UDK: 343.3/.7::004
004.738.52
doi: 10.5937/crimen2403325C
Originalni naučni rad
primljen / prihvaćen: 29.102024 / 09.12.2024.

*Irena Čučilović**

DEEPFAKE TEHNOLOGIJA – *KRIVIČNOPRAVNE* IMPLIKACIJE

Apstrakt. Pojam i dometi veštačke inteligencije postali su nezaobilazna tema stručnjaka i laičke javnosti još pre nekoliko godina, kada je postalo očigledno da je njen razvoj nezaustavljiv i da će ona doneti korenite promene u mnogim oblastima našeg života. Uz brojne nesumnjive prednosti, veštačka inteligencija je sobom donela i brojne opasnosti i izazove sa kojima ćemo se u budućnosti tek suočavati. Tema ovog rada su upravo izazovi koje veštačka inteligencija, preciznije tehnologija *deepfake*, koja se zasniva na veštačkoj inteligenciji, postavlja pred krivično pravo i kakav je odgovor pre svega našeg krivičnog zakonodavstva na izazove sa kojima je suočeno.

Ključne reči: visokotehnološki kriminalitet, *deepfake* tehnologija, *deepfake* prevare, *deepfake* pornografija, *deepfake* dečja pornografija

UVODNA RAZMATRANJA

Razvoj informacionih tehnologija, a posebno pojava i razvoj veštačke inteligencije (u daljem tekstu: *AI*),[1] omogućavaju konstantan napredak savremenog društva i značajno poboljšavaju kvalitet života građana. Uz brojne koristi, ekspanzivni razvoj informacionih tehnologija i *AI* istovremeno je otvorio neka nova pitanja i postavio nove dileme pred naučnu i stručnu javnost, za koje se, bar u ovom trenutku, čini da nema adekvatnog odgovora. U kontekstu krivičnog prava pre svega mislimo na pojavu i ekspanziju tzv. visokotehnološkog kriminaliteta[2], pod kojim podrazumevamo

* Advokat, irena@advokatskitim.rs, ORCID 0009-0000-5823-780X

1 Veštačka inteligencija podrazumeva raznolik stepen upotrebe nauke i tehnologije radi omogućavanja mašinama da preduzimanjem radnji koje zahtevaju inteligenciju postignu određene ciljeve, poput pobede u šahu ili razgovora sa ljudima. Više o definicijama veštačke inteligencije vid. u: S. Nenadić, I. Miljuš (2022). Krivična pravda u eri veštačke inteligencije. *Digitalizacija u kaznenom pravu i pravosuđu* (ur. J. Kostić, M. Matić Bošković), Beograd, p. 292

2 Polazeći od vladajućeg mišljenja u našoj literaturi da je teorijsko-terminološki i naučno posmatrano izraz „kriminalitet" korektniji od izraza „kriminal", u radu će se koristiti izraz „kriminalitet" iako je u našem pozitivnom zakonodavstvu i u javnom prostoru postao ustaljen izraz „kriminal". Više o tom terminološkom sporu vid. u: M. Škulić (2007). Uloga posebnih dokaznih radnji u suzbijanju organizovanog kriminaliteta. *Primena međunarodnog krivičnog prava*, Tara,

sva ona protivpravna ponašanja koja se preduzimaju upotrebom informacionih tehnologija ili u digitalnom prostoru – na internetu i društvenim mrežama.[3] Visokotehnološki kriminalitet obuhvata određene kriminalne aktivnosti koje se po svojoj prirodi, načinu, sredstvu izvršenja i drugim specifičnostima odnose na zloupotrebu informacionih tehnologija, odnosno računara i mreža, sa ciljem izvršenja određenog krivičnog dela.[4] Osim doprinosa razvoju novih formi tradicionalnih krivičnih dela, usavršavanje informacionih tehnologija je doprinelo i efikasnijem funkcionisanju pojedinih vidova kriminaliteta, pre svega organizovanog, razvijanjem otpornosti učinilaca takvih krivičnih dela na radnje koje preduzimaju nadležni organi krivičnog gonjenja radi otkrivanja, razjašnjavanja i dokazivanja tih oblika kriminalne aktivnosti.[5]

Svesne rizika da se računarske mreže i elektronske informacije mogu koristiti i za izvršenje krivičnih dela i da dokazi koji se odnose na takva krivična dela mogu biti sačuvani i preneti putem tih mreža te neophodnosti saradnje između država i privatnih privrednih subjekata u suzbijanju i sprečavanju određenih protivpravnih aktivnosti kojima se vrši zloupotreba informacionih tehnologija, pri čemu efikasna borba protiv visokotehnološkog kriminaliteta zahteva povećanu, brzu i funkcionalnu saradnju u krivičnim stvarima, države članice Saveta Evrope su 2001. godine u Budimpešti usvojile Konvenciju o visokotehnološkom kriminalu.[6] Države potpisnice Konvencije preuzele su obavezu da u svom nacionalnom zakonodavstvu inkriminišu određena krivična dela visokotehnološkog kriminaliteta te da kontinuirano rade jačaju kapacitete državnih organa radi otkrivanja, krivičnog gonjenja i suđenja za ta krivična dela, ali i dužnost da uspostavljaju adekvatnu saradnju i pružaju međunarodnu pravnu pomoći u tim predmetima.

Uprkos inkriminisanju dela visokotehnološkog kriminaliteta, sama priroda informacionih tehnologija prouzrokovala je brojne probleme u otkrivanju, dokazivanju i gonjenju učinilaca tih krivičnih dela. Pre svega mislimo na kontinuiranu globalizaciju računarskih mreža i računarskih sistema, gotovo potpunu anonimnost korisnika na internetu[7] i postojanje tzv. *dark neta* (*Deep Web*) kome je nemoguće pristupiti putem uobičajenih brauzera, odnosno veb-pretraživača, na kojima je mo-

---

p. 35. Za tu vrstu kriminaliteta u širu upotrebu je ušao i termin „sajber kriminalitet", mada ima mišljenja da bi, budući da je sajber engleski oblik poreklom iz grčkog jezika „kiber", ispravnije bilo koristiti termin „kiber kriminalitet". Više o tome: Z. Stojanović (2021). *Komentar krivičnog zakonika*, Službeni glasnik, str. 952

3 S. Ma. Baron Quintero (2023). Los delitos realizados mediante la Dark Net, *Revista Penal Mexico* 23, str. 176

4 S. Karović, M. Simović (2022). Krivičnopravno suprotstavljanje visokotehnološkom – kompjuterskom kriminalitetu: savremeni izazovi, dileme, perspektive. *Digitalizacija u kaznenom preavu i pravosuđu* (ur. J. Kostić, M. Matić Bošković), Beograd, str. 47

5 M. Škulić (2024). Dokazni značaj informacija iz komunikacije ostvarene aplikacijama/modifikovanim uređajima za kriptovanje – kao što su Sky ECC i EnchroChat, *CRIMEN – Časopis za krivične nauke* 1, str. 4

6 Republika Srbija je navedenu konvenciju potpisala 2005. godine, a ratifikovala 2009. godine. Vidi: Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu, *Sl. glasnik RS – broj 19/09*

7 M. Pisarić (2013). Potrebni normativni odgovor na probleme otkrivanja i dokazivanja dela visokotehnološkog kriminala. *Zbornik radova Pravnog fakulteta u Novom Sadu*, str. 292

guće pronaći najrazličitije sadržaje, počev od dečje pornografije do najosetljivijih državnih tajni.[8]

Problemi sa kojima su se inače suočavali zakonodavni, pravosudni i drugi državni organi u sprečavanju i suzbijanju krivičnih dela visokotehnološkog kriminaliteta praktično su se umnožili pojavom i razvojem veštačke inteligencije i *deepfake* tehnologije koja je zasnovana na veštačkoj inteligenciji.

Prvi međunarodnopravni akt kojim je na sveobuhvatan način regulisana veštačka inteligencija donet je na nivou Evropske unije 12. jula 2024. godine. Tim aktom su zabranjeni aplikacije i sistemi koji stvaraju neprihvatljiv rizik, kao što je društveno bodovanje koje vodi vlada, koji se koriste u Kini, te propisana posebna ograničenja za visokorizične aplikacije, poput alata za skeniranje biografija kojima se rangiraju kandidati za posao. Osim toga, *EU AI* aktom[9] je u značajnoj meri regulisan i *deepfake* sadržaj, pri čemu je uvedeno načelo transparentnosti i jasno označavanje da je sadržaj modifikovan. Članom 50(4) kreatori *deepfake* sadržaja se obavezuju da javnost obaveste o činjenici da je sadržaj koji objavljuju nastao korišćenjem *deepfake* tehnologije. Uvodna izjava 136 tog akta naglašava ključnu ulogu provajdera pojedinih *AI* sistema u identifikaciji i označavanju modifikovanog sadržaja kao takvog. Međutim, u tom aktu je izostala regulativa koja se odnosi na mnogobrojne krivičnopravne implikacije *deepfake* tehnologije.[10]

2. ŠTA JE *DEEPFAKE* SADRŽAJ I KOJE IZAZOVE DONOSI?

Termin *deepfake* je prvi put upotrebljen na popularnom onlajn forumu *Reddit*, na kome se postavljaju teme za diskusiju, tzv. *subreddits*, u vezi sa kojima korisnici mogu da ostavljaju komentare i da glasaju. U novembru 2017. godine korisnik tog foruma, pod korisničkim imenom *u/deepfakes*, postavio je video-snimak seksualnog odnosa glumice *Gal Gadot* i njenog polubrata. Ubrzo su fanovi *u/deepfakes* kreirali *subreddit* pod nazivom *r/deepfakes*, na kome su isključivo postavljani lažni video-snimci poznatih ličnosti pornografskog sadržaja, koji je za samo dva meseca stekao preko 50.000 pratilaca. Nedugo zatim, žrtve lažnih pornografskih video-snimaka postale su i osobe nepoznate široj javnosti. *Reddit* je u nekom trenutku zabranio, odnosno „*banovao*" *r/deepfakes* zbog kršenja pravila zajednice, ali je šteta već bila učinjena.[11]

8 S. Ma. Baron Quintero, p. 176.

9 EU Atrificial Intelligence Act. https://artificialintelligenceact.eu/the-act/, 16. septembar 2024.

10 Osim što su članom 50(4) Zakona o veštačkoj inteligenciji organi krivičnog gonjenja izuzeti iz obaveze da jasno označe upotrebu *deepfake* tehnologije prilikom sprovođenja istrage i prikupljanja dokaza, čime je data prednost ostvarivanju određenih legitimnih pravnih ciljeva u odnosu na načelo transparentnosti. Vid. F. Romero Moreno (2024). Generative AI and deepfakes: a human rights approach to tackling harmful content. *International review of law, computers & technology*, Routledge, p. 5

11 A. Pechenik Gieseke (2020). „The New Weapon of Choice": Law's Current Inability to Properly Address Deepfake Pornography. *Vanderbilt Law Review*, p. 1484–1485

Deepfake je munjevitom brzinom proširio svoje domete, te su osim pornografskih video-snimaka poznatih i anonimnih ličnosti, viralni postali i *deepfake* snimci političkih lidera i drugih uticajnih ličnosti, koji su usmereni ka potkopavanju njihovog autoriteta i širenju dezinformacija radi sticanja političke ili vojne prednosti.[12] Rečju, *deepfake* sadržaji ne predstavljaju samo kršenje prava na poštovanje privatnosti onih lica koja su mimo svoje volje postala „zvezde" neautentičnih fotografija i video-snimaka već istovremeno poseduju ozbiljan potencijal da otvore mnoge društvene, političke i bezbednosne probleme u bilo kojoj zemlji.[13]

Deepfake je audio, video ili audio-vizuelni sadržaj koji je potpuno ili delimično izmišljen ili postojeći audio, video ili audio-vizuelni sadržaj kojim je manipulisano. U tu svrhu se može koristiti više različitih tehnologija, ali je najefikasnija i najpopularnija tehnologija koja se zasniva na tzv. generativnoj adversijalnoj mreži (tzv. *Generative Adverssial Networks –GAN*).[14] Samu tehnologiju osmislio je tim stručnjaka sa Univerziteta u Montrealu 2014. godine, koje je predvodio *Ian Goodfellow.*[15] Tehnologija je predstavljena javnim prikazivanjem video-snimka bivšeg predsednika Sjedinjenih Američkih Država (SAD) *Baraka Obame* u kome on govori reči koje zapravo nije izgovorio.[16]

Generativna adversijalna mreža – *GAN* sastoji se od dva neuronska modela: *generatora*, koji stvara nove podatke koji su slični postojećim podacima, sa ciljem da generiše podatke koji izgledaju što je moguće realističniji, i *diskriminatora*, koji pokušava da razlikuje stvarne podatke od onih koje je generisao generator. Cilj diskriminatora je da prepozna lažne podatke i označi ih kao takve.[17] Ta dva neuronska modela postavljena su kao pozicija i opozicija, oni su suprotnost jedan drugom i takmiče se jedan protiv drugog. U iterativnom procesu, ta dva modela uče jedan od drugog, tako što ocene diskriminatora informišu generator koji ispravlja greške na

12 Nakon što je Rusija započela invaziju ili specijalnu vojnu operaciju u Ukrajini 24. februara 2022. godine, ukrajinski zvaničnici su upozorili da bi Rusija mogla da kreira *deepfake* video u kome bi se ukrajinski predsednik Volodimir Zelenski predao Rusiji. Ubrzo nakon tog upozorenja došlo je do hakerskog napada na veb-sajt jednog ukrajinskog medija, na kome je postavljen *deepfake* video predsednika Zelenskog koji svojim vojnicima govori da se predaju. Više o tome: Facing reality? Law enforcement and challenge of deepfakes, An Observatory Report from the Europol Innovation Lab (u daljem tekstu: Europol Observatory Report), p. 6. https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes, 20. jul 2024.

13 O rizicima *deepfake* tehnologije vid. u: T. Brooks *et al*., Increasing Threat of Deepfake Identities, *Homeland Security*. https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf, 20. avgust 2024. Jedna od očiglednih opasnosti koje donose modifikovani video-sadržaji jeste stvaranje nove i potpuno razumljive sumnje u sve što vidimo. Političari i javne ličnosti će obilato iskorišćavati te sumnje – svaki put kada budu uhvaćeni u „nedelu" proglasiće da je materijalni dokaz tog nedela modifikovan *deepfake* sadržajem. Više o tome: D. Citron, R. Chesney (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review* 107, p. 1777

14 B. van der Sloot *et al.* (2021). *Summary Deepfakes: The legal challenges of a synthetic society*, Tilburg Institute for Law, Technology, and Society, p. 1

15 A. Pechenik Gieseke, p. 1487.

16 D. K. Citron, R. Chesney, p. 1760; Fake Obama created using AI video tool – BBC News. https://www.youtube.com/watch?v=AmUC4m6w1wo, 5. avgust 2024.

17 A. Pechenik Gieseke, p. 1487.

osnovu kojih je diskriminator generisane podatke prepoznao kao lažne, dok istovremeno sve sofisticiraniji podaci generatora pozitivno utiču na razvoj diskriminatora.[18]

Upravo zahvaljujući opisanom iterativnom procesu modela *GAN*, konstantnom usavršavanju *deepfake* tehnologija, te onlajn dostupnosti ogromnih baza podataka, produkcija izuzetno ubedljivih *deepfake* fotografija, audio i video snimaka beleži neslućene razmere. Zahvaljujući tim faktorima, *deepfake* tehnologija postaje sve savršenije sredstvo izvršenja brojnih krivičnih dela.

3. *DEEPFAKE* TEHNOLOGIJA KAO SREDSTVO IZVRŠENJA POJEDINIH KRIVIČNIH DELA

Softveri koji kreiraju *deepfake* sadržaje vrlo brzo su postali moćno oružje u rukama učinilaca različitih krivičnih dela. Zahvaljujući tome je, uz prethodnu zloupotrebu tih sadržaja u političke svrhe i širenje dezinformacija, uočeno da je *deepfake* tehnologija ozbiljna kriminalna i bezbednosna pretnja u nacionalnim i međunarodnim okvirima. Nakon *deepfake* pornografije, pojavili su se i *deepfake* sadržaji iz domena dečje pornografije. Zatim su, sredinom 2023. godine, mediji počeli da upozoravaju na *deepfake* prevare čije su žrtve uglavnom pripadnici manjina, koje učinioci krivičnog dela navedu da sa njima podele svoje eksplicitne fotografije dovođenjem u zabludu ili upotrebom *deepfake* tehnologije kreiraju takve fotografije. Nakon toga, izvršioci žrtvi traže određeni iznos novca pod pretnjom da će u suprotnom njihove eksplicitne fotografije učiniti dostupnim javnosti na internetu.[19]

Početkom ove godine, *CNN* je objavio uznemirujuću vest iz Hong Konga, gde je zaposleni u jednoj multinacionalnoj kompaniji, zloupotrebom *deepfake* tehnologije, doveden u zabludu da putem video-konferencijske veze razgovara sa načelnikom finansijske službe te kompanije, pa je, izvršavajući naloge navodnog načelnika, izvršiocu tog krivičnog dela isplatio sumu od 25 miliona dolara.[20] Nedugo zatim, svet je obišla vest o novom vidu *deepfake* prevare, u kojoj izvršioci zloupotrebom *deepfake* tehnologije žrtvu dovode u zabludu o svojoj ličnosti, započinju i razvijaju sa žrtvom emotivnu vezu, da bi žrtvu, nakon što zadobije poverenje u svog navodnog emotivnog partnera, naveli da im uplati određeni iznos novca, nakon čega, naravno, sa žrtvom prekidaju svaki kontakt i žrtva tek tada shvata da je prevarena.[21] U julu ove godine španski sud je osudio 15 tinejdžera koji su kreirali i delili *deepfake* pornografske slike svojih školskih drugarica.[22]

18 D. K. Citron, R. Chesney, p. 1760.

19 E. Busch, J. Ware (2023). *The Weaponisation of Deepfakes – Digital Deception by the Far-Right*, International Centre for Counter-Terrorism, p. 3

20 Finance worker pays out $25 million after video call with deepfake „chief financial officer". https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html, 12. avgust 2024.

21 How AI and deepfakes are taking romance scams to another level. https://www.thestar.com.my/tech/tech-news/2024/06/26/how-ai-and-deepfakes-are-taking-romance-scams-to-another-level, 12. avgust 2024.

22 Spain: Court punishes schoolboys for spreading AI deepfakes of girls. https://www.scottishlegal.com/ articles/spain-court-punishes-schoolboys-for-spreading-ai-deepfakes-of-girls, 10. septembar 2024.

O tim i brojnim drugim zabrinjavajućim primerima zloupotrebe *deepfake* tehnologije kao sredstva za izvršenje najrazličitijih krivičnih dela moramo razmišljati u kontekstu činjenice da će se *deepfake* tehnologija vremenom samo dalje usavršavati te da je pitanje trenutka kada više nećemo biti u mogućnosti da razlikujemo autentičan od *deepfake* sadržaja. Prema istraživanju koje je sproveo *New York Times*, nijedan od trenutno dostupnih softvera namenjenih otkrivanju *deepfake* sadržaja nije stoprocentno uspešan, što znači da već u ovom trenutku postoje *deepfake* sadržaji kojima postojeći softveri ne uspevaju da ospore autentičnost.[23] S tim u vezi postavlja se pitanje da li je postojeći normativni okvir adekvatan da se efikasno suprotstavi svim oblicima i manifestacijama zloupotreba *deepfake* tehnologija?

3.1. Deepfake kao visokotehnološko krivično delo

Prema Zakonu o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala[24], visokotehnološki kriminal je vršenje krivičnih dela u kojima se kao objekt ili sredstvo izvršenja javljaju računari, računarski sistemi, računarske mreže, računarski podaci i njihovi proizvodi u materijalnom ili elektronskom smislu. Prema članu 3, taj zakon se primenjuje radi otkrivanja, krivičnog gonjenja i suđenja za tri grupe krivičnih dela:

1) krivičnih dela protiv bezbednosti računarskih podataka propisanih Krivičnim zakonikom,[25]
2) krivičnih dela protiv intelektualne svojine, imovine, privrede i pravnog saobraćaja, u kojima se kao objekt ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže i računarski podaci i njihovi proizvodi u materijalnom ili elektronskom obliku, ako broj primeraka autorskih dela prelazi 2.000 ili nastala materijalna šteta prelazi iznos od 1.000.000 dinara, te
3) krivičnih dela protiv sloboda i prava čoveka i građanina, polne slobode, javnog reda i mira i ustavnog uređenja i bezbednosti Republike Srbije, koja

23 Advisory Commitee on Evidence Rules, April 19, 2024 (u daljem tekstu: Advisory Commitee on Evidence Rules), p. 30. https://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-evidence-rules-april-2024, 21. jul 2024.

24 Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala – Zakon, *Službeni glasnik RS* 61/05, 104/09, 10/23 i 10/23 – drugi zakon.

25 U pitanju su sledeća krivična dela: oštećenje računarskih podataka i programa, računarska sabotaža, pravljenje i unošenje računarskih virusa, računarska prevara, neovlašćen pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka, sprečavanje i ograničavanje pristupa javnoj računarskoj mreži, neovlašćeno korišćenje računara ili računarske mreže i pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka. Vidi: Krivični zakonik – KZ, *Službeni glasnik RS* 85/05, 88/05, 107/05, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16 i 35/19. Iako su ta krivična dela u naše zakonodavstvo prvi put uneta 2003. godine, a kasnije su preuzeta i u novi KZ, koji je stupio na snagu 1. januara 2006. godine, ona su formulisana tako da uglavnom potpuno odgovaraju obavezama koje je naša država preuzela ratifikacijom Konvencije Saveta Evrope o visokotehnološkom kriminalu 2009. godine. Više o tome: Z. Stojanović (2021), str. 953. Nakon ratifikacije Konvencije Saveta Evrope, u naš KZ je uneto samo jedno novo krivično delo, i to krivično delo iz člana 304a – pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka. Više o tome: Z. Stojanović (2021), str. 962.

se zbog načina izvršenja ili upotrebljenih sredstava mogu smatrati krivičnim delima visokotehnološkog kriminala.

Budući da su *deepfake* sadržaji proizvod računarskih mreža u materijalnom ili elektronskom obliku, govorićemo o visokotehnološkom kriminalitetu uvek kada se *deepfake* sadržaji pojave kao sredstvo izvršenja nekog od nabrojanih krivičnih dela. U praksi smo se do sada susretali sa tri vrste krivičnih dela izvršenih zloupotrebom *deepfake* sadržaja: krivičnim delima protiv imovine, krivičnim delima protiv sloboda i prava čoveka i građanina i krivičnim delima protiv polne slobode.

3.1.1. Krivična dela prevare i ucene

Kao što smo videli iz primera pomenutih u ranijem tekstu, učinioci krivičnih dela visokotehnološkog kriminaliteta na različite načine zloupotrebljavaju *deepfake* tehnologiju sa namerom da sebi ili drugom pribave protivpravnu imovinsku korist. Ukoliko se *deepfake* sadržaj kreira i koristi radi dovođenja ili održavanja nekog lica u zabludi kako bi se to lice navelo da nešto učini ili ne učini na štetu svoje ili tuđe imovine, reč je o krivičnom delu prevare iz člana 208 KZ. Ako neko kreira pornografski *deepfake* materijal nekog lica ili se nekom licu lažno predstavi koristeći se *deepfake* tehnologijom („pozajmi" nečiji tuđi lik ili generiše potpuno nepostojeći lik) pa to lice navede da mu dobrovoljno pošalje svoje eksplicitne fotografije, kojima kasnije to lice prinudi da nešto učini ili ne učini na štetu svoje ili tuđe imovine, učiniće krivično delo ucene iz člana 215 KZ.

U krivičnopravnom tretmanu tih krivičnih dela u našem zakonodavstvu postoje dva ključna problema. Prvo, prema izričitoj odredbi člana 3 stav 1 tačka 2) Zakona, ta će krivična dela biti smatrana visokotehnološkim kriminalitetom ukoliko preskoče imovinski cenzus od 1.000.000 dinara prouzrokovane materijalne štete. Drugim rečima, ako je učinilac tih krivičnih dela pribavio protivpravnu imovinsku korist manju od 1.000.000 dinara, za krivično gonjenje neće biti nadležno Posebno odeljenje za borbu protiv visokotehnološkog kriminala u Višem javnom tužilaštvu u Beogradu, koje poseduje specifična znanja iz oblasti informacionih tehnologija, već javno tužilaštvo opšte nadležnosti koje takvim znanjima ne raspolaže, što se može negativno odraziti na dokazivanje tih krivičnih dela.

Drugi problem leži u činjenici da krivična dela izvršena zloupotrebom veštačke inteligencije, konkretno *deepfake* tehnologije, nisu tradicionalna krivična dela prevare ili ucene. Ta krivična dela imaju dodatni element koji ostaje potpuno zanemaren i koji se ne iscrpljuje u formulaciji „krivična dela kod kojih se kao objekt ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom smislu" jer se tom formulacijom ne objašnjava suština pomenutih krivičnih dela. Naime, u našem primeru o radniku multinacionalne kompanije koji je doveden u zabludu da razgovara sa svojim rukovodiocem, u pravnoj kvalifikaciji (krivično delo prevare) gubi se iz vida rukovodilac čiji je lik zloupotrebljen pomoću *deepfake* tehnologije. Slično je sa „pozajmljenim" likom koji je započeo i održavao vezu sa žrtvom krivičnog dela ucene. No, ovde treba imati u vidu da u najvećem broju slučajeva osobe čiji je lik zloupotrebljen radi kreiranja *deepfake* sadržaja to i ne saznaju, te će se u praksi

retko postaviti pitanje krivičnopravne zaštite njihovih prava, i to prava na sopstveni vizuelni prikaz i fotografiju *in concreto*.

Situacija je neuporedivo složenija kada je u pitanju pornografski sadržaj koji je kreiran pomoću *deepfake* tehnologije, koji se kasnije koristi za prinudu osobe na koju se takav sadržaj odnosi da nešto učini ili ne učini na štetu svoje ili tuđe imovine. U tom slučaju bi se moglo raditi o sticaju krivičnog dela ucene i krivičnog dela polno uznemiravanje iz člana 182a KZ, o čemu će više reči biti u nastavku teksta.

3.1.2. Procesna prevara

Pre nekoliko meseci advokatska kancelarija iz Velike Britanije *Brighton$Hove Law* objavila je da je u postupku koji se vodi radi vršenja roditeljskog prava sudu kao dokaz podnet *deepfake* audio-snimak, na kome se čuje kako njihov klijent (otac dece) preti drugoj strani u sporu (majci dece) u vezi sa konkretnim sudskim postupkom.[26] Ta uznemirujuća vest nas je, iznenadno i trenutno, suočila sa svim opasnostima koje prete integritetu dokaznog postupka, koji je centralna faza svakog sudskog postupka, i sasvim nam jasno pokazala da smo kao stručna i naučna javnost nespremno dočekali razvoj veštačke inteligencije i *deepfake* tehnologije. Imajući u vidu da još uvek ne postoje softveri koji sa stoprocentnom sigurnošću mogu utvrditi da je neki materijal generisan pomoću *deepfake* tehnologije, opasnost o kojoj govorimo je dvosmerna. Prvo, postoji opasnost da fabrikovan dokaz bude prihvaćen na sudu kao autentičan i, drugo, postoji opasnost da autentičan dokaz bude odbačen kao fabrikovan.

Upotreba *deepfake* dokaza u sudskom postupku bila bi kvalifikovana kao oblik krivičnog dela procesne prevare u onim zakonodavstvima koja poznaju takvo posebno krivično delo prevare, poput krivičnog zakonodavstva Italije.[27] U našem KZ procesna prevara nije propisana kao posebno krivično delo, ali, onako kako je prevara definisana u našem KZ, ostavljena je mogućnost da to krivično delo bude učinjeno u sudskom, upravnom ili drugom postupku.[28] Neophodno je da učinilac, u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist, kreira *deepfake* materijal, podnese ga sudu ili drugom organu kao dokaz i time sud ili organ postupka dovede u zabludu ili ga održava u zabludi[29] te ga navede da donese odluku zbog koje za neko lice nastupi imovinska šteta.

U članu 334 našeg KZ propisano je krivično delo lažnog prijavljivanja, čija bi primena takođe došla u obzir ukoliko bi se u krivičnom postupku na jedan specifičan način iskoristili *deepfake* dokazi. Naime, teži oblik tog krivičnog dela čini onaj ko podmetanjem tragova krivičnog dela ili na drugi način izazove pokretanje krivičnog postupka zbog krivičnog dela za koje se goni po službenoj dužnosti protiv

26 Doctored audio evidence used to damn father in custody battle. https://brightonandhovelaw.co.uk/the-dangers-of-doctored-deep-fake-evidence-that-is-being-submitted-to-courts/, 13. septembar 2024.

27 Z. Stojanović (2021), str. 706.

28 *Ibidem.*

29 U zabludu se, po prirodi stvari, ne može dovesti ili održavati sud ili drugi organ već se u zabludu dovodi ili se u zabludi održava fizičko lice koje u konkretnom slučaju istupa u ime suda ili drugog nadležnog organa.

lica za koje zna da nije učinilac tog krivičnog dela. Ukoliko bi, na osnovu i zbog *deepfake* dokaza bio pokrenut krivični postupak zbog krivičnog dela za koje se goni po službenoj dužnosti, protiv lica na koje se odnosi kreirani *deepfake* sadržaj, moglo bi postojati krivično delo iz člana 334 stav 2 KZ. Podrazumeva se da izvršilac krivičnog dela (lice koje kreira *deepfake* dokaz i na određeni način ga učini dostupnim organima krivičnog gonjenja) zna da lice na koje *deepfake* dokaz ukazuje nije učinilac.

Posebnu dilemu u tom kontekstu otvara pitanje odbrane u krivičnom postupku. Naime, osnovno pravo okrivljenog je da se brani na način koji smatra najboljim i najdelotvornijim, što mu praktično daje pravo da se brani i lažima. Advokati, s druge strane, imaju dužnost da pravnu pomoć pruže stručno i savesno, u skladu sa zakonom, statutom advokatske komore i kodeksom.[30] Advokati, dakle, imaju profesionalnu dužnost da sudu podnose isključivo autentične dokaze. Istovremeno, oni su dužni da u pružanju pravne pomoći prioritet daju zaštiti interesa klijenta te da sudu predstave njegovu verziju događaja. Poznato je da ta verzija događaja nije uvek ona verzija koju u presudi utvrdi sud. Jasno je, stoga, da nije jednostavno odgovoriti u kojoj meri se advokat u zastupanju može služiti argumentima za koje se u kasnijem toku postupka ispostavi da su netačni. Posebno se postavlja pitanje da li je advokat dužan da proverava autentičnost dokaza koje mu dostavlja klijent. U razmatranju tog pitanja treba imati u vidu da bi nametanje takve obaveze advokatima podrazumevalo dodatna ulaganja u infrastrukturu advokatskih kancelarija kako bi se stvorili neophodni materijalni i ljudski resursi koji bi takvo postupanje advokata omogućili, što bi višestruko podiglo cenu pružanja pravne pomoći građanima kojima je ta pomoć neophodna.[31]

O procesnopravnim aspektima *deepfake* sadržaja govorilo se na zasedanju Savetodavnog komiteta o Pravilima dokazivanja u SAD u aprilu 2024. godine. Savetodavni komitet je, uzimajući u obzir kompleksnost i izazove koje donose dokazi koje je generisala veštačka inteligencija, zaključio da je neophodno formulisati nova dokazna pravila, koja bi posebnu pažnju posvetila novom fenomenu *deepfake* sadržaja.[32] Prema predloženom pravilu, ako strana koja osporava autentičnost kompjuterski generisanog ili nekog drugog dokaza dokaže sudu da je veća verovatnoća da je on fabrikovan ili izmenjen, u celini ili delimično, nego da je dokaz autentičan, takav dokaz će biti prihvatljiv jedino ako predlagač uveri sud da njegova dokazna vrednost prevazilazi štetan uticaj tog dokaza na stranu koja ga osporava.[33] Navedeni predlog uvodi dvostepenost pri odlučivanju o prihvatljivosti kompjuterski generisanog ili drugog elektronskog dokaza čija se autentičnost osporava. Naime, neuspeh strane koja osporava autentičnost dokaza da dokaže da je veća verovatnoća da je taj dokaz u celini ili delimično fabrikovan nego da je autentičan ne čini taj dokaz po automatizmu prihvatljivim za sud. Naprotiv, u tom slučaju dokaz će biti prihvatljiv tek ukoliko

30 Zakon o advokaturi, *Službeni glasnik RS* 31/11 i 24/12.

31 B. van der Sloot *et al*., p. 13.

32 U tom predlogu se ne koristi termin *deepfake* dokaz već se dokazi opisuju kao kompjuterski generisani (što obuhvata i dokaze generisane veštačkom inteligencijom) ili kao elektronski dokazi koji obuhvataju druge oblike elektronskih dokaza, koje ne mora generisati veštačka inteligencija. Vid. Advisory Commitee on evidence rules, p. 20

33 Advisory Commitee on Evidence Rules, p. 18.

strana koja dokaz predlaže uveri sud da je njegova dokazna vrednost veća od štetnog uticaja tog dokaza na stranu koja ga osporava.[34] Takođe, s obzirom na opasnosti koje sobom nosi *deepfake*, Savetodavni komitet je izneo mišljenje da bi o autentičnosti kompjuterski generisanih dokaza morao da odlučuje sud a ne porota.[35]

Iako delotvornost i adekvatnost predloženog rešenja mogu biti predmet debate, taj predlog je izuzetno značajan budući da je to jedan od prvih pokušaja da se u procesnom zakonu definišu odgovarajuća pravila kojima bi se regulisalo postupanje suda u slučaju sumnje u autentičnost dokaznog materijala koji je generisala veštačka inteligencija. Ipak, treba pomenuti da predložene dopune još uvek nisu usvojene i konačne te da, imajući u vidu trajanje i složenost zakonodavne procedure, postoji opasnost da će bilo koji amandman koji se odnosi na veštačku inteligenciju biti zastareo i prevaziđen kada stupi na snagu.[36]

3.1.3. Deepfake pornografija

Ako *deepfake* definišemo kao neautentičan audio-vizuelni prikaz neke osobe generisan od softvera koji koriste veštačku inteligenciju,[37] onda nam je jasno da svaki slučaj kreiranja takvog sadržaja bez saglasnosti osobe čiji se lik, glas ili fotografija koristi predstavlja neki oblik povrede prava na poštovanje privatnosti.[38] Jasno je da se ničiji privatni život ne može poštovati ukoliko mu nije dat određeni stepen privatnosti, niti bilo koji pojedinac može uživati u poštovanju svog privatnog života ukoliko je on učinjen javnim na način koji taj pojedinac ne može da kontroliše.[39] Stoga neovlašćeno korišćenje nečije fotografije ili lika za kreiranje neautentičnog audio-vizuelnog sadržaja predstavlja povredu prava pojedinca na svoj vizuelni prikaz i fotografiju u svakom slučaju, a u velikom broju slučajeva i povredu prava na ugled pojedinca. Oba ta prava obuhvaćena su pravom na poštovanje privatnosti[40] koje, zajedno sa pravom pojedinca na fizički, psihički i moralni integritet i pravom na integritet i autonomiju, čini kompleksno pravo na poštovanje privatnog života.

Međutim, kada govorimo o povredi prava na poštovanje privatnosti koje je prouzrokovano kreiranjem i širenjem *deepfake* sadržaja, mi na prvom mestu govorimo o kreiranju *deepfake* pornografskog sadržaja i širenju takvog sadržaja putem interneta i društvenih mreža.

---

34 Advisory Commitee on Evidence Rules, p. 20.

35 Advisory Commitee on Evidence Rules, p. 35.

36 Advisory Commitee on Evidence Rules, p. 14.

37 Advisory Commitee on Evidence Rules, p. 30.

38 Pravo na poštovanje privatnosti je jedan od segmenata složenog i kompleksnog prava na poštovanje privatnog života, koje predstavlja jedno od osnovnih ljudskih prava i koje je kao takvo proklamovano nekim od najvažnijih međunarodnih dokumenata.

39 B. Braitwaite *et al*., eds. (2021). *Pravo na poštovanje privatnog života (član 8. EKLJP): vodič kroz konvencijsko i nacionalno pravo i praksu*, AIRE centar, Podgorica, p. 22

40 Prema stavu Evropskog suda za ljudska prava, pravo na poštovanje privatnosti obuhvata: pravo pojedinca na svoj vizuelni prikaz i fotografije, zaštitu ugleda pojedinca, zaštitu podataka, pravo na pristup ličnim informacijama, pravo na informacije o sopstvenom zdravlju, prikupljanje podataka ili dosijea od službi bezbednosti ili drugih državnih organa, policijski nadzor, ovlašćenje policije da zaustavi i pretresa, odnos advokata i klijenta i pravo na privatnost tokom lišenja slobode u pritvoru i zatvoru. Suština tih različitih elemenata prava na poštovanje privatnosti leži u zaštiti od prikupljanja i javnog širenja ličnih informacija. Više o tome B. Braitwaite *et al*.

Iako na prvi pogled deluje da bi u našem krivičnom zakonodavstvu *deepfake* pornografija mogla biti pravno kvalifikovana kao krivično delo neovlašćenog objavljivanja i prikazivanja tuđeg spisa, portreta ili snimka iz člana 145 KZ, takav zaključak nije sasvim održiv. Naime, krivično delo iz člana 145 KZ čini onaj ko objavi ili prikaže spis, portret, fotografiju, film ili fonogram ličnog karaktera bez pristanka lica koje je spis sastavilo ili na koje se spis odnosi, odnosno bez pristanka lica koje je prikazano na portretu, fotografiji ili filmu ili čiji je glas snimljen na fonogramu ili bez pristanka drugog lica čiji se pristanak po zakonu traži i time osetno zadre u lični život tog lica. Objaviti ili prikazati nešto podrazumeva da je više lica imalo mogućnost da se upozna sa onim što se objavljuje ili prikazuje, pri čemu je irelevantno da li se bilo koje lice zaista i upoznalo sa sadržajem koji se objavljuje ili prikazuje.[41]

Međutim, zakonski opis krivičnog dela iz člana 145 KZ podrazumeva postojanje autentičnog snimka, fotografije ili fonograma koji se neovlašćeno objavljuje ili prikazuje, dok je *deepfake* pornografski sadržaj neautentičan snimak koji ne samo da je objavljen bez pristanka lica na koje se snimak odnosi već je nastao i bez pristanka tog lica. Reč je, naime, o *deepfake* materijalu koji je kreiran putem društvenih medija za fabrikovanje pornografije, a koji se kasnije deli i širi na raznim pornografskim sajtovima i onlajn forumima, što izaziva ozbiljno narušavanje psihičkog zdravlja žrtve, ali može imati i šire zdravstvene, socijalne, porodične i profesionalne negativne posledice po žrtvu.[42]

Čini se da bi kreiranje i širenje *deepfake* pornografskog sadržaja bilo najispravnije pravno kvalifikovati kao krivično delo polnog uznemiravanja iz člana 182a KZ. To krivično delo čini onaj ko polno uznemirava drugo lice, pri čemu zakonodavac u stavu 3 tog člana definiše u čemu se polno uznemiravanje sastoji. Prema slovu zakona, polno uznemiravanje je svako verbalno, neverbalno ili fizičko ponašanje koje ima cilj da povredi ili predstavlja povredu dostojanstva lica u sferi polnog života, a koje izaziva strah ili stvara neprijateljsko, ponižavajuće ili uvredljivo okruženje. U nedostatku posebnog krivičnog dela koje bi eksplicitno inkriminisalo kreiranje i širenje *deepfake* pornografskog sadržaja, kao prednost su se pojavili svi pravnotehnički nedostaci na koje je sa osnovom ukazivano, a koji se u osnovi svode na primedbe da je u sadržinskom smislu gotovo nemoguće odrediti alternativno propisane radnje koje imaju značaj radnje izvršenja[43] jer upravo neodređenost radnje izvršenja omogućuje da se kreiranje i širenje *deepfake* pornografskog sadržaja podvede pod inkriminaciju iz člana 182a KZ.

Kreiranje *deepfake* pornografskog sadržaja podrazumeva fizičko ili neverbalno ponašanje koje predstavlja povredu dostojanstva lica u sferi polnog života, što je dovoljno za postojanje krivičnog dela, budući da je posledica alternativno određena, te nije neophodno da je u konkretnom slučaju nastupio strah ili da je stvoreno neprijateljsko, ponižavajuće ili uvredljivo okruženje.[44]

41 Z. Stojanović (2021), str. 542.

42 F. Romero Moreno, p. 3.

43 N. Delić (2024). *Krivično pravo – posebni deo*, Beograd, str. 128

44 N. Delić (2024).

Krivičnopravni značaj kreiranja i širenja *deepfake* pornografskog sadržaja prepoznao je hrvatski zakonodavac, koji je eksplicitno kao krivično delo propisao zloupotrebu snimka polno eksplicitne sadržine u članu 144a Kaznenog zakona.[45] To krivično delo ima dva osnovna oblika. Najpre, krivično delo čini onaj ko, zloupotrebom poverenja i bez pristanka snimane osobe, trećoj osobi učini dostupnim snimak polno eksplicitnog sadržaja koji je snimljen uz pristanak te osobe za ličnu upotrebu i na taj način povredi privatnost te osobe. Drugi osnovni oblik krivičnog dela čini onaj ko upotrebom računarskih sistema ili na drugi način izradi novi ili preinači postojeći snimak polno eksplicitnog sadržaja i taj snimak upotrebi kao pravi te time povredi privatnost osobe na tom snimku. Ukoliko je neki od osnovnih oblika krivičnog dela učinjen putem računarskog sistema ili mreže ili na drugi način, čime je snimak učinjen dostupnim većem broju osoba, postojaće teži oblik tog krivičnog dela.

U državi Njujork je u junu 2019. godine usvojen Zakon o odgovornosti u vezi sa *deepfake* materijalom (*Deepfakes Accountability Act*) koji kao krivično delo propisuje svesno propuštanje da se na video-snimku jasno označi da je snimak generisala *AI*, pri čemu je neophodno da se to propuštanje čini sa namerom da se ponizi ili na drugi način uznemirava lice koje je na sadržaju koji je generisan pomoću naprednih tehnologija lažno prikazano nago ili u seksualno eksplicitnim radnjama.[46]

3.1.4. Dečja pornografija

Pojava i razvoj *deepfake* tehnologije izazvali su ozbiljne dileme u oblasti sprečavanja i suzbijanja dečje pornografije. Pojavila su se i određena specifična pitanja koja nisu predmet debate o prethodno pomenutim krivičnim delima koja se vrše zloupotrebom *deepfake* tehnologije. Konkretno, postavlja se pitanje ima li mesta krivičnopravnoj intervenciji ukoliko se na pornografskom materijalu nalazi nepostojeće dete, odnosno dete kreirano pomoću *deepfake* tehnologije.

Jedan od najznačajnijih međunarodnopravnih dokumenata u oblasti sprečavanja i suzbijanja dečje pornografije jeste Konvencija Saveta Evrope o zaštiti dece od seksualnog iskorišćavanja i seksualnog zlostavljanja.[47] U toj konvenciji se dečja pornografija definiše kao svaki materijal koji vizuelno prikazuje dete koje se stvarno

45 Kazneni zakon Hrvatske – KZH, *Narodne novine* 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, 114/22, 114/23 i 36/24.

46 Deepfake Accountability Act. https://www.congress.gov/bill/116th-congress/house-bill/3230/text, 20. septembar 2024. godine

47 Zakon o potvrđivanju Konvencije Saveta Evrope o zaštiti dece od seksualnog iskorišćavanja i seksualnog zlostavljanja (u daljem tekstu: Konvencija), *Službeni glasnik RS – Međunarodni ugovori* 1/10. U članu 9 stav 1 pomenute Konvencije o visokotehnološkom kriminalu propisana su dela u vezi sa dečjom pornografijom, u kome obavezuje strane ugovrnice da usvoje zakonodavne i druge mere neophodne da bi se kao krivično delo u domaćem zakonodavstvu propisale sledeće radnje, kada su učinjene sa namerom i protivpravno: a) proizvodnja dečje pornografije, u svrhu njene distribucije preko računarskog sistema; b) nuđenje ili činjenje dostupnim dečje pornografije preko računarskog sistema; v) distribucija ili prenošenje dečje pornografije preko računarskog sistema; g) nabavljanje dečje pornografije preko računarskog sistema, za sebe ili za drugo lice, te d) posedovanje dečje pornografije u računarskom sistemu ili na medijumima za čuvanje računarskih podataka.

ili simulirano eksplicitno seksualno ponaša ili svaki prikaz detetovih polnih organa za prvenstveno seksualne svrhe (čl. 20 st. 2). U stavu 3 citiranog člana, Konvencija ovlašćuje države potpisnice da ne inkriminišu kao krivično delo proizvodnju i posedovanje dečje pornografije ako se proizvodnja i posedovanje odnose na materijal koji se sastoji isključivo od simuliranih predstava ili od realističnih slika nepostojećeg deteta.

Sličnu definiciju sadrži i član 9 stav 2 Konvencije o visokotehnološkom kriminalu, prema kojoj dečja pornografija obuhvata pornografski materijal koji vizuelno prikazuje: a) maloletnika koji učestvuje u eksplicitno seksualnoj radnji; b) lice koje izgleda kao maloletnik, koje učestvuje u eksplicitno seksualnoj radnji, te c) realistične slike, koje predstavljaju maloletnika koji učestvuje u eksplicitno seksualnoj radnji. U stavu 4 citiranog člana strane ugovornice su ovlašćene da, u celini ili delimično, ne primenjuju odredbu člana 9 stav 2 tačke b) i c).

Konvencija o zaštiti dece od seksualnog iskorišćavanja i seksualnog zlostavljanja predstavlja međunarodnopravni osnov krivičnog dela prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju iz člana 185 KZ.[48] U kontekstu tog krivičnog dela, predmetima pornografske sadržine nastalim iskorišćavanjem maloletnog lica (dečja pornografija) smatra se svaki materijal koji vizuelno prikazuje maloletno lice koje se bavi stvarnim ili simuliranim seksualno eksplicitnim ponašanjem i svako prikazivanje polnih organa deteta u seksualne svrhe. Kao što vidimo, naš zakonodavac je delimično iskoristio ovlašćenje iz člana 20 stav 3 Konvencije o zaštiti dece od seksualnog iskorišćavanja i seksualnog zlostavljanja i ovlašćenje iz člana 9 stav 4 Konvencije o visokotehnološkom kriminalu, te je kao krivično delo predvideo proizvodnju i posedovanje materijala koji vizuelno prikazuje maloletno lice koje se bavi simuliranim seksualno eksplicitnim ponašanjem, ali ne i proizvodnju ili posedovanje materijala koji prikazuje nepostojeće dete koje se bavi seksualno eksplicitnim ponašanjem. To znači da će, prema našem krivičnom zakonodavstvu, krivično delo iz člana 185 KZ postojati ukoliko je reč o *deepfake* pornografskom materijalu koji prikazuje realno postojeće dete, dok krivično delo neće postojati u slučaju *deepfake* pornografskog materijala koji prikazuje nepostojeće dete.

Opravdanje za takvo rešenje naslanja se na *ratio legis* krivičnog dela iz člana 185 KZ, koji se svodi na zaštitu maloletnika od određenih za njih štetnih aktivnosti ili manipulacija povezanih sa pornografijom.[49] Naime, u pornografskom materijalu u kojem se prikazuje nepostojeće dete *de facto* ne postoji dete kome bi se pružila krivičnopravna zaštita jer ne postoji ni dete koje je iskorišćeno za proizvodnju tog sadržaja.

48 Krivično delo iskorišćavanje maloletnih lica za pornografiju je u našem krivičnom zakonodavstvu prvi put propisano 2003. godine. To krivično delo je u KZ iz 2006. godine propisano pod nazivom prikazivanje pornografskog materijala i iskorišćavanje dece za pornografiju, čime je krivičnopravna zaštita pružena samo deci. Međutim, izmenama iz 2009. godine, došlo je do vraćanja na prvobitne pozicije iz 2003. godine i širenja kruga lica koja imaju svojstvo pasivnog subjekta zamenom reči „deca" rečima „maloletnog lica". Više o tome: N. Delić, str. 128.

49 M. Škulić (2022). Krivičnopravna reakcija na dečiju pornografiju/pornografiju maloletnih lica – plasiranu/nastalu zloupotrebom računarske mreže/komunikacije drugim tehničkim sredstvima. *RKKP* 2, str. 24.

Pitanje kažnjivosti kompjuterski generisane dečje pornografije se postavilo i u SAD još 1996. godine kada je donet Zakon o prevenciji dečje pornografije (*Child Pornography Prevention Act*).[50] Tim zakonom nisu inkriminisane samo pornografske predstave stvarno postojeće dece već i kompjuterski generisane fotografije ili slike iz kojih proizilazi da je maloletno lice uključeno u seksualno eksplicitno ponašanje.[51] Te odredbe zakona su osporavane pred Vrhovnim sudom SAD u poznatom slučaju *Achcroft v. Free Speach Coalition* kao neustavne, odnosno kao protivne Prvom amandmanu na Ustav SAD o slobodi govora. Vrhovni sud SAD je 2002. godine doneo presudu u kojoj je utvrdio da su odredbe Zakona o prevenciji dečje pornografije koje se odnose na inkriminisanje simulirane dečje pornografije protivne Prvom amandmanu na Ustav SAD i posebno naglasio da u situaciji kada se deca simuliraju u scenama dečje pornografije praktično ne nastaje „žrtva" takve pornografije jer njeni akteri nisu stvarno postojeća deca.[52] *Deepfake* dečja pornografija koja prikazuje nepostojeću decu u seksualno eksplicitnom ponašanju zapravo potpada pod tu odluku Vrhovnog suda SAD iz 2002. godine jer *deepfake* dečja pornografija koja prikazuje nepostojeće dete nije nastala seksualnim zlostavljanjem i iskorišćavanjem dece, odnosno ne postoji žrtva takve pornografije.[53]

Međutim, naše je mišljenje da takvo rezonovanje može biti predmet debate. Naime, ako iz prakse znamo da se proizvodnja i posedovanje dečje pornografije javlja kao prethodni stadijum u izvršenju nekih teških krivičnih dela protiv polne slobode dece te ukoliko smo posedovanje dečje pornografije inkriminisali jer se i samo držanje predmeta dečje pornografije načelno smatra opasnim i društveno štetnim,[54] opravdano je preispitati postojeće rešenje. Inkriminisanjem proizvodnje i posedovanja pornografskog materijala na kojem se prikazuje nepostojeće dete, iako ne postoji konkretna žrtva te pornografije, pružila bi se krivičnopravna zaštita deci kao posebno osetljivoj kategoriji, s jedne strane, dok bi se istovremeno jačala svest o nedopuštenosti proizvodnje i posedovanja materijala dečje pornografije, bez obzira na to da li se materijal odnosi na postojeće ili realno prikazano nepostojeće dete.

Na tim pozicijama stoji KZH, koji u članu 164 stav 6 pornografsku predstavu definiše kao prikazivanje uživo ili putem komunikacionih sredstava pravog deteta ili realno prikazanog nepostojećeg deteta ili osobe koja izgleda kao dete u pravom ili simuliranom polno eksplicitnom ponašanju ili polnih organa pravog deteta, realno prikazanog nepostojećeg deteta ili osobe koja izgleda kao dete, u polne svrhe.

---

50 Child Pornography Prevention Act. https://www.congress.gov/bill/104th-congress/house-bill/4123, 18. septembar 2024.

51 R. Spivak (2019). „Deepfakes": The Newest Way to Commit One of the Oldest Crimes. *Georgetown Law Technology review* 3.2, p. 362

52 M. Škulić (2022), str. 48.

53 R. Spivak, str. 363.

54 M. Škulić (2022), str. 24.

4. ZAKLJUČAK

U digitalnoj eri, koju dominanto karakteriše sveopšta povezanost ljudi putem globalne telekomunikacione mreže kakav je internet, sve veća zavisnost stanovništva od društvenih mreža i ubrzan razvoj veštačke inteligencije, beležimo izostanak odgovarajuće pravne regulative na nacionalnom, ali i na globalnom nivou, koja bi stvorila normativni okvir adekvatan izazovima koji su pred nama. Tome svedoči činjenica da je prvi međunarodnopravni akt koji na sveobuhvatan način tretira veštačku inteligenciju usvojen tek sredinom ove godine na nivou Evropske unije (Zakon o veštačkoj inteligenciji EU). Međutim, taj akt ne sadrži krivičnopravne norme, te je u kontekstu krivičnog prava i dalje ključan međunarodnopravni dokument Konvencija Saveta Evrope o visokotehnološkom kriminalu iz 2001. godine, sa pratećim protokolima.

Sama činjenica da se u borbi protiv visokotehnološkog kriminaliteta oslanjamo na dokument iz 2001. godine deluje prilično obeshrabrujuće. U našem zakonodavstvu normativni okvir za borbu protiv visokotehnološkog kriminaliteta propisan je Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, koji ne sadrži nova materijalna krivičnopravna rešenja, u smislu propisivanja posebnih krivičnih dela visokotehnološkog kriminaliteta, već taksativno nabraja koja se sve krivična dela, propisana Krivičnim zakonikom, i pod kojim uslovima imaju smatrati krivičnim delima visokotehnološkog kriminaliteta.

Krivična dela protiv bezbednosti računarskih podataka, koja su u naše krivično zakonodavstvo prvi put uvedena Zakonom o izmenama i dopunama KZS iz 2003. godine, a kasnije preuzeta u nov KZ koji je stupio na snagu 2006. godine, gotovo do danas su ostala neizmenjena. Uprkos očiglednom razvoju i konstantnom usavršavanju informacionih tehnologija, pojavi i razvoju veštačke inteligencije i *deepfake* tehnologije i uprkos činjenici da je od stupanja na snagu KZ više puta noveliran, samo se jedna izmena odnosila na ta krivična dela, i to na krivično delo pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih sistema iz člana 304a, koje je u naše krivično zakonodavstvo uvedeno Zakonom o izmenama i dopunama KZ iz 2009. godine.

Gotovo je nemoguće logično obrazložiti da je jedna od najdinamičnijih oblasti ostala neizmenjena skoro 20 godina, dok se intervenisalo u nekim drugim oblastima koje bi se mogle opisati kao prilično statične. U tom smislu, posebno zabrinjava činjenica da se u predloženim izmenama i dopunama KZ koje su objavljene u vreme pisanja ovog rada, samo jedna izmena odnosi na krivična dela protiv bezbednosti računarskih podataka, i to ona kojom se pojam računarskog virusa menja pojmom zlonamernog računarskog programa.[55]

55 U skladu sa članom 13 Nacrta zakona o izmenama i dopunama Krivičnog zakonika, zlonamerni računarski program je program koji je napravljen sa svrhom da nanese štetu računaru, računarskoj mreži ili računarskim podacima i koji se ubacuje u računar sa namerom ugrožavanja poverljivosti, celovitosti ili dostupnosti računarskih podataka, aplikacija i operativnih sistema ili na neki drugi način ometa rad računara ili računarske mreže. Sledstveno tome, predloženo je da krivično delo iz člana 300 KZ više ne nosi naziv „pravljenje i unošenje računarskog virusa" već „pravljenje i unošenje zlonamernog računarskog programa". Vid. Nacrt zakona o izmenama i do-

Jasno je da predlagač nije prepoznao izazove veštačke inteligencije i *deepfake* tehnologije kao krivičnopravno relevantne, te će se, ukoliko zakonodavno telo bude usvojilo objavljeni Nacrt, još neko vreme na krivična dela izvršena zloupotrebom *deepfake* tehnologije primenjivati postojeća zakonska rešenja, odnosno postojeća tzv. tradicionalna krivična dela, sa svim ograničenjima i manjkavostima na koje je u ovom radu ukazano.

LITERATURA

Baron Quintero S. Ma. (2023). Los delitos realizados mediante la Dark Net. *Revista Penal Mexico* 23.

Braitwaite B. *et al*., eds. (2021). *Pravo na poštovanje privatnog života (član 8. EKLJP): vodič kroz konvencijsko i nacionalno pravo i praksu*, AIRE centar, Podgorica

Busch E., Ware J. (2023). *The Weaponisation of Deepfakes – Digital Deception by the Far-Right*, International Centre for Counter-Terrorism.

Citron D. K., Chesney R. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review* 107.

Delić N. (2024). *Krivično pravo – posebni deo*, Beograd.

Karović S., Simović M. (2022). Krivičnopravno suprotstavljanje visokotehnološkom – kompjuterskom kriminalitetu: savremeni izazovi, dileme, perspektive. *Digitalizacija u kaznenom preavu i pravosuđu* (ur. J. Kostić, M. Matić Bošković), Beograd.

Nenadić S., Miljuš I. (2022) Krivična pravda u eri veštačke inteligencije. *Digitalizacija u kaznenom pravu i pravosuđu* (ur. J. Kostić., M. Matić Bošković), Beograd.

Pechenik Gieseke A. (2020). „The New Weapon of Choice": Law's Current Inability to Properly Address Deepfake Pornography. *Vanderbilt Law Review.*

Pisarić M. (2013). Potrebni normativni odgovor na probleme otkrivanja i dokazivanja dela visokotehnološkog kriminala. *Zbornik radova Pravnog fakulteta u Novom Sadu.*

Romero Moreno F. (2024). Generative AI and deepfakes: a human rights approach to tackling harmful content. *International review of law, computers & technology*, Routledge.

Spivak R. (2019). „Deepfakes": The Newest Way to Commit One of the Oldest Crimes. *Georgetown Law Technology review* 3.2.

Stojanović Z. (2021). *Komentar krivičnog zakonika*, Službeni glasnik.

Škulić M. (2007). Uloga posebnih dokaznih radnji u suzbijanju organizovanog kriminaliteta. *Primena međunarodnog krivičnog prava*, Tara.

Škulić M. (2022). Krivičnopravna reakcija na dečju pornografiju/pornografiju maloletnih lica – plasiranu/nastalu zloupotrebom računarske mreže/komunikacije drugim tehničkim sredstvima. *RKKP* 2.

Škulić M. (2024). Dokazni značaj informacija iz komunikacije ostvarene aplikacijama/modifikovanim uređajima za kriptovanje – kao što su Sky ECC i EnchroChat. *CRIMEN – Časopis za krivične nauke* 1.

van der Sloot B. *et al.* (2021). *Summary Deepfakes: The legal challenges of a synthetic society*. Tilburg Institute for Law, Technology, and Society.

punama Krivičnog zakonika. https://www.mpravde.gov.rs/sekcija/53/radne-verzije-propisa.php, 5. oktobar 2024.

PRAVNI IZVORI

Kazneni zakon Hrvatske, *Narodne novine* 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, 114/22, 114/23 i 36/24.

Krivični zakonik, *Službeni glasnik RS* 85/05, 88/05, 107/05, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16 i 35/19.

Zakon o advokaturi, *Službeni glasnik RS* 31/11 i 24/12.

Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, *Službeni glasnik RS* 61/05, 104/09, 10/23 i 10/23 – drugi zakon.

Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu, *Sl. glasnik RS* 19/09.

Zakon o potvrđivanju Konvencije Saveta Evrope o zaštiti dece od seksualnog iskorišćavanja i seksualnog zlostavljanja, *Službeni glasnik RS – Međunarodni ugovori* 1/10.

INTERNET IZVORI

Advisory Commitee on Evidence Rules, April 19, 2024. https://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-evidence-rules-april-2024, 21. jul 2024.

Brooks T. *et al*. Increasing Threat of Deepfake Identities. *Homeland Security*. https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf, 20. avgust 2024.

Child Pornography Prevention Act. https://www.congress.gov/bill/104th-congress/house-bill/4123, 18. septembar 2024.

Deepfake Accountability Act. https://www.congress.gov/bill/116th-congress/house-bill/3230/text, 20. septembar 2024.

Doctored audio evidence used to damn father in custody battle. https://brightonandhovelaw.co.uk/the-dangers-of-doctored-deep-fake-evidence-that-is-being-submitted-to-courts/, 13. septembar 2024.

EU Atrificial Intelligence Act. https://artificialintelligenceact.eu/the-act/, 16. septembar 2024.

Facing reality? Law enforcement and challenge of deepfakes, An Observatory Report from the Europol Inovation Lab. https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes, 20. jul 2024.

Fake Obama created using AI video tool – BBC News. https://www.youtube.com/watch?v=AmUC4m6w1wo, 5. avgust 2024.

Finance worker pays out $25 million after video call with deepfake „chief financial officer". https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html, 12. avgust 2024.

How AI and deepfakes are taking romance scams to another level. https://www.thestar.com.my/tech/tech-news/2024/06/26/how-ai-and-deepfakes-are-taking-romance-scams-to-another-level, 12. avgust 2024.

Nacrt zakona o izmenama i dopunama Krivičnog zakonika. https://www.mpravde.gov.rs/sekcija/53/radne-verzije-propisa.php, 5. oktobar 2024.

Spain: Court punishes schoolboys for spreading AI deepfakes of girls. https://www.scottishlegal.com/articles/spain-court-punishes-schoolboys-for-spreading-ai-deepfakes-of-girls, 10. septembar 2024.

*Irena Čučilović**

DEEPFAKE TECHNOLOGY – CRIMINAL LAW IMPLICATIONS

SUMMARY

The accelerated development of artificial intelligence (hereinafter: AI) and advanced technologies that are based on software that uses AI, such as deepfake technology, among many others, has significant criminal law implications. It is obvious that deepfake technology very quickly became a tool for committing numerous crimes, starting from the most diverse forms of fraud and blackmail, to the creation and dissemination of pornographic content, including the child pornography. The fact is that AI and deepfake technology will only further improve in the future. It is certainly one of the most dynamic areas, which could not be concluded based on the legal regulations in that area. Namely, the first international document that comprehensively regulates AI (including the deepfakes) is the EU AI Act, adopted in July 2024, which, however, does not contain criminal law provisions. Therefore, at least when it comes to the European area, the fundamental document in combating cybercrimes remains the Convention of the Council of Europe on Cybercrime, adopted in 2001.

In the Republic of Serbia, the normative framework for combating cybercrimes is prescribed by the Law on Organization and Competence of State Agencies for Combating Cybercrime, which doesn't contain new substantive criminal law solutions, in terms of prescribing specific cybercrimes, but enumerates which crimes, prescribed by the Criminal Code (hereinafter: CC), and under what conditions should be considered cybercrimes. Criminal offenses against the security of computer data, which were first introduced into our criminal legislation by the Law of Amendments to the CC from 2003, and later adopted into the new CC from 2006, have remained almost unchanged to this day. Despite the obvious development and constant improvement of AI, advanced technologies and deepfake technology, even though the CC has been amended several times since its entry into force, only one amendment was related to these criminal offenses – namely, Law of Amendments to the CC from 2009 introduced one new criminal offense. It is impossible to logically explain why one of the most dynamic areas remained unchanged for almost 20 years, while interventions were made in some other areas that could be described as quite static.

In this sense, the author points out as a particularly worrying the fact that in the proposed amendments to the CC, that were published by the Ministry of Justice during the writing of this paper, only one amendment refers to the criminal offenses against the security of computer data, and that is one that replaces the term "computer virus" with the term "malicious computer program," while the existence and development of AI, more precisely its criminal law implications, remain outside the scope of the proposed amendments.

Key words: cybercrime, deepfake technology, deepfake fraud, deepfake pornography, deepfake child pornography

* Lawyer, irena@advokatskitim.rs