IUSTORIA
Advokátní kancelář

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

1. Souhrnný briefing: Regulace, rizika a dopady v České Republice

Shrnutí

Tento dokument poskytuje komplexní analýzu současného a budoucího právního, etického a obchodního prostředí souvisejícího s umělou inteligencí (AI) v České republice. Syntetizuje klíčové poznatky z nařízení EU, soudních rozhodnutí, odborných analýz a etických stanovisek s cílem poskytnout ucelený a prakticky orientovaný přehled pro strategické rozhodování.

Klíčové závěry:

2. **Akt o umělé inteligenci (AI Act) je stěžejní regulací:** Nařízení EU 2024/1689 je přímo použitelným právním předpisem v ČR a zavádí komplexní rámec založený na míře rizika. Společnosti musí identifikovat, do které ze čtyř kategorií (nepřijatelné, vysoké, omezené, minimální riziko) jejich používané AI systémy spadají, a plnit příslušné povinnosti.
3. **Časový harmonogram je neúprosný:** Implementace AI Actu je postupná. Nejpřísnější zákazy pro AI s nepřijatelným rizikem vstoupily v platnost již v únoru 2025. Povinnosti transparentnosti pro systémy s omezeným rizikem (např. označování AI obsahu) platí od srpna 2025. Nejsložitější povinnosti pro vysoce rizikové systémy mají delší přechodné období do srpna 2027, jejich příprava je však natolik náročná, že je nutné ji zahájit neprodleně.
4. **Autorská práva k výstupům AI jsou v ČR nechráněná:** Přelomový rozsudek Městského soudu v Praze (č. j. 10 C 13/2023-16) stanovil, že dílo vytvořené AI není autorským dílem ve smyslu českého práva, protože postrádá jedinečný výsledek tvůrčí činnosti fyzické osoby. To představuje značné obchodní riziko, neboť takto vytvořený obsah (např. marketingové materiály, grafika) může být kýmkoli volně kopírován.
5. **Odpovědnost zůstává na firmě:** Společnost, která AI systém používá (tzv. „zavádějící subjekt“), nese konečnou odpovědnost za jeho provoz a výstupy. To zahrnuje povinnost lidského dohledu, řízení rizik, zajištění kvality dat a pečlivé prověřování dodavatelů. V případě škody způsobené AI (např. chybnou radou chatbota klientovi) je odpovědná firma, nikoli AI.
6. **Důvěrnost a bezpečnost jsou prvořadé:** Používání AI nástrojů, zejména těch spotřebitelských, pro zpracování citlivých klientských, osobních nebo obchodních údajů představuje kritické riziko porušení povinnosti mlčenlivosti a GDPR. Výběr dodavatele AI musí být podložen hloubkovou analýzou jeho bezpečnostních politik, zásad uchovávání dat a možností datové rezidence v EU.
7. **Národní implementace probíhá:** Ačkoli je AI Act přímo použitelný, za jeho implementaci a dohled v ČR odpovídají národní orgány v čele s Ministerstvem průmyslu a obchodu (MPO) jako hlavním koordinátorem. Pro firmy je klíčové sledovat pokyny a aktivity těchto institucí, včetně Českého telekomunikačního úřadu (ČTÚ) a České agentury pro standardizaci (ČAS), která spravuje regulační pískoviště.

1. Právní rámec pro AI v EU a ČR

Základním kamenem regulace AI v Evropě je **Nařízení Evropského parlamentu a Rady (EU) 2024/1689**, známé jako **Akt o umělé inteligenci (AI Act)**. Jeho cílem je podporovat inovace a zavádění důvěryhodné AI a zároveň zajistit vysokou úroveň ochrany zdraví, bezpečnosti a základních práv.

25.9.2025 byl zveřejněn návrh zákona o AI v gesci MPO. Více info na https://odok.gov.cz/portal/veklep/material/KORNDLSJSEUC/

1.1. Akt o umělé inteligenci: Přístup založený na riziku

AI Act klasifikuje systémy AI do čtyř kategorií podle úrovně rizika, které představují. Od této klasifikace se odvíjí míra regulační zátěže.

- **Nepřijatelné riziko (Zakázané praktiky):** Tyto systémy jsou považovány za hrozbu pro základní práva a jsou v EU zakázány. Mezi příklady patří:
    - Systémy sociálního hodnocení (social scoring) prováděné veřejnými orgány.
    - Využívání podprahových technik nebo manipulativních praktik, které způsobují fyzickou či psychickou újmu.
    - Zneužívání zranitelnosti specifických skupin (např. dětí, osob se zdravotním postižením) vedoucí k podstatné újmě.
    - Používání systémů pro rozpoznávání emocí na pracovištích a ve vzdělávacích institucích (s úzkými výjimkami).
    - Většina systémů dálkové biometrické identifikace v reálném čase ve veřejně přístupných prostorech pro účely vymáhání práva (s úzkými výjimkami pro závažné trestné činy).
    - **Datum účinnosti:** Tyto zákazy jsou platné již od **února 2025**.
- **Vysoké riziko:** Sem spadají systémy, jejichž selhání může mít závažný dopad na bezpečnost nebo základní práva. AI Act je explicitně vyjmenovává v Příloze III. Patří sem AI používaná v oblastech jako:
    - **Kritická infrastruktura:** Řízení dopravy, dodávek vody, plynu a elektřiny.
    - **Vzdělávání:** Hodnocení studentů nebo rozhodování o přístupu ke vzdělání.
    - **Zaměstnávání:** Nástroje pro nábor, hodnocení a řízení zaměstnanců.
    - **Přístup k základním službám:** Posuzování úvěruschopnosti (credit scoring), rozhodování o nároku na sociální dávky.
    - **Vymáhání práva, migrace a správa soudnictví.**
    - **Povinnosti:** Poskytovatelé a zavádějící subjekty těchto systémů musí splnit přísné požadavky, včetně zavedení systému řízení rizik, zajištění vysoké kvality trénovacích dat pro prevenci diskriminace, vedení podrobné technické dokumentace, zajištění transparentnosti a robustního lidského dohledu, dosažení vysoké úrovni přesnosti a kybernetické bezpečnosti, provedení posouzení shody a registrace v databázi EU.
    - **Datum účinnosti: Srpen 2027**.
- **Omezené riziko:** U těchto systémů je klíčovou povinností transparentnost.
    - **Chatboti:** Uživatelé musí být srozumitelně informováni, že komunikují se systémem AI.
    - **Generovaný obsah:** Obsah vytvořený nebo podstatně upravený AI (tzv. "deepfakes", obrázky, audio, texty) musí být jasně označen jako uměle generovaný. To je zásadní pro marketingové a komunikační materiály.
    - **Datum účinnosti: Srpen 2025**.

- **Minimální nebo žádné riziko:** Většina v současnosti používaných AI systémů (např. spamové filtry, doporučovací systémy v e-shopech). Pro tyto systémy AI Act nestanovuje žádné povinnosti, pouze podporuje dobrovolné přijímání kodexů chování.

1.2. Implementace a vymáhání v ČR

Jako nařízení EU je AI Act v ČR přímo použitelný. Národní orgány však hrají klíčovou roli v jeho praktickém uplatňování, dohledu a sankcionování. Vláda ČR schválila svůj implementační přístup 29. května 2025.

Klíčové národní instituce:

- **Ministerstvo průmyslu a obchodu (MPO):** Hlavní koordinátor pro implementaci AI Actu.
- **Český telekomunikační úřad (ČTÚ):** Bude pravděpodobně vykonávat dozor nad trhem, tedy kontrolovat, zda AI systémy na trhu splňují požadavky.
- **Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ):** Působí jako oznamující orgán pro subjekty posuzování shody.
- **Česká agentura pro standardizaci (ČAS):** Zodpovídá za zřizování a provoz tzv. **regulačních pískovišť**, které umožňují firmám testovat inovativní AI řešení v kontrolovaném prostředí pod dohledem regulátora.

1.3. Vztah k GDPR

AI Act a Obecné nařízení o ochraně osobních údajů (GDPR) se vzájemně doplňují. Kdykoli systém AI zpracovává osobní údaje, vztahuje se na něj plně GDPR. To znamená nutnost mít platný právní základ pro zpracování, zajistit plnou transparentnost vůči subjektům údajů, minimalizovat zpracovávaná data a provést posouzení vlivu na ochranu osobních údajů (DPIA), zejména u vysoce rizikových systémů. Požadavky AI Actu na kvalitu dat a transparentnost často rozšiřují a konkretizují povinnosti vyplývající z GDPR.

2. Autorské právo a generativní AI

Nástup generativní AI otevřel zásadní otázky v oblasti autorského práva, které mají přímý dopad na obchodní praxi.

2.1. Autorství výstupů generovaných AI

Česká justice zaujala v této věci jasné stanovisko. V rozsudku Městského soudu v Praze (č. j. 10 C 13/2023-16 ze dne 11. října 2023) soud konstatoval, že obrázek vytvořený AI na základě textového zadání **není autorským dílem** dle § 2 autorského zákona.

- **Odůvodnění soudu:** Dílo postrádá klíčový znak – **jedinečný výsledek tvůrčí činnosti autora (fyzické osoby)**. Systém AI není fyzickou osobou a nemůže být autorem. Samotné zadání (prompt) je považováno pouze za námět či myšlenku, které samy o sobě autorským právem chráněny nejsou.
- **Srovnání:** Tento přístup je v souladu s praxí v USA, kde Úřad pro autorská práva v případu komiksu *Zarya of the Dawn* odmítl registrovat obrázky vytvořené AI Midjourney. Naopak právo Spojeného království zná koncept "díla vytvořeného počítačem", kde autorství připadá osobě, která učinila nezbytná opatření pro vznik díla.

- **Obchodní dopad:** Obsah generovaný AI bez významného lidského tvůrčího zásahu není v ČR chráněn autorským právem. To znamená, že konkurence může takový obsah (např. grafiku, reklamní texty) volně kopírovat a využívat, aniž by se dopustila porušení autorských práv.

2.2. Využití chráněného obsahu pro trénování AI

Klíčovou právní otázkou je legalita "scrapování" internetu a využívání existujících děl k trénování AI modelů.

- **Právní základ v EU/ČR:** Transpozicí směrnice o jednotném digitálním trhu (DSM) byla do českého autorského zákona vložena ustanovení o **vytěžování textů a dat (Text and Data Mining, TDM)**.
    - **§ 39c autorského zákona** umožňuje vytěžování dat pro jakýkoli účel, včetně komerčního. Nositelé práv však mají možnost toto využití **výslovně zakázat** (tzv. "opt-out"), například v podmínkách užití webu nebo strojově čitelným způsobem. Poskytovatelé GPAI modelů musí dle AI Actu tyto výhrady respektovat.
- **Právní nejistota:** Globální AI modely jsou často trénovány v USA pod režimem "fair use", který je flexibilnější a nezná formální "opt-out". Vzniká tak riziko, že model dostupný v ČR byl trénován na datech, jejichž evropští autoři si jejich využití nepřáli, což představuje právní šedou zónu. Probíhající soudní spory (např. Getty Images vs. Stability AI) tuto oblast dále zpřesní.

3. Povinnosti a odpovědnost zavádějících subjektů (využívajících AI)

AI Act klade značné povinnosti nejen na vývojáře, ale především na organizace, které AI nasazují do praxe – tzv. **zavádějící subjekty**.

3.1. Klíčové povinnosti

- **Lidský dohled:** U vysoce rizikových systémů je povinnost zajistit efektivní lidský dohled, který umožňuje monitorovat, správně interpretovat a v případě potřeby zasáhnout do fungování AI nebo zvrátit její rozhodnutí.
- **Použití v souladu s účelem:** Systém musí být používán v souladu s pokyny a technickou dokumentací poskytovatele.
- **Kvalita vstupních dat:** Pokud firma poskytuje data pro AI systém, nese odpovědnost za jejich relevanci a vhodnost. Princip "garbage in, garbage out" zde platí s plnou právní vahou.
- **Monitorování a hlášení:** Zavádějící subjekt je povinen monitorovat provoz systému a hlásit závažné incidenty a rizika poskytovateli a případně příslušným orgánům.
- **Vedení záznamů:** Uchovávání automaticky generovaných logů o provozu systému je klíčové pro pozdější kontrolu a vyšetřování.
- **Posouzení dopadu na základní práva (FRIA):** Subjekty veřejné moci a firmy v citlivých sektorech musí před nasazením vysoce rizikového systému provést toto posouzení.
- **Informování zaměstnanců:** Při využití vysoce rizikové AI na pracovišti (např. při náboru) je nutné informovat zaměstnance a jejich zástupce.

3.2. Právní odpovědnost za škodu

Odpovědnost za škodu způsobenou AI systémem je komplexní. Obecně však platí, že **konečnou odpovědnost nese subjekt, který AI provozuje**.

- **Příklad z praxe:** V případu *Moffett vs. Air Canada* byla letecká společnost shledána odpovědnou za nesprávné informace, které její chatbot poskytl zákazníkovi, což vedlo k finanční ztrátě. Tento princip je plně přenositelný i do českého prostředí.
- **Odpovědnost advokátů:** V kontextu právních služeb je AI považována za "pomocníka". Advokát plně odpovídá za její výstupy a nese odpovědnost i za samotný výběr vhodného a bezpečného nástroje (*culpa in eligendo*).
- **Legislativní vývoj:** Revidovaná **Směrnice o odpovědnosti za vadné výrobky (PLD)** explicitně zahrnuje software a AI mezi produkty, což usnadňuje vymáhání náhrady škody. Návrh specifické směrnice o odpovědnosti za AI byl však Evropskou komisí stažen, což zvyšuje význam smluvních ujednání mezi poskytovateli a uživateli AI pro alokaci odpovědnosti.

4. Bezpečnost a etika v advokátní a obchodní praxi

Pro obory pracující s důvěrnými informacemi, jako je advokacie, je výběr a používání AI nástrojů zásadním rozhodnutím v oblasti řízení rizik.

4.1. Analýza nástrojů a povinnost mlčenlivosti

Hloubková analýza předních AI nástrojů ukazuje na kritické rozdíly relevantní pro jakoukoli firmu nakládající s citlivými daty.

Kritérium	OpenAI ChatGPT (Enterprise/API)	Google Gemini (Workspace/Placené API)	Anthropic Claude (Komerční)	Perplexity AI (Enterprise/API)
Trénování na datech zákazníka	Standardně **Ne**	Standardně **Ne**	Standardně **Ne** (pro všechny úrovně)	Standardně **Ne**
Lidská kontrola dat	Omezena na monitorování zneužití	**Ne** pro vylepšování produktu	Standardně **žádný přístup** (s úzkými výjimkami)	Nespecifikováno, důraz na "žádné trénování"
Datová rezidence v EU	**Ano** (pro oprávněné zákazníky)	**Ano** (pro Workspace)	Nutné **individuální sjednání** / SCC	**Nejasné** / Nespecifikováno
Politika pro žádosti orgánů	Specifická politika, rozlišení US/Irsko	Oznámení administrátorovi, pokud zákon nezakazuje	Žádosti směřovány primárně na zákazníka	Obecná ustanovení, menší transparentnost
Klíčové silné stránky	Možnost Zero Data Retention, EU rezidence	Integrace a bezpečnost ekosystému Google	Nejsilnější ochrana soukromí "by design"	Rychlé mazání nahraných souborů (7 dní)
Klíčová rizika	Minulé problémy s GDPR, složitost politik	Globální cachování u API, složitost značky	Nutnost sjednat EU rezidenci	**Absence informací o EU rezidenci**, hlášené zranitelnosti

Zásadní doporučení: Je naprosto nezbytné používat výhradně **podnikové (Enterprise/Commercial) verze** těchto nástrojů. Spotřebitelské verze mohou využívat uživatelská data pro trénování modelů, což je pro firemní a klientská data nepřijatelné.

4.2. Etické a praktické povinnosti

- **Kompetence a AI gramotnost:** Odborníci a firmy mají povinnost udržovat si přehled o technologickém vývoji, včetně výhod a rizik AI, aby mohli efektivně a bezpečně poskytovat své služby.
- **Informování klienta:** Je doporučeno informovat klienty o využití AI. Pro zpracování jejich dat v AI systémech je nutný jejich výslovný souhlas, který zahrnuje poučení o nepředvídatelnosti AI.
- **Přiměřenost odměny:** Zvýšená efektivita díky AI by se měla projevit v přiměřené ceně služeb pro klienta.

5. Praktické kroky a doporučení pro byznys

Pro zvládnutí výzev a využití příležitostí, které AI přináší, by firmy v ČR měly přijmout následující strategické kroky:

1. **Zaveďte interní správu AI (AI Governance):**
    - Vytvořte jasné interní směrnice pro výběr, nasazování a monitorování AI nástrojů.
    - Určete osobu nebo tým zodpovědný za soulad s AI regulací.
    - Proveďte inventuru a rizikovou klasifikaci všech aktuálně používaných AI nástrojů.
2. **Zvyšujte AI gramotnost zaměstnanců:**
    - Proškolte zaměstnance o základních principech AI Actu, GDPR a autorského práva ve vztahu k AI.
    - Klíčové je vzdělávání o rizicích vkládání citlivých osobních nebo firemních dat do externích, zejména veřejně dostupných, AI nástrojů.
3. **Pečlivě prověřujte dodavatele (Supplier Vetting):**
    - Před pořízením jakéhokoli AI nástroje proveďte důkladnou prověrku dodavatele.
    - Vyžadujte dokumentaci prokazující shodu s AI Actem (EU prohlášení o shodě), informace o trénovacích datech, výsledky testování a bezpečnostní certifikace.
    - Zajistěte si robustní smluvní podmínky, které jasně definují odpovědnost a pravidla pro nakládání s daty.
4. **Využívejte národní zdroje a podporu:**
    - Sledujte Národní strategii umělé inteligence (NAIS 2030) a pokyny vydávané MPO a dalšími orgány.
    - Pro inovativní projekty zvažte účast v **regulačních pískovištích** spravovaných ČAS. Umožňují testovat AI v reálných podmínkách s podporou a dohledem regulátora, což výrazně snižuje riziko nesouladu při vstupu na trh.