30. 4. 2024

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

K právní regulaci AI a některým požadavkům kladeným na advokáty v souvislosti s tím

Ve světě, kde technologický pokrok neustále posouvá hranice našich možností, se umělá inteligence (AI, tj. artificial intelligence) rychle stává neoddělitelnou součástí našich osobních i profesních životů. Zejména v posledních měsících jsme svědky toho, jak AI proniká do celé řady odvětví a mění způsob, jakým tato odvětví fungují. Výjimkou není ani odvětví práva, resp. právních služeb, kde AI nabízí nové možnosti pro zefektivnění způsobu poskytování právních služeb a jejich inovaci.

V této nové éře, kdy právníci a technologie úzce spolupracují, je důležité porozumět nejen přínosům, ale rovněž výzvám, které AI přináší.

Právní úprava

Nejvýznamnější právní normou na poli AI je v současné chvíli dosud neúčinný návrh nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (akt o umělé inteligenci) a mění určité legislativní akty unie (dále jen „**AI akt**“ nebo „**nařízení**“), který má za cíl regulovat vývoj, nasazení a využívání umělé inteligence v členských státech EU.[1] Původní návrh AI aktu byl představen již v dubnu 2021.[2] V návaznosti na významné změny na poli AI, mj. v souvislosti s masivním rozšířením systémů AI typu ChatGPT, ovšem vyvstala potřeba do původního znění zasáhnout.[3] S ohledem na zprávy v mediálním prostoru v souvislosti s touto poslední verzí AI aktu lze předpokládat, že bude znění AI aktu v současné podobě předloženo ke schválení Evropskému parlamentu a mohlo by být finálně přijato na jaře tohoto roku.

AI akt poskytuje v rámci své poslední verze upravenou definici systému AI, která zní následovně: *„Systém AI je strojový systém navržený tak, aby fungoval s různou úrovní autonomie a který může vykazovat adaptivitu a který pro explicitní nebo implicitní cíle odvodí ze vstupů, které obdrží, jak generovat výstupy, jako jsou předpovědi, obsah, doporučení nebo rozhodnutí, která mohou ovlivnit fyzické nebo virtuální prostředí.“*[4]

Systém AI, jak vyplývá z citované definice, je strojový systém schopný autonomního fungování a adaptace. To znamená, že AI může provádět úlohy a reagovat na změny bez lidského zásahu a dokáže se „učit“ a přizpůsobovat se na základě přijímaných dat – právě aspekt „učení“ spojený s potenciálním sdílením vložených dat se třetími osobami je významným rizikovým aspektem, o kterém bude řeč níže. Příkladem systému AI, který odpovídá dotčené definici, je nyní nejpoužívanější ChatGPT (společnosti OpenAI), který autonomně a adaptivně generuje relevantní výstupy na základě obdržených vstupních dat a dotazů.

Pojďme si nyní ve stručnosti představit dílčí části úpravy AI aktu.

AI akt v čl. 2 definuje subjekty, na které se nařízení vztahuje, přičemž pro účely tohoto článku uvádíme pouze ty z našeho pohledu nejvýznamnější. Mezi tyto subjekty spadají zejm. poskytovatelé[5] (nehledě na to, zda jsou z EU či nikoliv) a uživatelé AI systémů[6] (v rámci EU), a dále dovozci[7] a distributoři AI systémů[8] (i ze zemí mimo EU, pokud je výstup systému AI používán v rámci EU).

I v případě vyjmenovaných subjektů ovšem AI akt nemá dopadat na určité systémy AI, a to příkladmo na systémy AI, potažmo jejich výstupy, které mají sloužit výhradně pro účely výzkumu a vývoje.[9] Dále nemá regulovat ani výzkum, testování a vývoj systémů AI před jejich uvedením na trh[10] – jinými slovy má poskytnout volné působiště pro vývojáře a regulovat až samotný výsledný (komerční) produkt. AI akt tedy záměrně nezahrnuje právě výše jmenované AI systémy do své působnosti s cílem působit pozitivně na podporu inovací a technologického pokroku, kdy je poskytnut vývojářům volný prostor pro experimentování a inovace před uvedením samotných AI systémů na trh.

Významné je dále také to, že úprava AI aktu nemá dopadat na uživatele systémů AI, pokud jsou fyzickými osobami, v rámci jejich osobního užití (tedy „nepodnikatelského“).[11]

Velmi významnou je v rámci AI aktu úprava spočívající v rozdělení systémů AI de facto dle míry jejich rizika[12] (či potenciálního negativního společenského dopadu). V rámci AI aktu jsou definovány celkem 4 kategorie: 1) zcela zakázané postupy v souvislosti s AI,[13] 2) postupy s vysokým rizikem („high risk systems“), 3) další systémy s vymezenými povinnostmi,[14] 4) zbytková kategorie (bez rizika či rizikem nízkým).

Do první kategorie AI akt zařazuje následující zakázané činnosti/postupy (čl. 5):

1. Uvádění na trh, provozování nebo používání AI systémů, které využívají podprahové nebo záměrně klamavé techniky. Tyto techniky mohou významně zkreslovat informace nebo manipulovat s chováním jednotlivců či skupin, což vede k rozhodnutím, která by osoby bez této manipulace neučinily.[15]
2. Uvádění na trh, provozování nebo používání AI systémů, které cíleně zneužívají zranitelnosti jednotlivců nebo skupin na základě jejich věku, zdravotního stavu, sociální nebo ekonomické situace.[16]
3. Uvádění na trh, provozování nebo používání biometrických kategorizačních systémů, které klasifikují jednotlivce na základě biometrických dat s cílem odhalit jejich rasu, politické názory, odborové příslušnosti, náboženské nebo filozofické přesvědčení, sexuální život nebo orientaci. Tento zákaz však neplatí pro práci v oblasti vymáhání práva, kde je možné biometrická data legálně získaná používat.[17]
4. Uvádění na trh, uvedení do provozu nebo používání AI systémů určených pro hodnocení nebo klasifikaci jednotlivců či skupin („social scoring“)[18] založené na jejich sociálním chování nebo předpovídaných osobnostních charakteristikách – pokud by takové hodnocení mělo vést k znevýhodnění nebo nepříznivému, nepřiměřenému či jinak neodůvodněnému zacházení.
5. Uvádění na trh, provozování nebo používání biometrických identifikačních systémů v reálném čase ve veřejně přístupných prostorách pro účely vymáhání práva.[19] Použití je přípustné toliko ve striktně vymezených případech (např. při pátrání po pohřešovaných osobách).[20]
6. Uvádění na trh, uvedení do provozu nebo používání AI systémů, které hodnotí rizika trestné činnosti jednotlivců pouze na základě profilování nebo posouzení osobnostních rysů.[21],[22]
7. Uvádění na trh, uvedení do provozu nebo používání AI systémů, které vytvářejí nebo rozšiřují databáze rozpoznávání obličejů prostřednictvím necíleného shromažďování obrazů z internetu nebo kamerových záznamů.
8. Uvádění na trh, uvedení do provozu nebo používání AI systémů sloužících k odvozování emocí osob v kontextu práce a vzdělávacích institucí.

Kategorii 2) vysoce rizikových systémů (článek 6) pak definuje AI akt ve stručnosti následovně.

Vysoce rizikový je systém, pokud je *„určen k použití jako bezpečnostní součást výrobku nebo je sám výrobkem, na který se vztahují harmonizační právní předpisy*“ (uvedené v příloze AI aktu)

a zároveň na *„produkt, jehož je daný systém AI bezpečnostní součástí, případně na samotný tento systém AI jako produkt se vztahuje povinnost posouzení shody třetí stranou za účelem uvedení tohoto produktu na trh nebo do provozu“* (opět dle předpisů uvedených v příloze AI aktu).

Kromě těchto případů jsou jako vysoce rizikové systémy AI považovány také samostatně vyjmenované systémy v příloze III, přičemž se jedná o 8 kategorií systémů, a to např. systémů fungujících za účelem biometrické identifikace fyzických osob na dálku; určování přístupu fyzických osob ke vzdělávacím institucím; určených k použití při náboru nebo výběru fyzických osob, zejména pro inzerování volných pracovních míst; určených pro použití veřejnými orgány nebo jménem veřejných orgánů za účelem hodnocení nároků fyzických osob na dávky a služby veřejné podpory. Z uvedeného výčtu vyplývá, že se jedná o systémy, které se týkají vysoce citlivých oblastí, které mohou mít potenciálně významný dopad do základních lidských práv, ochrany osobních údajů, zdraví apod.

S ohledem na citlivou povahu činností spadajících do působnosti rizikových systémů AI stanovuje AI akt dodatečná/nadstandardní opatření pro jejich použití. Mezi opatření související s vysoce rizikovými systémy spadá následující (čl. 8 a násl. AI aktu): Zavedení systému řízení rizik (čl. 9), specifické požadavky na data a jejich správu (čl. 10, zejm. v kontextu trénování AI modelů), vytvoření technické dokumentace (čl. 11) a vedení záznamů, resp. protokolů o průběhu činnosti systému (čl. 12), transparentnost co do poskytování možnosti intepretace a vhodného použití ze strany uživatelů, tj. např. opatření systému návodem (čl. 13), zajištění toho, že užití systému bude pod efektivním dohledem fyzické osoby s cílem minimalizovat rizika pro zdraví, bezpečnost nebo základní práva, která mohou vzniknout v souvislosti s užíváním systému; zajištění přesnosti, spolehlivosti a kybernetické bezpečnosti.[23]

Zbývající dvě kategorie se oproti dvěma dosud představeným vyznačují podstatně nižší až (v případě poslední kategorie) žádnou mírou regulace. V rámci třetí kategorie („povinnosti transparentnosti určitých systémů AI“, čl. 52) jsou založeny zejména povinnosti co do transparentnosti. Jmenovitě jde o poskytnutí takových informací, aby byly fyzické osoby informovány o tom, že komunikují se systémem AI, pokud to není zřejmé z okolností a kontextu použití. A stejně tak informací, že jsou fyzické osoby vystaveny případnému systému rozpoznávání emocí nebo systému biometrické kategorizace. Uživatelé jsou povinně informováni dále v případě systému vytvářejícího obrazový, zvukový nebo video obsah, který se znatelně podobá existujícím osobám, objektům, místům nebo jiným subjektům nebo událostem a který by se určité osobě mohl nepravdivě jevit jako autentický nebo pravdivý (tj. případ tzv. deep fake).[24]

V kontextu dosud řečeného lze učinit následující závěry. Použití první kategorie systémů bude na základě AI aktu zcela vyloučeno a použití druhé kategorie systémů s vysokým rizikem navázáno na přísná kritéria. Přičemž tyto dvě kategorie s ohledem na svou povahu nebudou zpravidla představovat systémy spadající mezi běžné nástroje používané advokátními kancelářemi. V rámci činnosti advokátních kanceláří ovšem mohou být relevantní systémy spadající do zbylých dvou kategorií s nižší mírou regulace, příkladmo lze poukázat zejm. na systémy, které budou samy komunikovat s klienty („chatboti“), kdy bude nutné zajistit poskytnutí jednoznačných informací, že osoby komunikují se systémem AI, a nikoliv člověkem.

Jak již bylo řečeno, v současné chvíli není v kontextu užití systémů AI účinný žádný komplexní právní předpis (na úrovni EU ani na úrovni tuzemské). V tomto směru je ovšem nutné připomenout, že celá řada aspektů souvisejících s užitím systémů AI je již upravena v jiných právních předpisech či je z nich minimálně odvoditelná (autorský zákon, GDPR atd.). Jedním z právních předpisů je mj. i zákon č. 128/1990 Sb., o advokacii, ve znění pozdějších předpisů, přičemž nedostatek relevantní právní úpravy ve vztahu k systémům AI se alespoň rámcově pokusila substituovat Advokátní komora právě v návaznosti na úpravu zákona o advokacii tím, že uveřejnila Stanovisko k využívání AI při

poskytování právních služeb (dále jen „**stanovisko**“).[25]

V rámci stanoviska se uvádí mj. následující: *„AI je nástrojem, který advokát v souladu se zákonem a stavovskými předpisy může využít v souvislosti s poskytováním právních služeb. (…) AI v jakékoliv formě nemůže být poskytovatelem právní služby ve smyslu §1 zákona o advokacii.“* Z citované pasáže stanoviska vyplývá, že systém AI sám o sobě nikdy nemůže být poskytovatelem právních služeb. Systém AI nicméně může sloužit jako nástroj nápomocný advokátům v rámci výkonu jejich činnosti. Je tudíž zcela vyloučeno, aby systém AI poskytoval typicky odpovědi na dotazy týkající se konkrétního právního problému.[26] To by bylo možné si představit právě např. v případě již zmíněného chatbota, který by byl umístěn na webových stránkách advokátní kanceláře, kde by samostatně generoval odpovědi na vybrané právní otázky, případně i celé právní listiny jako třeba návrhy smluv či právních podání. Užití samostatně komunikujících chatbotů ze strany advokátních kanceláří je tudíž přípustné jen co do komunikace nespadající do režimu poskytování právního poradenství.

Ze stanoviska rovněž vyplývá, že v souvislosti s užitím systémů AI v rámci výkonu činnosti advokacie není jakkoliv omezena zákonná odpovědnost advokáta.

V závěru stanoviska se poukazuje na povahu systémů AI co do jejich autonomie a nepředvídatelnosti. A dále také na aspekt tzv. „učení“ systémů AI (ten byl zmíněn v úvodu článku v souvislosti s definicí systému AI v rámci AI aktu), který de facto znamená, že vstupy, které jsou do systému AI vloženy, mohou být přímo či nepřímo sdíleny s dalšími uživateli daného systému, protože vstupy/výstupy mohou být využívány pro rozšiřování vědomostní databáze systému. Stanovisko v tomto směru poukazuje na skutečnost, že v případě aspektu „učení“ bude nemožné ze strany advokátů zajistit dodržování povinnosti mlčenlivosti (resp. i ochranu klientských dat či osobních údajů).

Stanovisko v návaznosti na dosud řečené stanovuje povinnost advokátů obstarat si pro účely zpracování informací či údajů (dále též jako „**klientské údaje**“ nebo „**klientská data**“), které mu byly poskytnuty klientem nebo které obsahují informace o klientech či jejich případech, v rámci systémů AI (i kdyby se jednalo pouze o „zpracování“ pro účely „učení“ nástroje) souhlas klienta, ze kterého bude výslovně vyplývat prohlášení, že je klient srozuměn s tím, že systémy AI mohou fungovat nepředvídatelně a rovněž s tím, že AI systémy mohou poskytnuté klientské informace (byť anonymizované) sdílet s blíže neurčenými podobnými systémy.

Stanovisko tak má zcela zjevně za cíl (obdobně jako v případě třetí kategorie systémů dle AI aktu viz výše) zajistit vůči klientům dostatečnou míru transparentnosti. Pokud bychom shrnuli požadavky stanoviska kladené na advokáty, vyplývá z nich následující:

1. Advokát je za všech okolností povinen zachovávat mlčenlivost – jakékoliv užití systémů AI v rozporu s touto povinností je tudíž vyloučeno;
2. Pokud má advokát v úmyslu užívat v souvislosti s klientskými údaji systémů AI, je povinen si obstarat od klienta jeho souhlas s tímto zpracováním;
3. Dotčený souhlas musí zároveň obsahovat výslovně prohlášení klienta o tom, že je srozuměn se skutečností, že AI systémy jsou nepředvídatelné a zároveň, že klientská data mohou být sdílena „s blíže neurčenými podobnými systémy“.

V návaznosti na právě řečené lze s jistotou podpořit povinnost nakládat s klientskými údaji při používání systému AI pouze za zachování zákonné povinnosti mlčenlivosti viz bod 1).

Zbývající dvě povinnosti je ovšem namístě podrobit bližší analýze. V současné chvíli již existuje nespočet systémů AI, které nabízejí různorodé funkce a generují diametrálně odlišné výstupy.

Stanovisko zjevně pracuje s konceptem systému AI odpovídajícímu ChatGPT, který funguje na bázi přijímání vstupů a generování výstupů (na základě své rozsáhlé databáze dat), přičemž v průběhu tohoto procesu dochází mj. právě ke zmíněnému „učení“ systému. Důsledkem toho může být mj. to, že vstupy poskytnuté ChatGPT se propisují do vědomostní báze systému, a nelze tak zajistit jejich bezpečnost a privátnost – jinými slovy dochází k prolomení povinnosti mlčenlivosti; pokud se totiž data stávají součástí vědomostní databáze, nelze vyloučit, že systém nebude jinému uživateli systému generovat odpovědi obsahující právě i tyto klientské údaje. Samotný ChatGPT ovšem nabízí uživatelské rozhraní,[27] které na obdobné bázi učení nefungují (resp. v rámci jejich užívání k „učení“ a sdílení nedochází).[28] Vedle ChatGPT samozřejmě existuje i řada jiných systémů AI s obdobnou funkcionalitou „nesdílení“. Tyto jiné systémy přitom mohou nabízet advokátům různorodé služby spočívající např. v úpravách textu, překladech, zpracování shrnutí textů či rešerších – použití těchto systémů AI se tudíž dotčené povinnosti mlčenlivosti nemusí vůbec dotýkat.

V návaznosti na právě řečené se jeví v případě užití těchto „neškodných“ systémů AI (u nichž je vyloučeno prolomení povinnosti mlčenlivosti, potažmo dalších povinností jako např. zákaz zneužití osobních údajů) jako nadbytečné. Jedná se s trochou nadsázky o to samé jako kdyby byla nově stanovena povinnost advokáta žádat souhlas klienta s tím, že bude v souvislosti s jeho klientskými údaji používat tiskárnu a kopírku.

V rámci požadavku pod bodem 3) má být klient pro vyloučení všech pochybností srozuměn s tím, že výstupy systému AI jsou nepředvídatelné a že klientská data mohou být dále sdílena. V úvodu stanoviska je ovšem zcela správně uvedeno, že poskytovatelem právních služeb může být toliko advokát, který mj. za výstupy svých služeb plně odpovídá. Smyslem povinnosti pod bodem 3) tedy zřejmě není to, že advokát má klienta jaksi „připravit“ na to, že výstup, který od něj obdrží byl generován v rámci systému AI, je tudíž „nepředvídatelný“ a klient má tedy do jisté míry počítat i s tím, že nemusí být tak úplně správně. Právě popsané užití systému AI by totiž bylo jednoznačně v rozporu s úpravou zákona o advokacii a dle názorů autorů tohoto článku i se samotným záměrem stanoviska. Kdybychom použili obdobný příměr jako v předchozím odstavci, advokát by klienta skrze souhlas *připravoval* na skutečnost, že jeho tiskárna nemusí tak úplně správně tisknout, a tudíž se může stát, že některá ustanovení smlouvy budou chybět nebo nepůjdou přečíst. Srozumění klienta se skutečností týkající se nepředvídatelnosti systémů AI se tudíž jeví jako nadbytečné – pouze vznášející otazníky na straně klienta v tom, proč by pro něj – jako příjemce profesionálních služeb měla být nepředvídatelnost určitých nástrojů v rukou jeho advokáta jakkoliv relevantní.

V obdobném duchu pak vyznívá povinnost upozornit klienta na to, že jeho klientská data mohou být dále sdílena. Jak jsme si již potvrdili v rámci požadavku pod bodem 1), klientská data chráněná povinností mlčenlivosti, není možné v rámci „učících se“, otevřených či jinak nechráněných systémů AI vůbec možné sdílet. Jinými slovy, advokát by v souladu s povinností mlčenlivosti neměl být oprávněn dotčená klientská data do systému AI jako vstup vůbec vložit – je tak zcela vyloučena např. situace, kdy by do ChatGPT advokát při zahájení poskytování právní služby nahrál pro prvotní analýzu převzaté věci dokument obsahující důvěrné, citlivé či osobní údaje, jejichž nesdílení s třetími osobami není schopen zajistit. Cílem stanoviska přitom jistě nebylo vést advokáty k tomu, aby skrze dotčený souhlas klient získali jakési *sui generis* zproštění mlčenlivosti.

S ohledem na právě řečené lze učinit závěr, že buď bude advokát používat systémů AI, které jsou uzpůsobené k zachování a garantování povinnosti mlčenlivosti (a v tom případě logicky nepotřebuje souhlas klienta s tím, že bude s klientskými daty nakládáno odlišně), nebo k užívání systémů AI, které „nesdílení“ klientských údajů nejsou schopné zajistit (prolamují mlčenlivost), **nebude vůbec oprávněn přistoupit**. Současně advokát nebude za žádných okolností oprávněn postupovat tak, že by užil systému AI pro generování výstupu, který by následně bez revize a případné korektury

poskytl klientovi jako výstup své právní služby. Použití systému AI advokátem, které nemají vazbu na klientská data (advokát např. používá systém AI pro zpracování rešerše související judikatury) by zároveň nemělo nic bránit – souhlas klienta se ovšem v takovém případě jeví opět jako nadbytečný (viz příměr s kopírkou).

Obstarání výslovného souhlasu pod bodem 3) se tak s ohledem na výše uvedenou argumentaci jeví jako nadbytečné, když ani jedna ze situací by za žádných okolností vůbec neměla nastat (prolomení mlčenlivosti), potažmo klienta ovlivnit (nepředvídatelnost výstupu, použití systému AI při souvisejících činnostech, které ovšem nemají provazbu na klientské údaje).

V návaznosti na výše řečené lze při poskytování právních služeb doporučit minimálně následující kroky.

1. Vydefinovat systémy AI, se kterými pracují – jejich povahu, bezpečnost, míru sdílení dat atd. (např. skrze analýzu obchodních podmínek poskytovatelů systémů AI)
2. Podle povahy vydefinovaných nástrojů nastavily pravidla práce se systémy AI v rámci kanceláře mj. právě s ohledem na povahu rizika prolomení mlčenlivosti a ochrany dat;
3. Stanovit pravidla revize výstupů tak, aby byl pro účely klientských výstupů zcela eliminován popsaný element „nepředvídatelnosti“ (potažmo nespolehlivosti).

Závěr:

Chystaná právní úprava AI aktu přináší první ucelenější právní rámec stále aktuálnější problematiky AI. Jednou ze stěžejních částí AI aktu bude výčet základních subjektů, na které má AI akt dopadat, a dále také výčet výjimek, na které se AI akt vztahovat nebude (příkladmo systémy AI určené výhradně pro výzkum a vývoj).

AI akt vymezuje čtyři kategorie systému AI odstupňovaných podle jejich rizikovosti. Tyto kategorie zahrnují zcela zakázané postupy v souvislosti s AI, systémy s vysokým rizikem, další systémy s vymezenými povinnostmi a zbytkovou kategorii s nízkým nebo žádným rizikem, přičemž z hlediska použití systémů AI nebudou zřejmě systémy z prvních dvou kategorií pro advokátní kanceláře zpravidla příliš relevantní – povaha těchto systémů neodpovídá požadavkům či standardním činnostem advokátních kanceláří.

Co se týká relativně nově vydaného stanoviska advokátní komory k možnému využití AI systémů při poskytování právních služeb, stanovisko dle názorů autorů článku správně uvádí, že systém AI může být nástrojem používaným advokáty v souladu se zákonem a stavovskými předpisy, ale nemůže být samostatným poskytovatelem právních služeb. Současně platí, že advokáti mají za všech okolností povinnost zajistit ochranu klientských dat a mlčenlivost.

V návaznosti na tuto výchozí premisu nicméně stanovisko stanovuje advokátům povinnost (pro případ využívání systému AI) obstarat si od klientů výslovný souhlas, ze kterého bude výslovně vyplývat prohlášení, že je klient srozuměn s tím, že systémy AI mohou fungovat nepředvídatelně a rovněž s tím, že AI systémy mohou poskytnuté klientské informace (byť anonymizované) sdílet s blíže neurčenými podobnými systémy.

V kontextu této *nové* povinnosti advokátů je však otázkou, zda je povinnost nastavena skutečně tak, aby plnila svůj cíl (kterým byla zřejmě co nejvyšší míra transparentnosti vůči klientům). Advokáti jsou totiž už ze zákona povinni zajistit ochranu dat, mlčenlivost a dále také profesionalitu svých právních služeb. Jakékoliv obstarání souhlasu či srozumění klienta s tím, že klientská data mohou být sdílena dál nebo že obdržené výstupy právních služeb mohou být nepředvídatelné tak z logiky věci nejsou s popsanými povinnostmi v souladu. Jinými slovy, poskytnutí informací o používání systémů AI

klientům (a zajištění jejich srozumění s touto skutečností) sice může zajistit vyšší míru transparentnosti co do *odhalení* vnitřních postupů či pracovních procesů advokátních kanceláří, ale samo o sobě nemůže mít dle názoru autorů článku žádný dopad do vyjmenovaných povinností advokátů.

Současně lze z hlediska využívání AI systémů při poskytování právních služeb doporučit zmapování si rizikovosti jednotlivých systémů AI, který advokát používá či hodlá používat,
a nastavit související pravidla tak, aby jejich využívání bylo v soulad s právními předpisy.

JUDr. Petr Novotný, LL.M.
advokát a partner

JUDr. Jan Musil, LL.M.,
advokátní koncipient

MT Legal s.r.o., advokátní kancelář

Praha | Brno | Ostrava

Tel.: +420 222 866 555
Fax: +420 222 866 546
e-mail: info@mt-legal.com

---

[1] Vedle toho vzniká též směrnice Evropského parlamentu a Rady o přizpůsobení pravidel mimosmluvní občanskoprávní odpovědnosti umělé inteligence (zkráceně směrnice o odpovědnosti za umělou inteligenci), která má za cíl upravit pravidla a postupy pro vymáhání škody v souvislosti s používáním AI. Dostupné >>> zde.

[2] Znění v českém jazyce z roku 2O21, dostupné >>> zde. Návrh byl schválen Evropským parlamentem dne 13. 3. 2024:
https://cc.cz/europarlament-schvalil-regulaci-umele-inteligence-eu-je-prvni-kdo-prisel-s-pravidly-pro-ai/.

[3] Poslední znění >>>zde.

[4] Jedná se o překlad autorů tohoto článku z anglického znění.

[5] Provider - a natural or legal person, public authority, agency or other body that develops an AI

system or a general purpose AI model or that has an AI system or a general purpose AI model developed and places them on the market or puts the system into service under its own name or trademark, whether for payment or free of charge.

[6] Deployers of AI systems - any natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional aktivity.

[7] Importer - any natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established outside the Union.

[8] Distributor - any natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market.

[9] Článek 2, 5a.: „This Regulation shall not apply to AI systems and models, including their output, specifically developed and put into service for the sole purpose of scientific research and development.

[10] Článek 2, 5b.: „This Regulation shall not apply to any research, testing and development activity regarding AI systems or models prior to being placed on the market or put into service; those activities shall be conducted respecting applicable Union law. The testing in real world conditions shall not be covered by this exemption.“

[11] Článek 2, 5c.: „This Regulation shall not apply to obligations of deployers who are natural persons using AI systems in the course of a purely personal non-professional aktivity.“

[12] Z odůvodnění návrhu AI aktu (bod 1.1) se podává, že se jedná o významná rizika pro zdraví a bezpečnost nebo základní práva osob.

[13] Prohibited Artificial Intelligence Practices.

[14] Č. 52 Transparency obligations for providers and deployers of certain ai systems / povinnosti transparentnosti určitých systémů UI.

[15] Příkladem mohou být systémy, které budou vyvolávat u jednotlivců podvědomé reakce ovlivňující chování např. zaměstnanců. Příkladem může AI systém k analýze finančního chování a osobních preferencí klientů tak, aby podprahově apelovaly na obavy a touhy klientů, například ohledně zabezpečení budoucnosti nebo dosažení rychlého zisku. V tomto směru je nutné poukázat na skutečnost, že podobná forma ovlivňování zcela nepochybně probíhá již v současnosti např. v rámci reklamy na sociálních sítích.

[16] Příkladem může být použití AI marketingu se zaměřeném na starší osoby. AI systém zde

zneužívá jejich zranitelnosti, jako je osamělost nebo zdravotní stav, pro prodej produktů, které mohou být nevhodné nebo finančně zatěžující pro tuto demografickou skupinu.

[17] Příkladem může být AI systém, který po provedené analýze bude cílit reklamu podle parametrů odpovídajících vydefinované specifické skupině lidí na základě jejich charakteristik.

[18] V tomto směru lze pro představu fungování „social scoringu“ doporučit následující díl seriálu Black mirror, dostupné >>> zde.

[19] Příkladem může být AI systém městské správy, který nepřetržitě analyzuje biometrické údaje, aniž by to bylo pro účely jednoho z přípustných důvodů viz uvedené výjimky (takový monitoring je v rozporu se zásadami ochrany soukromí a osobních údajů).

[20] - Pátrání po Obětech a Pohřešovaných Osobách: Použití je dovoleno pro cílené pátrání po obětech únosu, obchodování s lidmi, sexuálního vykořisťování a pro hledání pohřešovaných osob.

- Prevence Ohrožení Bezpečnosti: Povoluje se použití v případech, kde je to nezbytné k prevenci konkrétního a bezprostředního ohrožení života nebo fyzické bezpečnosti osob, nebo k předcházení reálné a předvídatelné hrozbě teroristického útoku.

- Identifikace Podezřelých z Trestných Činů: Systémy lze použít pro lokalizaci nebo identifikaci osob podezřelých ze spáchání trestných činů, které jsou v daném členském státě trestány odnětím svobody na dobu nejméně čtyř let. (zakázáno sledování např. veřejných kamerových systémů pro nalezení osoby.

[21] Jako příklad lze uvést to, že vězeňská správa implementuje AI systém, který analyzuje osobnostní rysy a sociální profil vězňů s cílem predikovat pravděpodobnost jejich recidivy po propuštění. Systém shromažďuje data jako jsou minulé chování, sociální vazby a psychologické profily a vytváří na jejich základě rizikový skór. Tento skór je pak používán k rozhodování o podmínkách propuštění, přidělení do určitých rehabilitačních programů, nebo k určení úrovně dohledu po propuštění.

[22] Tento zákaz neplatí pro AI systémy podporující lidské posouzení, které je založeno na objektivních a ověřitelných skutečnostech.

[23] V navazujícím čl. 16 pak AI akt poskytuje výčet povinností poskytovatelů a uživatelů vysoce rizikových systému AI a dalších stran. Rozbor této materie již nicméně přesahuje záběr tohoto rámcově orientovaného článku.

[24] K příkladům „deepfakes“ >>> zde, >>> zde.

[25] Stanovisko ČAK k využívání AI při poskytování právních služeb ze dne 15. 9. 2023. Dostupné >>> zde.

[26] Ze stanoviska: „Odpovědi na dotazy, které se týkají řešení konkrétního právního problému, je třeba považovat za právní poradu ve smyslu zákona o advokacii, a proto za poskytování právní pomoci, které je vyhrazeno jen oprávněným osobám. Za velmi nevhodnou je třeba považovat situaci, kdy je AI používána na webových stránkách advokáta způsobem, z něhož může potenciální klient nabýt dojmu, že je mu poskytována právní porada oprávněným advokátem v souladu s právními předpisy.“

[27] ChatGPT Team, ChatGPT Enterprise, or our API Platform. Viz obchodní podmínky dostupné z: https://openai.com/enterprise-privacy.

[28] Viz obchodní podmínky. Bod 3.2 „(…) We will not use Customer Content to develop or improve the Services.“ Dostupné z: https://openai.com/policies/business-terms. Enterprise privacy at OpenAI: „We do not train on your business data (data from ChatGPT Team, ChatGPT Enterprise, or our API Platform)“ Dostupné z: https://openai.com/enterprise-privacy.

© EPRAVO.CZ – Sbírka zákonů, judikatura, právo | www.epravo.cz

Další články:

- Civilněprávní prostředky ochrany při koupi falzifikátu
- Novela zákona o pyrotechnice: likvidace profesionálů namísto zmírnění negativních vlivů
- Konec zákonné koncentrace řízení? Návrh Nejvyššího soudu před Ústavním soudem
- Soudní poplatky v řízení o rozvodu manželství a úpravy poměrů k nezletilému dítěti po tzv. rozvodové novele
- Imise ve stavebním řízení aneb kde končí veřejný zájem a začíná soukromé právo?
- Užívání prostoru nad pozemkem třetí osobou
- Přístup k nemovitosti přes pozemek třetí osoby
- PŘEHLEDNĚ: Jak funguje předkládání plné moci? Postačí soudu jen její „fotokopie“? Aneb vývoj právní úpravy požadavků na plnou moc v našem právním systému.
- Využívání nástrojů umělé inteligence: proč je GDPR relevantní?
- Transfer Pricing: Na co si dát pozor s blížícím se koncem roku
- Byznys a paragrafy, díl 24.: Digitalizace korporátního práva: EU cílí na snížení administrativy při přeshraničním podnikání