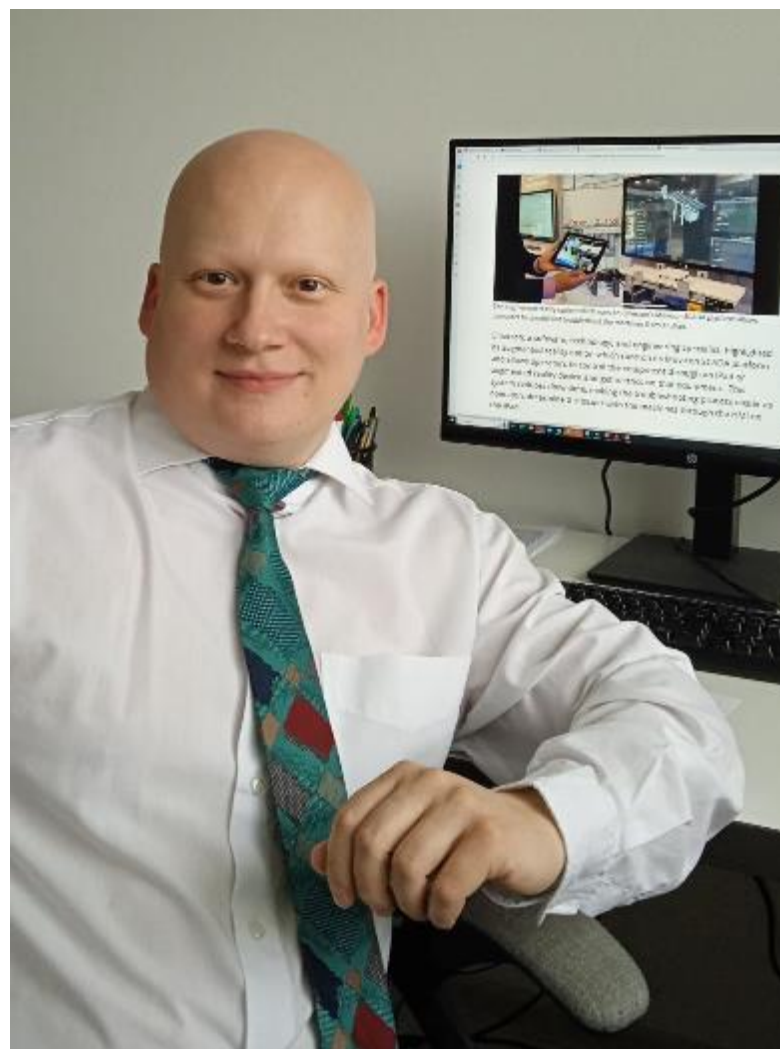
<https://www.instagram.com/madeinslovakai/>

Generovanie obrázku

- Vygeneruj mi obrázok, kde reptiliáni stavajú pyramídy
- Chcel by som sa vidieť na fotke niekde na pláži v bare

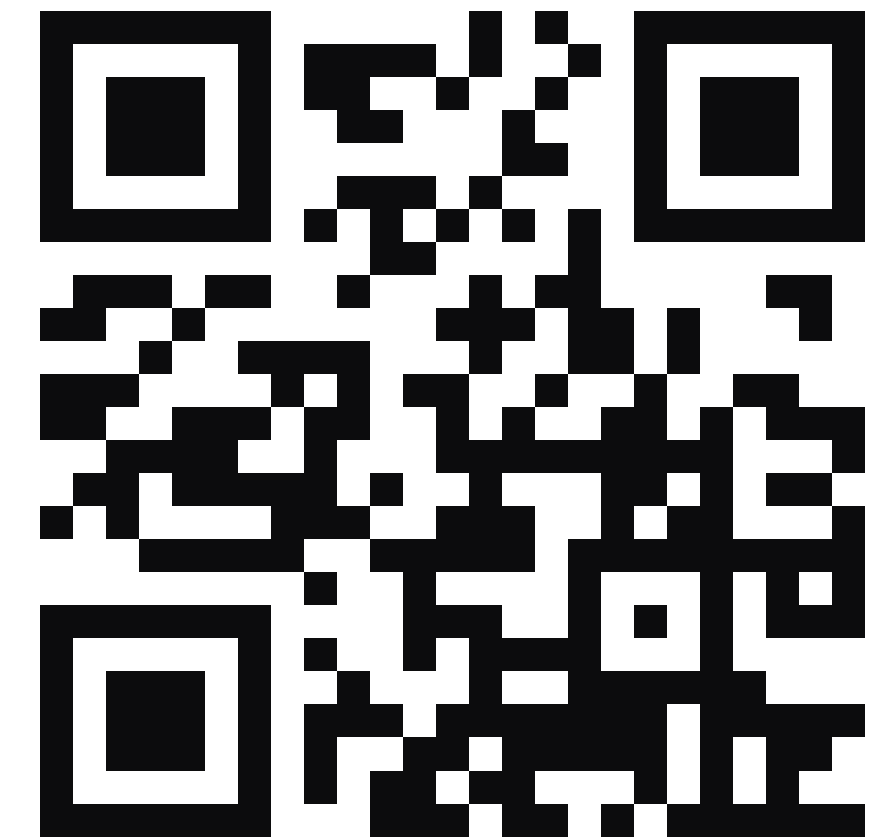


<https://chatgpt.com/>



Generovanie obrázkov bez filtrov

- Grok nepoužíva filtre pri známych osobnostiach
- „Generate image of Robert Fico as thief in grocery store, realistic style“



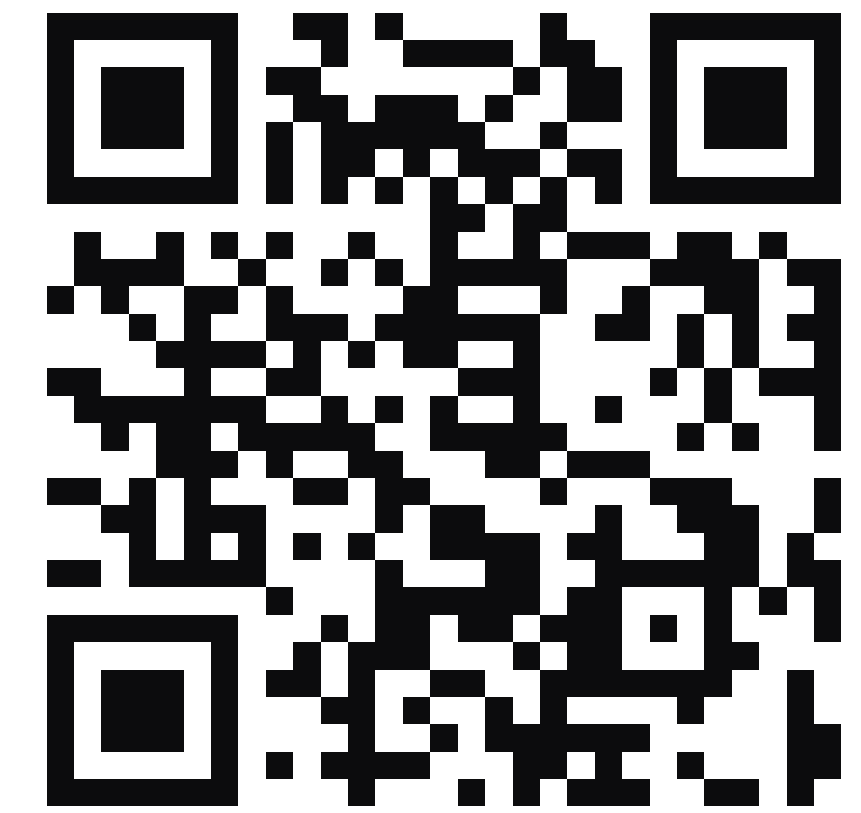
<https://grok.com/>

Generovanie videa

- Video s krajinou, malou dedinkou a jazerom
- Vygeneruj mi video na ktorom uvidím celú planétu zem a postupne sa budem približovať ku kontinentu Európa

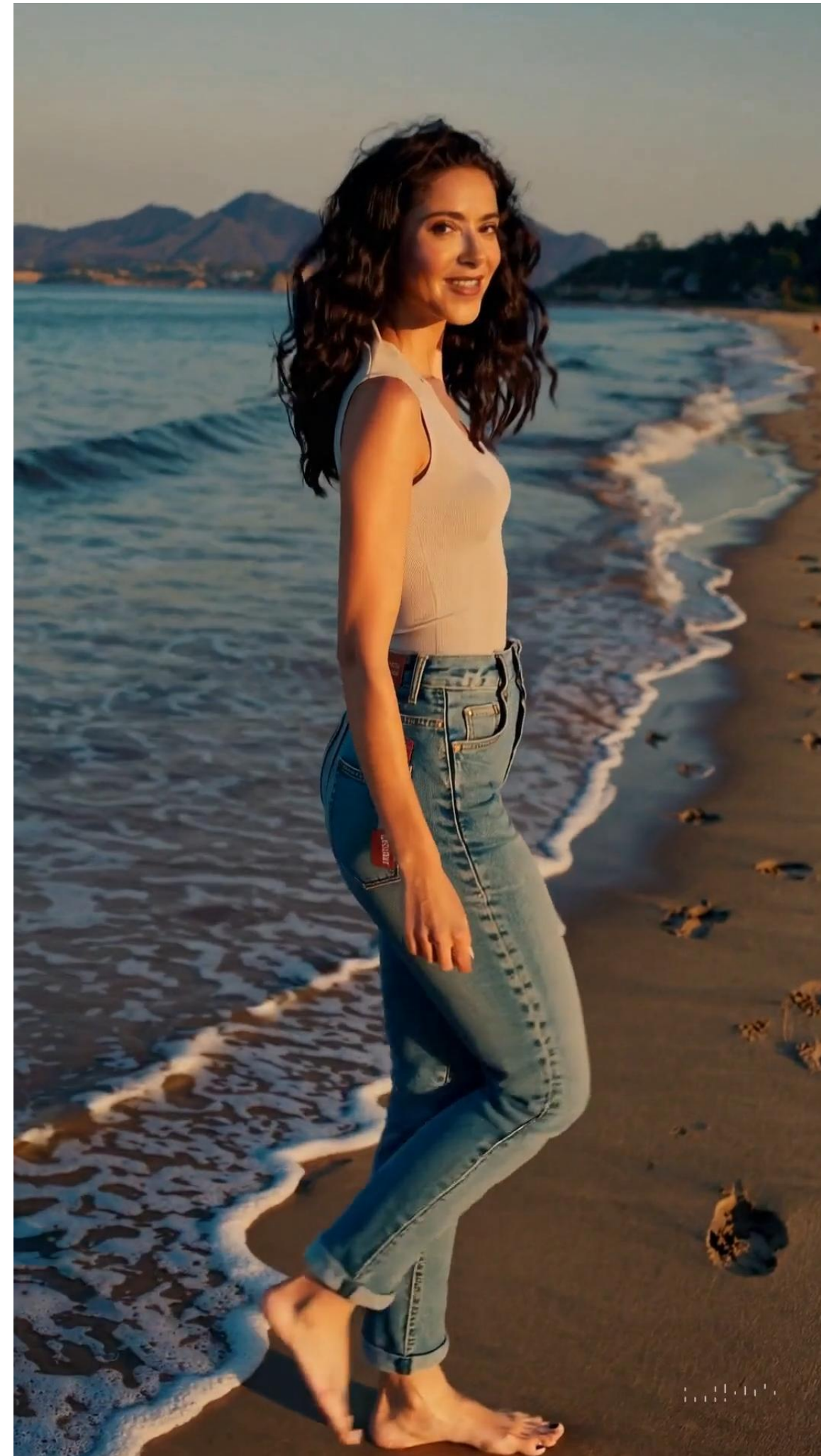


<https://sora.chatgpt.com/explore>



<https://app.runwayml.com/login>

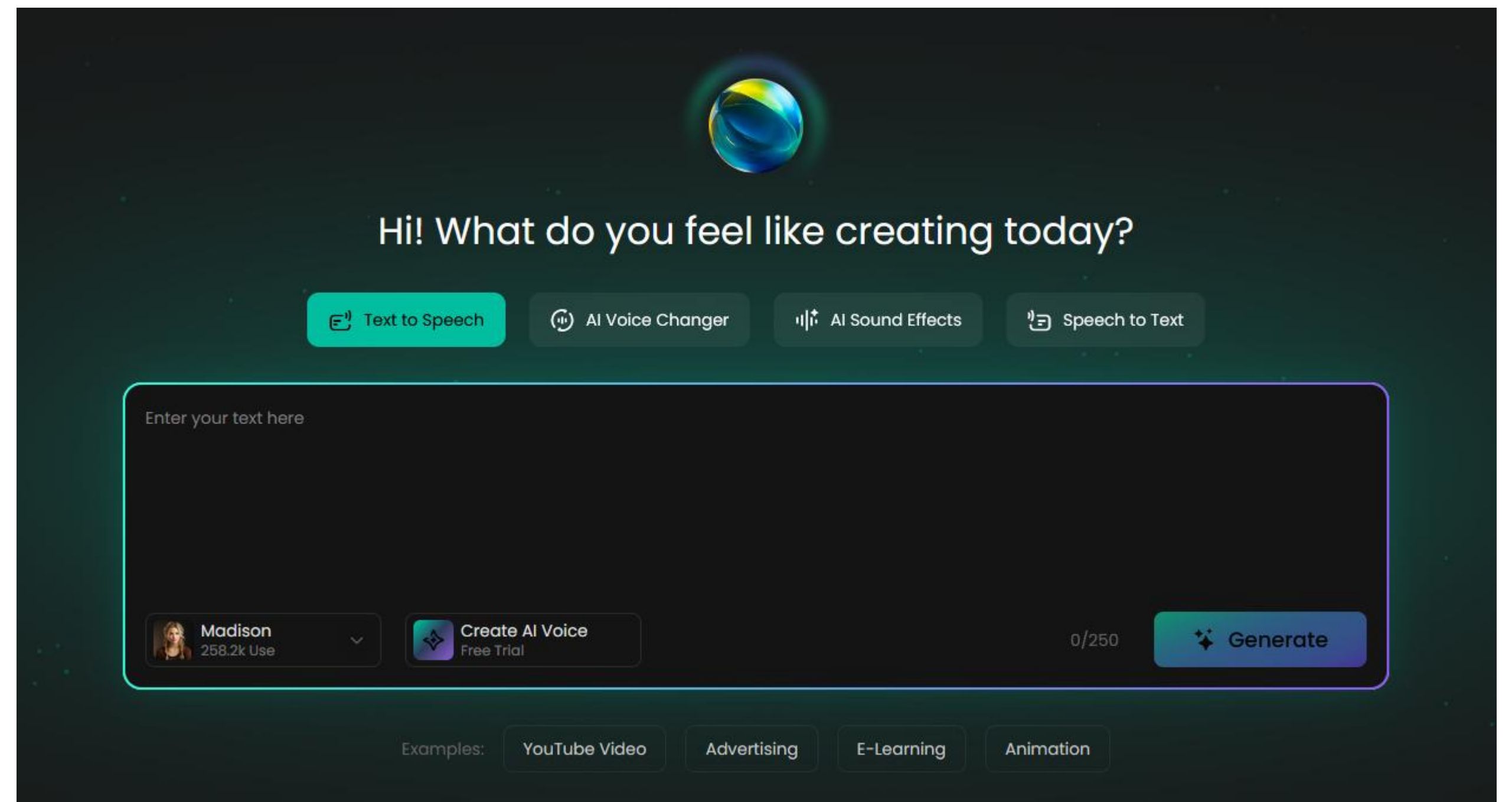
Výměna tváře (Salma Hayek)



<https://tools.dreamfaceapp.com/other-tools/face-swap>

Generovanie zvuku

- Výber z veľkej knižnice hlasov
- Vlastný hlas
- hlasová autentifikácia (banky, operátory)



<https://www.stvr.sk/televizia/archiv/14356/533256#1834>



<https://finevoice.fineshare.com/>

Útoky

Italian Defence Minister AI Voice clone

This vishing example is really interesting as it leverages voice cloning technology.

Italian businessman Massimo Moratti got scammed for \$1,04 million from an AI-powered vishing attack.

The attack targeted prominent business figures, from Giorgio Arman to Prada co-founder, as well as Massimo Moratti. Moratti is the former owner of the Inter Milan soccer club, a wealthy target.

The pretext for the attack was one we already saw in France years ago. The attacker impersonated the Italian defence Minister.

He pretended to need urgent external funding for the release of kidnapped Italian journalists in the Middle East.

The twist here is that they used voice cloning technology to reinforce their pretext and trick their targets.

Slovensko

Sociálnymi sieťami kolujú falošné videá s Pellegrinim. Prezidentská kancelária hovorí o podvode, chce zakročiť

TASR ta3 ta3

2.7.2024 16:16

Na internete sa objavili podozrivé videá, na ktorých vystupuje prezident. Ide o takzvané deepfake videá vytvorené umelou inteligenciou.



Foto: TASR/Kancelária prezidenta SR

techbyte

DomovTechRecenzieVedaElektromobilitaDomácnosťGaming

Ministerstvo financií BIJE NA POPLACH: Potvrdili ďalší útok na Slovákov, mnohí už prišli o peniaze

Internetom sa začal šíriť podvod, ktorý zneužíva ministra financií SR a známeho moderátorku TV JOJ. Ide o deepfake video vygenerované AI.

Lucia Bihuncová

17. júla 2025

Zdieľať

fX

2 min

World / Asia

Finance worker pays out \$25 million after video call with deepfake ‘chief financial officer’

By Heather Chen and Kathleen Magramo, CNN
2 min read · Published 2:31 AM EST, Sun February 4, 2024

fX



Vishing Energy Firms and next-gen CEO fraud

In 2019, a UK-based energy firm was scammed out of \$243,000 with a vishing attack.

The target was a UK executive. The attackers seem to have used an AI software to produce a clone of the boss of the German parent company’s voice. With this borrowed authority, they asked for a transfer of \$243,000 to a Hungarian supplier.

The money was supposed to be refunded very quickly but of course, the funds were laundered through different banks in different countries and never to be seen again.

A similar attack, targeting an unnamed bank, yielded a \$35 million loss. Attackers used AI voice cloning to impersonate a company director, convincing a bank manager to transfer \$35 million during a fake acquisition process.

This is the next generation of the CEO fraud: small technical improvements that increase the yield of tried and tested scam.

Zneužívanie multimodálnych LLM

- profily na sociálnych sieťach (zárobková činnosť, diskreditácia, menenie verejnej mienky)
- odpovedanie na inzeráty a ťahanie osobných informácií
- fishing, vishing, poisoning, ...
- detekcia generovaného obsahu
- regulácia obsahu (Európska komisia, sociálne siete)

Zneužívanie rozpoznávania tváre a hlasu

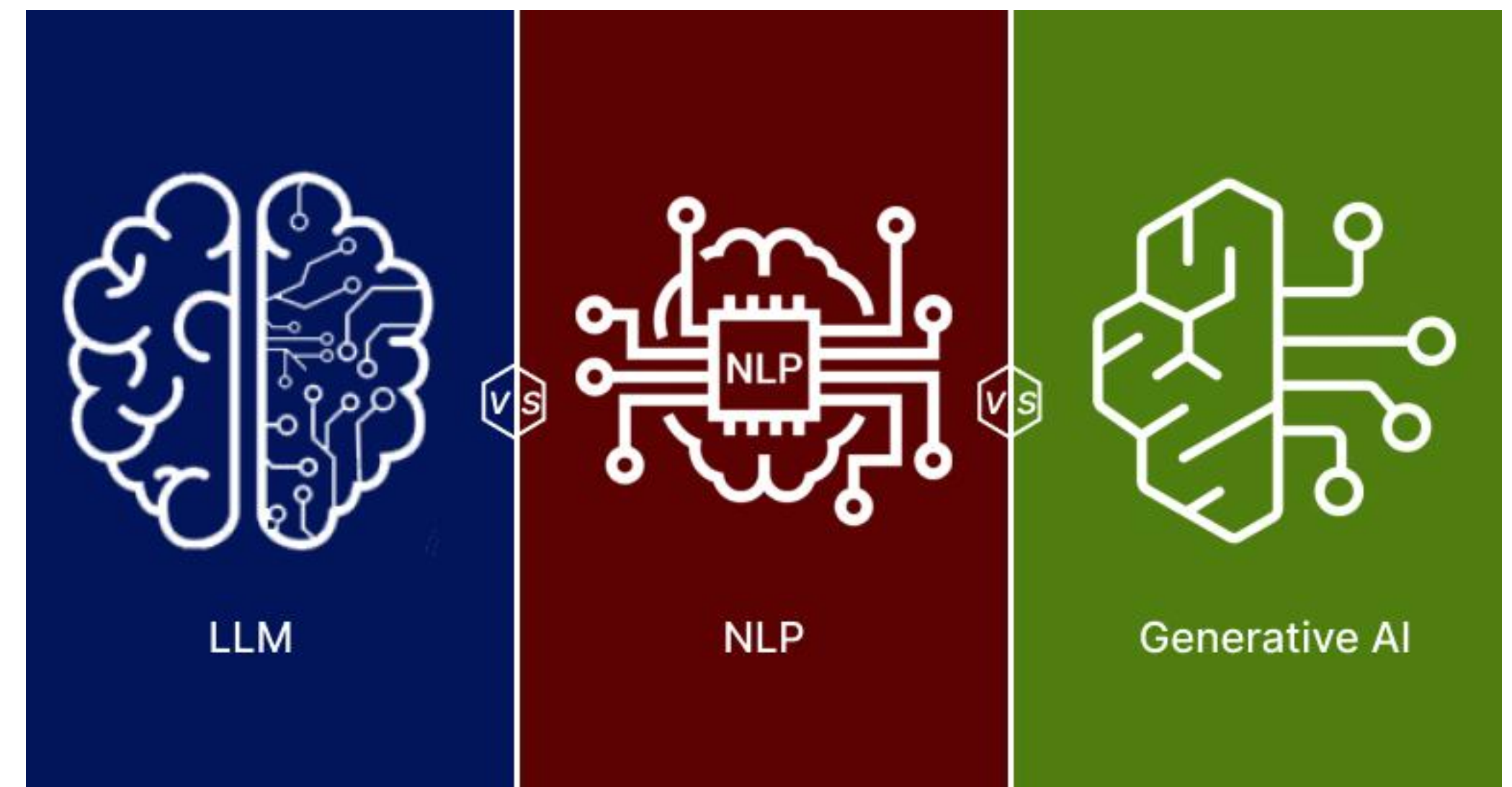
- meta smart glasses – kamera rozpozná tvár a cez mikrofón podáva informácie
- rozpoznávanie tváre (zámky, mobilné telefóny, hĺbka)
- hlasová autentifikácia

Odkazy k webovým stránkam a aplikáciám

- https://www.youtube.com/shorts/bVfDa_In2cQ
- <https://www.youtube.com/watch?v=oxXpB9pSETo>
- https://www.instagram.com/vivat_slovakia/
- <https://www.instagram.com/madeinslovakai/>
- <https://chatgpt.com/>
- <https://grok.com/>
- <https://sora.chatgpt.com/explore>
- <https://app.runwayml.com/login>
- <https://tools.dreamfaceapp.com/other-tools/face-swap>
- <https://finevoice.fineshare.com/>

Záver

- Generatívna UI je veľký pomocník, ale aj nebezpečný
- Deep Fake: zvuk, obrázky, videá (od generatívnych sieti po prompty)
- Zneužívanie LLM a rozpoznávanie obrazov
- Šírenie informácií (médiá, školy, ...)



Ďakujem za pozornosť

