ACTA FACULTATIS IURIDICAE UNIVERSITATIS COMENIANAE
Tomus XXXVII
2/2019

DEEP FAKES A OCHRANA SÚKROMIA

JUDr. Matúš Mesarčík, LL.M.

Univerzita Komenského v Bratislave, Právnická fakulta
Katedra správneho a environmentálneho práva
Ústav práva informačných technológii a práva duševného vlastníctva
matus.mesarcik@flaw.uniba.sk

JUDr. Ondrej Zimen

Dagital Legal, s.r.o
ondrej.zimen@dagital.eu

Deep Fakes a ochrana súkromia

Autori sa v tomto príspevku zaoberajú technológiou deep fakes. V prvej stati je predmetná technológia definovaná vrátane jej pozitívnych a negatívnych vplyvov. Následne je podrobená právnej analýze právna úprava týkajúca sa zodpovednosti za cudzí obsah na internete a ochrany osobných údajov s ohľadom na vhodnosť právnej úpravy a diskutovanej technológie.

Deep fakes y privacidad

Los autores se centran en la tecnología falsa profunda. La primera parte del artículo está dedicada a la definición de la tecnología, incluidos los impactos positivos y negativos en un individuo y en la sociedad en general. Posteriormente, el análisis legal se centró en la responsabilidad por el contenido de terceros y la protección de los datos personales en términos de idoneidad de la legislación actual.

Deep Fakes and Privacy

Authors focus on deep fake technology. The first part of the article is devoted to the definition of the technology including positive and

negative impacts on an individual and society as a whole. Subsequently the legal analysis focused on liability for third-party content and protection of personal data follows in terms of suitability of current legislation.

Kľúčové slová: deep fakes, GDPR, zodpovednosť

Las palabras claves: deep fakes, GDPR, la responsabilidad

Keywords: deep fakes, GDPR, liability

1. Úvod

Technológie tvoria v súčasnosti imanentnú súčasť ľudských životov, pričom tradičný konzervativizmus práva častokrát nestačí reflektovať technologickému vývoju pri prijímaní právnej úpravy, ktorá by reguláciu nových technológií dostatočne obsiahla. V súčasnosti je takmer nemožné predstaviť si spoločnosť bez využívania (nielen) informačných a komunikačných technológii[1] na dennej báze. Tieto technológie však nemajú iba pozitívny vplyv na spoločnosť, ale produkujú aj negatívne zásahy do základných ľudských práv a slobôd, ktoré už viac nie sú iba doménou sci-fi literatúry alebo filmovej tvorby, ale stávajú sa bežnou realitou našich životov. Bezprecedentné sociálne experimenty využívajúcu umelú inteligenciu v Číne, zneužívanie dát zhromaždených na sociálnych sieťach, mobilné aplikácie schopné analyzovať a predpokladať naše správanie, kyber-bezpečnostné riziká spojené s čoraz rozšírenejšími technológiami internetu vecí, ktoré obklopujú naše životy v automobiloch, domácnostiach, či nemocniciach sú len niekoľkými príkladmi nezastaviteľného trendu, v ktorom využívanie moderných technológií vyvoláva pnutie s právom v rovine potreby zabezpečovania a garancií dotknutých základných ľudských práv.

V ostatnom období sa v kontexte technologického vývoja ujal termín *disruptive technologies*. Ide o technológie, ktoré majú (alebo budú mať) zásadný vplyv na formovanie spoločnosti a jednotlivca. Philip Brey ich definuje ako technológie, ktoré menia každodenný život, sociálne dogmy, inštitúcie, kultúrne aspekty a organizáciu života, práce a komerč-

[1] Jozef Andraško definuje informačné a komunikačné technológie ako *„technológie používané na spracovanie informácií, ktoré vznikli koncom minulého storočia spojením počítačov, telekomunikačných systémov a masovokomunikačných prostriedkov.“* ANDRAŠKO, J.: Elektronický občiansky preukaz a iné spôsoby autentifikácie pri prístupe k elektronickým službám verejnej správy. *QUAERE 2017* [elektronický zdroj]. - ISBN 978-80-87952-20-7. - Hradec Králové : Magnanimitas, 2017, s. 235.

ného styku.[2] Za takúto technológiu bol v minulosti považovaný internet a v súčasnosti predmetný koncept odzrkadľuje analýza veľkých dát (*big data analysis*) alebo umelá inteligencia.

Umelú inteligenciu možno zjednodušene definovať ako počítačový program, ktorý je schopný učiť sa z vlastnej skúsenosti a pristupovať k riešeniu problémov podobne ako ľudská myseľ.[3] Táto technológia zároveň zahŕňa rôzne typy strojového učenia (*machine learning*). Strojové učenie je súbor techník, ktoré umožňujú stroju „myslieť" prostredníctvom vytvárania matematických algoritmov na základe získaných údajov.[4] Množstvo týchto techník využíva tzv. hlboké učenie (*deep learning*) – proces, ktorý sa snaží umelo napodobiť fungovanie neurónových sietí v ľudskom mozgu. Hlboké učenie je typom AI technológie, ktorý je zameraný na napodobňovanie prístupu ľudského učenia sa vo vzťahu k získavaniu určitého typu znalostí, čo sa často využíva najmä pri automatizovanej prediktívnej analytike predvídajúcej určité správanie.[5]

Umelá inteligencia je v súčasnosti často využívaná vo verejnom a súkromnom sektore. Či už ide o algoritmy, ktoré posudzujú bonitu žiadateľa o úver alebo profilovanie či cielenie reklamy na návštevníkov webstránky, táto technológia sa stáva súčasťou nášho každodenného života. Definovaním základných konceptov umelej inteligencie sme náš článok začali zámerne, keďže imanentne súvisí s predmetom skúmania predkladaného príspevku – *deep fakes.*

Deep Fake[6] je AI technológia používaná na produkovanie alebo pozmeňovanie video obsahu takým spôsobom, že prezentuje niečo, čo sa v skutočnosti nedeje prípadne neudialo.[7] Deep fake nie je teda iba obyčajné editovanie videa ľudským používateľom cez dostupné soft-

---

[2] BREY, P. : Ethics of Socially Disruptive Technologies *In Ian Ayres and John Braithwaite, Responsive Regulation: Transcending the Deregulation Debate*, Oxford University Press 1992.

[3] Datatylsinet: Artificial intelligence and privacy Report, January 2018, https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf. (dostupné 26.7.2019), s. 5.

[4] https://iq.intel.com/artificial-intelligence-and-machine-learning/ (dostupné 26.7.2019)

[5] https://searchenterpriseai.techtarget.com/definition/deep-learning-deep-neural-network (dostupné 26.7.2019).

[6] Gramaticky je slovo „Deep Fake" zložené z dvoch slov, ktoré prispievajú k jeho významu. V angličtine sú takéto slová označované pojmom „portmanteau", ktoré sa hojne využíva v IT, kde na trh prichádzajú nové produkty a služby veľmi často a vzniká marketingová potreba tvorenia výstižných opisných názvov (napr. kinect – kinetic and connect, webinar – web and seminar a pod.). V prípade deep fake ide tiež o tzv. „portmanteau" zložené z pojmov „deep learning" (doslova hlboké učenie) a „fake" (doslova falošné), ktoré však nemožno preložiť doslovne.

[7] Pozri COLE, S. : *We Are Truly Fucked: Everyone Is Making AI-Generated Fake Porn Now*, VICE: MOTHERBOARD, https://motherboard.vice.com/en_us/article/bjye8a/reddit-fakeporn-app-daisy-ridley (dostupné 26.7.2019).

véry umožňujúce takéto úkony (napr. photoshop). Vzhľadom na to, že deep fake využívajú aj metódu hlbokého učenia, predmetná technológia umožňuje prispôsobovať napr. výrazové prostriedky, mimiku a gestá obsahu videa, aby pôsobilo ešte vierohodnejšie. V praxi je tak možné na originálnom videu vkladať osobám do úst celé nové vety, ktoré nikdy nezazneli, či zamieňať celé postavy alebo tváre.

Už z tohto stručného úvodu vyplýva, že použitie deep fakes môže významne vplývať na súkromný život osôb a dokonca aj na demokratický chod štátu. Niektoré zdroje tiež uvádzajú[8], že použitie deep fakes technológie bude stále ťažšie detekovateľné pri skúmaní autenticity videa, pretože nástroje na detekciu deep fakes zaostávajú za rozvojom tejto technológie. Odlíšiť pravdu od manipulácie bude v budúcnosti čoraz ťažšie, čo je nepochybne jednou z najväčších súčasných výziev pre legislatívu i justičnú prax.

Cieľom predkladaného článku je poskytnúť základný prehľad pozitívnych a negatívnych vplyvov diskutovanej technológie na jednotlivca a spoločnosť a zároveň poukázať na možné riešenia prostredníctvom právnej úpravy. Základnou otázkou teda je: *Akým spôsobom môže deep fakes technológia ovplyvniť jednotlivca a spoločnosť a či súčasná právna úprava poskytuje dostatočné záruky pred negatívnymi vplyvmi tejto technológie?*

2. Pozitívny a negatívny vplyv technológie na jednotlivca a spoločnosť

Chesney a Citron vo svojej štúdií zaoberajúcej sa problematikou deep fakes[9] pragmaticky zhrnuli pozitívne a negatívne vplyvy technológie na jednotlivca a spoločnosť. Zároveň prognózujú masívne rozšírenie tejto technológie aj vzhľadom na to, že úprava alebo editovanie videa už nie je doménou filmových štúdií, ale tieto nástroje sú čoraz častejšie dostupné aj súkromným osobám. Laicky povedané, ktokoľvek a kdekoľvek si môže na svojom počítači prostredníctvom dostupného softvéru vytvoriť video s použitím deep fakes. Kvalita týchto výtvorov bude s vývojom technológie iba stúpať a častokrát už nebude možné rozlíšiť, čo je reálne a čo iba umeleckým výtvorom. Na nebezpečenstvo

[8] KOPECKÝ, K.: Deep fake – stručný úvod do problematiky, dostupné online: https://www.e-bezpeci.cz/index.php/70-projekt-fake-news/1417-deep-fake-strucny-uvod-do-problematiky (dostupné 26.7.2019).

[9] CHESNEY, R. – CITRON, D. : Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954 (dostupné 26.7.2019).

tejto technológie upozornil aj slovenský CSIRT vo svojej pravidelnej správe.[10]

Takéto diela sú prirodzene často vytvárané s cieľom diskreditácie osoby prostredníctvom simulácie situácií, v ktorých reálne neboli. Z psychologického hľadiska je práve toto materiál, na ktorý ľudská prirodzenosť reaguje s obrovským záujmom. Slovami Danah Boyd: *„Naše telá sú naprogramované konzumovať tuky a cukry pretože tieto látky sú v prírode vzácne... Analogicky, sme biologicky naprogramovaní, aby sme viac vnímali obsah, ktorý je nekultivovaný, násilný, sexuálny a klebety, ktoré sú ponižujúce, strápňujúce alebo útočné. Ak ľudia nebudú opatrní, je možné že sa vyvinie psychologický ekvivalent obezity. Ľudia budú konzumentmi obsahu, ktorý je najmenej prínosný pre nich a pre spoločnosť. "*[11]

2.1. Pozitívne vplyvy

Pozitívne vplyvy deep fakes možno pozorovať predovšetkým v troch oblastiach a to: vzdelanie, umenie a autonómia.

V oblasti **vzdelávania** je možné prostredníctvom tejto technológie kompletne transformovať formy výučby napr. prostredníctvom historických osobností, ktoré sa priamo prihovárajú študentom. Ďalej by bolo možné simulovať situácie, ktoré v skutočnosti nenastali a zároveň ich technologicky upraviť, aby zároveň pôsobili edukačne.[12]

Technológia deep fakes je prirodzene spätá s **umením**. Vďaka tejto technológie je možné na filmové plátno priniesť hercov a herečky, ktorí už dlhšie nežijú.[13]

Posledným benefitom je rozvíjanie **autonómie** osobnosti. S využitím deep fakes sa môže spájať aj seba-prezentácia virtuálneho avataru jednotlivca, ktorý ho reprezentuje v online svete. Osoby so zdravotným postihnutím tak môžu prostredníctvom deep fakes a svojich virtuálnych avatarov „zažívať" situácie, ktoré sú im v reálnom svete odopreté.[14]

---

[10] MESAČNÁ SPRÁVA CSIRT, JÚN 2019, https://www.csirt.gov.sk/doc/MS2019-06verejnost.pdf (dostupné 26.7.2019).

[11] BOYD, D. : „Streams of Content, Limited Attention: The Flow of Information through Social Media", https://www.danah.org/papers/talks/Web2Expo.html (dostupné 26.7.2019).

[12] CHESNEY, R. – CITRON, D. : Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954 (dostupné 26.7.2019), s. 14.

[13] NARCISSE, I. : *It Took Some Movie Magic to Finish Carrie Fisher's Leia Dialogue in The Last Jedi*, GIZMODO, https://io9.gizmodo.com/it-took-some-movie-magic-to-complete-carrie-fisherslei-1821121635 (dostupné 26.7.2019).

[14] VOLPE, A.: *Deepfake Porn Has Terrifying Implications. But What If It Could Be Used for Good?* MEN'S HEALTH, https://www.menshealth.com/sex-women/a19755663/deepfakes-

Takéto použitie predmetnej technológie je vyobrazené aj v známej modernej filmovej tvorbe.[15]

2.2. Negatívne vplyvy

Chesney a Citron vo svojej štúdií diferencujú medzi negatívnym vplyvom na (i) jednotlivca/organizáciu a negatívnym vplyvom na (ii) spoločnosť ako celok.

V kontexte prvej kategórie negatívnych vplyvov na jednotlivca/organizáciu ide predovšetkým o posilnenie kredibility falošných správ (*fake news*). Využitím deep fakes naberajú falošné správy na intenzite a dôveryhodnosti v dvoch modalitách: falošné odhalenia a sabotáž.

Modalita **falošných odhalení** zahŕňa také použitie technológie deep fakes, ktoré určitým spôsobom poškodzujú jednotlivca alebo organizáciu. Môže ísť o krádeže identity za účelom výberu finančných prostriedkov z účtu prostredníctvom tretej strany alebo vydieranie na základe vytvorenia videa, v ktorom vydieraná osoba v skutočnosti nikdy nefigurovala. Osobitným problémom je vývoj sexuálneho priemyslu, kde sú do pornografických videí „vložené" tváre nielen známych osobností. V ostatnom čase zaujal prípad vytvorenia takéhoto videa prostredníctvom sekvencie kvalitných fotografií.[16] Technológia deep fakes tak môže podporiť rôzne formy *cyber-stalkingu*[17]a pornografie vyhotovenej bez súhlasu. Psychologická ujma dotknutých osôb môže byť v takýchto prípadoch značná a spôsobilá zároveň výrazne ovplyvniť súkromie a spoločenský život jednotlivca.[18]

Druhou modalitou negatívnych vplyvov na jednotlivca a organizáciu je **sabotáž.** V tejto súvislosti sabotáž spočíva predovšetkým spôsobenej škode na reputácií jednotlivca alebo organizácie. Prostredníctvom diskutovanej technológie možno vytvoriť videá, na ktorých jednotlivec ničí verejný majetok alebo sa hanlivo vyjadruje o príslušníkoch inej rasy či sexuálnych menšín. Výsledkom môže byť strata výhodnej obchodnej ponuky alebo uzavretia zmluvy. Sabotáž prostredníctvom falošné-

porn-redditpornhub (dostupné 26.7.2019).

[15] Pozri napr. Ready Player One (2017).

[16] Pozri napr. ADAM DODGE & ERICA JOHNSTONE, DOMESTIC VIOLENCE ADVISORY: USING FAKE VIDEO TECHNOLOGY TO PERPETUATE INTIMATE PARTNER ABUSE 6 (Apr. 25 2018), http://withoutmyconsent.org/blog/newadvisory-helps-domestic-violence-survivors-prevent-and-stop-deepfake-abuse (dostupné 26.7.2019).

[17] STRÉMY, T. – TURAY, L. : Stalking a jeho trestnoprávne súvislosti In *Acta Facultatis Iuridicae Universitatis Comenianae. - Roč. 37, č. 2* (2018), s. 274-285.

[18] CHESNEY, R. – CITRON, D. : Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954 (dostupné 26.7.2019), s. 17 – 18.

ho videa môže ovplyvniť schopnosť uchádzača nájsť si zamestnanie.[19] Tieto úvahy sa prirodzene netýkajú iba jednotlivcov, ale môžu ovplyvniť aj obchodný život spoločnosti napr. ak sa počas priebehu akvizície alebo fúzie obchodných spoločností sa na internete objaví video konateľa, ktoré ho nevykresľuje v najlepšom svetle.[20]

Pri negatívnych vplyvoch na spoločnosť ide naozaj o variabilný diapazón možnosti potenciálnej škody. Pre lepšiu čitateľnosť uvádzame tieto negatívny vplyvy v bodoch s príkladmi pre plastickejšiu predstavu. V prípade hlbšieho záujmu o problematiku odkazujeme na odbornú literatúru.[21] Negatívne vplyvy na spoločnosť ako celok teda môže predstavovať:

- *Narušenie demokracie* – chod demokracie stojí a padá na akceptovaní faktov a pravdy, ktorá je podporená empirickými dôkazmi. V prípade falošných správ by bolo možné začať pochybovať o každom probléme súčasného sveta napr. o klimatickej kríze. Spoliehanie sa na falošné správy stavia štatistiky a skutočné dôkazy o pravde na okraj spoločenského diškurzu a záujmu.[22]
- *Volebná manipulácia* – falošné videá a fotografie politikov môžu spôsobiť zásadné rozdiely vo vnímaní verejnosti. Systematická práca s deep fake technológiami má potenciál významne ovplyvniť politický boj.[23]
- *Narušenie dôvery vo verejné inštitúcie* – sudcovia, predstavitelia cirkví alebo tajných služieb vo falošných pozíciách môžu spôsobiť úplne alebo čiastočné narušenie dôvery vo verejné inštitúcie.
- *Prehĺbenie sociálnych rozdielov* – vymyslené video zachytávajúce brutálny policajný zásah na príslušníkov minority môže byť povestnou iskrou pri kultúrnych alebo iných bojoch prehlbujúcich sociálne rozdiely v spoločnosti.
- *Podkopávanie verejnej bezpečnosti* – videá alebo fotografie, ktoré zobrazuje prírodné katastrofy, šírenie nákazlivých chorôb ale-

[19] CAREERBUILDER: PRESS ROOM, NUMBER OF EMPLOYERS USING SOCIAL MEDIA TO SCREEN CANDIDATES AT ALL-TIME HIGH, FINDS LATEST CAREERBUILDER STUDY http://press.careerbuilder.com/2017-06-15-Number-of-Employers-Using-Social-Media-to-Screen-Candidates-at-All-Time-High-Finds-Latest-CareerBuilder-Study (dostupné 27.7.2019).

[20] CHESNEY, R. – CITRON, D. : Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954 (dostupné 26.7.2019), s. 19 – 20.

[21] Tamže, s. 20 – 29.

[22] Tamže, 21-22.

[23] Napr. NOSSITER, A. et al. : *Hackers Came, But the French Were Prepared*, N.Y. TIMES, https://www.nytimes.com/2017/05/09/world/europe/hackers-came-but-the-french-were-prepared.html ((dostupné 27.7.2019).

bo nehody môže v konečnom dôsledku podkopať verejnú bezpečnosť a spôsobiť bezprecedentnú paniku.
– *Narušenie diplomacie* – deep fakes videá o vysokých štátnych predstaviteľoch môžu iniciovať medzinárodnú diplomatickú krízu.[24]
– *Ohrozenie národnej bezpečnosti* – videá ozbrojených síl vraždiace civilné obyvateľstvo vo vojnových oblastiach alebo „pridelená" identita vojakovi prostredníctvom predmetnej technológie môže predstavovať v konečnom dôsledku riziká pre národnú bezpečnosť.[25]
– *Podkopanie žurnalistiky* – použitie falošného videa alebo fotografie v správach bez overenia základných faktov alebo nemožnosti rozoznať, že ide o počítačom vytvorenú simuláciu môže prehĺbiť nedôveru v žurnalistiku a jej predstaviteľov.

Ako je uvedené vyššie, deep fakes technológia so sebou prináša pozitívne, ale aj negatívne vplyvy. Ohrozeným nie je len jednotlivec a jeho súkromný alebo rodinný život, ale negatívne vplyvy často majú potenciál zasiahnuť spoločnosť ako takú a ohroziť chod inštitúcií a samotné demokratické zriadenie postavené na vláde práva a rešpektovaní základných ľudských práv.

3. Právo a deep fakes

V tejto stati autori analyzujú právny poriadok a jeho trecie plochy s deep fakes technológiou. Vzhľadom na šírku problematiky je pozornosť predovšetkým zameraná na situáciu, keď jednotlivec zistí, že video v ktorom je použitá jeho podobizeň sa šíri na internete. Nasledujúce riadky sú teda zamerané predovšetkým na zodpovednosť za cudzí obsah na hostingových platformách a ochranu osobných údajov.

3.1. Zodpovednosť za cudzí obsah

Zodpovednosť za cudzí obsah je predmetom úpravy smernice 2000/31/ES Európskeho parlamentu a Rady z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu,

[24] CALAMUR, K.: *Did Russian Hackers Target Qatar?* THE ATLANTIC (June 6, 2017), https://www.theatlantic.com/news/archive/2017/06/qatar-russian-hacker-fake-news/529359/ (dostupné 27.7.2019).

[25] Viac CHESNEY, R. – CITRON, D. : Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954 (dostupné 26.7.2019), s. 26 – 27.

najmä o elektronickom obchode („**Smernica o elektronickom obchode**“).[26] Ustanovenia tejto smernice sú v slovenskom právnom poriadku implementované v zákone č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení zákona č. 284/2002 Z. z.[27]

Systém zodpovednosti za cudzí obsah podľa Smernice o elektronickom obchode funguje na princípe tzv. bezpečných prístavov. Tie sa vzťahujú na prevádzkovateľov služieb informačnej spoločnosti.[28] Z hľadiska kategorizácie Smernica o elektronickom obchode rozlišuje typy prevádzkovateľov služieb informačnej spoločnosti na *mere conduit* (článok 12), *caching* (článok 13) a *hosting* – uloženie informácií na hostiteľskom počítači (článok 14). Z hľadiska zamerania tohto článku je pre nás najdôležitejší typ prevádzkovateľa informačnej spoločnosti v podobe *hostingu,* keďže k tomuto vymedzeniu má najbližšie vymedzenie konceptu poskytovateľa online služieb zdieľania obsahu. Ako príklady hostingových služieb možno uviesť webhosting, úložis-

[26] Uloženie informácií na hostiteľskom počítači

„1. Ak sa poskytuje služba informačnej spoločnosti, ktorá pozostáva z uloženia informácií, ktoré sú poskytované príjemcom tejto služby, musia členské štáty zabezpečiť, aby poskytovateľ služby nebol zodpovedný za informácie uložené na žiadosť príjemcu služby, pod podmienkou, že:

(a) poskytovateľ nič nevie o nezákonnej činnosti alebo informáciách a čo sa týka nárokov na náhradu škody, nie je si vedomý skutočností alebo okolností, z ktorých by bolo zrejmé, že ide o nezákonnú činnosť alebo informácie; alebo

(b) poskytovateľ, po zistení alebo uvedomení si týchto skutočností, koná promptne, aby odstránil alebo znemožnil prístup k informáciám.

2. Odsek 1 sa neuplatní, ak príjemca služby koná na základe právomoci od poskytovateľa alebo pod jeho vedením.

3. Tento článok nemá vplyv na možnosť súdu alebo správneho orgánu požiadať poskytovateľa služieb, v súlade s právnymi systémami členských štátov, aby ukončil alebo predchádzal porušovaniu predpisov, a nemá vplyv ani na možnosť členských štátov, aby začali konanie, ktoré by nariadilo odstránenie alebo znemožnenie prístupu k informáciám.“

[27] Pozri § 6 Zákona o elektronických komunikáciách.

[28] Prevádzkovatelia služieb informačnej spoločnosti sú definovaní ako *„každá služba poskytovaná informačnou spoločnosťou, to jest každá služba, ktorá sa bežne poskytuje za odmenu, na diaľku, elektronickým spôsobom a na základe individuálnej žiadosti príjemcu služieb. Na účely tejto definície:*

– *„na diaľku“; znamená, že služba sa poskytuje bez toho, aby pri tom boli obe strany súčasne prítomné,*

– *„služba poskytovaná elektronicky“; znamená, že služba sa z miesta pôvodu odošle a na mieste určenia prijíma prostredníctvom elektronického zariadenia, určeného na spracovávanie (vrátane digitálneho komprimovania) a uskladňovanie údajov a je úplne vysielaná, prenášaná a prijímaná po drôte, prostredníctvom rádiových vĺn, optickým spôsobom, alebo inými elektromagnetickými prostriedkami,*

– *„na základe individuálnej žiadosti príjemcu služieb“; znamená, že služba sa prostredníctvom prenosu údajov poskytuje na individuálnu žiadosť.“*

ko videí, súborov, internetové aukcie, sociálne siete, blogové platformy či funkcionality pridávania komentárov alebo recenzií.[29]

Článok 14 Smernice o elektronickom obchode uvádza 3 podmienky nadobudnutia bezpečného prístavu: (i) príjemca služby nekoná na základe poverenia poskytovateľa alebo pod jeho kontrolou, (ii) poskytovateľ nemá skutočnú vedomosť o protiprávnosti činnosti alebo informácií a (iii) nie je si vedomý skutočností alebo okolností, z ktorých by bolo zrejmé, že ide o nezákonnú činnosť alebo informácie. Súdny dvor Európskej únie vo svojej judikatúre k týmto podmienkam pridal ešte štvrtú, a to že prevádzkovateľ *hosting* služby nesmie hrať aktívnu rolu takej povahy, že by bolo možné konštatovať, že uložené dáta pozná alebo kontroluje, ale musí sa naopak správať neutrálne.[30] V prípade ak prevádzkovateľ služby spĺňa podmienky bezpečného prístavu, nie je zodpovedný za obsah nahrávaný užívateľmi tejto služby.

Povedané ľudskou rečou na príklade: Google nezodpovedá za deep fakes, ktoré nahrá používateľ Youtube na servery tejto služby dovtedy, kým sa nedozvie o protiprávnom obsahu videa alebo o protiprávnom konaní používateľa, pričom po tomto zistení musí bezodkladne zabrániť ďalšiemu zobrazovaniu videa.

Splnenie právnych podmienok pre bezpečný prístav v podstate vylučuje vznik právnej zodpovednosti za obsah zverejnený na internete, pričom tieto podmienky sú definované spôsobom, ktorý umožňuje právne stanoviť dokedy je vznik zodpovednosti vylúčený. *„Po strate bezpečných prístavov je založenie zodpovednosti na vnútroštátnom práve. Ak teda napríklad poskytovateľ neodstráni údajne difamačný príspevok, pretože si nie je istý o jeho protiprávnosti, takpovediac „vypláva" z bezpečného prístavu do všeobecných vôd zodpovednosti. A je na vnútroštátnom súde, aby vo vnútroštátnom práve našiel prípadný dôvod jeho zodpovednosti."*[31] Je však treba dodať, že aj keď aktuálny právny stav spojený s vyvodzovaním zodpovednosti za obsah zverejnený na internete nie je ideálny, nová legislatíva týkajúca sa ochrany osobných údajov má potenciál túto situáciu vylepšiť z viacerých aspektov.

[29] HUSOVEC, M: *Zodpovednosť na internete podľa slovenského a českého práva*. Praha: CZ NIC, 2019, s. 104-105.

[30] Rozhodnutie Súdneho dvora Európskej únie vo veci L'Oreal v. eBay C-324/09.

[31] HUSOVEC, M: *Zodpovednosť na internete podľa slovenského a českého práva*. Praha: CZ NIC, 2019, s. 93.

3.2. Ochrana osobných údajov

Ochrana osobných údajov je v rámci EÚ unifikovaná prostredníctvom nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES („**GDPR**"). Priestor v oblasti vymožiteľnosti práv jednotlivca vidíme predovšetkým v práve na vymazanie podľa článku 17 GDPR. Z hľadiska prevádzkovateľov služieb informačnej spoločnosti je potrebné pozornosť upriamiť na inštitúty posúdenia vplyvu na ochranu údajov podľa článku 35 GDPR a špecificky navrhnutej a štandardnej ochrany údajov v zmysle článku 25 GDPR.

3.2.1. Právo byť zabudnutý (pohľad užívateľov)

V prípade, ak užívateľ žiada o vymazanie určitého obsahu z platformy zdieľania obsahu, je nutné aspoň stručne vymedziť, komu by mala byť takáto žiadosť adresovaná. Na prvý pohľad totiž nemusí byť automaticky zrejmé, kto je tzv. prevádzkovateľom osobných údajov t.j. osoba zodpovedná za dodržiavanie GDPR.[32] V prípade Youtube to môže byť prevádzkovateľ kanála Youtube alebo samotný Youtube. Pre zjednodušenie a bez potreby zachádzania do komplexných právnych analýz uvádzame, že je možné žiadosť o výkon práva podať tomu subjektu, na ktorého webstránke je deep fakes video alebo fotografie zverejnené.[33] Kontaktovanie prevádzkovateľa kanála by mohlo byť v niektorých prípadoch náročnejšie a z tohto dôvodu odporúčame kontaktovať poskytovateľa služby ako celku.

V zmysle článku 17 ods. 1 GDPR má dotknutá osoba právo dosiahnuť u prevádzkovateľa bez zbytočného odkladu vymazanie osobných údajov, ktoré sa jej týkajú, a prevádzkovateľ je povinný bez zbytočného odkladu vymazať osobné údaje, ak je splnený niektorý z dôvodov ustanovených v GDPR. Navyše, podľa článku 17 ods. 2 GDPR ak prevádzkovateľ zverejnil osobné údaje je povinný vymazať osobné údaje, so zreteľom na dostupnú technológiu a náklady na vykonanie opatrení

[32] Prevádzkovateľ je definovaný v článku 4 bod 7 GDPR: *„prevádzkovateľ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov."*

[33] Európsky súdny dvor vo veci C-210/2016, Unabhängiges Landeszentrum für Datenschutz SchleswigHolstein vs Wirtschaftsakademie SchleswigHolstein GmbH z 05. júna 2018 konštatuje, že: *„Článok 2 písm. d) smernice Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov sa má vykladať v tom zmysle, že pojem [„prevádzkovateľ"] v zmysle tohto ustanovenia zahŕňa správcu fanúšikovskej stránky umiestnenej na sociálnej sieti."*

podnikne primerané opatrenia vrátane technických opatrení, aby informoval prevádzkovateľov, ktorí vykonávajú spracúvanie osobných údajov, že dotknutá osoba ich žiada, aby vymazali všetky odkazy na tieto osobné údaje, ich kópiu alebo repliky.

Judikatúra Súdneho dvora Európskej únie v minulosti spoľahlivo potvrdila, že videá zachytávajúce identifikovateľné fyzické osoby sú považované za osobné údaje.[34] Otázkou ostáva, či v takejto situácií je splnený niektorý z dôvodov na vymazanie a či sa neuplatňuje niektorá z výnimiek podľa článku 17 ods. 3 GDPR. Podľa nášho názoru v prípade zverejnenia deep fakes videa sa otvára hneď niekoľko dôvodov na ich vymazanie, a to konkrétne neexistencia právneho základu spracúvania osobných údajov (osobné údaje sa spracúvali nezákonne)[35] prípadne osobné údaje sa získavali v súvislosti s ponukou služieb informačnej spoločnosti (v súvislosti s maloletými).[36] Žiadosť dotknutej osoby zasiahnutej zverejnením jej osobných údajov v deep fakes videu by mala byť úspešne vybavená. Vzhľadom na to, že v prípade deep fakes pôjde takmer vždy aj o zverejnenie osobných údajov na internete je vhodné požadovať nielen vymazanie, ale aj to aby prevádzkovateľ cez dostupné technológie (napr. nástroje na odstraňovanie obsahu zo služieb Google[37]) zamedzil ďalšiemu šíreniu takéhoto videa a notifikoval všetkých príjemcov, ktorým boli tieto dáta poskytnuté, aby ich vymazali.

3.2.2. Niektoré povinnosti prevádzkovateľov (pohľad poskytovateľov služieb informačnej spoločnosti)

V druhom rade GDPR obsahuje aj preventívne regulačné povinnosti, ktoré od určitého typu prevádzkovateľov vyžadujú, aby rátali s hrozbami, ktoré nové technológie (vrátane deep fakes) predstavujú pre práva a slobody dotknutých osôb. Konkrétne máme na mysli povinnosť

[34] Európsky súdny dvor vo veci C-212/13, Ryneš vs Úřad pro ochranu osobních údaju z 11. decembra 2014 konštatuje, že: „*Obraz osoby zaznamenaný prostredníctvom kamery teda predstavuje osobný údaj v zmysle ustanovenia citovaného v predchádzajúcom bode (pozn.: definícia osobných údajov), lebo umožňuje identifikovať dotknutú osobu.*“ Súdny dvor EÚ ostáva naďalej konzistentný aj vo veci C345/17 Sergejs Buivids vs Datu valsts inspekcija z 14. februára 2019, kde konštatuje, že: *„Článok 3 smernice Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov sa má vykladať v tom zmysle, že videozáznam policajtov zhotovený počas výpovede na policajnej stanici a zverejnenie takto zhotoveného videozáznamu v internetovej databáze videí, v ktorej môžu užívatelia nahrávať, sledovať a zdieľať tieto videozáznamy, patrí do pôsobnosti tejto smernice.“*

[35] Článok 17 ods. 1 písm. d) GDPR.

[36] Článok 17 ods. 1 písm f) GDPR.

[37] https://support.google.com/legal/troubleshooter/1114905.

vykonať posúdenie vplyvu na ochranu osobných údajov (čl. 35 GDPR) a povinnosť zabezpečovať v čase určenia prostriedkov spracúvania, ako aj v čase samotného spracúvania špecifickú ochranu osobných údajov (čl. 25 ods. 1 GDPR).

V zmysle článku 35 ods. 1 GDPR: *„Ak typ spracúvania, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ pred spracúvaním vykoná posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov."* Pri prevádzkovaní platformy zdieľania obsahu je viac než pravdepodobné, že užívatelia budú na takýto portál nahrávať aj obsah, ktorý môžu predstavovať riziko pre práva a slobody dotknutých osôb. Pri výklade tohto ustanovenia je nutné vziať do úvahy aj stanovisko Pracovnej skupiny článku 29 ku posúdeniu vplyvu.[38] Toto stanovisko uvádza kritéria, ktoré indikujú povinnosť vykonať toto posúdenie vplyvu na ochranu údajov s tým, že ak sú splnené aspoň 2 kritéria, posúdenie vplyvu je vhodné vykonať. Ide o tieto kritéria:

- Vyhodnocovanie určitých aspektov týkajúcich sa dotknutej osoby (vrátane profilovania) napr. pri pracovnoprávnych vzťahov, hodnotenie majetkových pomerov, zdravia alebo osobných preferencií;
- Automatizované rozhodovanie s právnym alebo podobne závažným účinkom;
- Systematické monitorovanie osobných údajov;
- Spracúvanie citlivých osobných údajov;
- Spracúvanie údajov vo veľkom rozsahu;
- Spájanie alebo kombinovanie súborov a údajov pochádzajúcich z rôznych spracovateľských operácií;
- Spracúvanie údajov týkajúcich sa „zraniteľných" dotknutých osôb;
- Využitie nových technológií, technologických alebo organizačných riešení a postupov;
- Spracúvanie bráni dotknutým osobám uplatniť svoje právo alebo využiť službu alebo zmluvu.

Domnievame sa, že pri vývoji technológie deep fakes a prevádzkovaní služby zdieľania obsahu sú niektoré z vyššie uvedených kritérií významne zastúpené (môže ísť aj o spracúvanie citlivých osobných

[38] Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679, s. 9-11.

údajov, spracúvanie údajov vo veľkom rozsahu, videá alebo fotografie sa môžu týkať zraniteľných dotknutých osôb napr. detí a pod.).

Navyše, podľa článku 25 ods. 1 GDPR *„So zreteľom na najnovšie poznatky. náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou, ktoré spracúvanie predstavuje pre práva a slobody fyzických osôb, prevádzkovateľ v čase určenia prostriedkov spracúvania aj v čase samotného spracúvania prijme primerané technické a organizačné opatrenia, ako je napríklad pseudonymizácia, ktoré sú určené na účinné zavedenie zásad ochrany údajov, ako je minimalizácia údajov, a začlení do spracúvania nevyhnutné záruky s cieľom splniť požiadavky tohto nariadenia a chrániť práva dotknutých osôb.“* Inými slovami, prevádzkovatelia osobných údajov by mali vplyv nových technológií vziať do úvahy už pri začiatku spracúvania osobných údajov (napr. pri tvorbe aplikácie alebo spustení služby).[39]

Interakcia týchto dvoch povinností by tak podľa nášho názoru v praxi mala znamenať to, že prevádzkovatelia webov s obsahom (videami) toto riziko posúdia z hľadiska možných dopadov na práva a slobody dotknutých osôb a prijmú nadväzné protiopatrenia, aby tieto riziká zmiernili alebo úplne eliminovali. Práve v tomto vie dôsledné a zmysluplné dodržiavanie GDPR reálne pomôcť bežným ľuďom.

4. Záver a budúci výskum

Deep fakes technológia má dopad na vnímanie reality v dnešnej dobe šírenia falošných správ. Ako bolo uvedené vyššie, predmetná technológia má potenciál ovplyvniť nielen jednotlivca a jeho reputáciu či dobré meno organizácie, ale pri dynamike jej vývoja je možné predpokladať negatívny vplyv aj na demokratické zriadenie a chod verejných inštitúcií.

Záverom je teda možné skonštatovať, že v prípade deep fakes aktuálna úprava zodpovednosti za obsah zverejnený na internete je súladná s možnosťami, ktoré ponúka GDPR. Ak by prevádzkovateľ zodpovedný za zverejnený obsah na internete i ochranu osobných údajov nerešpektoval riadne uplatnené právo dotknutej osoby podané podľa GDPR niesol by nielen zodpovednosť za porušenie GDPR, ale teoreticky aj akúkoľvek ďalšiu zodpovednosť, ktorú by s daným skutkovým stavom

[39] MESARČÍK, M. : Naozaj sa bojím tmy? Zopár úvah o technologicom determinizme v kontexte ochrany osobných údajov In *Acta Facultatis Iuridicae Universitatis Comenianae. - Roč. 36, č. 2 (2017)*, s. 204-217.

spájali normy vnútroštátneho práva (napr. občianskoprávna zodpovednosť za neoprávnený zásah do ochrany osobnosti, či trestno-právna zodpovednosť za porušovanie autorského práva, poškodzovanie cudzích práv, ohrozovanie mravnosti, ohováranie, rozširovanie extrémistických materiálov, či iné trestné činy, ktorých objektívnu stránku možno naplniť zverejnením videa s protiprávnym obsahom). Tieto aspekty plánujú autori skúmať vo svojej ďalšej vedeckej činnosti.

Použitá literatúra

1. ADAM DODGE & ERICA JOHNSTONE, DOMESTIC VIOLENCE ADVISORY: USING FAKE VIDEO TECHNOLOGY TO PERPETUATE INTIMATE PARTNER ABUSE 6 (Apr. 25 2018), http://withoutmyconsent.org/blog/newadvisory-helps-domestic-violence-survivors-prevent-and-stop-deepfake-abuse (dostupné 26.7.2019).
2. ANDRAŠKO, J.: Elektronický občiansky preukaz a iné spôsoby autentifikácie pri prístupe k elektronickým službám verejnej správy. QUAERE 2017 [elektronický zdroj]. - ISBN 978-80-87952-20-7. - Hradec Králové : Magnanimitas, 2017.
3. Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk“ for the purposes of Regulation 2016/679.
4. BOYD, D.: „Streams of Content, Limited Attention: The Flow of Information through Social Media“, https://www.danah.org/papers/talks/Web2Expo.html (dostupné 26.7.2019).
5. BREY, P.: Ethics of Socially Disruptive Technologies In Ian Ayres and John Braithwaite, Responsive Regulation: Transcending the Deregulation Debate, Oxford University Press 1992.
6. CALAMUR, K.: Did Russian Hackers Target Qatar? THE ATLANTIC (June 6, 2017), https://www.theatlantic.com/news/archive/2017/06/qatar-russian-hacker-fake-news/529359/ (dostupné 27.7.2019).
7. COLE, S.: We Are Truly Fucked: Everyone Is Making AI-Generated Fake Porn Now, VICE: MOTHERBOARD, https://motherboard.vice.com/en_us/article/bjye8a/reddit-fakeporn-app-daisy-ridley (dostupné 26.7.2019).
8. Datatylsinet: Artificial intelligence and privacy Report, January 2018, https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf. (dostupné 26.7.2019).
9. https://iq.intel.com/artificial-intelligence-and-machine-learning/ (dostupné 26.7.2019)
10. https://searchenterpriseai.techtarget.com/definition/deep-learning-deep-neural-network (dostupné 26.7.2019).

11. HUSOVEC, M: Zodpovednosť na internete podľa slovenského a českého práva. Praha: CZ NIC, 2019.
12. CHESNEY, R. – CITRON, D.: Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954 (dostupné 26.7.2019).
13. KOPECKÝ, K.: Deep fake – stručný úvod do problematiky, dostupné online: https://www.e-bezpeci.cz/index.php/70-projekt-fake-news/1417-deep-fake-strucny-uvod-do-problematiky (dostupné 26.7.2019).
14. MESARČÍK, M.: Naozaj sa bojím tmy? Zopár úvah o technologicom determinizme v kontexte ochrany osobných údajov In Acta Facultatis Iuridicae Universitatis Comenianae. - Roč. 36, č. 2 (2017), s. 204-217.
15. NARCISSE, I.: It Took Some Movie Magic to Finish Carrie Fisher's Leia Dialogue in The Last Jedi, GIZMODO, https://io9.gizmodo.com/it-took-some-movie-magic-to-complete-carrie-fisherslei-1821121635 (dostupné 26.7.2019).
16. NOSSITER, A. et al.: Hackers Came, But the French Were Prepared, N.Y. TIMES, https://www.nytimes.com/2017/05/09/world/europe/hackers-came-but-the-french-were-prepared.html (dostupné 27.7.2019).
17. STRÉMY, T. – TURAY, L.: Stalking a jeho trestnoprávne súvislosti In Acta Facultatis Iuridicae Universitatis Comenianae. - Roč. 37, č. 2 (2018), s. 274-285.
18. VOLPE, A.: Deepfake Porn Has Terrifying Implications. But What If It Could Be Used for Good? MEN'S HEALTH, https://www.menshealth.com/sex-women/a19755663/deepfakes-porn-redditpornhub (dostupné 26.7.2019).