TECHNOLOGICKÉ CENTRUM PRAHA
Ve Struhách 1076/27, 160 00 Praha 6
234 006 100
tc@tc.cz
www.tc.cz

Tisková zpráva

UMÍME ČELIT DEEPFAKE PODVODŮM?

***Praha, 8. července 2024*: Zneužití deepfake v podvodných kampaních se už dotklo i Česka a s rozvojem umělé inteligence lze očekávat nárůst padělaných vyjádření politiků či falešný pornografický obsah s tváří celebrit. Problematice deepfake videí nebo zvukových nahrávek se však česká věda a výzkum věnuje jen okrajově a systematická podpora výzkumu problematiky deepfake v Česku chybí, jak ukazují výsledky studie Technologického centra (TC) Praha.**

V iniciativě TC Spotlight posuzují analytické týmy z Oddělení strategických studií TC Praha aktuální technologicko-společenská témata z pohledu jejich zastoupení v české vědě a výzkumu a první zkoumanou oblastí se stal syntetický multimediální obsah. Deepfake videa a klonování hlasu využívající umělou inteligenci k vytváření falešných záznamů se staly výrazným tématem po roce 2016, kdy začaly vznikat výkonnější jazykové modely. V Česku se problematika deepfake videí nejvýrazněji projevila v podvodné kampani, ve které upravené video s prezidentem Petrem Pavlem doporučovalo investovat do pochybných finančních produktů, přičemž kvalita videa byla odborníky hodnocena jako velmi zdařilá. *„Obavám z využití podvržených videí se v Česku věnuje pozornost více v souvislosti s blížícími se parlamentními volbami,"* říká Kristýna Meislová, analytička TC Praha.

Mezi lety 2019 a 2021 došlo ke čtyřnásobnému nárůstu patentových přihlášek na technologie spojené s výrobou a detekcí deepfake videí na současných 70 ročně. Počet vědeckých publikací s volným přístupem rostl ještě rychleji, až na 1000 článků za rok. V prestižní databázi Web of Science je asi 300 publikací ročně. Čeští vědci se v období 2020–2023 podíleli na 11 publikacích na Web of Science, které se týkaly problematiky deepfake, jak ukazuje analýza TC Praha.

„Vytváření videoobsahu s využitím umělé inteligence má i celou řadu zcela legitimních využití ve filmařině, umění, vzdělávání, či reklamě, takže porozumět technologickému i společenského vývoji v této oblasti je zásadní. Česká věda by mohla přispět k výzkumu deepfake obsahu, jeho odhalování, a i nastavení vhodné regulace nástrojů a služeb," doplňuje Kristýna Meislová.

V českém Rejstříku informací o výsledcích (RIV) se téma deepfake objevilo pouze u osmi výsledků, z toho jen tři byly recenzované odborné články. Momentálně probíhají čtyři velké mezinárodní výzkumné projekty v rámci programu Horizont Evropa zaměřené na deepfake, avšak žádný z nich nezahrnuje účast českých vědců. Podle dat z Informačního systému výzkumu, vývoje a inovací nebyly z veřejných zdrojů v Česku do konce roku 2023 podpořeny žádné výzkumné projekty zaměřené na toto téma. Od letoška si nechává Ministerstvo vnitra ČR zpracovat projekt „Nástroje boje proti hlasovým deepfakes", v němž se bude mimo jiné vyhodnocovat schopnost lidí rozpoznat hlasové deepfakes a hledat způsob zvýšení bezpečnostního povědomí cílových uživatelů.

Analýza prestižních technologických médií v anglosaském světě (viz word cloud v infografice) ukazuje, že problematika deepfake videí se týká širší oblasti témat než jen podvrhů v politických kampaních, šíření dezinformací či generovaného sexuálního nebo pornografického obsahu, ale je spojována i s kriminalitou v oblasti sociálního inženýrství a krádežemi firemních či bankovních údajů a jiných citlivých dat. Věrné kopírování hlasu a vytváření realistické podoby řeči v reálném čase dosáhlo vysoké technologické úrovně s minimálními náklady a na základě pouze krátkých vzorků

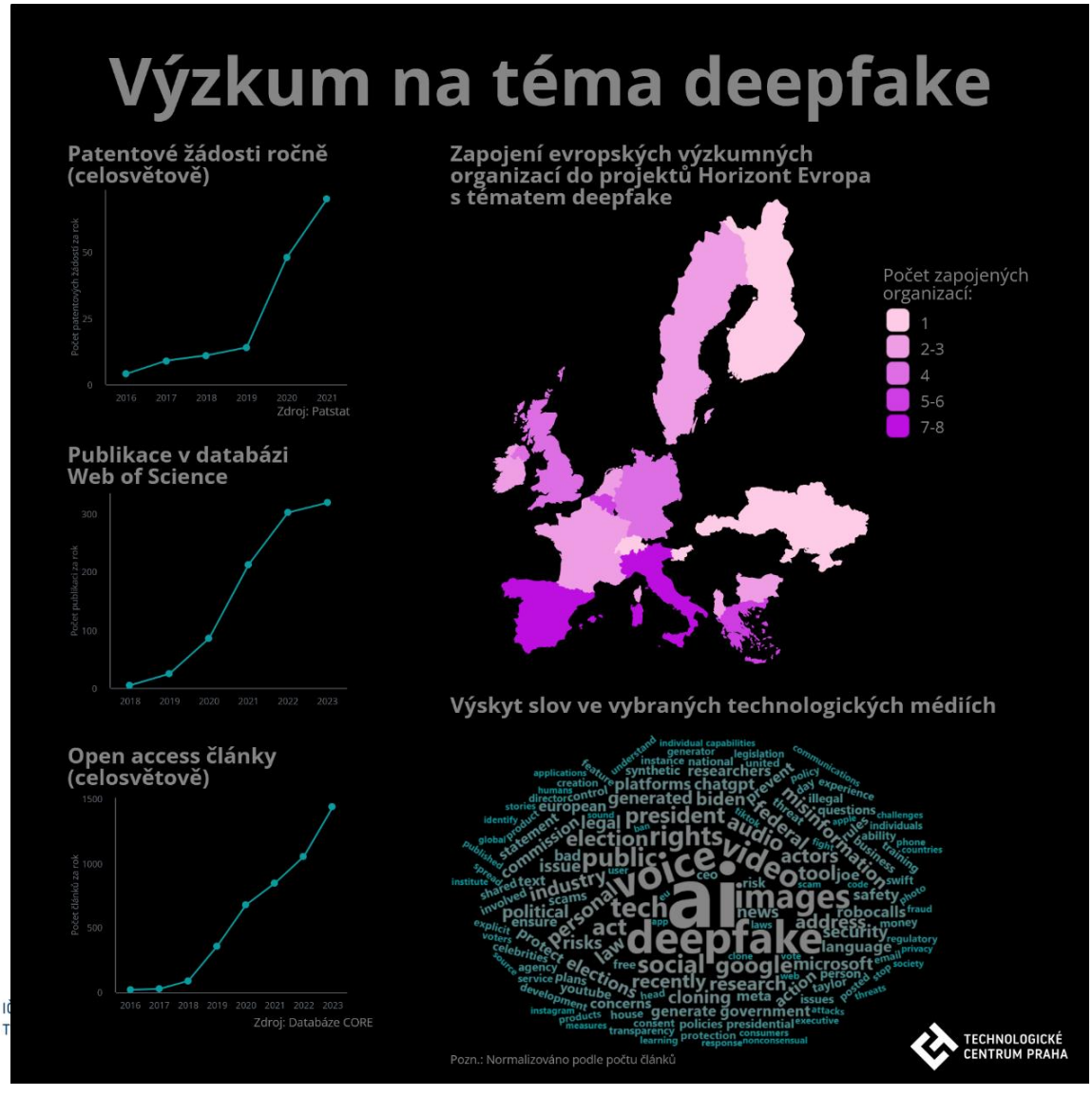
TECHNOLOGICKÉ CENTRUM PRAHA
Ve Struhách 1076/27, 160 00 Praha 6
234 006 100
tc@tc.cz
www.tc.cz

hlasu. Podvržený hlas lze využít zejména v telefonátech, které mohou být díky umělé inteligenci zcela automatizované a velmi důvěryhodné.

Ve volebním roce 2024 je ve Spojených státech audiovizuální deepfake obsah velmi aktuální a objevují se snahy o jeho zákonné regulace. Výrazně se deepfake videa již projevila v letošních indických volbách, kde prostřednictvím uměle generovaných videí vystupovali politici, celebrity i dávno zesnulé osobnosti. Šíření falešných zpráv, zmanipulovaného obsahu a dezinformací na platformách sociálních médií zpochybnilo úsilí o ověřování faktů. Na druhou stranu velmi časté bylo i využití AI generovaného obsahu k legitimnímu účelu lepší komunikace politiků s veřejností a navázání pozitivního emocionálního vztahu s voliči.

„Technologické nástroje pro odhalování podvrhů a pravidla pro označování uměle generovaného AI obsahu se v době zdokonalujících se technologických prostředků ukazují jako zásadní pro zajištění férové politické soutěže, ochranu osobnosti a pro obranu proti dezinformacím v hybridních konfliktech,“ dodává Kristýna Meislová.

Infografika: Výzkum na téma deepfake



TECHNOLOGICKÉ CENTRUM PRAHA

Ve Struhách 1076/27, 160 00 Praha 6
234 006 100
tc@tc.cz
www.tc.cz

Technologické centrum Praha (TC Praha) je neziskovým sdružením právnických osob, které plní více rolí. Je národním pracovištěm pro podporu výzkumu a vývoje v Evropském výzkumném prostoru a národním kontaktním bodem rámcových programů EU. Specializovanou činností TC Praha jsou analytické a koncepční práce zabývající se strategiemi výzkumu, vývoje a inovací v souvislosti s ekonomickými a sociálními potřebami České republiky.

Kontakty pro média:

Michaela Blšťáková, tel.: 725 047 814, email: blstakova@tc.cz

Oddělení strategických studií: Petra Karnetová, tel.: 724 155 357, karnetova@tc.cz

Odborné dotazy k analýze: Kristýna Meislová, tel.: 724 353 611, email: meislova@tc.cz

více informací na www.tc.cz