

„TAHÁK DO KAPSY“: RIZIKA VYUŽÍVÁNÍ AI

1.

Riziko zneužití dat

Do AI nevkládáme nic, co bychom neřekli cizí osobě.

- Osobní údaje (jméno, datum narození, adresa)
- Doklady a dokumenty
- Finanční údaje
- Firemní data a informace
- To, co nechceme zveřejnit

2.

Faktické chyby

Výstupy AI vždy ověřujeme ideálně z více zdrojů.

Mohou obsahovat nepravdivé nebo zavádějící informace.

To může být způsobeno tím, že se nám AI snaží maximálně vyhovět, nepřesně zadaným dotazem nebo chybnými daty, na kterých se AI učí.

3.

Deepfake, podvody

Deepfake: realistické falešné video, audionahrávka nebo fotografie skutečné osoby

To umožňuje:

- Sofistikované podvody
- Personalizovaný phishing
- Cílenou manipulaci veřejného mínění

4.

Závislost na AI

Při využívání AI budme opatrní. Její nadužívání může zhoršit například schopnost ověřovat si informace, rozpoznat podvod nebo myslet tvůrčím způsobem. Problémem může být také přílišné spoléhání na automatické rozhodování.