E-Bezpečí 2024, 9(1): Page 41-45. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=3884

GENERATIVNÍ UMĚLÁ INTELIGENCE VÝRAZNĚ MĚNÍ NÁŠ POHLED NA INFORMACE. ČEMU BUDEME VĚŘIT? A JAK OVLIVNÍ NAPŘ. VOLBY?

Kamil KOPECKÝ

Výtvory umělé inteligence jsou stále dokonalejší a v blízké době již nebudeme schopni rozeznat autentické záznamy skutečných událostí (např. v případě fotografií a videí) od vygenerovaných produktů umělé inteligence. AI tak razantně změní způsob, jak přistupujeme k informacím - fotografie a videa již nebudou zárukou pravdivosti, protože mohou (ale také nemusí) být vytvořeny uměle, prostřednictvím umělé inteligence.

Stále větší důležitost pak bude kladena především na **mediální gramotnost** uživatelů online médií a jejich schopnost kriticky hodnotit, pochybovat a ověřovat si informace - jenže v reálném světě nelze ověřovat vše (to bychom nedělali nic jiného). Vzroste také důležitost konkrétních zdrojů informací, např. konkrétních osob či organizací, u kterých lze předpokládat, že jejich informace budou kvalitní a nezkreslené. Tak či onak - musíme si postupně zvyknout na to, že to, co na internetu vidíme a slyšíme, nemusí vůbec zachycovat realitu.

Problémem je, že než si většina populace navykne na změnu tohoto paradigmatu (což může trvat i několik let), umělá inteligence způsobí mnoho problémů. Jedním z nich bude např. **cílené ovlivňování voleb** (tedy jednoho ze základních demokratických procesů). Pomocí AI bude možné vytvořit a rozšířit internetem ve velkém měřítku videa či zvukové nahrávky politiků,

kteří budou říkat naprosto cokoli nás napadne. Tzv. politický marketing bude masově AI používat k poškozování politických oponentů a vylepšování image svých vlastních kandidátů, aktivní budou i samotní příznivci či odpůrci jednotlivých politických soupeřů.

Toto se již v praxi děje, příkladem mohou být podvodné nahrávky šířené v rámci předvolebního klání na Slovensku (o kterých jsme psali zde), ale třeba také aktuální případy z předvolebního klání voleb prezidenta USA (2024). Zde nyní např. dochází k šíření podvržených deep fake fotografií Donalda Trumpa obklopeného Afroameričany, které mají povzbudit právě černošské voliče, aby volili Donalda Trumpa. Jde však o podvrhy vytvořené pravděpodobně samotnými příznivci tohoto politika. Na první pohled jsou materiály velmi věrohodné, při detailním prozkoumání však lze odhalit např. příliš lesklou kůži či chybějící prsty, případně různé nadbytečné fragmenty.

Fotografie vygenerované pomocí AI využité v rámci volebního boje v USA

Bohužel vytvořit podobné materiály je extrémně snadné, a to jak v podobě fotografií, tak i videí. Josef Šlerka se svým týmem nedávno zveřejnil experiment s deep fake videem Václava Klause, který pronáší věty o globálních změnách klimatu, které by v reálném světě pravědpodobně nikdy neřekl. Příspěvek vzbudil značný ohlas, mnoho uživatelů se skutečně nechalo napálit, video komentovalo a nerozpoznalo, že jde o podvod. Velká část uživatelů internetu si bohužel neuvědomuje, že podobná videa nyní dokáže vyrobit kdokoli, kdo se naučí pracovat s nástroji umělé inteligence. A to během několika minut. Paleta zneužití těchto výtvorů je pak extrémně široká.

Deep fake videa byla doposud využívána především **v rámci podvodů**, stačí zmínit klasické příklady podvodných investic, ve kterých se objevila např. deep fake videa známých politiků, kteří slibují zázračné zbohatnutí. Terčem podvodníků se stal např. Andrej Babiš, Michal Žantovský, Daniel Beneš, ale také např. prezident Petr Pavel a další známé osobnosti, zneužito bylo také např. logo ČEZu, Úřadu vlády či CNN Prima News. Více o tomto typu podvodů např. zde.

Deep fake video s Andrejem Babišem zneužité v rámci podvodu

Lze však s jistotu předpokládat, že v blízké volbě začnou být produkty umělé inteligence masově **zneužívány právě v rámci voleb** - a budou aktivně ovlivňovat nálady a preference voličů. Představme si např., že nám zavolá známý politik (třeba prezident či premiér) a bude nás přesvědčovat, abychom mu dali svůj hlas. Nebo nás naopak bude přesvědčovat, abychom k volbám vůbec nechodili. Že to zní jako sci-fi? Tak právě toto se děje v USA, kde uměle vytvořený hlas Joe Bidena přesvědčoval demokratické voliče, aby nechodili k volbám (více na CNN).

Podobné scénáře lze předpokládat i v ostatních zemích, ostatně na rizika ovlivnění voleb upozorňuje i samotná Evropská unie, která se chystá na eurovolby a která apeluje na významné technologické platformy X, TikTok a Facebook, aby identifikovaly a označovaly obsah generovaný umělou inteligencí. Ovlivňování voleb pomocí deep fake videí se obává také např. Velká Británie a další evropské země.

Na co je třeba se před volbami nachystat v ČR? Na záplavu deep fake videí českých politiků a dalších známých osobností, které budou ovlivňovat voliče.

Je vysoce pravděpodobné, že se před volbami objeví vlna deep fake videí také v České republice. Jak ukazují dosavadní experimenty, **velká část uživatelů sociálních sítí nedokáže deep fake videa identifikovat** a odhalit jako falešná, vnímají je jako autentická - zachycující realitu.

Deep fake video s Tomiem Okamurou (další videa např. zde)

Deep fake video s Alenou Schillerovou (přišlo WhatsAppem)

Výše uvedená videa politiků jsou velmi jednoduchá a je patrné, že byla vytvořena ze zdrojových fotografií nalezených na internetu. Vytvořit podvodné deep fake video pak zabere několik málo minut - k jeho výrobě je nutné získat pouze **vzorek hlasu** (několik minut projevu) a **podobu člověka** (ať už původní fotografii či video). Poté postačí využít právě online aplikace (jejich jména nebudeme uvádět, nicméně jsou veřejně dostupné) a vytvořit jednoduché, nebo pokročilejší video. Deep fake videa kolující internetem jsou často amatérská, nalezneme mezi nimi však i povedenější a realističtější kousky, ve kterých již bylo využito složitějších algoritmů.

Příkladem může být nedávné video "omluvy" Andreje Babiše za jeho e-mailové snahy najít kompromitující materiály na ministra Lipavského. Zde je již využití AI podstatně pokročilejší a pro laika může být velmi těžké odhalit, že jde o deep fake.

Deep fake video s Andrejem Babišem putující Facebookem

Několik doporučení k problematice deep fake videí

A. Prozkoumejte zdroj: Vždy zkontrolujte, odkud video pochází. U důvěryhodných zdrojů lze předpokládat, že budou sdílet ověřené informace. Pokud video pochází z neznámého nebo pochybného zdroje, mějte se na pozoru.

B. Zaměřte se na kvalitu: Deep fake videa často obsahují vizuální nebo zvukové nedostatky. Hledejte chyby, jako jsou neobvyklé pohyby rtů, podezřelé stíny, špatná intonace, příliš dokonalý jazyk apod., které by mohly naznačovat manipulaci.

C. Ověřujte informace: Pokud se vám video zdá podezřelé, zkuste najít další zdroje, které by informace mohly potvrdit nebo vyvrátit. Pokud o daném tématu nemůžete najít žádné další informace, buďte opatrní. Využít můžete také různé aplikace, které mohou pomoci identifikovat deep fake videa.

D. Vzdělávejte se: Čím více se dozvíte o deep fake technologiích a jejich metodách/fungování, tím lépe budete schopni je rozpoznat. Sledujte nejnovější vývoj v oblasti umělé inteligence a mediální gramotnosti. Pomoci vám může např. kurz AI od E-Bezpečí.

E. Dávejte si pozor na videa vyvolávající emoce: Pokud se video snaží vyvolat silnou emoční reakci nebo se zdá být příliš šokující nebo kontroverzní, mělo by to být varovné znamení, že může jít podvrh. Dezinformace a hoaxy často působí na emoce, které mají zastřít racionální úsudek a přimět uživatele k ukvapené reakci.

F. Naučte se reagovat: Pokud narazíte na deep fake video, nešiřte ho dále. Místo toho informujte příslušné platformy (sociální sítě) a varujte ostatní. Posílení komunity proti šíření dezinformací je klíčové.

G. Aktivně upozorňujte na zdroje šířící nepravdivé informace a podporujte důvěryhodné instituce.

Pro E-Bezpečí
prof. Kamil Kopecký
Univerzita Palackého v Olomouci