



IUSTORIA
Advokátní kancelář

AI Act v praxi:

Co musí vědět každá česká firma

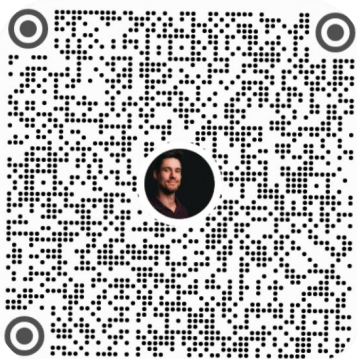
Mgr. Gabriel Kožík


Advokát | AI nadšenec a lektor

www.iustoria.cz

www.gabrielkozik.com

ai-podnikani.cz



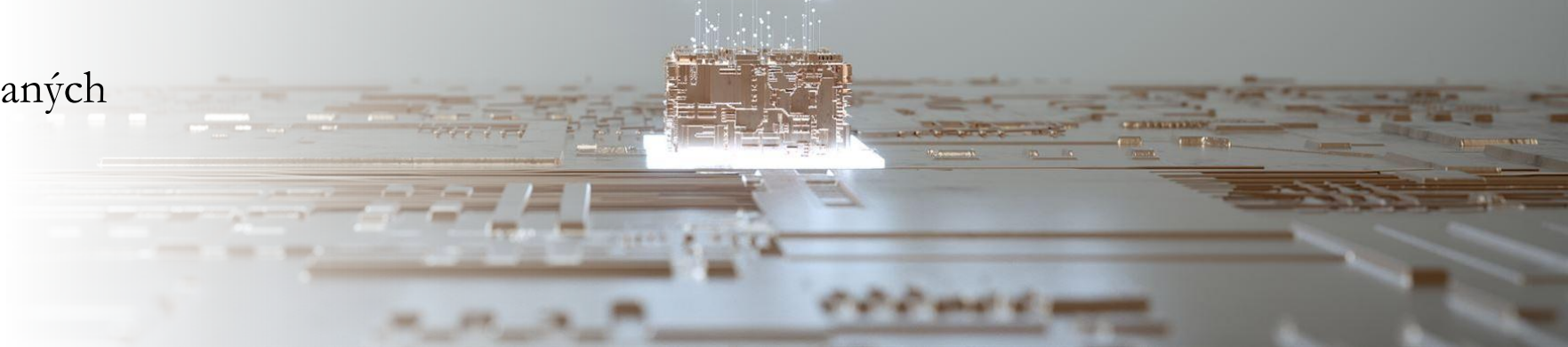
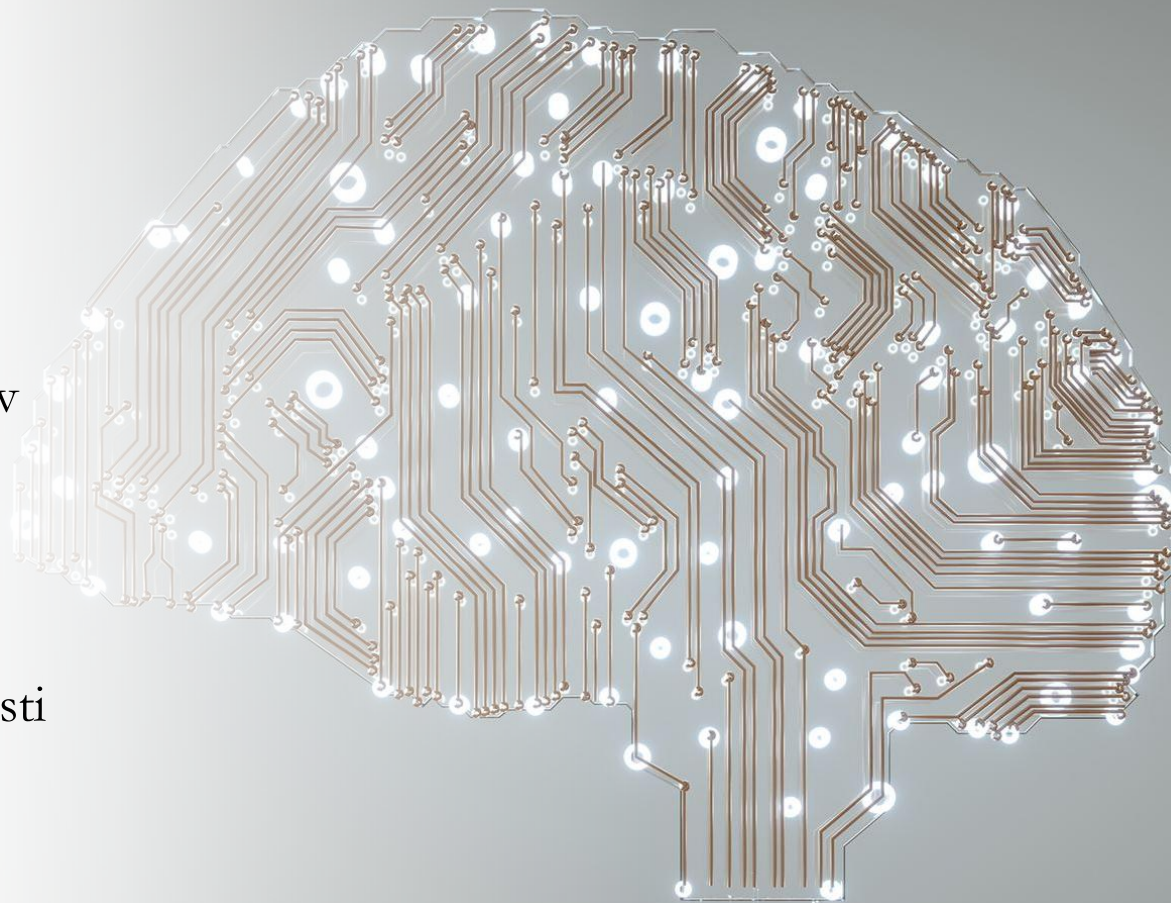


AI ve vašem podnikání: risk-based approach

- Nařízení EU č. 2024/1689
 - přímá použitelnost
 - postupné zavádění pravidel
- Bezpečnostní a zdravotní hrozby, etické otázky, rizika pro základní lidská práva
- Sledovat výkladová stanoviska MPO, ČTÚ, ÚOOÚ, ČAS (sandboxy)
 - Příprava prováděcího předpisu o AI v gesci MPO
- Čím dříve organizace pochopí principy, tím snazší bude implementace pravidel
- Odpovědnost nese koncový uživatel AI systému

AI je všude – pravidla také!

- Rostoucí trend v používání AI v byznysu
- Účel pravidel: důvěryhodná, bezpečná a transparentní AI a zdravé konkurenční prostředí
- Základem je gramotnost v oblasti AI (čl. 4)
 - týká se všech, kteří s AI v rámci organizace pracují
- Pravidelná revize vysoce rizikových systémů a zakázaných postupů



2024/1689: Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci) (Text s významem pro EHP) PE/24/2024/REV/1

NAŘÍZENÍ

EVROPSKÉHO PARLAMENTU A RADY (EU)

[2024/1689](#)

ze dne 13. června 2024,

kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. [300/2008](#), (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice [2014/90/EU](#), (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci)

(Text s významem pro EHP)

Článek 4

Gramotnost v oblasti AI

Poskytovatelé systémů AI a subjekty zavádějící AI přijímají opatření, aby v co největší možné míře zajistili dostatečnou úroveň gramotnosti v oblasti AI u svých zaměstnanců i u všech dalších osob, které se jejich jménem zabývají provozem a používáním systémů AI, s přihlédnutím k jejich technickým znalostem, zkušenostem, vzdělání a odborné přípravě a prostředí, v němž mají být systémy AI používány, a s ohledem na osoby nebo skupiny osob, na kterých mají být systémy AI používány.

AI Act: Ne každá AI je stejná



- Regulace dle míry rizika daného AI systému
 - v závislosti na účelu užití – zakázané, vysoce rizikové a s omezeným rizikem
- Nepříjemné a vysoké riziko: co to znamená?
 - use-case neslučitelný se základními právy vs.
 - use-case s potenciálně významným dopadem na zdraví, bezpečnost a základní práva
- Většina dostupných nástrojů má omezené riziko
 - hlavně informovat (typicky chatboti a „deepfake“)
 - Pozor však na účel využití daného nástroje!

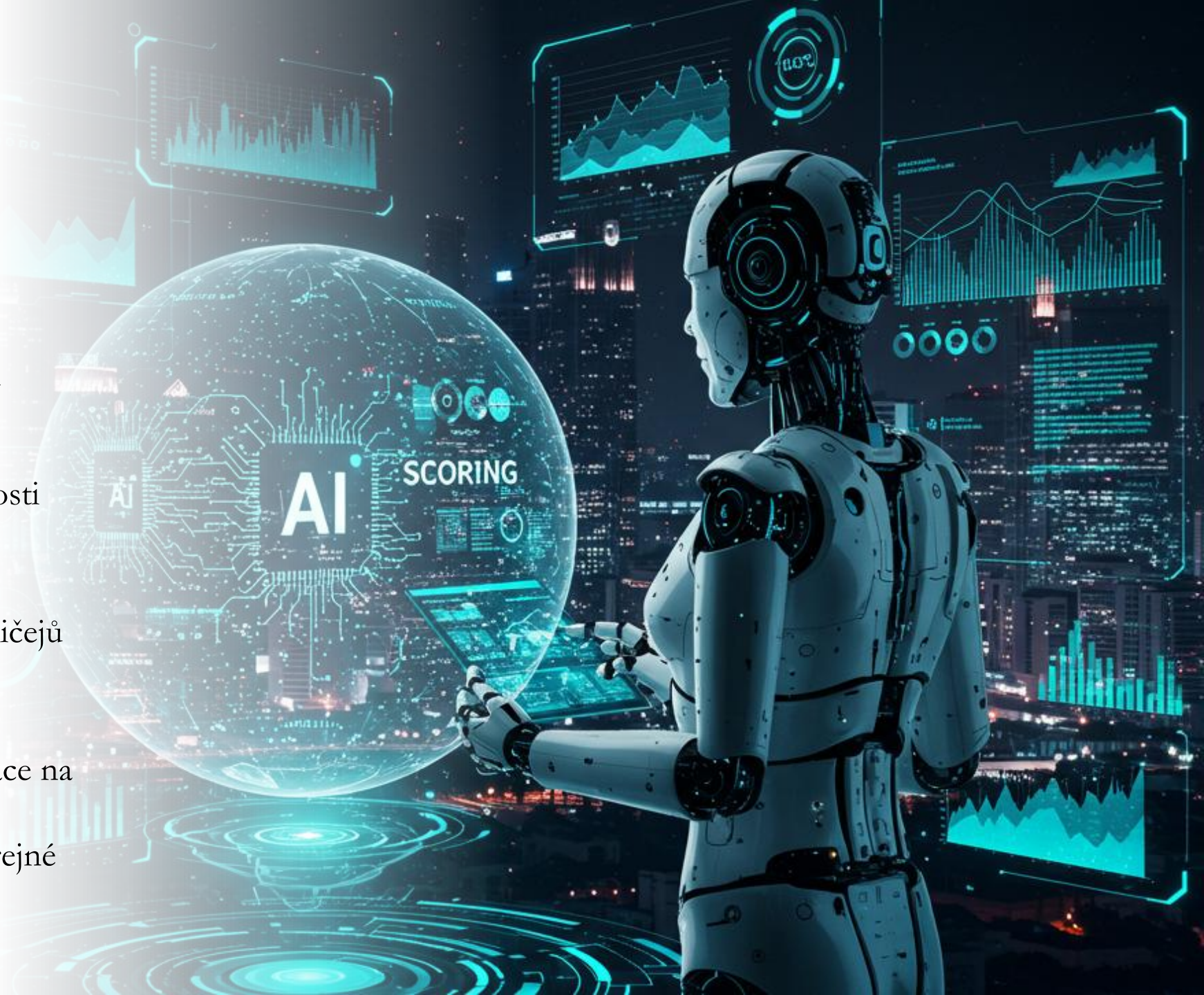



Příklady AI nástrojů a jejich rizika

- Generování textů – ChatGPT, Gemini, Copilot (zahrnuje i chatbota)
 - Riziko: omezené, v zásadě pouze interní = únik informací, ztráta důvěry klientů, poškození značky
 - Povinnost: transparentnost vůči veřejnosti – výstup z AI musí být označený jako „generovaný AI“
- HR nástroj pro třídění CV nebo systém v eshopu pro hodnocení úvěruschopnosti
 - Riziko: vysoké, diskriminace, bias
 - Povinnost: human-in-the-loop, kontrola, logování, evidence dat, AI compliance, školení
- Social scoring nebo manipulace v rozhodování (jakýkoliv nástroj s tímto cílem)
 - Riziko: nepřijatelné

AI systémy s nepřijatelným rizikem

- Zneužívání znevýhodněných osob či používání klamavých technik s cílem ovlivnit rozhodování
- Systémy pro předvídání trestné činnosti založené na profilování osob
- Systémy sociálního kreditu
- Vytváření databází rozpoznávání obličejů
- Automatizované hodnocení emocí a chování ve školách a na pracovištích
- Biometrická identifikace a kategorizace na dálku
- Několik výjimek platí pro orgány veřejné moci či z bezpečnostních důvodů





AI systémy s vysokým rizikem

- S vysoce rizikovým dopadem na zdraví, bezpečnost a základní práva
- Zdravotnické prostředky / Kritická infrastruktura / Vzdělávání a odborná příprava / Zaměstnanost, řízení pracovníků a přístup k SVC / Přístup k základním soukromým a veřejným službám / Vymáhání práva, migrace, azyl a správa hranic / Správa spravedlnosti a demokratických procesů
- Většina povinností od 2. 8. 2027
 - Systém řízení rizik / human-in-the-loop / monitoring / správa vstupních dat / uchovávání logů / FRIA / **transparentnost** vůči závadějícím subjektům

The background of the slide is a complex, abstract digital pattern. It features a grid of binary digits (0s and 1s) in various shades of blue and white. Overlaid on this grid is a network of glowing blue lines and dots, resembling a neural network or a data flow diagram. The overall aesthetic is high-tech and futuristic.

Transparentnost u vysoce rizikové AI

Jasně informace a interpretace výstupů

Provozovatelé musí uživatelům poskytovat srozumitelné informace, které umožňují správně interpretovat a používat výstupy AI systému.

Správné používání a specifikace

Návod zahrnující informace o účelu, přesnosti, předvídatelných rizicích pro zdraví, bezpečnost a FR, trénovacích datech, způsobu interpretace výstupů a další.

Změny, dohled a logování

Musí být zajištěno informování o změnách systému, lidský dohled, požadavky na zdroje a logování činnosti systému.

AI s omezeným rizikem

- Pro většinu dnešního use-case
 - chatbot na e-shopu nebo pro zaměstnance / generování textů a audiovizuálního obsahu pro marketing / vyhodnocování uživatelského chování bez sběru osobních údajů (jinak pozor na GDPR) /
- Hlavní povinnost
 - transparentnost – informovat o využívání AI
 - označovat AI obsah
- Co je to „deepfake“ (čl. 50)
 - pro marketing legální, ale opatrně - pozor na GDPR a ochranu spotřebitelů (klamavé praktiky..)



Jak bys definoval deep fake?




Zobrazit uvažování ▼

Deepfake je termín označující manipulativní technologii, která využívá umělou inteligenci (AI), konkrétně hluboké učení (deep learning), k vytváření falešného, avšak vysoce realistického digitálního obsahu. Nejčastěji se jedná o videa, obrázky nebo zvukové nahrávky, ve kterých jsou obličeje, hlasy nebo celé postavy osob nahrazeny či pozměněny tak, aby působily autenticky.

Jak deepfake funguje?

Tvorba deepfake obvykle zahrnuje trénování algoritmů umělé inteligence, jako jsou generativní adverzní sítě (GANs). Tyto sítě se skládají ze dvou částí:

- **Generátor:** Snaží se vytvořit co nejpřesvědčivější falešný obsah (např. video s cizím obličejem).

 Zadejte pokyn pro Gemini



Deep Research



Canvas



60) „deep fake“ obrazový, zvukový nebo video obsah vytvořený nebo manipulovaný umělou inteligencí, který se podobá existujícím osobám, objektům, místům subjektům či událostem a který by se dané osobě mohl nepravdivě jevit jako autentický nebo pravdivý;

4. Subjekty zavádějící systém AI, který vytváří obrazový, zvukový nebo video obsah představující tzv. „deep fake“ nebo s ním manipuluje, musí zveřejnit, že obsah byl uměle vytvořen nebo s ním bylo manipulováno. Tato povinnost se nevztahuje na případy, kdy je použití povoleno zákonem k odhalování trestných činů, předcházení jim, jejich vyšetřování nebo jejich stíhání. Pokud je obsah součástí zjevně uměleckého, tvůrčího, satirického, fiktivního či obdobného díla nebo programu, povinnosti týkající se transparentnosti stanovené v tomto odstavci jsou omezeny na zveřejnění existence takového vytvořeného nebo zmanipulovaného obsahu vhodným způsobem, který nebrání zobrazení nebo užívání díla.

1. Zakazují se následující postupy v oblasti AI:

a) uvádění na trh, uvádění do provozu nebo používání systémů AI, které využívají podprahových technik mimo vědomí osob nebo záměrně manipulativních či klamavých technik, jejichž cílem nebo důsledkem je podstatné narušení chování osoby nebo skupiny osob tím, že znatelně zhoršují jejich schopnost učinit informované rozhodnutí, což vede k tomu, že přijmou rozhodnutí, které by jinak neučinily, což dotčené osobě, jiné osobě nebo skupině osob způsobuje nebo by s přiměřenou

- Ochrana dat a GDPR
- Nevkládejte osobní údaje do AI
- Anonymizujte/pseudonymizujte
- Čtěte podmínky AI nástrojů
- Lidský dohled, i když to není skriktně vyžadováno (omezené riziko) – pozor na odpovědnost za výstupy

4 cesty úniku firemních dat

- 1. Shadow IT a neproškolení zaměstnanci
 - Nedostatečné organizační zajištění
 - Řízený přístup k aplikacím, proškolení, prověření dodavatelů
- 2. Paměť modelů – trénink dat
 - Spotřebitelské vs. Enterprise licence
- 3. Cílené útoky třetích osob
 - Prompt injection, data poisoning, nezabezpečené výstupy
 - Agentní přístup – ChatGPT / Perplexity Comet
 - LLM firewally, řízený přístup k aplikacím
- 4. Kompromitace platformy
 - Útoky na dodavatele SW

• Pro další informace sledujte můj blog
<https://www.gabrielkozik.com/blog>



Výtvor AI – Čí jsou práva?

- Autorská práva a AI
- AI jako autor?
 - MSP 10 C 13/2023-16
 - lidský faktor / výsledek kreativní lidské činnosti (USA: Thaler v. Perlmutter)
- Riziko porušení cizích práv
- Co vytvoříte není „váše“ – konkureční boj?
- Důležitá je kontrola nad výstupy
- Pozor na licencování – marketingové agentury
- Využívejte smlouvy – zákaz zpracovávat data ke generování obsahu pomocí AI



Zjištění tréninku na autorských datech a jejich ochrana

- Klíčové je přijetí Kodexu zásad umělé inteligence pro obecné účely

- Google, Microsoft, OpenAI, Anthropic a další

<https://digital-strategy.ec.europa.eu/cs/policies/contents-code-gpai>

- Nedostatek transparentnosti
 - Zjištění, zda byl AI model trénován na autorských datech, je složité
 - Dosud byl trénink zcela netransparentní, přijetím Kodexu se to může změnit
- Analýza výstupů (využití memorizace)
 - Cílené dotazování se za účelem pokusu zrekonstruovat části autorských děl
- Uplatnění opt-out
 - Strojově čitelným způsobem: robots.txt
 - Metadata v souborech
 - Smluvní a licenční podmínky

Obecné modely AI (GPAI)

Široké využití AI modelů

Obecné AI modely poskytují základ pro různé aplikace a usnadňují mnoho typů úkolů v různých odvětvích.

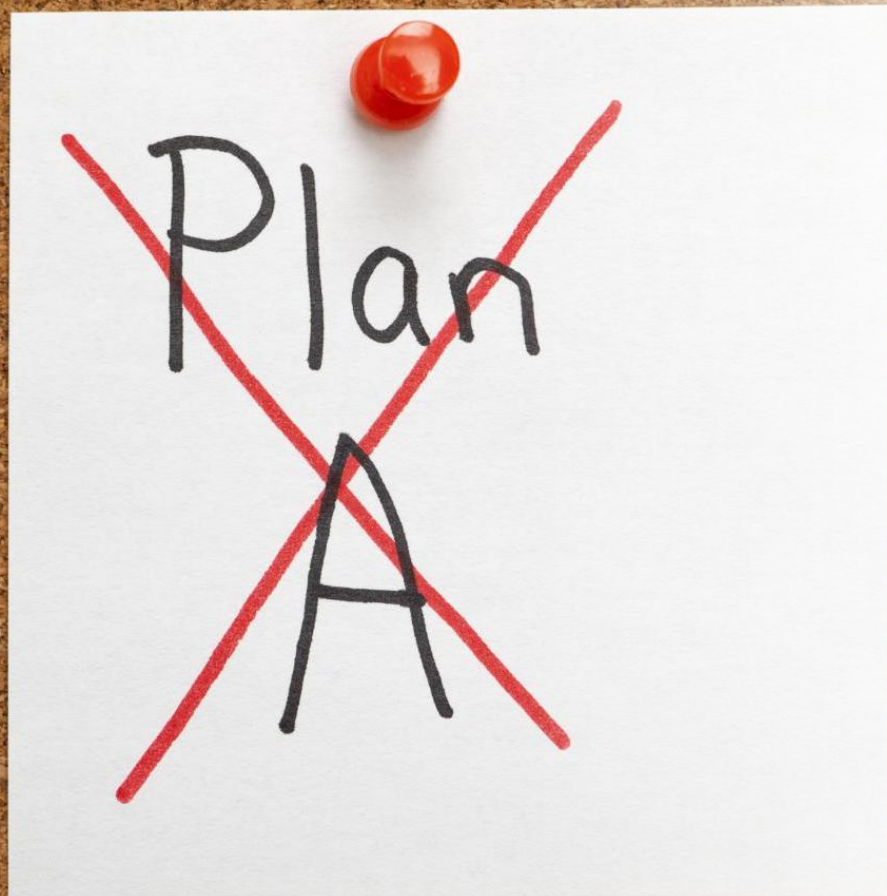
Transparentnost a práva

Modely musí splňovat požadavky na transparentnost, respektovat autorská práva (opt-out režim) a zveřejňovat souhrn tréninkových dat.

Bezpečnost a řízení rizik

Vysoce výkonné AI modely vyžadují testování, řízení rizik, hlášení incidentů a silná opatření kybernetické bezpečnosti.





Co si odnést a co dělat zítra?

- Informujte se o novinkách
- Čtěte podmínky AI nástrojů (sumarizujte pomocí AI)
- Buďte transparentní v komunikaci
- Chraňte citlivá data
- Ověřujte výstupy AI
 - Moffatt v. Air Canada
- Využívejte služeb profesionálu a školení

Klíčové státní orgány a zdroje informací

- MPO – gestor implementace AI Aktu v ČR
 - ČTÚ – dodržování pravidel v oblasti tržní regulace
 - ÚNMZ – udělování certifikace pro posuzovatele shody AI systémů
 - ČAS – správa regulatorního sandboxu
-
- <https://mpo.gov.cz/cz/podnikani/digitalni-ekonomika/umela-inteligence/>
 - <https://asociace.ai/>
 - <https://digital-strategy.ec.europa.eu/cs/policies/contents-code-gpai>



Q&A

Průvodní materiály na <https://ai-podnikani.cz>



JEŠTĚ JEDNA VĚC

Prosím, věnujte chvíli vyplnění formuláře
pro zpětnou vazbu k této přednášce.

Najdete ho v aplikaci **EVENTEE**.

Týden ↪ inovací 2025

