7. 3. 2025

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Kybernetické hrozby spojené s umělou inteligencí a deepfake technologiemi: Výzvy pro bezpečnost a právní rámce

V posledních letech se technologie umělé inteligence (AI) a deepfake staly klíčovými tématy v oblasti kybernetické bezpečnosti. Tato nová vlna inovací přináší nejen obrovský potenciál pro zlepšení různých oblastí lidské činnosti, ale i významné bezpečnostní hrozby, které ohrožují jak jednotlivce, tak i organizace na globální úrovni. V tomto článku se zaměříme na analýzu kybernetických hrozeb spojených s AI a deepfake technologiemi, s ohledem na konkrétní příklady z praxe, právní regulace a globální události.

1. Definice a základní principy AI a deepfake technologií

Umělá inteligence (AI) se rozumí jako technologie, která umožňuje strojům napodobovat lidské chování a rozhodování. Aplikace AI se nacházejí v širokém spektru od analýzy dat, přes autonomní vozidla až po pokročilou kybernetickou bezpečnost. Deepfake je specifická aplikace AI, která umožňuje manipulaci s multimediálními soubory – především videi a audiosoubory – a vytváření realistických, ale falešných záznamů.

Deepfake využívá technologií strojového učení a generativních adversariálních sítí (GAN), které mohou vytvářet fotorealistická videa, na kterých jsou lidé vidět, jak vykonávají nebo říkají něco, co ve skutečnosti nikdy neudělali. Tento nástroj je schopný nejen měnit tváře v obrazech a videích, ale i syntetizovat falešný zvuk nebo text.

2. Kybernetické hrozby a rizika spojená s AI a deepfake

2.1. Kybernetické útoky využívající deepfake

Jedním z nejzávažnějších rizik, které AI a deepfake technologie představují, je možnost zneužití pro kybernetické útoky. Nejvíce znepokojující jsou útoky, které mohou vést k narušení důvěryhodnosti informací, což je základním pilířem nejen pro jednotlivce, ale i pro instituce a vlády. Phishing je jednou z nejběžnějších metod, kdy útočníci používají deepfake k napodobení hlasu nebo tváře důvěryhodných osob, jako jsou obchodní partneři nebo vedoucí pracovníci. Tímto způsobem mohou zmanipulovat oběť, aby provedla neoprávněné finanční transakce nebo sdílela citlivé informace. Případ z roku 2019, kdy byla ve Velké Británii zmanipulována nahrávka hlasu CEO společnosti, což vedlo k podvodu ve výši 243 000 dolarů, ukázal, jak realističnost deepfake technologií může být zneužita pro finanční zločiny. Tento případ upozornil na zranitelnost moderních firemních systémů, které spoléhají na autentifikaci prostřednictvím hlasu.

2.2. Dezinformace a politické manipulace

Dalším závažným rizikem jsou politické manipulace a šíření dezinformací. Deepfake technologie umožňují vytváření videí, ve kterých mohou být politici nebo veřejné osobnosti citovány za věci,

které nikdy neřekly. Tato forma dezinformace může podkopat důvěru veřejnosti v politické instituce, ovlivnit volby nebo vyvolat sociální nepokoje. V roce 2020 v USA došlo k několika incidentům, kdy byly na sociálních médiích šířeny deepfake videa, která měla za cíl poškodit pověst kandidátů během volebního období. Jedním z příkladů je manipulovaná videa, kde politici údajně říkají kontroverzní nebo nepravdivé výroky, což se ukázalo jako silný nástroj pro destabilizaci politického klimatu.

2.3. Útoky na soukromí a šikana

Deepfake technologie rovněž představují hrozbu pro ochranu soukromí. Zneužívání deepfake k vytváření pornografických videí s falešnými tvářemi je stále častější formou kyberšikany a online zneužívání. Mnoho obětí tohoto typu útoků se potýká nejen s emocionálními následky, ale i s vážnými právními problémy, když se zmanipulovaná videa šíří po internetu a mohou poškodit jejich pověst. Tento problém není lokální a stává se globálním. Případ z roku 2018, kdy byl falešně vytvořen pornografický materiál s tvářemi několika celebrit, ukázal, jak těžké je zastavit šíření těchto materiálů. Právní rámce jsou často nedostatečné, a tak je obtížné chránit oběti před trvalými následky.

4. Právní rámec a regulace AI a deepfake

Když se kybernetické hrozby spojené s AI a deepfake začaly masivněji projevovat, došlo k rozvoji právních iniciativ zaměřených na řešení této problematiky. V roce 2018 byla v USA konference na téma Malicious Deep Fake Accountability Act, kde se řešila rizika spojené s umělou inteligencí a postihy osob, které vytvoří nebo šíří deepfake s úmyslem poškodit jiné osoby. Tato konference byla reakcí na rostoucí obavy o bezpečnost voleb, soukromí a ochranu jednotlivců. K dispozici >>> zde.

V Evropské unii jsou od roku 2018 účinná Obecná nařízení o ochraně osobních údajů (GDPR), které zahrnují i otázky spojené s manipulací s osobními daty, a tím pádem i s hlubokými podvody. K dispozici >>> zde.

V roce 2021 Evropská komise navrhla nový právní rámec týkající se AI, který by měl upravit její etické využívání, a zmínil i problém deepfake technologií, který vstoupil v platnost 1.8.2024 . Jedná se o první právní předpis o AI na světě. Cílem tohoto aktu je, aby systémy umělé inteligence byly využívány a tvořeny zodpovědně. Taktéž se tento akt zabývá riziky, které jsou s AI spojeny. K dispozici >>> zde.

5. Budoucnost kybernetické bezpečnosti v kontextu AI a deepfake

Před námi stojí složitá výzva v oblasti kybernetické bezpečnosti a ochrany soukromí v kontextu rychlého rozvoje umělé inteligence a deepfake technologií. I když mohou vzniknout nové nástroje pro detekci a prevenci deepfake, jako jsou algoritmy na rozpoznání manipulovaných obrazů a zvuků, útočníci budou i nadále zlepšovat své techniky. Spolupráce mezi státy, technologickými firmami a právními experty bude klíčová k tomu, abychom vytvořili účinné a realistické regulační mechanismy. Je důležité, aby veřejnost byla informována o rizicích spojených s těmito technologiemi a aby existovala efektivní opatření na ochranu jednotlivců i organizací před těmito hrozbami. Závěr Kybernetické hrozby spojené s umělou inteligencí a deepfake technologiemi představují v současnosti jednu z největších výzev pro bezpečnostní a právní systémy. Nejen jednotlivci, ale i státy, organizace a technologické firmy musí přijmout opatření, která zajistí ochranu před těmito hrozbami. Budoucnost kybernetické bezpečnosti závisí na schopnosti adaptovat se na rychlý technologický pokrok a na vytváření mezinárodních právních rámců, které budou schopny efektivně reagovat na nové výzvy.

Bc. Sophia Karešová

Další články:

- Poučení z krizového vývoje v kauze bitcoiny
- EUDAMED: Jednotná databáze mění pravidla hry na trhu zdravotnických prostředků
- Nový zákon o veřejných dražbách, aukce a obálkové metody
- Pohled přes hranice – natáčení pornografických klipů jako důvod výpovědi z nájmu bytu
- Nařízení EU o umělé inteligenci a jeho dopady na využití jazykových modelů v advokátní praxi
- Revize zájezdové směrnice: co přináší, co hrozilo a co to znamená pro praxi
- Kupní smlouva o převodu nemovitosti bez uvedení výše kupní ceny
- Druhá „tlačítková novela": povinné tlačítko pro odstoupení od smlouvy
- Souhlas s veřejným užíváním pozemku jako překážka nároku na bezdůvodné obohacení – nález Ústavního soudu sp. zn. I. ÚS 2541/25
- Kupní smlouva bez přesného určení kupní ceny
- Byznys a paragrafy, díl 36.: Doložka o mlčenlivosti