IUSTORIA
Advokátní kancelář

telefon: (+420) **777 366 857**
email: info@iustoria.cz
web: www.iustoria.cz

Generujete s AI? Těchto 5 právních rizik vás v Česku může stát miliony.

Úvod: Vítejte v nové realitě

Generativní umělá inteligence zažívá boom. Nástroje jako ChatGPT, Midjourney nebo Claude se z technologické hračky staly běžnou součástí firemních procesů i každodenního života. Pomáhají psát e-maily, tvořit marketingové kampaně a analyzovat data. Víte ale, jaká právní úskalí se skrývají za jedním kliknutím na tlačítko „Generovat“?

---

1. Váš výtvor z AI? Podle českého práva na něj nemáte autorská práva.

Tento fakt je pro mnohé šokující, ale česká justice má jasno. Obsah, který pro vás vygeneruje umělá inteligence, není vaším autorským dílem. Tento princip vyplynul z přelomového rozsudku Městského soudu v Praze z října 2023 (č. j. 10 C 13/2023-16). Soud žalobu primárně zamítl, protože žalobce neprokázal, že daný pokyn vůbec zadal. Nad rámec toho však soud vyslovil přelomový závěr: podle českého autorského zákona může být autorem pouze **fyzická osoba** a dílo musí být **„jedinečným výsledkem tvůrčí činnosti autora“**.

Soud argumentoval, že samotný textový příkaz (prompt), kterým AI dáváte pokyny, je považován pouze za námět či myšlenku. A námět sám o sobě autorským dílem není. Umělá inteligence, která na základě promptu vytvoří obrázek nebo text, není fyzická osoba, a proto výsledek její činnosti nemůže být autorským dílem ve smyslu zákona.

Tento přístup není jen českým specifikem. Podobný závěr přijal i Úřad pro autorská práva v USA v případu grafické novely *Zarya of the Dawn*. Ačkoliv uznal autorství textu a kompozice díla, odmítl přiznat autorství k jednotlivým obrázkům, protože byly vygenerovány nástrojem Midjourney a nebyly tak výsledkem lidské tvorby.

Reflexe: Pro firmy a kreativce to má drtivý praktický dopad. Pokud na vytvořený obsah (logo, marketingový text, grafiku) nemáte autorská práva, nemůžete nikomu bránit v jeho kopírování a volném užívání. Váš konkurent si může váš AI vygenerovaný vizuál jednoduše stáhnout a použít ho pro vlastní kampaň. To představuje značné obchodní riziko a znehodnocuje investice do tvorby obsahu.

2. Používáte AI? Jste právně odpovědní za její chyby.

Zlaté pravidlo nové éry zní: odpovědnost nenese tvůrce AI modelu, ale ten, kdo jej používá a nasazuje (v terminologii EU tzv. „zavádějící subjekt“ nebo „deployer“). Pokud AI, kterou integrujete do svých služeb, způsobí škodu, odpovědnost leží na vás.

Perfektním příkladem je kanadský případ *Moffatt v. Air Canada*. Letecká společnost byla soudem shledána odpovědnou za to, že její chatbot poskytl zákazníkovi chybné informace o slevách na letenky. Argumenty aerolinky, že za slova chatbota neodpovídá, soud smetl ze stolu. Zákazník se na základě mylných informací rozhodl a firma musela nést následky.

Dalším rizikem jsou tzv. „halucinace", kdy si AI jednoduše vymýšlí fakta, citace nebo dokonce i soudní rozhodnutí, jak se stalo v nechvalně proslulém případu newyorského advokáta. Pro profesionály je spoléhání se na neověřené výstupy AI profesním selháním, což může vést k disciplinárnímu řízení, ztrátě licence nebo žalobě na náhradu škody za profesní pochybení.

Reflexe: Z právního hlediska je AI nástroj nebo pomocník. Stejně jako firma odpovídá za chyby, které udělá její zaměstnanec, odpovídá i za škody způsobené umělou inteligencí. Lidská kontrola klíčových výstupů není jen doporučení, ale absolutní nutnost pro řízení právních a reputačních rizik.

3. Některé AI praktiky jsou v EU už zakázané. Pokuty dosahují stovek milionů korun.

Mnozí se domnívají, že regulace AI je hudbou daleké budoucnosti. Opak je pravdou. Klíčové nařízení EU, známé jako AI Act, již vstoupilo v platnost a některé praktiky rovnou zařadilo do kategorie „nepřijatelného rizika" a zcela je zakázalo.

Zde je několik příkladů technologií, které je v EU zakázáno uvádět na trh nebo používat:

- **Systémy sociálního hodnocení** prováděné orgány veřejné moci, které hodnotí důvěryhodnost občanů na základě jejich sociálního chování.
- **Systémy využívající manipulativní či klamavé techniky,** které obcházejí lidskou vůli a mohou vést k významné újmě.
- **Systémy pro rozpoznávání emocí** na pracovištích a ve vzdělávacích institucích.
- **Necílené stahování obličejů z internetu nebo kamer** za účelem vytváření databází pro rozpoznávání.

A co je nejdůležitější: tyto zákazy začnou platit extrémně rychle, a to již **od února 2025**. Jedná se o první a nejurgentnější vlnu povinností z AI Actu, která předchází dalším pravidlům pro transparentnost (srpen 2026) a vysoce rizikové systémy (srpen 2027). Sankce za porušení zákazů jsou drakonické: až **35 milionů EUR nebo 7 % celosvětového ročního obratu** společnosti, podle toho, která částka je vyšší.

Reflexe: Nejedná se o teoretická pravidla. Jde o tvrdé, vymahatelné zákazy. Firmy musí provést okamžitý audit nástrojů a procesů, které využívají, aby se ujistily, že se nedopouštějí zakázaných praktik – často i nevědomky prostřednictvím softwaru třetích stran.

4. „Zdarma" neznamená bezpečně: Vaše citlivá údaje mohou sloužit k trénování AI.

Existuje zásadní rozdíl mezi spotřebitelskými (často bezplatnými) a podnikovými (placenými) verzemi AI nástrojů. Pokud vy nebo vaši zaměstnanci používáte bezplatnou nebo standardní placenou verzi ChatGPT pro pracovní účely, vystavujete firmu obrovskému riziku.

Obsah, který vložíte do spotřebitelských verzí, může být ve výchozím nastavení použit pro další trénování jazykových modelů. Ačkoliv uživatelé mají možnost se z tohoto procesu odhlásit, mnozí o tom nevědí. Obchodní podmínky některých poskytovatelů (například starší verze

podmínek nástroje LawGeex) si dokonce vyhrazovaly širokou a trvalou licenci k jakémukoliv využití nahraných dat.

Česká advokátní komora (ČAK) k tomuto vydala jasné stanovisko, které by mělo být varováním pro všechny profese pracující s důvěrnými informacemi. Požaduje, aby souhlas klienta s použitím AI byl naprosto explicitní.

"Předchozí souhlas klienta... musí obsahovat výslovné prohlášení, že klient ví, že AI může fungovat nepředvídatelně, a také výslovný souhlas, že může AI sdílet tyto informace (byť anonymizované) s blíže neurčenými podobnými systémy."

Reflexe: Vkládáním citlivých firemních dat, obchodních tajemství nebo klientských informací do veřejně dostupných AI nástrojů můžete nevědomky porušovat GDPR, profesní tajemství a důvěru, na které stojí vaše podnikání. Jediným bezpečným řešením je používání výhradně podnikových (Enterprise) verzí. U dodavatele hledejte konkrétní smluvní záruky: trvejte na **Dodatku o zpracování údajů (DPA)**, ověřte si možnost **nulové retence dat (Zero Data Retention – ZDR)** a zajistěte si **datovou rezidenci v EU**. Tyto prvky transformují obecný slib bezpečnosti v právně vymahatelný závazek. Toto není jen teoretické riziko porušení GDPR; je to přímá cesta k naplnění odpovědnosti „zavádějícího subjektu“, o které jsme mluvili dříve.

5. Označení „Vytvořeno s AI“ se stává zákonnou povinností.

Transparentnost je jedním z pilířů AI Actu. Pro systémy s tzv. „omezeným rizikem“ zavádí nařízení jasnou povinnost informovat uživatele.

Konkrétně to znamená, že jakýkoliv obsah, který je uměle vytvořen nebo zmanipulován a který se podobá existujícím osobám, objektům nebo událostem a mohl by být mylně považován za autentický (tzv. „deepfakes“), musí být jasně a zřetelně označen jako uměle generovaný. Tato povinnost se vztahuje na obrázky, audio i video. Stejně tak chatboty a jiné systémy, které interagují s lidmi, musí uživatele předem informovat, že nekomunikují s člověkem.

Reflexe: Smyslem tohoto opatření je boj proti dezinformacím a klamání veřejnosti. Nejde však jen o etické vodítko; je to i technický požadavek, který pomáhá online platformám plnit jejich vlastní právní povinnosti podle nařízení o digitálních službách (DSA). Označování obsahu jim totiž usnadňuje zmírňování systémových rizik, jako je právě šíření dezinformací. Pro firmy to znamená praktický úkol: pokud používáte AI k tvorbě marketingových materiálů nebo obsahu na sociální sítě, měli byste už nyní zavádět procesy pro jejich označování, abyste byli připraveni.