24. 5. 2024

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

Regulace umělé inteligence v EU, co nás čeká?

Umělá inteligence (dále jen "AI") se stala celosvětovým fenoménem a akt o umělé inteligenci (dále jen "AI ACT") přichází jako první komplexní regulace AI na světě, přináší sjednocená pravidla a požadavky v rámci Evropské Unie, to jak na poskytovatele, tak i na provozovatele služeb umělé inteligence. AI ACT byl 13. března schválen jednomyslnou většinou Evropského parlamentu. V článku níže vysvětlíme co je to AI, rozebereme její kategorizaci a jaké povinnosti z nařízení pro poskytovatele a provozovatele vyplývají.

Nyní probíhá finalizace textu právníky a lingvisty, přičemž formální schválení se očekává na přelomu dubna a května. **Co Vás jakožto poskytovatele nebo provozovatele těchto služeb čeká, co musíte dodržet a jaké sankce Vám případně hrozí? Právě o tom pojednává tento článek.**

I. Základní informace

Evropská Unie převzala definici AI z nedávno aktualizované definice OECD (Organizace pro hospodářskou spolupráci a rozvoj), které je EU v plném rozsahu součástí, zároveň jsou součástí i USA, Kanada a další.

"Systém umělé inteligence je strojově založený systém, který na základě explicitních nebo implicitních cílů odvozuje ze vstupů, které obdrží, jak generovat výstupy, jako jsou předpovědi, obsah, doporučení nebo rozhodnutí, která mohou ovlivnit fyzické nebo virtuální prostředí. Různé systémy umělé inteligence se liší úrovní autonomie a adaptability po nasazení."

Jak již bylo zmíněno výše AI ACT dopadá jak na poskytovatele systémů, tak i na jejich provozovatele.

1. **Poskytovatelem systému AI** je subjekt, který systém vyvíjí a pod svým jménem uvádí na trh EU, přičemž tímto poskytovatelem může být fyzická, právnická osoba, ale i orgán veřejné moci.
2. **Provozovatelem systému AI** se na druhou stranu rozumí subjekt, který systém používá při výkonu své pravomoci, s výjimkou, kdy je tento systém využíván pro osobní účely, nikoliv pro profesionální činnost. *Pozn.: Zde došlo ke změně, původní návrh totiž používal pojem "uživatel", což bylo matoucí, protože se tím nerozuměl koncový uživatel, ale právě provozovatel.*

II. Rozdělení AI systémů do kategorií dle rizika

AI ACT je založen na rozdělení AI systémů do kategorií dle rizika, které jednotlivé systémy představují nebo mohou představovat a následně se podle těchto kategorií odvíjejí požadavky na poskytovatele a uživatele. Těmi kategoriemi jsou jmenovitě:

1. **Nepřijatelně rizikové systémy AI** *(zakázané)*
2. **Vysoce rizikové systémy AI**
3. **Omezeně rizikové systémy AI** *(GPAI)*
4. **Minimálně rizikové systémy AI**

První kategorie nepřijatelně rizikových systémů je zakázána bez dalšího, druhá zmíněná kategorie podléhá silné regulaci, na třetí kategorii dopadá "pouze" požadavek transparentnosti a poslední nepodléhá regulaci žádné.

III. Nepřijatelně rizikové systémy AI

První výše zmíněnou kategorií jsou **nepřijatelně rizikové systémy AI, které jsou zcela zakázané. Zakázané jsou tyto systémy AI, protože nepřijatelně zasahují do práv garantovaných Listinou základních práv a svobod** (např.: právo na ochranu soukromí, svoboda projevu, shromažďovací, zákaz diskriminace a mnoho dalších). **Které systémy AI tedy mezi zakázané spadají?**

1. **AI využívající lidské zranitelnosti** (např. věk, postižení);
2. **biometrické kategorizační systémy využívající citlivé charakteristiky** (rasa, sexuální orientace, politické či náboženské názory atp.), s výjimkou:
    - označování nebo filtrování zákonně získaných souborů biometrických údajů nebo v případě kategorizace biometrických údajů orgány činnými v trestním řízení;
3. **použití** podprahových, **manipulativních** nebo klamavých **technik**, **které narušují chování** a obcházejí svobodnou vůli;
4. **systémy sociálního kreditního hodnocení;**
5. **shromažďování obličejů pro vytváření databáze pro rozpoznávání obličejů;**
6. **specifické aplikace prediktivního policejního dohledu**, tj. posuzování rizika, že se osoba na základě profilování nebo posuzování osobnostních rysů dopustí trestného činu, s výjimkou:
    - případů, kdy se používá k doplnění lidského posouzení založeného na objektivních, ověřitelných skutečnostech přímo souvisejících s trestnou činností;
7. **rozpoznávání emocí na pracovišti nebo ve vzdělávacích institucích**, s výjimkou:
    - zdravotních nebo bezpečnostních důvodů;
8. **používání RBI** *(Real time dálková biometrická identifikace)* **na veřejně přístupných místech pro účely vymáhání práva,** s výjimkou:
    - zabránění závažnému a bezprostřednímu ohrožení života nebo předvídatelnému teroristickému útoku;
    - pátrání po pohřešovaných osobách, obětech únosů a osobách, které se staly obětí obchodování s lidmi nebo sexuálního vykořisťování;
    - identifikace podezřelých ze závažných trestných činů (vražda, ozbrojená loupež, organizovaná trestná činnost a další).

Používání výjimek výše zmíněného RBI s AI je povoleno pouze za případů, kdy by nepoužití systému způsobilo značnou škodu, zároveň však musí být respektována základní práva a svobody dotčených osob. Systém musí být registrovaný v databázi EU (v naléhavých případech může být nasazení zahájeno bez registrace, pokud bude později bez odkladu zaregistrováno, zároveň to musí být řádně odůvodněno) a policie tak smí učinit pouze po dokončení posouzení dopadu na základní práva a svobody.

Povolení od soudního orgánu nebo nezávislého správního orgánu je před nasazením také vyžadováno (v naléhavých případech může být systém nasazen bez povolení, pokud je o něj požádáno do 24 hodin, avšak je-li povolení zamítnuto musí být nasazení ihned ukončeno a všechny výstupy, data smazány).

IV. Vysoce rizikové systémy AI

Další kategorií jsou ty systémy AI, které Evropská unie vyhodnotila jako vysoce rizikové, a to z toho důvodu, že jsou vysoce rizikové buďto pro zdraví, bezpečnost nebo pro základní lidská práva a

svobody osob. Tuto kategorii EU stanovuje v příloze II. a III.

Dle přílohy II. AI ACT jsou vysoce rizikové systémy AI ty, které jsou bezpečnostní součástí výrobku nebo výrobkem samotným a vztahují se na ně harmonizační předpisy EU v příloze uvedené. Těmi jsou systémy používané v autonomních nebo částečně autonomních vozidlech, nebo třeba zdravotnické systémy AI určené pro stanovení diagnózy nebo léčebného postupu.

Příloha III. stanoví, ve kterých oblastech jsou systémy AI vysoce rizikové:

1. **Biometrická identifikace, která není zakázaná**;
2. **Vzdělávání** (systémy, které mají za účel hodnocení studentů vzdělávacích institucí nebo institucí odborné přípravy a hodnocení účastníků zkoušek, které jsou vyžadovány pro přijetí ke studiu);
3. **Nábor a řízení pracovníků** (systémy hodnocení kandidátů v průběhu pohovorů před zaměstnáním osob a systémy hodnotící výkonnost, chování osob v rámci pracovněprávních vztahů);
4. **Správa spravedlnosti** (systémy AI určené na pomoc soudnímu orgánu při zkoumání a výkladu faktů a práva a při uplatňování práva na konkrétní soubor skutečností);
5. **Správa kritické infrastruktury** (voda, plyn, elektřina apod.);
6. **Vymáhání práva, pohraniční kontrola, migrace a azyl** (detektor lží, posouzení ilegální migrace nebo zdravotních rizik atp.);
7. **Přístup ke službám** (bankovnictví, pojištění, sociální dávky, resp. systémy, které vyhodnocují sociální kredit v této oblasti);
8. **Specifické produkty a/nebo bezpečnostní komponenty specifických produktů**

I v této kategorii jsou však výjimky a těmi jsou ty systémy AI, které vykonávají pouze úzkou procedurální úlohu, zlepšují výsledek dříve dokončené lidské práce nebo provádí přípravný úkol k posouzení, které je relevantní pro účely případů použití v příloze III.

Systémy AI, které jsou zařazeny v této kategorii podléhají přísné regulaci a na jejich provozovatele a poskytovatele jsou kladeny přísné požadavky.

Požadavky na <u>poskytovatele</u> vysoce rizikových systémů AI:

1. **systém řízení rizik** (zavést systém řízení rizik, který nepřetržitě, v rámci celého životního cyklu systému AI vyhodnocuje rizika, která mohou vzniknout a zároveň přijímat vhodná opatření);
2. **data a správa dat**, používaných k trénování modelů, za účelem ověření jejich případných nedostatků, chyb nebo rizika zkreslení;
3. **technická dokumentace a vedení záznamů.** Prokazatelnost, že má systém AI vlastnosti požadované AI ACT;
4. **transparentnost a poskytování informací provozovatelům AI,** povinnost poskytnout provozovatelům systému AI transparentní informace nezbytné k jeho užívání, včetně informací o jeho účelu, přesnosti, spolehlivosti a kybernetické bezpečnosti, jeho výkonnosti a specifikaci vstupních údajů;
5. **lidský dohled**
6. **přesnost, spolehlivost a kybernetická bezpečnost**

Požadavky na <u>provozovatele</u> vysoce rizikových systémů AI:

1. **přiměřená a relevantní data** s ohledem na účel systému AI;
2. **monitorovat provoz** vysoce rizikového **systému AI**, za účelem předcházení rizik a zjišťování

incidentů, případně informovat poskytovatele systému AI;
3. **uchovávat** po dobu **nejméně 6 měsíců vybrané protokoly automaticky generované** vysoce rizikovým **systémem AI**;
4. **povinnost provést posouzení vlivu na ochranu osobních údajů** podle GDPR.

V. Omezeně rizikové systémy AI – GPAI

Jednotlivá ustanovení AI ACT se věnují i tzv. GPAI *(General Purpose Artifficial Intelligence)*, tedy umělé inteligenci určené pro všeobecné účely, kterou je například celosvětově známá ChatGPT, ale i grafický Stable Difusion nebo překladač DeepL. V souvislosti s GPAI se vyskytují dva pojmy: model GPAI a systém GPAI.

1. **Model GPAI**, tím se rozumí takový model umělé inteligence, který je vycvičen na velkém množství dat, vykazuje značnou obecnost a je schopen kompetentně vykonávat širokou škálu různých úloh a který lze integrovat do různých návazných systémů nebo aplikací *(výjimkou jsou výzkumné a vývojové modely GPAI)*.
2. **Systém GPAI** je založen na výše zmíněném modelu GPAI a je schopen sloužit různým účelům, a to jak pro přímé použití, tak pro integraci do jiných systémů AI.

Požadavky na poskytovatele GPAI

Jiné požadavky se vztahují na „běžné“ GPAI, na GPAI s „volnou a otevřenou licencí“, na systémy GPAI s jistým „systémovým rizikem“, a systémy GPAI, které mohou být použity jako vysoce rizikové systémy AI nebo do nich mohou být integrovány. Na poslední zmíněné dále dopadá povinnost spolupracovat s následnými poskytovateli, aby umožnili jejich soulad.

Požadavky jsou následující:

1. **technická dokumentace**, včetně procesu školení, testování a hodnocení výsledků *(tento bod se nevztahuje na GPAI s volnou a otevřenou licencí)*;
2. **informace a dokumentace, jež mají být poskytnuty poskytovatelům**, kteří budou model GPAI dále integrovat do svých vlastních systémů AI, aby tito poskytovatelé znali možnosti a omezení modelu GPAI. *(tento bod se nevztahuje na GPAI s volnou a otevřenou licencí)*;
3. **respektování autorských práv**;
4. **dostatečně podrobné shrnutí obsahu použitého** pro trénink modelu GPAI.

Další povinnosti plynou pro ty poskytovatele, jejichž systém je kategorizován jako GPAI se „systémovým rizikem“. To se posuzuje podle výpočetního výkonu, jehož kumulativní objem pro trénování musí přesáhnout 10^{25} operací s pohyblivou desetinnou čárkou za sekundu. AI ACT však stanoví i výjimky, kdy model přesahující výpočetní výkon nebude zařazen mezi ty se „systémovým rizikem“.

Nařízení zavádí u těchto systémů další povinnosti proto, že vysoký výpočetní výkon zvyšuje riziko případného zneužití, činí obtížnější kontrolu a provádění auditů.

Mimo čtyři výše zmíněné požadavky na tyto poskytovatele dopadají i požadavky:

1. **dokumentování a hodnocení modelu** kontradiktorního testování s cílem identifikace systémových rizik;
2. **posuzování systémových rizik** s cílem je zmírňovat;
3. **sledovat, dokumentovat a hlásit závažné incidenty** a nápravná opatření úřadu pro umělou inteligenci
4. **kybernetická bezpečnost**, respektive zajistit odpovídající úroveň.

VI. Minimálně rizikové systémy AI

Do této kategorie spadají systémy AI, které se využívají například k filtrování nevyžádané pošty v e-mailových schránkách, či k integraci ve videohrách. A tyto nařízení nereguluje nijak.

VII. Kdy začne AI ACT "platit"?

AI ACT se stane platným 20 dní od vyhlášení v Úředním věstníku EU, podstatné je ale, kdy vejde v účinnost, a to je rozděleno následovně:

1. 6 měsíců – nepřijatelně rizikové systémy AI
2. 12 měsíců – omezeně rizikové systémy AI
3. 24 měsíců – vysoce rizikové systémy AI podle přílohy III.
4. 36 měsíců – vysoce rizikové systémy AI podle přílohy II.

VIII. Závěr

Umělá inteligence s sebou kromě velkých příležitostí přináší i velká rizika a ovlivňuje každodenní život lidí. Je tedy nepochybné, že je její regulace třeba, není však přílišná regulace zhoubou pokroku?

JUDr. Jakub Dohnal, Ph.D., LL.M.,
advokát, partner

Matěj Menšík,
paralegal

ARROWS advokátní kancelář, s.r.o.

Plzeňská 3350/18
150 00 Praha 5 – Smíchov

Tel.: +420 245 007 740
e-mail: office@arws.cz

Další články:

- Nový zákon o veřejných dražbách, aukce a obálkové metody
- Pohled přes hranice – natáčení pornografických klipů jako důvod výpovědi z nájmu bytu
- Nařízení EU o umělé inteligenci a jeho dopady na využití jazykových modelů v advokátní praxi
- Revize zájezdové směrnice: co přináší, co hrozilo a co to znamená pro praxi
- Kupní smlouva o převodu nemovitosti bez uvedení výše kupní ceny
- Druhá „tlačítková novela": povinné tlačítko pro odstoupení od smlouvy
- Souhlas s veřejným užíváním pozemku jako překážka nároku na bezdůvodné obohacení – nález Ústavního soudu sp. zn. I. ÚS 2541/25
- Kupní smlouva bez přesného určení kupní ceny
- Byznys a paragrafy, díl 36.: Doložka o mlčenlivosti
- Detekce podezřelého obchodu v kontextu hazardních her
- AI omnibus