E-Bezpečí 2024, 9(1): Page 62-65. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=3975

EVROPSKÁ UNIE PŘEDSTAVILA PRVNÍ PRÁVNÍ RÁMEC O RIZICÍCH AI NA SVĚTĚ. O ČEM JE TAKZVANÝ AKT O UMĚLÉ INTELIGENCI A CO ČESKÉ REPUBLICE PŘINESE?

Karolína ZIBUROVÁ

Akt o umělé inteligenci je vůbec prvním komplexním právním rámcem v oblasti umělé inteligence na světě. Tento dokument se zabývá právní úpravou a riziky použití umělé inteligence. V platnost by měl vstoupit v roce 2026, avšak již koncem tohoto roku lze očekávat platnost některých zákazů, které jsou popsány v článku níže. Evropská unie s tímto dokumentem přišla především proto, aby doplnila chybějící pravidla a požadavky týkající se AI. V minulém roce jsme zaznamenali mnoho apelů směřovaných na EU ohledně nutnosti zavést takový dokument. Nejvýraznější byl zřejmě krok ze strany italského úřadu pro ochranu osobních údajů, který zahájil vyšetřování s ohledem na porušení legislativy Evropské unie o ochraně osobních údajů u modelu GPT od OpenAI. Nyní se pojďme podívat na to, co tento rámec upravuje.

Regulační rámec a čtyři úrovně rizik

Regulační rámec navrhuje pravidla, která jasně specifikují systémy, které mají být zakázány, protože jsou moc riskantní z hlediska bezpečnosti a další systémy určitým způsobem omezuje. Některé systémy například bude třeba testovat, než se dostanou na trh.

Dokument rozlišil systémy na základě čtyř úrovní rizik, která představují pro uživatele a demokracii.

Rizika jsou rozdělena následovně:
1. Nepřijatelné riziko
2. Vysoké riziko
3. Omezené riziko
4. Minimální riziko

1. Nepřijatelné riziko

Systémy, které jsou označeny za nepřijatelně rizikové budou zakázány. Jedná se například o systémy, které jsou hrozbou pro bezpečnost a lidská práva. Příkladem mohou programy, které vyhodnocují **sociální kredit občanů** (tzv. social scoring) nastavené vládou nebo například hračky využívající hlasové asistenty, kteří nabádají k nebezpečnému chování.

2. Vysoké riziko

Systémy s vysokým rizikem pro bezpečnost jsou v dokumentu označeny jako systémy, kde je **AI využívána například v oblasti kritické infrastruktury** (např. dopravy). Tam by mohlo být dle EU ohroženo zdraví občanů. Dále jde například o oblast vzdělávání, v té by mohlo dojít k ovlivnění přístupu ke vzdělávání (např. hodnocení zkoušek). Podobným způsobem by mohly být ovlivněny výsledky náborů v oblasti hledaní pracovníků, které by využívaly AI. Za vysoce rizikové jsou také považovány AI systémy v oblasti zdravotnictví, které můžeme zaznamenat například v oblasti roboticky asistované chirurgii. V oblasti soudní jsou také za vysoce rizikové označeny procesy, které nějak zasahují do demokracie a základních práv (např. hodnocení spolehlivosti důkazů nebo vydávání soudních rozhodnutí). S tím souvisí také oblast migrace a kontroly hranic. Zde je za příklad rizika uvedeno například automatické vydávání víz.

Tyto systémy nebudou zakázány jako systémy s nepřijatelným rizikem, ale měly by podléhat přísným regulacím a kontrolám.

Půjde například o nutnost zveřejnění veškerých informací o systému, adekvátní dohled člověka nad výsledky, který bude schopen svou kontrolou minimalizovat rizika, zaznamenávání výsledků tak, aby bylo vše možné zpětně dohledat a zajištění vysoké míry bezpečnosti ze strany provozovatele.

Za vysoké riziko považuje EU také všechny systémy, které využívají biometrické identifikace a ty zakazuje. Výjimku zde tvoří pouze případy ohrožení. Využity by proto měly být například k hledání dítěte v ohrožení, k zabránění teroristickému útoku nebo ke stíhání pachatele, který je podezřelý z trestné činnosti.

3. Omezené riziko

Za omezené riziko Akt o umělé inteligenci považuje především **systémy, které mohou mást uživatele**. Akt totiž říká, že je třeba, aby byl systém vždy transparentní. Uživatel se s tím může setkat například ve chvíli, kdy komunikuje s chatbotem. EU totiž říká, že je třeba zajistit, aby uživatel vždy věděl, že komunikuje se strojem a mohl se tak rozhodnout, zda do této konverzace chce vstupovat. Toto omezení se týká také generovaného textu, i v tomto případě EU chce, aby takový text byl vždy označen a čtenář tak byl informovaný o tom, že čte text vytvořený umělou inteligencí nikoli člověkem. Tímto EU řeší například problematiku deep fake videí (videí vytvořených umělou inteligencí), které jsou dlouhodobě označovány za hrozbu. Tato videa mohou být totiž použita například při ovlivňování mínění voličů a ohrozit tak demokracii.

4. Minimální riziko

Akt o umělé inteligenci plně dovoluje systémy s minimálním rizikem. Pro nás se jedná o systémy, které jsou již dlouhodobě používané a nepředstavují žádné riziko. Jedná se o největší množství systémů, které v současné době můžeme zaznamenat. Typicky jde například o automatické mazání nevyžádaných zpráv v mailové poště nebo o efekty AI ve videohrách.

Jak bude vypadat budoucnost s AI

Jak jsme si již za posledních pár let všimli, umělá inteligenci je velice rychle se vyvíjející technologií, na kterou je třeba neustále reagovat. Tento vzniklý akt však promýšlí budoucnost a měl by být schopen reagovat na nově vzniklé problémy. Jestli tomu tak bude, uvidíme v budoucnu. Zatím je jisté, že Akt o umělé inteligenci je součástí velkého balíčku politických opatření, které by měly přinést snazší zavedení AI a také inovace, které mohou usnadnit mnoho práce. Tento balíček by měl také zaručit vyšší bezpečnost, jasnější etické zásady a zajištění základních práva lidí a podniků, což byly dodnes často diskutované problémy bez jasného řešení.

V únoru letošního roku byl také zřízen Evropský úřad pro umělou inteligenci. Jeho cílem by mělo být vytvořit v EU vhodné prostředí pro rozvoj technologií, výzkumu a zajistit spolupráci s dalšími světovými aktéry. Dalším cílem je také vytvoření globálního dialogu o využití AI, ve kterém by EU měla mít vedoucí postavení v oblasti etických zásad a udržitelného rozvoje.

Pro E-Bezpečí
Mgr. Karolína Ziburová
Univerzita Palackého v Olomouci