Др Наташа МРВИЋ ПЕТРОВИЋ[1]
научна саветница Института за упоредно право у Београду

ДОИ: 10.5937/bezbednost2402005P
УДК: 343.542.1:[343.63:004.738.5(100+497.11)
Оригинални научни рад
Примљен: 16. 5. 2024. године
Ревизија: 23. 5.2024. године
Датум прихватања: 14. 6. 2024. године

Кривичноправни приступ регулисању дигиталне порнографије настале употребом вештачке интелигенције (*non-consesual deepfake porn*)[2]

Апстракт: *У раду се испитују потребе и могућности примене кривичноправног механизма ради спречавања ширења лажних дигиталних порнографских садржаја насталих употребом вештачке интелигенције. Описане су криминолошке карактеристике појаве. Анализирана су законодавства Сједињених Америчких Држава, Велике Британије, Швајцарске, Русије и Кине, као и прописи Европске уније који се односе на спречавање родно заснованог насиља и одговорност за ширење лажних дигиталних информација и садржаја. Анализа домаћег Кривичног законика показала је да постоји потреба да се постојеће норме осавремене, зато што се не може пружити адекватна заштита жртвама неовлашћено сачињених и објављених снимака са експлицитном сексуалном садржином. Закључак је да је кривичноправна интервенција неопходна, зато што се израдом и дистрибуцијом лажног дигиталног садржаја повређују права личности, друштвени морал и општи интерес. Инкриминисање*

[1] Имејл: natasa.mrvicpetrovic@pravnifakultet.rs; ORCID 0000-0003-0424-0610

[2] Рад је настао у оквиру научноистраживачког рада Института за упоредно право који финансира Министарство науке, технолошког развоја и иновација Републике Србије према Уговору о реализацији и финансирању научноистраживачког рада НИО у 2024. години (ев. број: 451-03-55/200049 од 5. 2. 2024).

таквих радњи било би пре свега у интересу заштите права жртве, иако се не очекује да има већи практични значај. Забрана израде и објављивања лажних дигиталних порнографских снимака мора бити усклађена са заштитом приватности корисника дигиталних услуга и проактивним мерама за безбедност на интернету.

Кључне речи: *сексуално злостављање, насиље на женама, вештачка интелигенција, безбедност на интернету.*

Увод

Предмет рада јесте испитивање потребе и могућности кривичноправног регулисања стварања и ширења на друштвеним мрежама или дигиталним платформама лажних порнографских видео-снимака, звучних записа или фотографија применом вештачке интелигенције научене да опонаша људе (*deepfake pornography*, популарно *deepfake porn*). Дипфејк (*deepfake*) технологија дозвољава да се синтетизује одговарајућа врста дигиталног записа помоћу алгоритма који анализира велики број фотографија, видеоснимака или звучних записа доступних на интернету и повезује њихове делове у складу са постављеним циљем, чиме настаје нови медиј, велике уверљивости – прави „оригинал фалсификата" у коме се нечије лице, тело и глас замењују туђим.[3] На тај начин коришћење вештачке интелигенције погодује ширењу феномена дигиталног сексуалног злостављања – нарочито у односу на жене, које су најчешће жртве – а самим тим и провоцира потребу да се према том феномену одреди кривично право.

[3] Израз дипфејк (*deepfake*) комбинује енглеске речи „дубоко" (у смислу способности дубоког учења којим располажу напредни системи вештачке интелигенције) и „лажно". Израз се односи на све случајеве монтирања лажних аудио-визуелних дигиталних записа који се користе у медијима, као што су сензационалне лажне вести и говори политичара или других популарних личности у сврхе забаве, сатире, политике или пропаганде, укључујући ту и ширење порнографског материјала, емитовање исказа наводних жртава измишљених тешких злочина (*deep true crime*) и слично. У недостатку адекватног израза на српском језику у раду се, иако нерадо и супротно правилима нашег језика, користи израз дипфејк порнографија уместо описне фразе: дигитални порнографски садржај генерисан вештачком интелигенцијом.

Како се савремено право са закашњењем прилагођава променама друштвених односа подстакнутим технолошким напретком, било је потребно, применом упоредно-правног и правнодогматског метода, испитати да ли би и на који начин било могуће постојеће норме кривичног права применити ради спречавања наведене злоупотребе вештачке интелигенције, или би било неопходно прописати нове. Анализом су обухваћена поједина страна законодавства и домаће кривично законодавство. Полазна претпоставка јесте да кривичноправна реакција треба да буде омогућена, нарочито због потребе заштите интереса жена и малолетника као жртава лажне порнографије, али би требало водити рачуна о начелу *ultima ratio* примене заштите путем кривичног права и о бројним фактичким ограничењима због којих кривичноправне норме не би могле да се примене.

Када се говори о забрани злоупотребе дипфејк технологије, укључујући ту и ширење лажних порнографских снимака, обично се превиђа да су такве појаве неминовне због тога што се данас социјална комуникација претежно одвија онлајн, у медијском простору у коме све важнији постају постистина, симулација, хиперреалност, аватаризација и спонтано прихватање и ширење информација подражавањем онога ко је износи („мемификација") уместо истините информације и стварног стања (Bañuelos Capistránm 2020: 53). Отуда не чуди појава бројних и све доступнијих апликација, које се могу користити на тзв. паметним мобилним телефонима, а које омогућавају свакоме да створи лажне аудио-визуелне записе које ће објавити на друштвеној мрежи или платформи. Социокултурни преображај који се дешава од почетка XXI века чини илузорним очекивања да ће традиционални механизми кривичног права бити делотворни ако буду једини начин спречавања дигиталног злостављања, укључујући и злоупотребе дипфејк технологије. Баш зато би требало пажљиво испитати потребу за кривичноправном интервенцијом и одредити границе њене примене у оквиру ширег система превенције, који чине примена мера техничке заштите, заштита права интелектуалне својине на интернету, заштита приватности и права потрошача дигиталних услуга и механизми вануговорне одговорности за накнаду штете.

Лажна порнографија као вид злоупотребе дипфејк технологије

Дипфејк технологија се примењује у различитим подручјима друштвеног живота, на пример, у медијском извештавању ради популаризације медија, у политици и политичким кампањама ради утицаја на јавно мњење, у привреди (маркетинг), у сврхе забаве или уметности (приликом израде филмова или дизајнирања графике за видео-игре). За разлику од класичне фото-монтаже фотографије, злоупотребом дипфејк технологије настају лажни дигитални записи као синтетички медиј – они су редовно повезани и добро уклопљени у одговарајућу „причу" (наратив) при чему је дискурзивно измењено право значење оригиналног записа (Bañuelos Capistrán, 2020: 53). На тај начин добија се нови аудио-визуелни медиј, тј. „производ" у коме су, сходно наративу, прилагођени говор, изглед лица или покрети тела одређене особе, тако да снимак може да се представи као аутентичан, а тако и другима изгледа. Отуда не треба да чуди што се нова технологија већ користи за извршења различитих врста кривичних дела у дигиталном окружењу, на пример, тероризма, јавних клевета, превара, уцена, изнуда, угрожавања сигурности, сексуалних злостављања и узнемиравања или за ширење порнографије.

Израз дипфејк, који се данас уобичајено користи и шире означава манипулацију дигиталним аудио-визуелним снимцима, повезан је са догађајем из новембра 2017. године, када је корисник под истоименим надимком на америчком веб-форуму *Редит* (*Reditt*) поставио први у серији порнографских видео-снимака, у коме је помоћу апликације *Фејкап* (*FakeApp*) комбиновао тело неке порно-глумице са лицем израелске манекенке и глумице Гал Гадот (Gal Gadot). Том приликом је учинио доступним софтвер отвореног кода и објаснио на који је начин користио поменуту апликацију за генерисање лажног видеоснимка. Иако је на сајту убрзо забрањена таква подтема, остало је забележено да је у периоду од неколико месеци по објављивању првог лажног порно-снимка апликација *Фејкап* преузета више од 100.000 пута (Toparlak, 2023: 3). Пример илуструје мрачну страну злоупотребе дипфејк технологије, иако она може бити корисна

и у складу са етиком, употребљена у уметности или у индустрији забаве. Међутим, у постојећем културном миљеу, према владајућем моралу, није могуће поставити јасне границе између дозвољене и етички неприхватљиве употребе дипфејк технологије, што би био основни предуслов да се нормама кривичног права забране злоупотребе. Проблем је у томе што се синтетички медији генеришу из података које корисници остављају на друштвеним мрежама или на дигиталним платформама, тако да, чак и када су анонимни, могу бити лако злоупотребљени. Стога и када су препознати посебни облици криминалне злоупотребе дипфејк технологије, укључујући ту и порнографију (Europol, 2022: 10)[4], не може се очекивати да ће се на њих ефикасно реаговати у пракси.

Опасност од злоупотребе дипфејк технологије веома је велика, зато што било који дигитални отисак који корисник несвесно остави на интернету води до оригиналног садржаја, који може бити преузет и неовлашћено искоришћен за лажни снимак, при чему је корисник, као пасивни субјект, укључен у процес његовог настанка (Durães, Freitas, Novais, 2024: 351; Архипцев *и др.*, 2021: 71). Нови лажни снимак ће најчешће бити порнографског садржаја. Према извештају амстердамске компаније за сајбер безбедност из 2019. године, лажни порнографски снимци чинили су 96% укупног броја откривених злоупотреба дипфејк технологије (Ajder *et al.*, 2019: 1). Када је реч о дипфејк порнографији, искључиве жртве су жене, и то најчешће познате глумице или певачице, а ако се користи снимак особе која није позната у јавности, онда се то обично чини да би се она застрашила, понизила или уценила.

У извештају је наведен занимљив податак да се дипфејк порнографски записи најчешће налазе на посебним сајтовима који нуде искључиво такве садржаје, док их је знатно мање на обичним порно-сајтовима; разлог је зарада која се остварује од наплате рек-

[4] У извештају се посебно помиње порнографија без сагласности особе која је на снимку (*non-consensual pornography*) као један од облика криминалне злоупотребе дипфејк технологије (Europol, 2022: 10). У претходном извештају (Europol, 2020: 52) на примеру случаја из 2017. године објашњено је порекло израза дипфејк, али се порнографија посебно не помиње – очигледно је била подведена под случајеве узнемиравања. Податак може да укаже на то да је у међувремену препозната опасност дипфејк порнографије.

лама емитованих на сајту (Ajder, 2019: 6). Према томе, постоје сви предуслови за развој индустрије дипфејк порнографских снимака, која у суштини зарађује на родно заснованом насиљу.[5] Сасвим у складу са прогнозама, у најновијем истоименом извештају који обухвата период од 2019. до 2023. године констатује се да је укупни број дипфејк снимака на мрежи порастао за 550%, од чега је 98% порнографских снимака, а 99% се односи на жене. Порнографски видео-садржај на мрежама има експоненцијални раст – 2022. године откривено је 3.725, а већ 2023. године 21.019 таквих садржаја (раст од 464%) (Home Security Heroes, 2023). Подаци показују да је оправдано запитати се како искористити правне механизме ради спречавања таквих злоупотреба.

Страна правна регулатива

Употреба вештачке интелигенције захтева свеобухватну правну регулативу различитих грана права. По значају се истичу: право интелектуалне својине, право потрошача у дигиталном окружењу, грађанско и кривично право. Када је реч о злоупотреби вештачке интелигенције за израду дигиталне порнографије, као уосталом и код других облика сајбер криминалитета, велику препреку ефикасној правној заштити, нарочито кривичноправној, представљају разлике између законодавстава и територијална ограничења надлежности националних полиција и правосуђа.

Прагматичност англосаксонског правног система допринела је да се најпре у праву Сједињених Америчких Држава статутима регулишу злоупотребе дипфејк технологије. Забрањује се дистрибуција злонамерног обмањујућег дигиталног садржаја, без обзира

[5] Одличан пример представља апликација *Дипнуд* (*DeepNude*) – основна верзија је бесплатна, док се напредна плаћа. Вештачка интелигенција анализира портрет жене са одређене фотографије и лицу додаје наго тело из базе података од 10.000 фотографија нагих тела преузетих са интернета, тако да корисник „свлачи" жену са доступне фотографије за неколико секунди. Апликација уверљивије „скида" жене ако су снимљене у купаћим костимима. Није у стању да креира наге слике мушкараца.

на то да ли настаје употребом вештачке интелигенције, ако се односи на политику или на угрожавање сигурности, сексуално угрожавање или ширење порнографије у дигиталном окружењу. На савезном нивоу у Конгресу је 2017. године усвојен *ENOUGH* акт (Ending Nonconsenual Online User Graphic Harassment Act, 2017), којим се мења и допуњује одељак 88 Кривичног закона САД (18 U.S.C.). Предвиђено је да се кажњава онај ко незаконито намерно дистрибуира или прети дистрибуцијом приватних визуелних интимних приказа особе или особе која предузима сексуално експлицитне радње, при чему безобзирно занемарује приватност те особе и околност да није пристала на дистрибуцију таквих снимака или на њихово коришћење у друге сврхе. Учиниоцу могу бити изречене новчана казна или казна затвора до пет година или обе казне. Описана радња пре свега одговара тзв. осветничкој порнографији *(revenge porn)*[6], али се и порнографски дипфејк подводи под ту норму. У међувремену су предложене нове измене, али предлог закона још увек није усвојен. У недостатку адекватније правне норме, Чавки (Chawki, 2024: 7) сматра да би најпримереније било користити одредбе о забрани сајбер прогањања, ако се може доказати да је жртва (или особе из њене најближе околине) трпела озбиљан страх по властити живот и телесни интегритет и да је умишљај учиниоца био усмерен на то да је убије, повреди, узнемирава, застраши или стави под своју контролу. Тужба ради накнаде штете искључиво се користи за дипфејк видео-снимке којима се износе клеветничке тврдње на рачун политичара (Chawki, 2024: 9).

И поједине државе, као што су Флорида, Тексас, Њујорк и Вирџинија, регулишу злоупотребу дипфејк снимака. Делфино (2020: 2) наводи да су у Калифорнији донета два закона – један, којим се забрањује дистрибуција лажних медијских садржаја у току изборних кампања, и други, који прописује одговорност онога ко са умишљајем сачињава и на интернету објављује сексуално експлицитан садржај без сагласности особе која је у њему приказана,

[6] Неовлашћено објављивање нечијих приватних фотографија и видео-снимака сексуално експлицитне садржине у циљу срамоћења, понижавања те особе, или претња њиховим објављивањем, обично ради уцене жртве.

при чему се оштећенима гарантује право на накнаду за причињену штету и судске трошкове у парничном поступку.

У септембру 2023. године у Великој Британији усвојене су најновије измене и допуне Закона о безбедности на мрежи (Online Safety Bill, 2023), с циљем да се промовише приступ „нулте толеранције" ради заштите деце у дигиталном окружењу и да се проактивно спречи ширење штетног садржаја којим се врши дигитално насиље према женама, које укључује и екстремну порнографију и тзв. осветничку порнографију. Изменама Закона проширује се одговорност провајдера за дигитални садржај који објављују корисници, уз обавезу да проверава да ли је садржај настао злоупотребом интимних снимака без сагласности особе која је на снимку и да уклања такав нелегални садржај са платформи.

На тај начин се жртве родног насиља у суштини третирају као потрошачи незадовољни услугом провајдера. Нема начина да се спречи стварање лажних порнографских снимака, него се само спречава њихова неовлашћена дистрибуција. С друге стране, жртве се не суочавају са тешкоћама да се учинилац мора идентификовати како би се против њега покренуо судски поступак, да се морају доказати његов умишљај и посебна намера узнемиравања ширењем порнографског снимка без пристанка жртве. Тиме се, на први поглед, решава проблем недовољне обучености локалне полиције да идентификује учиниоце дигиталног насиља.

Међутим, проблем се на тај начин не решава, зато што постоје доступни веб-сајтови са којих се врло једноставно могу преузети алати за стварање дипфејк порнографије, а закон се не односи, на пример, на апликације попут *Дипнуда* или оне које омогућавају замену лица на порнографским фотографијама које се управо и креирају да би се могле уновчити на дигиталном тржишту. Такође, није могуће очекивати да ће велике информатичке компаније које омогућавају услугу претраживања, на пример Гугл (*Google*), техничким мерама моћи да потпуно онемогуће видљивост и доступност сајтова са дипфејк порнографским снимцима. Стога се излаз тражи у изменама Кривичног законика које су најављене средином априла 2024. године и којима ће бити прописана забрана креирања злонамерних дипфејк порнографских снимака (Conney, 2024).

У Европској унији примарни начин спречавања дипфејк информација и дигиталног садржаја јесте примена правила о заштити потрошача и одговорности провајдера који је задужен да контролише дигитални садржај, док су од споредног значаја прописи о одговорности за употребу вештачке интелигенције, због недовољног степена опасног ризика према коме се градирају обавезе онога ко употребљава и ко надзире употребу вештачке интелигенције. Од провајдера се захтева да предузме мере како би контролисао и уклањао недопуштене садржаје који се појављују на платформи, али се као најбоље решење оцењује то што корисник мора истаћи да је садржај који је сачинио вештачки креиран и означити да је то производ вештачке интелигенције, који није аутентичног порекла (Durães, Freitas, Novais, 2024: 356). Није извесно да ће такве обавезе корисника битније утицати на смањење злоупотребе, зато што корисници желе да гледају монтирани садржај са „позајмљеним" популарним ликовима, иако знају да је лажан.

Потреба за криминализацијом дипфејк порнографије препозната је у члану 7 став 2 Предлога Директиве Европског парламента и Савета о спречавању насиља над женама и насиља у породици (*COM/2022/105 final*). У финалној верзији Директиве, коју је у априлу усвојио Савет ЕУ, у члану 5 предвиђено је да државе чланице треба да пропишу као посебно кривично дело дељење интимног или изманипулисаног материјала без сагласности жртве (Directive on combating violence against women and domestic violence, 2024). У ставу 2 описане су кажњиве радње под чији *modus operandi* може да се подведе употреба вештачке интелигенције за прављење лажне порнографије. Кажњиве радње су производња, манипулација или мењање видео-слика, видео-снимака или сличног материјала на основу ког изгледа као да је особа укључена у сексуално експлицитне активности, и накнадно чињење доступним таквог садржаја, без пристанка особе на коју се односе, помоћу информационо-комуникационе технологије. Како се види, радње су кумулативно повезане – да би дело било довршено, неопходно је да је произведен лажни снимак и да је он на одговарајући начин учињен доступним другима. Међутим, кажњиво би било само ако лажни дигитални запис садржи монтажу сексуално експлицитне ак-

тивности (полне радње), иако жртва трпи штету већ самим тим што се у лажном снимку њено лице повезује са туђим голим телом. Да би дело било кажњиво, неопходно је да је извршено са умишљајем и да радњом извршења може бити нанета велика штета тој особи чији је лик искоришћен у лажном дигиталном садржају. Тај критеријум ће представљати „камен спотицања" за праксу, јер начин извршења кривичног дела редовно упућује на то да интегритет и углед жртве трпе велику штету чим се такав лажни снимак неовлашћено појави на интернету, зато што врло брзо може да се преузима или дели између корисника, док, с друге стране, постоје тешкоће идентификације учиниоца и ефикасног уклањања садржаја са мрежа.

Недопуштено генерисање и дистрибуција дигиталног порнографског садржаја у суштини увек могу бити предвиђени као нови облик постојећих кривичних дела, будући да у већини законодавстава већ постоје норме којима се забрањује приказивање, поседовање, прибављање и ширење порнографског материјала на штету младих или различити облици дигиталног насиља према женама. На пример, у руском законодавству могли би да буду прописани нови облици кривичних дела допунама постојећих одредби чланова 137 Кривичног законика РФ (нарушавање неповредивости приватног живота) и 242 КЗРФ – незаконита производња и промет порнографских материјала или предмета или њихово приказивање малолетнима (Архипцев и др., 2021: 73). Као и у сваком другом случају сајбер злостављања, оштећени је овлашћен да на основу чл. 150-152 Грађанског кодекса РФ остварује право на накнаду штете – материјалне, на пример, изгубљене зараде ако је због последица ширења лажних снимака остао без посла, или нематеријалне, због повреде права личности клеветничким поступком. Као и у законодавству Републике Србије, чланови 1073 и 1074 ГКРФ дозвољавају да се позову на материјалну одговорност законски заступници (родитељи) малолетног лица које је поступцима нанело штету другом за поступке лица под њиховим старањем. Занимљив предлог руских аутора јесте да се размотре могућности прекршајне одговорности, тим пре што је у прекршајном законодавству могуће предвидети одговорност за другог (Архипцев и др., 2021: 73). Слично решење, иначе, постоји и у прекршајном праву Републике Србије.

И у Кини су, нарочито од 2000. године, све чешће злоупотребе дипфејк технологије омогућене популарношћу комуникације на мрежама, што показује кинеска изрека да сви воле да гледају синтетичке медије, а истовремено их се плаше (de Seta, 2021: 939). Посебно је тешко одредити границе до којих се медијски атрактиван и забаван дипфејк „несташлук" може толерисати, а када синтетизовање нових слика мора да се контролише и спречава пошто залази у домен етички недопуштеног понашања. Проблем је уочен још 1994. године, када је корисник са надимком Хуанлијан Ге (Huanlian Ge) на популарној платформи за дељење видео-записа искористио технологију вештачке интелигенције како би у видеоклипу који се односио на телевизијску серију *Леїенда о херојима кондора* заменио лице главне глумице Атене Чу лицем актуелне звезде Јанг Мина, створивши врло уверљиву фото-монтажу. Тим поводом поставило се питање повреде права личности (права на лик) и спречавања злоупотребе технологије назване замена лица (хуанлијан према надимку поменутог корисника). У складу са Законом о безбедности на интернету из 2016. године (Cybersecurity Law of the P. R. China, 2016) провајдер је обавезан да контролише садржаје које објављују и размењују корисници и да уклања штетне дигиталне садржаје. У међувремену је утврђен и нацрт Грађанског законика којим се употпуњава правна заштита приватности и личних података, како би се спречило „цурење" података са дигиталних платформи, што је један од најчешћих начина на који се вештачка интелигенција „храни" када сачињава лажне видео-снимке (Yangfei, 2020). Међутим, већ у августу исте године на тржишту је постала доступна нова мобилна апликација, која корисницима омогућава да постављају сопствене фотографије, а затим да применом технологије вештачке интелигенције на тим снимцима замене своја лица лицима популарних глумаца или глумица (*ZAO* – од мандаринског направити). Кинеска државна канцеларија за информације на Интернету је 28. јануара 2022. године објавила текст будуће уредбе о управљању информационим дигиталним услугама заснованим на технологији вештачке интелигенције, којом се мењају административни прописи из 2019. године. Предвиђено је обавезно означавање дигиталног садржаја који настаје применом

вештачке интелигенције, а прописане су и друге административне и техничке мере за случај кршења забрана, у складу са надлежностима државних органа да контролишу унутрашњи интернет и дигиталне медије. (Hine, Floridi, 2022: 608).

На примерима из швајцарског права Топарлак (Toparlak, 2023) испитује да ли би традиционални механизми заштите права личности (право на слику, глас и израз, част и углед) могли делотворно да се примене за спречавање појаве дипфејк порнографије. Она констатује да постоје проблеми у примени класичних грађанских механизама судске заштите због тешкоће идентификације учиниоца и потребе да се видео-запис ефикасно уклони са мреже. С обзиром на то да су приоритетне жртве жене, она сматра да цео проблем треба посматрати из другог аспекта – као кршење аутономије воље пасивног субјекта, те ефекте лажних снимака треба посматрати у ширем контексту забране сексуалног злостављања и дигиталног насиља (Toparlak, 2023: 3). Према тези коју пласира Топарлак, облици сексуалног насиља су међусобно повезани и имају континуирани карактер, па тако и лажни порнографски садржаји генерисани од вештачке интелигенције деле основне заједничке карактеристике са другим облицима сексуалног насиља и могу у њих да прерасту. Зато би у кривичном праву требало да буде уважена чињеница да се у дигиталном окружењу бришу границе између физичког и дигиталног чина насиља, што захтева да се изједначи положај жртава у погледу доступности кривичноправне заштите (Toparlak, 2023: 11).

Потребе за изменама кривичног законодавства Републике Србије

Због тога што представљају повреде права личности и облик родно заснованог дигиталног насиља, сачињавање и ширење лажних дигиталних порнографских садржаја требало би да буду прописани као радње кривичног дела, ако се не могу подвести под постојеће законске описе појединих кривичних дела.

У Кривичном законику Републике Србије (*Службени гласник РС*, бр. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019) одвојено су прописане радње кривичних

дела неовлашћено фотографисање (члан 144) и неовлашћено објављивање и приказивање туђег списа, портрета и снимка (члан 145). Под наведене законске описе могле би се врло условно подвести радње производње и објављивања лажних дигиталних порнографских садржаја, зато што је конститутивно обележје у законским описима оба кривична дела то што су радње предузете без пристанка пасивног субјекта. Међутим, сачињавање и дистрибуција дипфејк дигиталних порнографских садржаја по правилу изазивају много теже последице по углед и интегритет жртве него што је би то било „осетно задирање у (њен) лични живот" које прати „обично" неовлашћено фотографисање или објављивање и приказивање аутентичног туђег портрета или снимка. Прво, реч је не само о неовлашћено сачињеном, него о снимку који је лажан, друго, објава снимка порнографског садржаја не може да не изазове тешке последице по интегритет и углед особе на њему приказане, поготову што употреба вештачке интелигенције обезбеђује велику уверљивост таквог снимка. Када се узме у обзир да се за кривична дела из чланова 144 став 1 и 145 став 2 кривично гоњење предузима по приватној тужби, онда се кривичноправна заштита чини сасвим илузорном. Наиме, основни проблем код оваквих кривичних дела јесте што би приватни тужилац морао да зна идентитет окривљеног и да располаже довољним доказима о извршеном кривичном делу. То је практично немогуће обезбедити приватно, без адекватне форензичке провере аутентичности дигиталног садржаја, коју могу да обављају само полицијски службеници који располажу посебним знањима и вештинама. Аутентичност дипфејк записа проверава се анализом биолошких одлика (на пример, трага се одсуством покрета трептања очију на снимку), или се употребом вештачке интелигенције упоређују просторно-временске карактеристике снимака како би се издвојила типична просторна обележја и временске секвенце (Durães, Freitas, Paulo Novais, 2024: 363). Странка не може приватно да обезбеди доступност дигиталном садржају, без услуге провајдера, који, опет, уступа такав материјал само на захтев државних органа. Све и да располаже дигиталним материјалом, странка не може ни да организује специфично вештачење у сврхе обезбеђења доказа, што је основни разлог због кога не може да покрене парницу ради на-

кнаде штете због јавне клевете, а то јесте (на папиру) један од начина на који би могла да тражи судску заштиту својих права.

Законодавац би свакако требало да употпуни и осавремени законске описе поменутих кривичних дела, чији би тежи облици могли да се односе на осветничку и дипфејк порнографију. Само у недостатку бољих решења могло би се стварање и ширење лажних порнографских садржаја сачињених помоћу вештачке интелигенције изједначити са неовлашћеним ширењем нечијих слика на мрежи (осветничка порнографија); прво, зато што мотив освете не мора да буде разлог за стварање лажних фото-монтажа, и друго, зато што је реч о потпуно лажном садржају, што још више повређује жртву и чини је немоћном да реагује, иако, генерално, свакако постоји ширење сексуално експлицитних слика без пристанка жртве, али она овде не само да није дала пристанак, него није ни била у прилици да претпостави да би такве фото-монтаже могле настати.

Упркос учесталости измена Кривичног законика РС, глава 27 – кривична дела против безбедности рачунарских података – никада није мењана. А тема овог рада директно указује на шири проблем заштите права личности у дигиталном окружењу. О неусклађености нашег кривичног права са датим степеном развоја информационо-комуникационих технологија говори податак да се ширење дигиталних порнографских садржаја електронским путем изричито помиње само у члану 185 ставу 4 КЗРС у коме је прописан посебан облик кривичног дела приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију. Алтернативно су прописане следеће радње извршења тог облика кривичног дела: прибављање за себе или другог аудиовизуелних или других предмета порнографске садржине који су настали искоришћавањем малолетног лица, поседовање таквих предмета, продаја, приказивање, излагање или чињење доступним електронски или на друге начине. С обзиром на то да се прописаним кривичним делом штите интереси малолетних лица, чини се да не би било добро да се допуном члана 185 регулишу ситуације сачињавања и објављивања дипфејк порнографских снимака или записа.

Најновији примери иновирања права Европске уније, који су мотивисани потребом да се спречи свако, па и дигитално насиље

над женама, показују да се препоручује јачање кривичноправне интервенције којом ће бити обухваћена осветничка порнографија и дипфејк порнографија. Проблем је у томе што исхитрено усвајање нових инкриминација, како показују ранији примери увођења кривичних дела сакаћења женских полних органа, прогањања, полног узнемиравања итд. у наше кривично законодавство, може да представља проблем ако се врши без промишљања, при чему се не води рачуна о међусобном односу и довољној дистинктивности кривичноправних норми (Јовановић, 2019: 183).

Закључак

На примеру злоупотребе дипфејк технологије у сврхе сачињавања порнографских дигиталних садржаја показује се да право у целини, а и кривично право, заостаје за технолошким напретком. Упркос хитној потреби да се нови феномени регулишу, право стагнира. Због правних празнина, неефикасна је правна заштита која се остварује путем механизама грађанског и кривичног права. Ситуација покушава да се реши проактивним приступом, неформално или административно, приступом који се нуди кроз право које регулише заштиту потрошача на дигиталном тржишту.

Примена вештачке интелигенције, сама по себи, вредносно је неутрална – да ли ће бити употребљена на корист или на штету људи зависи од онога ко јој даје инструкције и усмерава процесе њеног „дубоког учења". Употреба дипфејк технологије за израду и дељење порнографских садржаја на мрежама има карактеристике дигиталног насиља према женама, које је утолико опасније што нехотично остављени информатички отисак може неовлашћено, лако и брзо да се искористи. Велика је илузија да подизање степена рачунарске писмености може битније да утиче на спречавање такве појаве. Истовремено, прављење дипфејк порнографских садржаја „позајмљивањем" лица и њихово дељење на мрежама страховито угрожава достојанство, углед и интегритет особа приказаних на снимку, захтева етички прекор и јачу реакцију државе на спречавању таквих појава, јер се директно повређују не само права појединца, него и друштвени морал и општи интерес. Поред тога, без помоћи

државних органа и подршке провајдера, који се укључује тек на захтев државних органа, немогуће је открити учиниоца и обезбедити доказе о извршеној злоупотреби. Из тог разлога, за жртве је веома важно да се предвиди могућност кривичног гоњења и кажњавања учиниоца, без обзира на то што ће постојати тешкоће у практичној примени.

С друге стране, кривичноправну интервенцију чине неделотворном територијални принцип важења законодавства и постериорност заштите, тако да кривичноправна забрана дипфејк дигиталне порнографије практично неће суштински допринети спречавању појаве све док постоји доступност апликација, тражња за таквим садржајима и изгледи да се оствари приход од њихове објаве на мрежама. Међутим, појава новог облика дигиталног злостављања жена и потреба да се домаће право усклади са прихваћеним међународним документима, као што је Истамбулска конвенција, могу бити поводи да се генерално преиспитају и осавремене законски описи кривичних дела у Кривичном законику Републике Србије, како би, *ultima ratio*, могли да се примене на најопасније радње које се чине у дигиталном окружењу, односно употребом информационо-комуникационих технологија.

Промене у друштвеним односима изазване технолошким напретком захтевају да се правним правилима регулишу нови феномени и поставе границе између онога што је допуштено и онога што штети правима појединца и друштву у целини када је реч о безбедности на интернету и употреби вештачке интелигенције. Зато треба водити рачуна да се и кривичноправна реакција складно уклопи у добро осмишљен, кохерентан систем који ће, у складу са новим изазовима, захтевати промене у свим областима права.

Литература

1. Ajder, H., Patrini, G., Cavalli, F., Cullen, L. (2019). *The State of Deepfakes: Landscape, Threats, and Impact.* Amsterdam: Deeptrace. https://regmedia.co.uk/2019/10/08/deepfake_report.pdf.
2. Архипцев, И. Н., Александров, А. Н., Максименко, А. В., Озеров, К. И. (2021). Порнографический дипфейк: вымысел или

виртуальная реальность?, *Социально-политические науки*, *11*(1), 69–74. https://doi.org/10.33693/2223-0092-2021-11-1-69-74.

3. Bañuelos Capistrán, J. (2020). Deepfake: la imagen en tiempos de la posverdad, *Revista Panamericana de Comunicación*, *1*(2), 51-61. https://www.redalyc.org/articulo.oa?id=664970407007.
4. Delfino, R. A. (2019). Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act. *Fordham Law Review*, *88*(3), 887-938. https://ir.lawnet.fordham.edu/flr/vol88/iss3/2.
5. De Seta, Gabriele. (2021). Huanlian, or changing faces: Deepfakes on Chinese digital media platforms, *Convergence – International Journal of Research into New Media Technologies*, 2021, Vol. *27*(4) 935–953. https://journals.sagepub.com/doi/pdf/10.1177/13548565211030185.
6. Directive (EU) on combating violence against women and domestic violence. (2024). PE-CONS 33/24. Brussels, 25 April 2024. 2022/0066(COD). https://data.consilium.europa.eu/doc/document/PE-33-2024-INIT/en/pdf.
7. Durães, D., Freitas, P. M., Novais, P. (2024). The Relevance of Deepfakes in the Administration of Criminal Justice. In: *Multidisciplinary Perspectives on Artificial Intelligence and the Law*, (eds.) Sousa Antunes, H., Freitas, P. M., Oliveira, A. L. Martins Pereira, C., Vaz de Sequeira, E., Barreto Xavier, L. Law, Governance and Technology Series 58. Cham: Springer International Publishing, 351-369. https://doi.org/10.1007/978-3-031-41264-6_19.
8. Ending Nonconsensual Online User Graphic Harassment Act. (2017). Bill no. S. 2162(IS). November, 28, 2017. 18 U.S.C. s and Chapters 88 and 88. https://www.govinfo.gov/app/details/BILLS-115s2162is.
9. European Commission (2022). Proposal for a Directive of the European Parliament and of the Council on combating violence against women and domestic violence (COM/2022/105 final). Strasbourg, 8. 3. 2022.
10. Europol (2020). *Malicious Uses and Abuses of Artificial Intelligence.* https://www.europol.europa.eu/publications-events/publications/malicious-uses-and-abuses-of-artificial-intelligence.
11. Europol. (2022). *Facing reality? Law enforcement and the challenge of deepfakes, an observatory report from the Europol Innovation Lab*. Luxembourg: Publications Office of the European Union.

12. Jovanović, Slađana (2019). Novi pravni odgovori Republike Srbije na nasilje nad ženama, *Temida, 22*(2), 169-187. https://doi.org/10.2298/TEM1092169J.
13. *Кривични законик Републике Србије*, Службени гласник РС, бр. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019.
14. Online Safety Act (2023). 2023 Chapter 50. September 19, 2023. https://www.legislation.gov.uk/ukpga/2023/50/introduction/enacted.
15. Toparlak, R. T. (2023). Criminalising Deep Fake pornography, A gender-specific Analysis of Image-Based Sexual Abuse. *Cognitio*, (1), 1-30, https://doi.org/10.5281/zenodo.7791799.
16. Hine, E., Floridi, L. (2022). New deepfake regulations in China are a tool for social stability, but at what cost?. *Nature Machine Intelligence*, *4*(July), 608-610. https://www.nature.com/articles/s42256-022-00513-4.
17. Home Security Heroes (2023). *State of deepfakes, Realities, Threats, and Impact*. Report. https://www.homesecurityheroes.com/state-of-deepfakes/#overview-of-current-state.
18. Chawki, M. (2024). Navigating legal challenges of deepfakes in the American context: a call to action, *Cogent Engieering*, *11*(1), 1-13. https://doi.org/10.1080/23311916.2024.2320971.
19. Conney, C. (2024). Creating sexually explicit deepfakes to become a criminal offence. *BBC*, 16 April. https://www.bbc.com/news/uk-68823042.
20. Cybersecurity Law of the P.R. China, (2016). Усвојен 7. Новембра 2016, у примени од 1. јуна 2017. https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.
21. Yanfei, Z. (2020). Draft civil code emphasizes personality rights. *China Daily*, 2020-05-21, https://global.chinadaily.com.cn/a/202005/21/WS5ec5d689a310a8b241157343_2.html.

Criminal Law Approach to Regulating Non-consensual Pornographic Deepfake

Abstract: *The paper examines the needs and possibilities of applying the criminal law mechanism to prevent the deepfake pornography (digital pornographic content created by the use of artificial intelligence). The criminological characteristics of the phenomenon are described. The legislation of the United States of America, Great Britain, Switzerland, Russia and China, as well as the regulations of the European Union related to the prevention of gender-based violence and liability for the dissemination of deepfakes, was analyzed. Analysis of the Criminal Code of Republic of Serbia showed that legal reform is required because adequate legal protections cannot be provided to the victims of unauthorized publishing of deepfake pornography. The conclusion is that criminal legal intervention to the non-consensual pornographic deepfakes is necessary, because the creation and distribution of deepfake porn violates personal rights, social morals and public interest. Criminalizing such behavior would be primarily in the interest of protecting the rights of victims, although it is not expected to have a greater practical significance. Prohibition of making and online distribution of sexually explicit deepfake porn must be harmonized with the legal protection of privacy of digital services users and with proactive measures of cyber security.*

Keywords: *sexual abuse, violence against women, artificial intelligence, cyber security.*