Umělá inteligence – otázky a odpovědi*

Brussels 12. prosince 2023

Proč musíme regulovat používání umělé inteligence?

Potenciální přínosy umělé inteligence pro naši společnost jsou rozmanité, od lepší zdravotní péče až po lepší vzdělávání. Vzhledem k rychlému technologickému rozvoji v oblasti umělé inteligence se EU rozhodla jednat jako jeden celek, aby tyto příležitosti využila.

Akt EU o umělé inteligenci je prvním komplexním zákonem o umělé inteligenci na světě. Jeho cílem je řešit rizika, jež představuje v oblasti zdraví, bezpečnosti a základních práv. Nařízení rovněž chrání demokracii, právní stát a životní prostředí.

Zatímco většina systémů umělé inteligence bude představovat nízké až nulové riziko, některé systémy umělé inteligence vytvářejí rizika, která je třeba řešit, aby se zabránilo nežádoucím výsledkům.

Například neprůhlednost mnoha algoritmů může vyvolat nejistotu a bránit účinnému prosazování stávajících právních předpisů v oblasti bezpečnosti a základních práv. V reakci na tyto výzvy bylo třeba přijmout legislativní opatření k zajištění dobře fungujícího vnitřního trhu pro systémy umělé inteligence, kde jsou náležitě řešeny přínosy i rizika.

To zahrnuje aplikace, jako jsou systémy biometrické identifikace nebo rozhodnutí činěná umělou inteligencí, která se dotýkají důležitých osobních zájmů, například v oblasti náboru pracovníků, vzdělávání, zdravotní péče nebo vymáhání práva.

Nedávný pokrok v oblasti umělé inteligence vedl ke stále silnější generativní umělé inteligenci. Tzv. „obecné modely umělé inteligence", které jsou integrovány do mnoha systémů umělé inteligence, nabývají natolik na významu, že je třeba hospodářství i společnost v tomto ohledu regulovat. S ohledem na možná systémová rizika zavádí EU účinná pravidla a dohled.

Jaká rizika budou nová pravidla v oblasti umělé inteligence řešit?

Zavádění systémů umělé inteligence má velký potenciál zajistit přínosy pro společnost, hospodářský růst a zvyšování inovací a globální konkurenceschopnosti EU. Avšak v některých případech mohou specifické aspekty některých systémů umělé inteligence vytvářet nová rizika spojená s bezpečností uživatelů a základními právy. Některé silné modely umělé inteligence, které jsou široce využívány, by mohly dokonce představovat systémová rizika.

Podnikům tak chybí právní jistota a zavádění technologií umělé inteligence ze strany podniků a občanů se potenciálně zpomaluje z důvodu nedostatku důvěry. Rozdílné regulační reakce vnitrostátních orgánů by představovaly riziko tříštění vnitřního trhu.

Na koho se akt o umělé inteligenci vztahuje?

Právní rámec se bude vztahovat na veřejné i soukromé subjekty v EU i mimo ni, pokud je **systém umělé inteligence** uváděn na trh Unie nebo pokud jeho používání ovlivňuje osoby nacházející se v EU.

Může se týkat jak poskytovatelů vysoce rizikových systémů umělé inteligence (např. vývojář nástroje pro procházení životopisů uchazečů o zaměstnání), tak provozovatelů těchto systémů (např. banka, která tento nástroj pro procházení životopisů koupí). Dovozci systémů umělé inteligence budou rovněž muset zajistit, aby zahraniční poskytovatel provedl příslušný postup posuzování shody těchto systémů, jež jsou opatřeny evropským označením shody (CE) spolu s požadovanou dokumentací a návodem k použití.

Kromě toho jsou pro poskytovatele obecných modelů umělé inteligence, jež zahrnují velké generativních modely umělé inteligence, stanoveny určité povinnosti.

Poskytovatelé bezplatných modelů s otevřeným zdrojovým kódem jsou od většiny těchto povinností osvobozeni. Tato výjimka se nevztahuje na povinnosti poskytovatelů obecných modelů umělé

inteligence se systémovými riziky.

Povinnosti se rovněž nevztahují na činnosti v oblasti výzkumu, vývoje a činností souvisejících s prototypy, které předcházejí uvolnění na trh, a nařízení se dále nevztahuje na systémy umělé inteligence, které jsou určeny výhradně pro vojenské, obranné nebo národní bezpečnostní účely, bez ohledu na typ subjektu, který tyto činnosti provádí.

Jaké jsou kategorie rizik?

Komise navrhuje přístup založený na posouzení rizik se čtyřmi úrovněmi rizika pro systémy umělé inteligence, jakož i určení rizik specifických pro obecné modely:

- **Minimální riziko**: Všechny ostatní systémy umělé inteligence lze vyvíjet a používat v souladu se stávajícími právními předpisy bez dalších zákonných povinností. Velká většina systémů umělé inteligence, které se v současné době v EU používají nebo pravděpodobně budou používat, spadá do této kategorie. Poskytovatelé těchto systémů se mohou dobrovolně rozhodnout, že uplatní požadavky na důvěryhodnou umělou inteligenci a budou dodržovat dobrovolné kodexy chování.
- **Vysoké riziko**: Omezený počet systémů umělé inteligence definovaných v návrhu, které by mohly mít nepříznivý dopad na bezpečnost lidí nebo jejich základní práva (chráněná Listinou základních práv EU), je považován za vysoce rizikový. K aktu je připojen seznam vysoce rizikových systémů umělé inteligence, který může být přezkoumán, aby odpovídal vývoji případů využití umělé inteligence.
- Mezi tyto systémy patří rovněž bezpečnostní komponenty výrobků, na něž se vztahují odvětvové právní předpisy Unie. Za vysoce rizikové se vždy budou považovat systémy, jejichž shodu musí podle uvedených odvětvových právních předpisů posuzovat třetí strana.
- **Nepřijatelné riziko**: Velmi omezený soubor zvláště škodlivých způsobů využití umělé inteligence, které jsou v rozporu s hodnotami EU, protože porušují základní práva, a budou proto zakázány:
  - **bodování občanů** pro veřejné i soukromé účely,
  - **zneužívání zranitelných míst osob, používání podprahových technik**,
  - **biometrická identifikace na dálku v reálném čase na veřejně přístupných místech donucovacími orgány**, s výhradou omezených výjimek (viz níže),
  - **biometrické kategorizace** fyzických osob na základě biometrických údajů za účelem vyvození nebo odvození jejich rasy, politických názorů, členství v odborových organizacích, náboženského nebo filozofického přesvědčení nebo sexuální orientace. Filtrování souborů údajů založených na biometrických údajích v oblasti prosazování práva bude stále možné,
  - individuální prediktivní policejní práce,
  - **rozpoznávání emocí na pracovišti a ve vzdělávacích institucích**, ledaže by to bylo ze zdravotních nebo bezpečnostních důvodů (např. sledování míry únavy pilota),
  - **Necílené automatické stahování dat z internetových stránek** nebo CCTV pro zobrazení obličeje za účelem vytvoření nebo rozšíření databází.
- **Specifické** riziko, pokud jde o transparentnost: U některých systémů umělé inteligence se ukládají zvláštní požadavky týkající se transparentnosti, například pokud existuje zjevné riziko manipulace (např. pomocí chatbotů). Uživatelé by si měli být vědomi, že komunikují se strojem.

Akt o umělé inteligenci navíc zohledňuje **systémová rizika**, která by mohla vyplynout z **obecných modelů umělé inteligence**, včetně **velkých generativních modelů umělé inteligence**. Ty lze využít pro různé úkoly a stávají se základem mnoha systémů umělé inteligence v EU. Některé z těchto modelů by mohly s sebou nést systémová rizika, pokud jsou velmi schopné nebo široce využívané. Silné modely by například mohly způsobit vážné nehody nebo být zneužity k rozsáhlým kybernetickým útokům. Mnoho jednotlivců by mohlo být zasaženo, pokud model v mnoha aplikacích šíří škodlivé předpojatosti.

Jak poznám, že je systém umělé inteligence vysoce rizikový?

Spolu s jasnou definicí pojmu „vysoce rizikové" stanoví akt v právním rámci solidní metodiku, která pomáhá identifikovat vysoce rizikové systémy umělé inteligence. Cílem je poskytnout podnikům a dalším provozovatelům právní jistotu.

Klasifikace rizik vychází ze zamýšleného účelu systému umělé inteligence v souladu se stávajícími

právními předpisy EU v oblasti bezpečnosti výrobků. Znamená to, že klasifikace rizika závisí na funkci, kterou systém umělé inteligence vykonává, na jeho konkrétním účelu a na podmínkách, za kterých se používá.

V příloze aktu je seznam případů použití, které jsou považovány za vysoce rizikové. Komise zajistí průběžnou aktualizaci a relevanci tohoto seznamu. Systémy na seznamu s vysokým rizikem, které plní úzké procedurální úkoly, zlepšují výsledky předchozích lidských činností, neovlivňují lidská rozhodnutí nebo se zabývají čistě přípravnými úkoly, se za vysoce rizikové nepovažují. Za vysoce rizikový se však vždy považuje takový systém umělé inteligence, který profiluje fyzické osoby.

Jaké jsou povinnosti poskytovatelů vysoce rizikových systémů umělé inteligence?

Před **uvedením vysoce rizikového systému umělé inteligence na trh EU** nebo jeho uvedení do provozu jiným způsobem musí poskytovatelé zajistit **posouzení shody**. To jim umožní prokázat, že jejich systém splňuje závazné požadavky na důvěryhodnou umělou inteligenci (jako je kvalita dat, dokumentace a sledovatelnost, transparentnost, lidský dohled, kybernetická bezpečnost, přesnost a robustnost). Pokud se systém nebo jeho účel podstatně změní, je třeba posouzení zopakovat.

Systémy EU, které jsou bezpečnostními komponenty produktů, na než se vztahují odvětvové právní předpisy EU, budou vždy považovány za vysoce rizikové, pokud jejich shodu musí podle uvedených odvětvových právních předpisů posuzovat třetí strana. Rovněž u biometrických systémů se vždy vyžaduje posouzení shody třetí stranou.

Poskytovatelé vysoce rizikových systémů umělé inteligence budou rovněž **muset zavést systémy řízení kvality a rizik**, aby zajistili jejich soulad s novými požadavky a minimalizovali rizika pro uživatele a dotčené osoby, a to i po uvedení produktu na trh.

Vysoce rizikové systémy umělé inteligence, které zavádějí orgány veřejné moci nebo subjekty jednající jejich jménem, budou muset být **registrovány ve veřejné databázi EU**, pokud se tyto systémy nepoužívají v oblasti prosazování práva a migrace. Tato databáze bude muset být zaregistrována v neveřejné části databáze, která bude přístupná pouze příslušným orgánům dozoru.

Orgány dozoru nad trhem budou podporovat monitorování po uvedení na trh prostřednictvím auditů a tím, že poskytovatelům poskytnou možnost podávat zprávy o závažných incidentech nebo porušeních povinností v oblasti základních práv, o nichž se dozvěděli. Orgán dozoru nad trhem může z výjimečných důvodů povolit uvedení konkrétní vysoce rizikové umělé inteligence na trh.

V případě porušení tyto požadavky umožní, aby vnitrostátní orgány měly přístup k informacím potřebným k prošetření toho, zda bylo dané použití systému umělé inteligence v souladu s právními předpisy.

Jaké jsou příklady vysoce rizikových případů použití definovaných v příloze III?

- Některé kritické infrastruktury, například v oblasti silniční dopravy a dodávek vody, plynu, tepla a elektřiny,
- **vzdělávání a odborná příprava**, např. za účelem hodnocení výsledků učení a řízení procesu učení a monitorování podvádění,
- **zaměstnání, řízení pracovníků** a přístup k samostatné výdělečné činnosti, např. umisťování cílených nabídek zaměstnání, analýza a filtrování žádostí o zaměstnání a hodnocení uchazečů,
- **přístup k základním soukromým a veřejným službám** a dávkám (např. zdravotní péče), **hodnocení úvěruschopnosti** fyzických osob a posouzení rizik a stanovování cen v souvislosti s životním a zdravotním pojištěním,
- některé systémy používané v oblasti **prosazování práva**, **ochrany hranic**, výkonu **spravedlnosti** a **demokratických procesů**,
- **hodnocení a klasifikace tísňových volání**,
- systémy biometrické identifikace, kategorizace a rozpoznávání emocí (mimo zakázané kategorie),
- doporučovací systémy velmi velkých online platforem sem nepatří, neboť jsou již upraveny v jiných právních předpisech (nařízení o digitálních trzích / nařízení o digitálních službách).

Jak jsou obecné modely umělé inteligence regulovány?

Obecné modely umělé inteligence, včetně **velkých generativních modelů umělé inteligence**, lze použít pro různé úkoly. Jednotlivé modely mohou být začleněny do velkého počtu systémů umělé

inteligence.

Je důležité, aby poskytovatel, který chce stavět na obecném modelu umělé inteligence, měl všechny nezbytné informace, aby zajistil, že jeho systém bude bezpečný a v souladu s aktem o umělé inteligenci.

Akt o umělé inteligenci proto poskytovatelům takových modelů ukládá povinnost **zpřístupnit určité informace poskytovatelům navazujícího systému.** Tato **transparentnost** umožňuje těmto modelům lépe porozumět.

Poskytovatelé modelů musí mít navíc zavedeny politiky, které zajistí, aby se při školení o jejich modelech **dodržovalo autorské právo**.

Navíc některé z těchto modelů by mohly zakládat na **systémová rizika**, neboť jsou velmi schopné nebo široce využívané.

Obecné modely umělé inteligence, které byly naučeny pomocí **celkového výpočetního výkonu vyššího než 10^25 FLOPs**, jsou prozatím považovány za modely se systémovým rizikem, protože modely naučené pomocí většího výpočetního výkonu bývají výkonnější. Úřad pro umělou inteligenci (zřízený v rámci Komise) může tuto prahovou hodnotu aktualizovat s ohledem na technologický pokrok a dále může v konkrétních případech určit jiné modely jako takové na základě dalších kritérií (např. počtu uživatelů nebo stupně autonomie modelu).

Poskytovatelé modelů se systémovými riziky jsou proto pověřeni **posuzováním a zmírňováním rizik**, **hlášením závažných incidentů**, **prováděním nejmodernějších testů a hodnocení modelů**, zajištěním **kybernetické bezpečnosti** a poskytováním **informací o spotřebě energie** svých modelů.

Za tímto účelem se od nich žádá, aby **ve spolupráci s Evropským úřadem pro umělou inteligenci** vypracovaly kodexy chování jako hlavní nástroj pro podrobné stanovení pravidel ve spolupráci s dalšími odborníky. **Vědecká komise** bude hrát ústřední úlohu při dohledu nad obecnými modely umělé inteligence.

Proč je 10^25 FLOPS vhodnou prahovou hodnotou pro obecnou umělou inteligenci se systémovými riziky?

Tato prahová hodnota zachycuje v současnosti nejpokročilejší obecné modely umělé inteligence, konkrétně GPT-4 od společnosti OpenAI a pravděpodobně Gemini od Google DeepMind.

Schopnosti modelů nad touto hranicí nejsou dosud dostatečně známy. Mohly by představovat systémová rizika, a proto je rozumné, aby jejich poskytovatelé splňovali další povinnosti.

FLOP je prvním zástupným ukazatelem schopností modelu a přesná prahová hodnota FLOP může být Evropským úřadem pro umělou inteligenci aktualizována směrem nahoru nebo dolů, např. s ohledem na pokrok v objektivním měření schopností modelu a na vývoj výpočetního výkonu potřebného pro danou úroveň výkonu.

Akt o umělé inteligenci lze změnit za účelem aktualizace prahové hodnoty FLOP (prostřednictvím aktu v přenesené pravomoci).

Obstojí akt o umělé inteligenci i v budoucnu?

Nařízení zavádí různou úroveň rizik a stanoví jasné definice, a to i pro obecnou umělou inteligenci.

Právní předpisy stanoví požadavky na vysoce rizikové systémy umělé inteligence zaměřené na výsledky, ale konkrétní technická řešení a zprovoznění ponechávají především na průmyslem žádaných normách, které zajistí, že právní rámec bude flexibilní, aby jej bylo možné přizpůsobit různým případům použití a umožnit nová technologická řešení.

Kromě toho lze akt o umělé inteligenci změnit prostřednictvím aktů v přenesené pravomoci a prováděcích aktů, včetně aktualizace prahové hodnoty FLOP (akt v přenesené pravomoci), doplnění kritérií pro klasifikaci obecných modelů umělé inteligence jako modelů představujících systémová rizika (akt v přenesené pravomoci), změny způsobů zřízení tzv. regulačních pískovišť a prvků plánu testování v reálném prostředí (prováděcí akty).

Jak akt o umělé inteligenci upravuje biometrickou identifikaci?

Používání **biometrické identifikace na dálku v reálném čase na veřejně přístupných místech** (tj. rozpoznávání obličeje pomocí CCTV) pro účely prosazování práva je zakázáno, pokud se nepoužije v jednom z těchto případů:

- činnosti v oblasti prosazování práva související s 16 konkrétními trestnými činy,

- cílené vyhledávání konkrétních obětí, únosů, obchodování s lidmi a sexuálního vykořisťování a pohřešovaných osob nebo
- předcházení ohrožení života nebo fyzické bezpečnosti osob nebo reakce na současnou nebo předvídatelnou hrozbu teroristického útoku.

Seznam 16 trestných činů obsahuje:

- terorismus,
- obchodování s lidmi,
- pohlavní vykořisťování dětí a materiály týkající se pohlavního zneužívání dětí,
- nedovolený obchod s omamnými a psychotropními látkami,
- nedovolený obchod se zbraněmi, střelivem a výbušninami,
- vraždu,
- těžké ublížení na zdraví,
- nedovolený obchod s lidskými orgány a tkáněmi,
- nedovolený obchod s jadernými nebo radioaktivními materiály,
- únos, nezákonné omezování osobní svobody a braní rukojmí,
- trestné činy spadající do pravomoci Mezinárodního trestního soudu,
- únos letadla nebo plavidla,
- znásilnění,
- trestné činy proti životnímu prostředí,
- organizovanou nebo ozbrojenou loupež,
- sabotáž, účast na zločinném spolčení zapojeném do jednoho nebo více trestných činů uvedených výše.

Biometrická identifikace na dálku v reálném čase ze strany donucovacích orgánů by podléhala **povolení soudního nebo nezávislého správního orgánu**, jehož rozhodnutí je závazné. V naléhavých případech lze povolení vydat do 24 hodin; je-li povolení zamítnuto, musí být všechny údaje a výstupy smazány.

Mělo by mu předcházet **posouzení dopadů na základní práva** a mělo by být **oznámeno příslušnému orgánu dozoru nad trhem a orgánu pro ochranu údajů**. V naléhavých případech se může systém začít používat bez registrace.

Používání systémů umělé inteligence pro **„zpětnou" biometrickou identifikaci na dálku** (identifikaci osob v dříve shromážděném videomateriálu) vyšetřovaných osob vyžaduje předchozí povolení soudního orgánu nebo nezávislého správního orgánu a oznámení orgánu pro ochranu údajů a dozor nad trhem.

Proč jsou pro biometrickou identifikaci na dálku zapotřebí zvláštní pravidla?

Biometrická identifikace může mít různé podoby. Lze ji používat pro ověřování totožnosti uživatele, tj. pro odemčení chytrého telefonu, nebo pro ověření či kontrolu totožnosti osob podle jejich cestovních dokladů (porovnání 1:1) při překročení hranic.

Biometrická identifikace by také mohla být využívána na dálku, k identifikaci osob v davu, kdy se například porovnává fotografie osoby s databází (porovnání 1:n).

Přesnost systémů pro rozpoznávání obličeje se může značně lišit v závislosti na široké škále faktorů, jako je kvalita kamery, světlo, vzdálenost, databáze, algoritmus a etnická příslušnost, věk nebo pohlaví dané osoby. Totéž platí pro rozpoznávání chůze a hlasu a další biometrické systémy. Velmi pokročilé systémy neustále snižují míru chybné shody.

I když se přesnost 99 % může zdát obecně dobrá, představuje značné riziko, pokud vede k podezírání nevinné osoby. Dokonce i 0,1% chybovost je vysoká, pokud se týká desítek tisíc lidí denně.

Jak tato pravidla chrání základní práva?

Na úrovni EU a členských států již existuje silná ochrana základních práv a nediskriminace, avšak složitost a neprůhlednost některých aplikací umělé inteligence („černé skříňky") představují problém.

Přístup k umělé inteligenci zaměřený na člověka znamená zajistit, aby aplikace umělé inteligence

byly v souladu s právními předpisy v oblasti základních práv. Požadavky na odpovědnost a transparentnost při používání vysoce rizikových systémů umělé inteligence spolu s lepšími kapacitami v oblasti vymáhání práva zajistí, že soulad s právními předpisy bude zohledněn ve fázi vývoje.

V případě porušení tyto požadavky umožní, aby vnitrostátní orgány měly přístup k informacím potřebným k prošetření toho, zda bylo dané použití umělé inteligence v souladu s právními předpisy EU.

Akt o umělé inteligenci navíc vyžaduje, aby provozovatelé, kteří jsou veřejnoprávními subjekty nebo soukromými provozovateli poskytujícími veřejné služby, a provozovatelé poskytující vysoce rizikové systémy provedli posouzení dopadu na základní práva.

Co je posouzení dopadu na základní práva? Kdo musí takové posouzení provést a kdy?

Používání vysoce rizikového systému umělé inteligence může mít dopad na základní práva. Provozovatelé, kteří jsou veřejnoprávními subjekty nebo soukromými provozovateli poskytujícími veřejné služby, a provozovatelé poskytující vysoce rizikové systémy proto provedou posouzení dopadu na základní práva a výsledky oznámí vnitrostátnímu orgánu.

Posouzení sestává z popisu procesů provozovatelů, v nichž bude vysoce rizikový systém umělé inteligence používán, doby a četnosti, v níž má být daný vysoce rizikový systém umělé inteligence používán, kategorií fyzických osob a skupin, které budou jeho používáním v konkrétním kontextu pravděpodobně dotčeny, specifických rizik újmy, která by mohla mít dopad na dotčené kategorie osob nebo skupiny osob, popis provádění opatření lidského dohledu a opatření, která mají být přijata v případě naplnění rizik.

Pokud poskytovatel již tuto povinnost splnil prostřednictvím posouzení vlivu na ochranu osobních údajů, provede se posouzení dopadu na základní práva ve spojení s tímto posouzením vlivu na ochranu osobních údajů.

Jak se toto nařízení zabývá rasovými a genderovými předpojatostmi v systémech umělé inteligence?

Je velmi důležité, aby systémy umělé inteligence **nevytvářely a nereprodukovaly předpojatosti**. Jsou-li **systémy umělé inteligence správně navrženy a používány, mohou naopak přispět ke zmírnění předsudků a stávající strukturální diskriminace**, a vést tak ke spravedlivějším a nediskriminačním rozhodnutím (např. při náboru pracovníků).

K tomuto účelu poslouží nové závazné požadavky na všechny vysoce rizikové systémy umělé inteligence. Systémy umělé inteligence musí být **technicky robustní**, aby bylo zaručeno, že daná technologie je vhodná pro zamýšlený účel a že falešně pozitivní/negativní výsledky neúměrně neovlivňují chráněné skupiny (např. pokud jde o rasový nebo etnický původ, pohlaví, věk atd.).

Vysoce rizikové systémy bude rovněž nutné **učit a testovat na dostatečně reprezentativních souborech dat**, aby se **minimalizovalo riziko zanesení nespravedlivých předpojatostí** do modelu, a bude třeba zajistit, že toto riziko lze řešit prostřednictvím vhodných opatření pro odhalování a korekci předpojatostí a dalších zmírňujících opatření.

Takové systémy musí být rovněž **vysledovatelné a kontrolovatelné**, přičemž je třeba zajistit, aby byla **uchovávána příslušná dokumentace**, včetně dat použitých pro učení algoritmu, která by měla klíčový význam při šetřeních ex post.

Systém kontroly dodržovaní požadavků před uvedením systémů umělé inteligence na trh a po jejich uvedení na trh bude muset zajistit **pravidelné sledování** těchto systémů a **rychlé řešení potenciálních rizik**.

Kdy bude akt o umělé inteligenci plně použitelný?

Po přijetí Evropským parlamentem a Radou vstoupí akt o umělé inteligenci v platnost dvacátým dnem po vyhlášení v Úředním věstníku. Bude plně použitelný 24 měsíců po vstupu v platnost s tímto odstupňovaným přístupem:

- šest měsíců po vstupu v platnost členské státy postupně ukončí zakázané systémy,
- 12 měsíců: povinnosti týkající se řízení obecné umělé inteligence se začínají uplatňovat,
- 24 měsíců: začínají se uplatňovat všechna pravidla aktu o umělé inteligenci, včetně povinností u vysoce rizikových systémů definovaných v příloze III (seznam vysoce rizikových případů použití),

- 36 měsíců: platí povinnosti pro vysoce rizikové systémy definované v příloze II (seznam harmonizovaných právních předpisů Unie).

Jak se bude akt o umělé inteligenci prosazovat?

Při uplatňování a prosazování tohoto nařízení hrají klíčovou úlohu členské státy. V tomto ohledu by měl každý členský stát určit jeden nebo více **příslušných vnitrostátních orgánů**, které budou dohlížet na uplatňování a provádění a provádět činnosti dozoru nad trhem.

V zájmu zvýšení efektivity a stanovení oficiálního kontaktního místa pro veřejnost a další protistrany by měl každý členský stát určit jeden vnitrostátní orgán dohledu, který bude danou zemi rovněž zastupovat v **Evropské radě pro umělou inteligenci**.

Další technické odborné znalosti poskytne **poradní fórum** zastupující vyvážený výběr zúčastněných stran, včetně průmyslu, začínajících podniků, malých a středních podniků, občanské společnosti a akademické obce.

Kromě toho bude v rámci Komise zřízen nový **Evropský úřad pro umělou inteligenci**, který bude dohlížet na modely obecné umělé inteligence, bude spolupracovat s Evropskou radou pro umělou inteligenci a bude podporován **vědeckou skupinou** nezávislých odborníků.

Proč je nutná Evropská rady pro umělou inteligenci a co bude dělat?

Evropská rada pro umělou inteligenci se skládá z **vysokých představitelů příslušných vnitrostátních orgánů dozoru**, evropského inspektora ochrany údajů a Komise. Jejím úkolem je usnadnit hladké, účinné a harmonizované provádění nového nařízení o umělé inteligenci.

Rada bude Komisi vydávat doporučení a stanoviska týkající se vysoce rizikových systémů umělé inteligence a dalších aspektů důležitých pro účinné a jednotné provádění nových pravidel. V neposlední řadě bude rovněž podporovat normalizační činnosti v této oblasti.

Jaké jsou úkoly Evropského úřadu pro umělou inteligenci?

Úkolem úřadu pro umělou inteligenci je **rozvíjet odborné znalosti a schopnosti Unie** v oblasti umělé inteligence a přispívat k provádění právních předpisů Unie v oblasti umělé inteligence v centralizované struktuře.

Úřad pro umělou inteligenci zejména **prosazuje nová pravidla pro obecné modely umělé inteligence a dohlíží na ně**. To zahrnuje vypracování kodexů postupů, které podrobně stanoví pravidla, jeho roli při klasifikaci modelů se systémovými riziky a sledování účinného provádění a dodržování nařízení. Posledně jmenované úloze napomáhá pravomoc požadovat dokumentaci, provádět modelová hodnocení, vyšetřovat výstrahy a požadovat od poskytovatelů, aby přijali nápravná opatření.

Úřad pro umělou inteligenci zajišťuje koordinaci politiky v oblasti umělé inteligence a spolupráci mezi zúčastněnými orgány, institucemi a jinými subjekty Unie, jakož i s odborníky a zúčastněnými stranami. Zejména bude poskytovat **silnou vazbu na vědeckou obec** v zájmu podpory prosazování práva, bude sloužit jako mezinárodní referenční bod pro nezávislé odborníky a odborné organizace a bude usnadňovat výměnu a spolupráci s podobnými institucemi na celém světě.

Jaký je rozdíl mezi radou pro umělou inteligenci, úřadem pro umělou inteligenci, poradním fórem a vědeckou skupinou nezávislých odborníků?

Rada pro umělou inteligenci rozšířila úkoly spočívající v poskytování poradenství a pomoci Komisi a členským státům.

Úřad pro umělou inteligenci je zřízen v rámci Komise a jeho úkolem je rozvíjet odborné znalosti a schopnosti Unie v oblasti umělé inteligence a přispívat k provádění právních předpisů Unie v oblasti umělé inteligence. Úřad pro umělou inteligenci zejména prosazuje nová pravidla pro modely obecné umělé inteligence a dohlíží na ně.

Činnost **poradního fóra** bude spočívat ve vyváženém výběru zúčastněných stran, včetně průmyslu, začínajících podniků, malých a středních podniků, občanské společnosti a akademické obce. Zřizuje se za účelem poradenství a poskytování technických odborných znalostí radě a Komisi, přičemž členové jsou jmenováni radou ze zúčastněných stran.

Vědecká skupina nezávislých odborníků podporuje provádění a prosazování nařízení, pokud jde o modely a systémy obecné umělé inteligence, a členské státy by měly přístup ke skupině odborníků.

Jaké jsou sankce za porušení předpisů?

Pokud budou na trh nebo do provozu uvedeny systémy umělé inteligence, které nesplňují požadavky nařízení, **budou členské státy muset stanovit účinné, přiměřené a odrazující sankce** v souvislosti s porušením předpisů, včetně správních pokut, a oznámit je Komisi.

Nařízení stanoví mezní hodnoty, které je třeba zohlednit:

- **až 35 milionů EUR nebo 7 %** celkového celosvětového ročního obratu za předchozí účetní období (podle toho, která hodnota je vyšší) za porušení týkající se **zakázaných praktik nebo nedodržení požadavků** na data,
- **až 15 milionů EUR nebo 3 %** celkového celosvětového ročního obratu za předchozí účetní období v případě **nedodržení ostatních požadavků** nebo povinností podle nařízení, včetně porušení pravidel pro **modely obecné umělé inteligence**,
- **až 7,5 milionu EUR nebo 1,5 %** celkového celosvětového ročního obratu za předchozí účetní období v případě **poskytnutí nesprávných, neúplných nebo zavádějících informací** oznámeným subjektům a příslušným vnitrostátním orgánům v odpovědi na žádost.
- Pro každou kategorii porušení by byla prahová hodnota pro malé a střední podniky ta nižší ze dvou částek a vyšší částka pro ostatní společnosti.

Za účelem harmonizace vnitrostátních pravidel a postupů při stanovování správních pokut **vypracuje Komise na základě doporučení Rady pro umělou inteligenci pokyny**.

Vzhledem k tomu, že orgány, agentury a instituce EU by měly jít příkladem, budou se pravidla a možné sankce vztahovat i na ně; evropský inspektor ochrany údajů bude mít pravomoc ukládat jim pokuty.

Co mohou učinit jednotlivci, kteří jsou porušením pravidel dotčeni?

Akt o umělé inteligenci stanoví právo podat stížnost u vnitrostátního orgánu. Na tomto základě mohou vnitrostátní orgány zahájit činnosti dozoru nad trhem v souladu s postupy uvedenými v nařízeních o dozoru nad trhem.

Cílem směrnice o odpovědnosti za umělou inteligenci je navíc poskytnout osobám usilujícím o náhradu škody způsobené vysoce rizikovými systémy umělé inteligence účinné prostředky k identifikaci potenciálně odpovědných osob a získání příslušných důkazů o nároku na náhradu škody. Za tímto účelem navrhovaná směrnice stanoví zpřístupnění důkazů o konkrétních vysoce rizikových systémech umělé inteligence, u nichž existuje podezření, že způsobily škodu.

Revidovaná směrnice o odpovědnosti za vadné výrobky navíc zajistí, že odškodnění bude dostupné pro jednotlivce, kteří zemřou, utrpí zranění nebo poškození majetku způsobené vadným výrobkem v Unii, a objasní, že na systémy umělé inteligence a na produkty, jejichž součástí jsou systémy umělé inteligence, se rovněž vztahují stávající pravidla.

Jak fungují dobrovolné kodexy chování v případě vysoce rizikových systémů umělé inteligence?

Poskytovatelé aplikací, které nejsou vysoce rizikové, mohou zajistit důvěryhodnost svých systémů umělé inteligence tím, že vypracují své vlastní dobrovolné kodexy chování nebo se připojí ke kodexům chování přijatým jinými reprezentativními sdruženími.

Tyto kodexy budou platit současně s povinnostmi v oblasti transparentnosti pro některé systémy umělé inteligence.

Komise bude průmyslová sdružení a další reprezentativní organizace vybízet k tomu, aby přijaly dobrovolné kodexy chování.

Jak fungují kodexy správné praxe v případě obecných modelů umělé inteligence?

Komise vyzývá poskytovatele obecných modelů umělé inteligence a další odborníky, aby společně pracovali na kodexu správné praxe.

Jakmile bude tento kodex za tímto účelem vypracován a schválen, mohou jej poskytovatelé obecných modelů umělé inteligence používat k prokázání souladu s příslušnými povinnostmi vyplývajícími z aktu o umělé inteligenci, a to po vzoru obecného nařízení o ochraně osobních údajů.

To je obzvláště důležité pro upřesnění pravidel pro poskytovatele obecného modelu umělé inteligence se systémovými riziky, aby byla zajištěna účinná pravidla pro posuzování a zmírňování rizik, která obstojí i v budoucnu, jakož i další povinnosti.

Obsahuje akt o umělé inteligenci ustanovení týkající se ochrany životního prostředí a udržitelnosti?

Cílem návrhu aktu o umělé inteligenci je řešit rizika pro bezpečnost a základní práva, včetně základního práva na vysokou úroveň ochrany životního prostředí. Životní prostředí je rovněž jedním z výslovně uvedených a chráněných právních zájmů.

Komise se vyzývá, aby požádala evropské normalizační organizace o výsledek normalizace týkající se postupů podávání zpráv a dokumentace s cílem zlepšit výkonnost systémů umělé inteligence v oblasti zdrojů, jako je snížení spotřeby energie a dalších zdrojů vysoce rizikového systému umělé inteligence během jeho životního cyklu, a energeticky účinný vývoj obecných modelů umělé inteligence.

Komise se dále vyzývá, aby do dvou let ode dne použitelnosti nařízení a poté každé čtyři roky předložila zprávu o přezkumu pokroku při vývoji produktů normalizace v oblasti energeticky účinného vývoje obecných modelů umělé inteligence a posoudila potřebu dalších opatření nebo kroků, včetně těch závazných.

Kromě toho jsou poskytovatelé obecných modelů umělé inteligence, které jsou naučeny na velkém množství dat, a mohou proto vykazovat vysokou spotřebu energie, povinni zveřejňovat informace o spotřebě energie.

Komise se žádá, aby pro toto posouzení vypracovala vhodnou metodiku.

V případě obecných modelů umělé inteligence se systémovými riziky je třeba rovněž posoudit energetickou účinnost.

Jak mohou nová pravidla podpořit inovace?

Regulační rámec může podpořit zavádění umělé inteligence dvěma způsoby. Na jedné straně důvěra uživatelů zvýší poptávku po umělé inteligenci, kterou používají společnosti a veřejné orgány. Na druhé straně poskytovatelé umělé inteligence budou mít díky větší právní jistotě a harmonizaci pravidel přístup k větším trhům s produkty, které uživatelé a spotřebitelé oceňují a nakupují. Pravidla se použijí pouze tehdy, je-li to nezbytně nutné, a to s jednoduchou strukturou řízení a způsobem, který minimalizuje zátěž pro hospodářské subjekty.

Akt o umělé inteligenci dále umožňuje vytváření **regulačních pískovišť** a **testování v reálném provozu**, jež poskytují kontrolované prostředí pro testování inovativních technologií po omezenou dobu, čímž v souladu s aktem o umělé inteligenci podporují inovace ze strany společností, malých a středních podniků a začínajících podniků. Společně s ostatními opatřeními, jako jsou další **sítě excelence center umělé inteligence** a **partnerství veřejného a soukromého sektoru v oblasti umělé inteligence, dat a robotiky** a přístup k **centrům pro digitální inovace** a k **testovacím a experimentálním zařízením**, pomohou vytvořit správné rámcové podmínky pro podniky, aby rozvíjely a zaváděli umělou inteligenci.

Testování vysoce rizikových systémů umělé inteligence v reálném provozu lze provádět po dobu nejvýše šesti měsíců (která může být prodloužena o dalších šest měsíců). Před testováním je třeba vypracovat plán, který musí být předložen orgánu dozoru nad trhem, který musí plán a zvláštní testovací podmínky schválit, se standardním tichým souhlasem, pokud do 30 dnů neobdrží odpověď. Příslušný orgán může testování bez ohlášení kontrolovat.

Testování v reálném provozu lze provádět pouze se zvláštními zárukami, např. uživatelé systémů v rámci testování v reálném provozu musí poskytnout informovaný souhlas, testování na ně nesmí mít negativní dopad, výsledky musí být vratné nebo ignorovatelné a jejich data musí být po ukončení testování smazána. Zvláštní ochrana má být poskytnuta zranitelným skupinám, tj. v důsledku jejich věku, tělesnému nebo mentálnímu postižení.

Jak EU vedle aktu o umělé inteligenci usnadní a podpoří inovace v oblasti umělé inteligence?

Přístup EU k umělé inteligenci je založen na excelenci a důvěře s cílem posílit výzkumnou a průmyslovou kapacitu a zároveň zajistit bezpečnost a ochranu základních práv. Lidé a podniky by měli mít možnost využívat výhod umělé inteligence a zároveň cítit bezpečí a ochranu. Cílem evropské strategie pro umělou inteligenci je učinit z EU centrum světové úrovně pro umělou inteligenci a zajistit, aby se umělá inteligence zaměřovala na člověka a byla důvěryhodná. V dubnu 2021 předložila Komise svůj balíček týkající se umělé inteligence, který zahrnuje: 1) přezkum koordinovaného plánu v oblasti umělé inteligence a 2) jeho návrh nařízení, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci.

Prostřednictvím koordinovaného plánu pro umělou inteligenci přijala Evropská komise komplexní strategii na podporu rozvoje a přijetí umělé inteligence v Evropě. Zaměřuje se na vytváření podmínek umožňujících rozvoj a zavádění umělé inteligence, zajištění nejvyšší úrovně od laboratoře až po trh, zvýšení důvěryhodnosti umělé inteligence a budování strategického vedení v odvětvích se značným dopadem.

Komise usiluje o využití aktivit členských států koordinací a harmonizací jejich úsilí, aby podpořila soudržný a synergický přístup k rozvoji a přijetí umělé inteligence. Komise rovněž vytvořila platformu Evropské aliance pro umělou inteligenci, která sdružuje zúčastněné strany z akademické obce, průmyslu a občanské společnosti za účelem výměny znalostí a poznatků o politikách v oblasti umělé inteligence.

Koordinované plány navíc počítají s několika opatřeními, jejichž cílem je uvolnit datové zdroje, posilovat kritickou výpočetní kapacitu, zvyšovat výzkumné kapacity, podporovat evropskou síť testovacích a experimentálních zařízení a podporovat malé a střední podniky prostřednictvím evropských center pro digitální inovace.

Jaký mezinárodní rozměr má přístupu EU?

Akt o umělé inteligenci a koordinovaný plán pro umělou inteligenci jsou součástí úsilí Evropské unie zastávat vůdčí roli v oblasti podpory důvěryhodné umělé inteligence na mezinárodní úrovni. Umělá inteligence se stala oblastí strategického významu na křižovatce ambicí v oblasti geopolitiky, obchodních zájmů a obav o bezpečnost.

Země na celém světě používají umělou inteligenci jako způsob, jak dát najevo, že si přejí prostřednictvím její užitečnosti a potenciálu dosáhnout technického pokroku. Regulace umělé inteligence je teprve v počátcích a EU přijme opatření na podporu stanovení celosvětových norem pro umělou inteligenci v úzké spolupráci s mezinárodními partnery v souladu s mnohostranným systémem založeným na pravidlech a hodnotami, které prosazuje. EU hodlá prohloubit partnerství, koalice a aliance s partnery EU (např. Japonskem, USA, Indií, Kanadou, Jižní Koreou, Singapurem nebo oblastí Latinské Ameriky a Karibiku), jakož i s mnohostrannými (např. OECD, G7 a G20) a regionálními organizacemi (např. Radou Evropy).

**Aktualizováno 14. prosince 2023*

QANDA/21/1683

Kontaktní osoby:

Johannes BAHRKE (+32 2 295 86 15)
Thomas Regnier (+32 2 29 9 1099)

Pro veřejnost: služba Europe Direct , tel 00 800 67 89 10 11 nebo e-mail