



# Máme se obávat umělé intelligence?

Magazín ■ Filip Brož

Umělá intelligence (AI) představuje významný pokrok v technologii, který má potenciál výrazně ovlivnit mnoho aspektů našeho života. Zároveň s tímto pokrokem však přicházejí i rizika a nebezpečí, která je třeba brát v úvahu. Asi víte, že poslední dva roky se pohybují v kyberbezpečnosti, a právě sběr osobních dat vidím jako klíčový.

**P**ojďme se však podívat i na jiná rizika, která časem budeme muset začít řešit. Jedním z nejčastěji diskutovaných rizik AI je ztráta pracovních míst. Automatizace a robotizace pracovních procesů mohou nahradit lidskou práci v mnoha odvětvích.

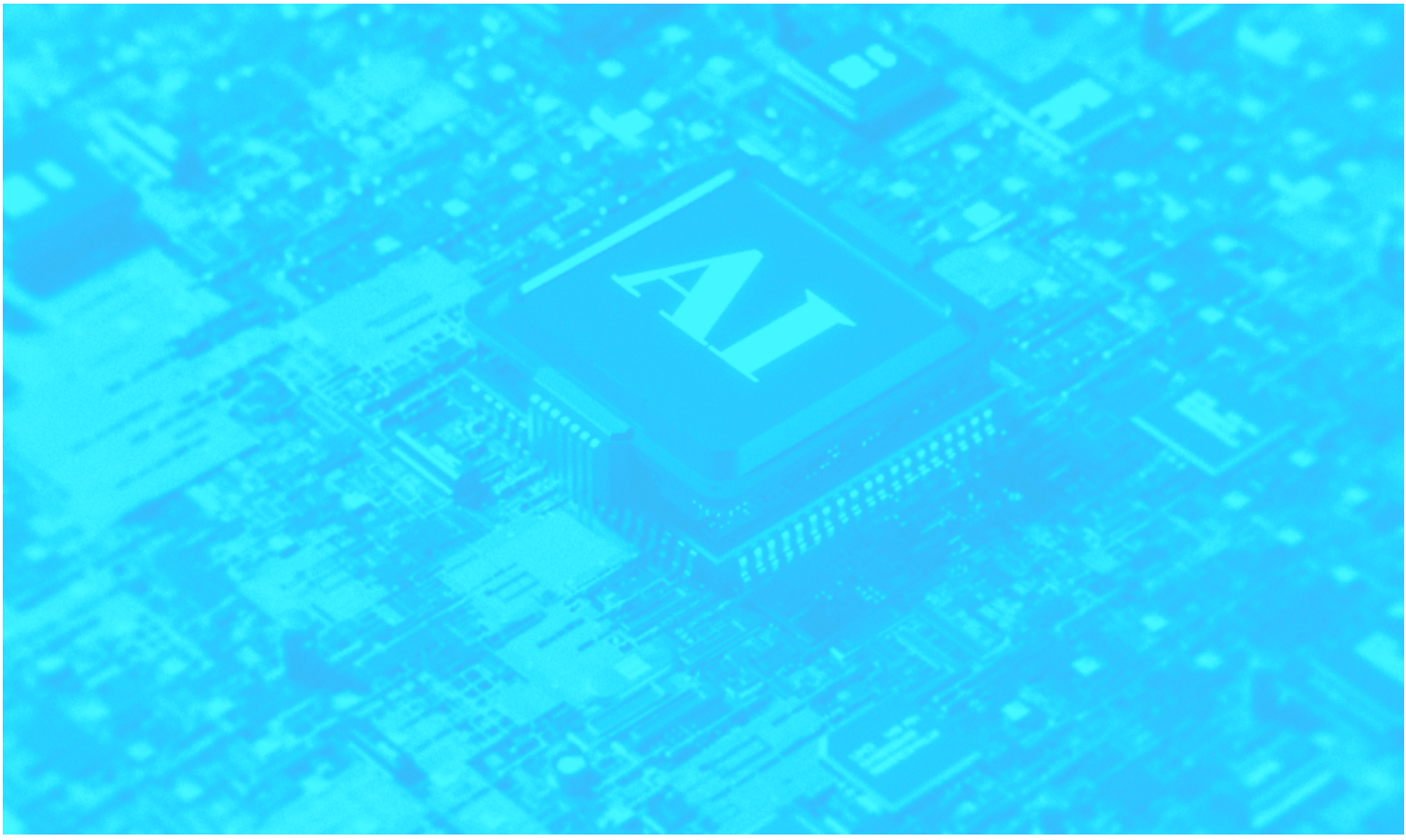
## PŘIJDETE O MÍSTO?

Například v průmyslu, logistice nebo administrativě mohou AI systémy vykonávat úkoly efektivněji a levněji než lidé. To může vést k masovým ztrátám pracovních míst a vyvolat sociální a ekonomické problémy, pokud nebudou přijata opatření na podporu rekvalifikace a tvorby nových pracovních příležitostí. Myslím si, že nebudu daleko od pravdy, že velmi brzy vzniknou pozice a kurzy, které budou lidi učit, jak s AI zacházet, jak správně používat ChatGPT nebo Gemini.

## ETICKÁ A MORÁLNÍ DILEMATA

AI přináší také mnoho etických a morálních otázek. Jedním z příkladů je rozhodování autonomních vozidel v krizových situacích. Jak by mělo auto řízené AI reagovat, když je nevyhnutelné, že dojde k nehodě? Který život má být upřednostněn? Další etické otázky se týkají použití AI v medicíně, kde může rozhodovat o diagnózách a léčebných postupech, což může mít přímý dopad na lidské životy.





Už teď můžeme vidět AI Elona Muska, jak řídí auta či taxíky Tesla. Mám doma Teslu a mohu říct, že autopilot od Tesly není jen „obyčejný“ autopilot. Opravdu se snaží vyhodnocovat dopravní situace a často mi zasáhne do řízení, když to nečekám, například při popojíždění v koloně, kdy mi tam někdo nečekaně hodí blinkr a vjede do pruhu. Auto ihned zareaguje.

### DISKRIMINACE A DATA

AI modely jsou tak chytré, jaká data jim poskytneme. Z toho důvodu vždy lidem říkám, ať opravdu přemýšlí, co do ChatGPT chatu píšou, jaké fotky si nechávají upravovat či kolik API povolení jim dáme. Už teď existují firmy a startupy, které se zabývají tím, co bude po životě, tzv. Griefbots. Stačí jim poskytnout přístup k vašemu telefonu, vzpomínkám, fotkám či zprávám a ihned můžete mít vedle sebe svůj klon, samozřejmě v podobně AI chatbota. A teď si představte, že se vám něco stane, třeba i to nejhorší – úmrtí. Vaše rodina může pak pomocí těchto firem vytvořit vaši kopii, a vy budete „žít“ dál. Je to už za hranou?

AI systémy se učí z dat, která jsou jim poskytnuta. Pokud jsou tato data neúplná nebo zaujatá, mohou být výsledky AI také zaujaté. To může vést k diskriminaci a nespravedlivému zacházení s určitou skupinou lidí. Příkladem může být AI používaná

při přijímání zaměstnanců, která může nevědomky preferovat určitý typ kandidátů na základě zkreslených dat.

### BEZPEČNOST A ZNEUŽITÍ

AI může být také zneužita pro nelegální a neetické účely. Hackeři mohou využít AI k vytvoření sofistikovaných kybernetických útoků, které je těžší odhalit a zastavit. AI může být také použita k vytváření deep fake videí a audionahrávek, které mohou být použity k šíření dezinformací, vydírání nebo poškozování pověsti jednotlivců a organizací.

Už teď umí ChatGPT vygenerovat phishingový email či jiný škodlivý kód, který stačí jen upravit a poslat dál. Hackeři mají mnohem méně práce. Už teď se na darknetu prodávají účty k ChatGPT s osobními daty. Jako u všeho, ChatGPT a AI může pomáhat i škodit zároveň. Opět to začíná u vašich dat. Přemýšlejte, než něco někam napíšete nebo požádáte o nějaké další „generování“ obsahu.

### ZTRÁTA SOUKROMÍ

Sběr a analýza velkého množství dat, na kterých jsou AI systémy založeny, představuje riziko pro soukromí jednotlivců. AI může být schopna analyzovat a predikovat osobní chování, což může vést k zneužití těchto informací například pro marketingové účely nebo sledování obyvatelstva.



Tato hrozba je zvláště relevantní v kontextu vládních a komerčních sledovacích systémů. Nechci si ani domýšlet, co vše nás v budoucnosti může čekat...

### AUTONOMNÍ ZBRANĚ

Jedno z nejnebezpečnějších potenciálních použití AI je v oblasti vojenské technologie. Autonomní zbraně, které jsou schopny samostatně rozhodovat o útocích, představují obrovské riziko pro globální bezpečnost. Takové systémy mohou jednat bez lidského zásahu, což zvyšuje riziko neúmyslných konfliktů a eskalace násilí.

Stačí si jen vzpomenout, co udělají s lidským chováním a názorem zmanipulované volby, byť o jen pár hlasů, či nějaká konkrétní situace, která se však nikdy nestala. Stále si vzpomínám na Facebook a incident Cambridge Analytica. Už tam fungovalo v praxi AI, ale rozhodně ne v takovém měřítku, jaký potenciál má dnes.

### ZTRÁTA KONTROLY

Nakonec je zde i riziko ztráty kontroly nad systémy AI. Pokud by se AI vyvinula do bodu, kdy by byla schopna sama sebe vylepšovat a učit se bez lidského dohledu, mohlo by dojít k situaci, kdy bychom nad ní ztratili kontrolu. Tento scénář, často diskutovaný v kontextu tzv. super inteligence, by mohl mít

Jedno z potenciálních použití je v oblasti vojenství. Autonomní zbraně, které jsou schopny samostatně rozhodovat o útocích, představují obrovské riziko.

nepředvídatelné a potenciálně katastrofální důsledky. Však si pusťte pár filmů, například Já robot.

### ZÁVĚR

AI představuje neuvěřitelnou příležitost pro lidstvo, ale zároveň přináší i značná rizika. Je důležité, aby vývoj a implementace AI byly prováděny s ohledem na etické, právní a sociální aspekty, aby byla minimalizována rizika a maximalizovány přínosy. V této souvislosti je klíčová spolupráce mezi vědci, vládami, průmyslem a společností, aby byl zajištěn bezpečný a spravedlivý rozvoj AI technologií.

Jak k tomu můžete přispět vy? Stačí selský rozum. Zkuste aplikovat pravidlo „zero trust“ aneb nikomu a ničemu nevěřte. Vždy si vše ověřte a přemýšlejte, co děláte a kam co píšete. 