Umělá inteligence, spotřebitel v ohrožení

13.4.2023 - Lucie Korbeliusová | DTest, o.p.s.

Pokud v současné době bují veřejná debata o umělé inteligenci (AI z angl. artificial intelligence), zpravidla se týká vyspělých jazykových modelů (systémů) založených na tzv. strojovém učení.

Systém nemá vlastní vědomí, ale na základě příkazů člověka pracuje s určitou databází informací. Tyto informace na základě definovaných algoritmů vyhodnocuje, propojuje a doplňuje. Fáze učení se následně projevuje v tom smyslu, že systém pracuje s určitou mírou pravděpodobnosti a sám rozpoznává charakteristické vzorce mezi modelovými dotazy a odpověďmi, které programátor označí za uspokojivé. Tuto „zkušenost" je systém schopen využít při dalších složitějších úkolech, aniž by bylo nutné jeho algoritmy dále ručně upravovat.

Řada příležitostí, ještě více rizik

Umělá inteligence se v nejbližší době patrně výrazně uplatní v řadě profesí. Její přínos bude patrný nejprve při řešení stereotypních kancelářských úloh, v přípravě odpovědí na stále se opakující dotazy, při vyplňování formulářů, plánování, třídění dat či při vytváření jednoduchých textových útvarů. S umělou inteligenci se však pojí také řada bezpečnostních rizik, které jsou navíc umocněny jejím překotným vývojem. Na co si však v souvislosti s umělou inteligencí musí dát spotřebitel pozor?

Schopnost efektivnějšího sběru a třídění dat bude dozajista lákavá pro společnosti, které se zabývají zpracováním osobních údajů a jejich marketingového využití. Umělá inteligence se tak může stát schopným pomocníkem nových šmejdů, které mohou získané informace o spotřebitelích, jejich historii vyhledávání na internetu a aktivitu na sociálních sítích využít k manipulaci s cílem ovlivnit jejich ekonomické chování. „Častěji se budeme setkávat s personalizovanými slevovými a cenovými nabídkami, s články a recenzemi, které nás budou utvrzovat v nákupu výrobku, který jsme se snažili vyhledat na internetu apod. Otázky ochrany osobních údajů, regulace zpracování osobních údajů a její vymahatelnost se tak stávají čím dál naléhavější. Personalizované nabídky navíc mohou zneprůhlednit nabídky na trhu a ve svém důsledku působit diskriminačně vůči jiným spotřebitelům,"vysvětluje Eduarda Hekšová, ředitelka spotřebitelské organizace dTest.

Manipulace však nemusí končit pouze u nakupování. Umělá inteligence může stejně dobře třídit a vyhodnocovat širokou paletu veřejně projevovaných názorů. V nesprávných rukou se proto může stát efektivním nástrojem k šíření dezinformací a nepravdivých zpráv přesně zacílenému publiku. „Při pohledu na obrázky vygenerované umělou inteligencí zobrazující papeže Františka v péřové bundě či dramatické zatýkání Donalda Trumpa, které se v poslední době objevily ve veřejném prostoru, se lze důvodně obávat například podoby příštích volebních kampaní. Z důvodů enormního pokroku se navíc můžeme brzy dočkat nejen obrázků ale i vygenerovaných videí, které budou k nerozeznání od skutečného záznamu," říká ředitelka dTestu.

Pozor si budeme muset dát také na bezpečnost a pravidelné aktualizace veškerých síťových zařízení jako jsou modemy, wifi routery, ale také mobilní telefony a počítače. Hackeři s využitím virů s prvky umělé inteligence budou mít snazší cestu k napadení těchto zařízení phishingovými a jinými útoky a k následné krádeži dat či identity. „Z možných rizik, která umělá inteligence představuje, je patrné, že spotřebitelé budou nuceni veškeré informace náležitě ověřovat z několika zdrojů a být více než kdy dříve obezřetní při sdílení osobních a citlivých údajů,"dodává Eduarda Hekšová ze spotřebitelské organizace dTest.

Je možné umělou inteligenci regulovat?

Z pohledu regulace AI představuje rovněž nebývalou výzvu. Na některé aspekty spojené s riziky, které plynou z jejího rozvoje, má na evropské úrovni odpovídat připravovaný akt o umělé inteligenci. Ten má umělou inteligenci především definovat, roztřídit jednotlivé systémy založené na umělé inteligenci podle toho, jaké pro společnost představují riziko a nastavit základní pravidla jejich užívání. Z návrhu aktu plyne, že některé vysoce rizikové systémy umělé inteligence by měly být zcela zakázány. Jedná se například o systémy využívající podprahové vnímání či takzvaný social-scoring, tedy oceňování spotřebitelů určitou hodnotou či skóre podle jejich vlastností a ekonomického či sociálního chování. Návrh má dále zavést řadu povinností pro poskytovatele systémů umělé inteligence související s hodnocením jejich rizik, transparentností a informováním spotřebitele. Povinnosti vůči spotřebiteli mohou zahrnovat uvedení informace o tom, zda a jakým způsobem je AI využívána, například ke zpracování dat spotřebitele, při koupi zboží a vytváření navazujících cílených nabídek. „Vedle těchto povinností se dále nabízí celá řada opatření, které teoreticky řeší některá rizika spojená s užíváním umělé inteligence. Mezi taková opatření může patřit zákaz použití podoby či hlasu reálných osobností bez jejich souhlasu, označení každého obsahu generovaného umělou inteligencí či povinnost informovat spotřebitele o tom, že komunikuje s umělou inteligencí a možnost „odvolat se“ v takovém případě k živé osobě. Většina těchto pravidel však přichází pozdě a ve světě gllobálního otevřeného internetu jsou navíc v podstatě nevymahatelná,“ popisuje Hekšová.

A jaká doporučení by spotřebitelům k potlačení rizik souvisejících s umělou inteligencí dala sama AI?

(*Odpověď získaná prostřednictvím ChatGPT Mar 23 Version)*

1. Buďte obezřetní při sdílení svých osobních dat. Přemýšlejte o tom, co sdílíte online a s kým. Sledujte, jak jsou vaše osobní údaje používány a jaké jsou vaše možnosti ochrany soukromí.
2. Využívejte spolehlivé softwarové nástroje. Zkontrolujte, zda jsou spolehlivé a zda vám poskytují dostatečnou ochranu. Ujistěte se, že vám nainstalovaný software nepřináší více škody než užitku.

3. Sledujte, jak se vývojáři a společnosti chovají k etickým otázkám týkajícím se umělé inteligence. Sledujte novinky v této oblasti, zúčastňujte se diskuzí a vzdělávejte se. Čím více budete rozumět této technologii, tím lépe budete schopni ji používat a minimalizovat přitom rizika spojená s jejím využitím.

Odpověď umělé inteligence lze doplnit i o odkaz na brožuru Peníze a (ne)bezpečný internet.

Pokud spotřebitelé mají otázky k tomuto tématu, mohou se obrátit na bezplatnou spotřebitelskou poradnu dTestu, a to elektronicky na www.dtest.cz/spotrebitelska-poradna nebo telefonicky na číslo 299 149 009.

dTest, o.p.s. je největší českou spotřebitelskou organizací, která v ČR působí již od roku 1992. Je vydavatelem spotřebitelského časopisu dTest, na jehož stránkách jsou publikovány výsledky nezávislých a objektivních testů produktů, varování před nebezpečnými a zdravotně závadnými výrobky, informace o spotřebitelských právech a rady, jak tato práva účinně uplatňovat. dTest je součástí mezinárodní organizace International Consumer Research and Testing (ICRT) a evropské spotřebitelské organizace BEUC.

Poradenská linka časopisu dTest – 299 149 009 – je v provozu každý pracovní den od 9 do 17 hodin a

spotřebitelé na ní mohou konzultovat s právními poradci časopisu dTest nejrůznější spotřebitelské problémy, a to za cenu běžného tarifu volání. Od spuštění v roce 2010 této možnosti využily již statisíce spotřebitelů a poradenská linka časopisu dTest se tak stala první a nejvyhledávanější cestou k řešení potíží, se kterými se zákazníci na trhu setkávají.

http://www.dtest.cz/clanek-10138/dtest-umela-inteligence-spotrebitel-v-ohrozeni