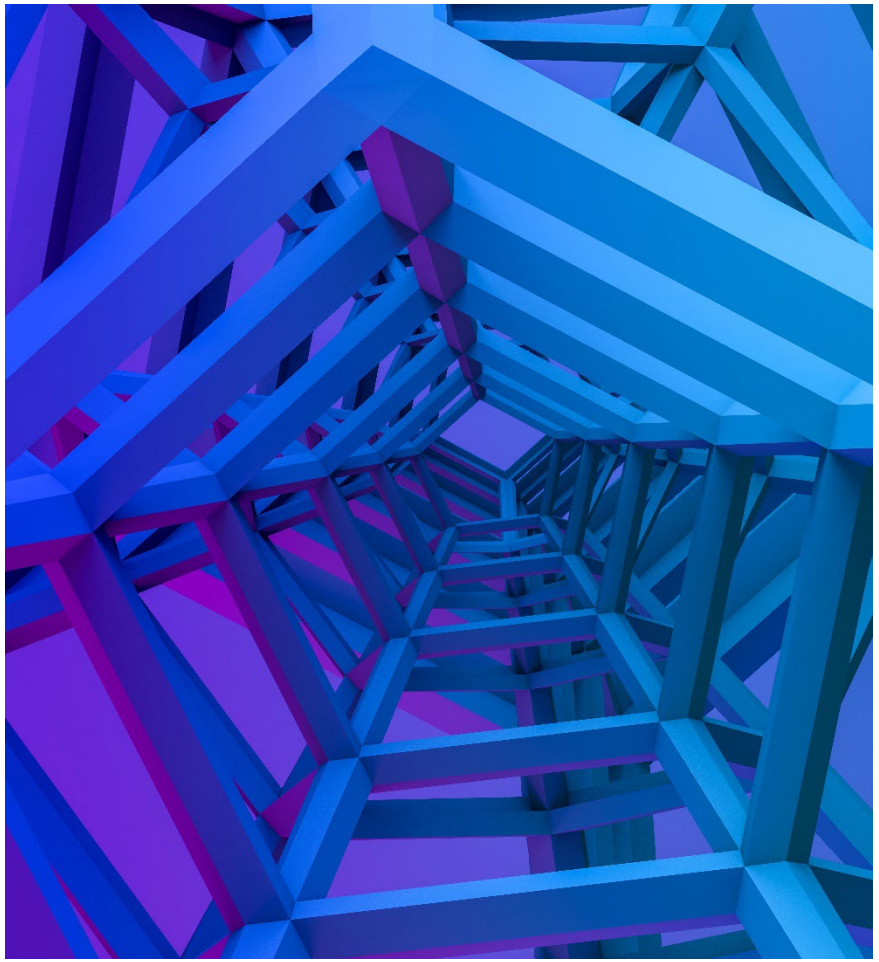
KPMG

Umělá inteligence a právo v praxi

Martin Čapek, KPMG Legal



Obsah

KPMG

01

AI Akt

Shrnutí zásadních informací o AI Aktu

Působnost nařízení

AI Akt

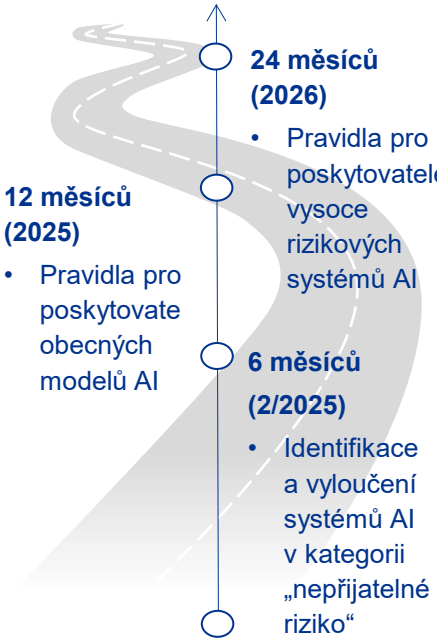
První soubor pravidel pro používání umělé inteligence.

Nařízení se vztahuje mimo jiné na poskytovatele a subjekty, které zavádějí/ poskytují systémy AI nebo obecné modely AI.

Klasifikace AI systémů

AI Akt využívá přístup založený na hodnocení rizik (risk-based approach). Je tedy důležité AI systémy klasifikovat (každá kategorie představuje konkrétní sadu povinností, kterou musíte splnit).

Implementace AI Aktu



12 měsíců (2025)

- Pravidla pro poskytovate obecných modelů AI

24 měsíců (2026)

- Pravidla pro poskytovatele vysoce rizikových systémů AI

6 měsíců (2/2025)

- Identifikace a vyloučení systémů AI v kategorii „nepřijatelné riziko“

Platnost AI Aktu – srpen 2024

Sankce a dohled

Za nesplnění povinností stanovených v AI Aktu lze uložit pokuty až do výše:

7 % celosvětového ročního obratu za nedodržení zákazu systémů s nepřijatelným rizikem

3 % celosvětového ročního obratu za nedodržení povinností poskytovatelů a „uživatelů“.

1 % celosvětového ročního obratu za poskytnutí nesprávných, neúplných nebo zavádějících informací.

KPMG

02

Digitální Omnibus

Digitální Omnibus k AI Aktu

- **Cíl:** zjednodušit implementaci AI Aktu a podpořit inovace při zachování ochrany práv
- Jasně stanovený harmonogram pro high-risk AI – **odklad**:
  - **2. prosince 2027** – samostatné high-risk systémy
  - **2. srpna 2028** – AI v regulovaných produktech
- **Označování AI generovaného obsahu** (watermarking) – odklad na **2. prosince 2026**
- **Zákaz AI pro generování nevyžádaného explicitního obsahu** (tzv. „nudification apps“)
- **Zjednodušení** pro podniky:
  - rozšíření výhod i na small mid-caps
  - omezení duplicity mezi AI Akt a sektorovou regulací (např. product safety)
- **Podpora inovací**: širší přístup k regulatory sandboxům (vč. EU-level sandboxu)
- **Posílení dohledu**: silnější role AI Office (zejména pro GPAI a platformy)
- Na začátku května dosažena **politická shoda**, následuje **formální přijetí**
- Týká se nejen poskytovatelů, ale i uživatelů

KPMG

03

Rizika AI

AI Akt je pouze špičkou ledovce

Mnohé společnosti se domnívají, že v souvislosti s umělou inteligencí by se měly zajímat pouze o AI Akt. To je však mylná představa. Nežijeme v právním vakuu.

01 GDPR

02 Autorské právo

03 Speciální regulace pro konkrétní sektory

04 DSA

05 Kyberbezpečnostní předpisy

... a mnohem více

Rizika, výzvy a etika

efektivita,
inovace,
dostupnost,
nové přístupy…

zkreslení a předsudky (bias),
soukromí,
autorská práva,
přílišný spoleh na výstupy,
únik dat…

Právo a etika jako balanční nástroj

Diskriminace a AI (Bias in AI)

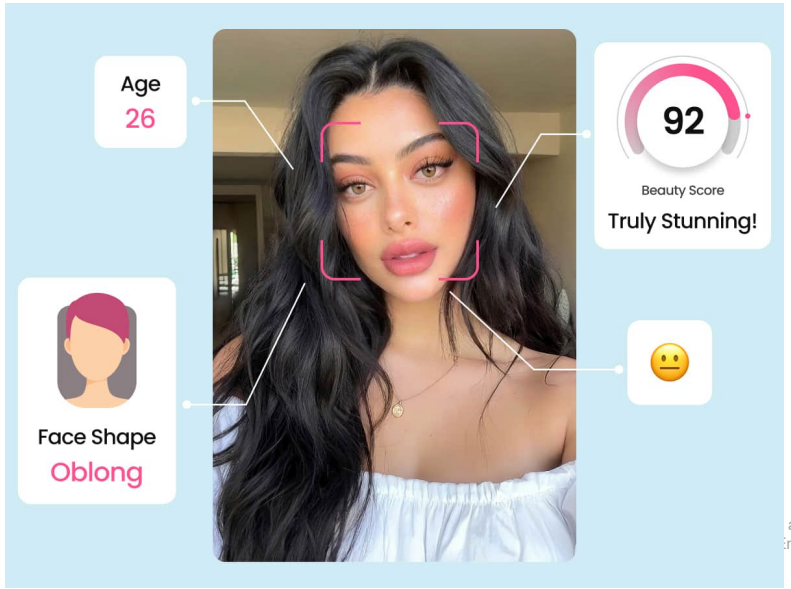
Amazon a náborový AI nástroj

AI nástroj se učil dle CV a vybíral vhodné kandidáty, jelikož se přihlásilo více mužů, bral to jako rozhodné stanovisko a penalizoval CVs, které obsahovaly slovo „žena“.

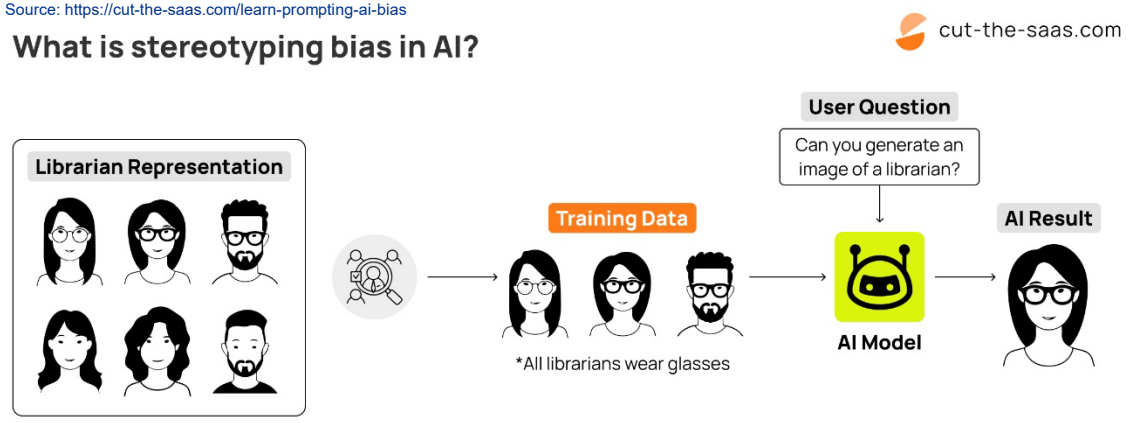
Beauty.AI – soutěž krásy hodnocená AI

Soutěž využívala algoritmy, které výrazně preferovaly bílou tvář.

Source: https://www.beautyplus.com/face-shape-detector/pretty-scale



Source: https://cut-the-saas.com/learn-prompting-ai-bias

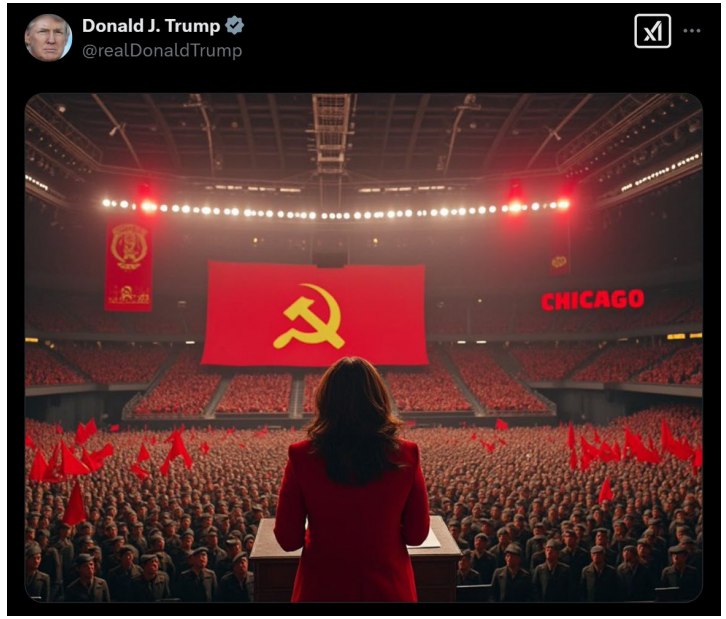


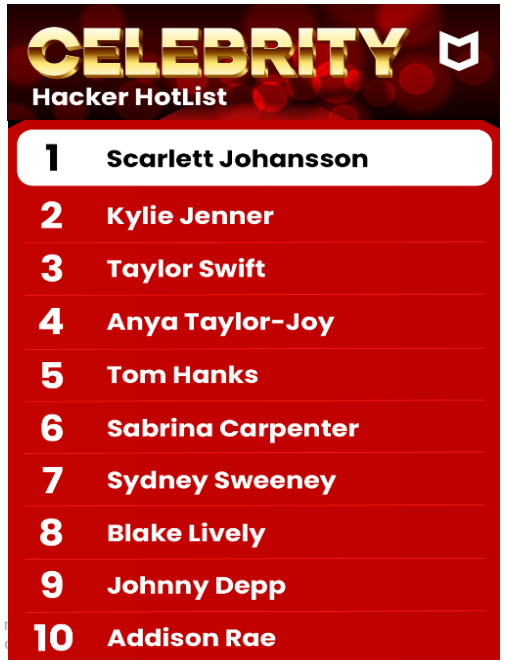
Stereotype bias occurs when certain characteristics are unfairly generalized to a group based on limited observations.

In this case, the training data shows all librarians wearing glasses, leading the model to reinforce the stereotype by consistently depicting librarians with glasses.

Deepfake

- = falešné obrázky, video, audio vytvořené **AI**
- **Dezinformace**
- Krádež identity
- **Social engineering** = manipulace s lidmi
- Poškození reputace





Copyright

Soudy se zabývají otázkou, zda může umělá inteligence mít autorská práva → celosvětově platí, že autorská práva mohou náležet **pouze fyzické osobě**

ČR

- Na podzim roku 2023 vydal Městský soud v Praze rozhodnutí ve věci určení autorství grafických děl vytvořených umělou inteligencí na základě zadání žalobce.
- Žaloba byla zamítnuta, protože nebylo prokázáno, že by žalobce byl autorem díla (jelikož bylo vytvořeno umělou inteligencí, a nikoli fyzickou osobou).

Like Company v Google (SDEU – 2026)

- Zveřejňování části podobných článků skrze chatbota – sdělování veřejnosti?
- Rozmnožování v rámci LLM tréninku
- Uplatnění TDM výjimky
- Když je v promptu obsažena část článku, dochází skrze output k rozmnožování ze strany AI poskytovatele? Přeshraniční uplatnění autorského práva EU?

zdroj: https://jolt.law.harvard.edu/digest/zarya-of-the-dawn-how-ai-is-changing-the-landscape-of-copyright-protection

- Komiks vytvořen za použití genAI
- **Americký úřad pro autorská práva** udělil autorská práva na text a uspořádání komiksu, ale **ne na samotné obrázky** vytvořené AI

USA

A Single Piece of American Cheese

- AI-generovaný obraz od Kenta Keirseyho (AI nástroj *Invoke*)
- Keirsey doložil svůj lidský tvůrčí vstup
- Invoke AI, Inc. získala autorská práva k obrázku

zdroj: https://news.artnet.com/art-world/invoke-snags-first-ai-image-copyright-2608219

Na co zapomínají uživatelé AI (podmínky služeb)

- Výstupy AI jsou „vaše“, ale:
  - nemusí být originální
  - nemusí být právně chráněné
- Data z konverzací mohou být použita pro **trénování modelů** (zejména u bezplatných / běžných účtů)
- Poskytovatel **nenese odpovědnost za použití výstupu** → odpovědnost nese uživatel

zdroj: https://www.terms.law/2024/08/24/who-owns-claudes-outputs-and-how-can-they-be-used/

Feature	ChatGPT Free	ChatGPT Plus ($20/mo)	API	Enterprise	Team
Output Ownership	✓ Yours	✓ Yours	✓ Yours	✓ Yours	✓ Yours
Training Data Usage	✗ Trains by default	⚠ Opt-out available	✓ Not trained on	✓ Never trains	✓ Never trains
Commercial Use	✓ Allowed	✓ Allowed	✓ Allowed	✓ Allowed	✓ Allowed
IP Indemnification	✗ No	✗ No	⚠ Limited	✓ Yes	⚠ Limited
Data Retention	30 days	30 days	0 days (API)	Custom	Custom
Rate Limits	Heavy limits	Moderate limits	Pay-per-use	Unlimited	High limits

Co to znamená pro Vás?

- AI používáte → nesete odpovědnost za výstup
- Práce s citlivými skupinami → vyšší právní i reputační riziko
- Vkládání dat do AI → GDPR riziko
- Výstupy AI nemusí být správné
- Nutnost interních pravidel (co smí a nesmí zaměstnanci používat)

Feature	Claude Free	Claude Pro ($20/mo)	Claude API	Claude Enterprise
Output Ownership	✓ Yours	✓ Yours	✓ Yours	✓ Yours
Training Opt-Out	✗ No opt-out	✓ Yes (in settings)	✓ Not trained on	✓ Never trained
Acceptable Use	⚠ Stricter limits	⚠ Stricter limits	✓ More flexible	✓ Custom policies
Rate Limits	Heavy limits	Moderate limits	Pay-per-token	Unlimited
Data Retention	90 days	90 days	0 days	Custom
Commercial Use	✓ Allowed	✓ Allowed	✓ Allowed	✓ Allowed

KPMG

04

Doporučení

Práce s AI nástroji – na co myslet?

Rozhodnutí o využití

- Využívejte AI tam, kde přináší **reálnou hodnotu**
- Zvažujte **přínosy i rizika** jejího použití
- Pracujte pouze se **schválenými nástroji**
- Vnímejte AI jako **podpůrný nástroj**, nikoli náhradu práce

Použití AI

- Výstupy vždy **kriticky ověřujte**
- **Nespoléhejte** se pouze na AI výstup
- **Ověřujte** zdroje a pracujte s kontextem
- Dodržujte **právní a etické zásady**
- **Chraňte citlivá data** a informace

Odpovědnost za výstup

- **Konečné rozhodnutí** zůstává **vždy na Vaší straně**
- Zachovejte **vlastní odborný úsudek**
- Zvažujte **dopady** své práce
- Použití AI komunikujte **transparentně**

Děkuji za pozornost!

Martin Čapek
mcapek@kpmg-cz
Advokát
KPMG Legal