УНИВЕРЗИТЕТ У НИШУ

ПРАВНИ ФАКУЛТЕТ

Видео снимци генерисани уз помоћ вештачке интелигенције (дипфејк) као облик сајбер криминалитета

(мастер рад)

Ментор
Проф. др Дарко Димовски

Студент
Милица Момчиловић
Број индекса: М 033/23-УП

Ниш, 2024. године

С А Д Р Ж А Ј

УВОД 1
I. ПОЈАМ И ОДЛИКЕ РАЧУНАРСКОГ КРИМИНАЛИТЕТА 3
1. Дефинисање рачунарског криминалитета 3
2. Карактеристике рачунарског криминалитета 5
3. Облици рачунарског криминалитета 8
3.1.Појавни облици рачунарског криминалитета 9
3.2.Савремени облици рачунарског криминалитета 12
II. УЛОГА ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ У САЈБЕР КРИМИНАЛУ 14
III. ПОЈАМ И ПОДЕЛА ДИПФЕЈКА 18
1. Подела дипфејка 21
1.1.Фото дипфејк 23
1.2.Аудио дипфејк 24
1.3.Видео дипфејк 26
1.4.Аудио-видео дипфејк 28
IV. ЗЛОУПОТРЕБА ДИПФЕЈК ТЕХНОЛОГИЈЕ 30
1. Лажне вести и дезинформације 30
2. Дипфејк у судским поступцима 33
3. Дипфејк у пословном окружењу 36
4. Преваре и крађе идентитета посредством дипфејка 38
5. Дипфејк порнографија 40
V.ПОЗИТИВНА ПРИМЕНА ДИПФЕЈК ТЕХНОЛОГИЈЕ 45
1. Уметност 45
2. Образовање 46
3. Медицина 47
VI. ОТКРИВАЊЕ, МОГУЋА РЕШЕЊА И БУДУЋНОСТ ДИПФЕЈКА 49
1. Детекција дипфејка 49
2. Могућа решења 51
3. Будућност дипфејка 53
VII. НОРМАТИВНО ПРАВНИ ОКВИР ДИПФЕЈК ТЕХНОЛОГИЈЕ 55
1. Међународне конвенције 55
1.1.Конвенција из Будимпеште 55
1.2.Ланзарот конвенција 57
1.3.Истанбулска конвенција 58
2. Европска Унија 59
2.1.Општа уредба о заштити података о личности (ГДПР) 59
2.2.Директива о електонској трговини (e-Commerce Directive) 61
2.3.Закон о дигиталним тржиштима и закон о дигиталним услугама 61
2.4.Закон о вештачкој интелигенцији (Artificial Intelligence Act) 63
2.5.Активности Европског Парламента 64
3. Међународне организације 66

3.1.Светска организација за интелектуалну својину ... **66**
3.2.Интерпол ... **67**
3.3.Еуропол ... **68**
VIII. НОРМАТИВНИ ОКВИР ДИПФЕЈКА У ПОЈЕДИНИМ ДРЖАВАМА ... **69**
1. САД ... **69**
2. Велика Британија ... **71**
3. Кина ... **72**
4. Тајван ... **74**
5. Јужна Кореја ... **75**
IX. НОРМАТИВНИ ОКВИР ДИПФЕЈКА У РЕПУБЛИЦИ СРБИЈИ ... **76**
1. Кривични законик ... **76**
2. Закон о ауторским и сродним правима ... **81**
3. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала ... **82**
X.НАДЛЕЖНОСТ И ПОСТУПАЊЕ ОРГАНА У ОБЛАСТИ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА, ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ И ДИПФЕЈКА И СТРАТЕШКИ ОКВИР ЗА БУДУЋНОСТ ... **83**
ЗАКЉУЧНА РАЗМАТРАЊА ... **88**
ЛИТЕРАТУРА ... **91**
САЖЕТАК И КЉУЧНЕ РЕЧИ ... **99**
SUMMARY AND KEYWORDS ... **101**
БИОГРАФИЈА ... **103**

УВОД

„Технологија је користан слуга
али опасан господар"
- Кристијан Лоус Ланге

Криминал је саставни део људског постојања. Диркем је сматрао да је криминал неизбежна појава и нормалан аспект друштвеног живота, да је неминовност у свим друштвима и да је стопа криминала чак и виша у напреднијим, индустријским друштвима[1] док је социолог Ричард Квини проучавајући везу између друштва и криминалитета дошао до закључка да је криминал друштвени феномен те да начин на који појединци и целокупна популација посматрају исти, зависи од самих друштвених норми.[2] У светлу нових технолошких достигнућа и ери Интернета, оно што је речено за традиционалне форме криминала може се, са мањим изменама рећи и за његове нове облике. Непрекидним усавршавањем нових технологија криминал је попримио и извесну дозу софистицираности, његово смањење постало је знатно отежано, а елиминација практично немогућа.

Пресудни утицај на друштво и његову еволуцију имали су технолошки проналасци, нарочито они који се односе на средства комуникације, од фонетског писма и штампарске пресе до појаве електронских медија - преобликовали су цивилизацију и људску осећајност, утицали на политику, економију, на наше способности опажања па чак и психичке одлике.

Као последицу горе наведеног размотрићемо суштинске ефекте нових технологија, њихову улогу и значај у будућности рачунарског криминалитета. Пре свега одредићемо појам рачунарског криминалитета, његову дефиницију и карактеристике, потом његове облике, појавне и савремене. Затим ћемо указати на појаву и улогу вештачке интелигенције и могућности које ствара за сајбер криминалце. Знатан део овог рада биће посвећен дипфејку (***„deepfake''***) - технологији вештачке интелигенције која је почела да се широко користи у многим индустријама.

[1] https://revisesociology.com/2016/04/03/functionalist-explanations-of-deviance/ приступљено дана 20.06.2022.године.
[2] Quinney, Richard, "Structural Characteristics, Population Areas, and Crime Rates in the United States," The Journal of Criminal Law, Criminology and Police Science, 57(1), стр. 45–52.

Сагледаћемо начине на које дипфејк може бити од користи читавом друштву, од образовања, медицине и уметности али и негативне ефекте и последице које његова употреба може изазвати, нарочито када се користи ради извршења кривичних дела. Како се сајбер криминалци али и малициозни појединци релативно брзо адаптирају новим технологијама, биће речи о употреби дипфејка у правцу креирања дезинформација и лажних вести, покушајима да се манипулише доказним материјалима у судским поступцима, његовом значају код извршења превара и крађа идентитета, злоупотреби у области пословања и на крају његова веза са појавом са којом је нераскидиво повезан – порнографијом. Овде ћемо испитати утицај који дипфејк има првенствено на жене, нарочито у ери глобалне повезаности, проблеме са којима се жртве дипфејк порнографије суочавају, етичку и нормативну перспективу овог феномена и његову повезаност са још једном нарочито опасном друштвеном појавом – осветничком порнографијом. Након тога биће речи о механизмима путем којих се дипфејк садржаји могу детектовати, (потенцијална) решења за проблеме које дипфјек може проузроковати и будућност ове технологије. На крају, бавићемо се међународном и домаћом регулативом у погледу вештачке интелигенције и дипфејка, недостацима у истој као и могућим решењима. Како вештачка интелигенција постаје све софистицираније али и доступнија просечном кориснику, сајбер криминалци и појединци са злонамерним тенденцијама имаће користи и од релативно малих помака у овој области. Из свега наведеног указује се на све већи значај и пажњу коју треба посветити овој теми.

I. ПОЈАМ И ОДЛИКЕ РАЧУНАРСКОГ КРИМИНАЛИТЕТА

1. Дефинисање рачунарског криминалитета

Рачунарски криминалитет је тешко дефинисати због његове феноменолошке разноврсности, као што је случај и са организованим криминалитетом, тероризмом и сличним појавама, превасходно јер представља новији облик криминалног деловања који се протеком времена све више усавршава и развија кроз нове методе у деловању и начину понашања (*modus operandi*).[3]

У кривичноправној литератури се за овај савремени облик криминалитета употребљавају различити термини: компјутерски криминалитет, високотехнолошки криминалитет, информатички криминалитет, сајбер криминалитет, еКриминал, кибернетички криминал док су у употреби најчешће: високотехнолошки, компјутерски, рачунарски и сајбер криминалитет.[4] У овом раду користиће се наизменично термини сајбер, рачунарски, компјутерски и високотехнолошки криминалитет.

Прва дефиниција рачунарског криминалитета настала је 1979. године, и може се наћи у Приручнику Кривичног правосуђа за компјутерски криминал Министарства правде САД-а (Criminal Justice Resource Manual on Computer Crime) где је наведено да компјутерски криминал представља сваку нелегалну радњу за чије извршење је неопходно добро познавање компјутерске технологије. Оваква дефиниција је прилично широко постављена али упркос томе одмах прихваћена, те је неколико година касније пронашла свој оквир у Студији о међународним правним аспектима компјутерског криминала из 1983. године.[5]

Данас, можемо одредити две дефиниције:

1. ширу, по којој у ову категорију спада било које кривично дело повезано са употребом или функционисањем рачунара и

[3]Лутовац, С., Рачић, Ј. (2021), Компјутерски криминал као савремени облик криминалитета. Мега, тренд ревија, 18(4), 281-292. стр. 283.
[4]Димитријевић, Предраг, Компјутерски криминал, Презентације, Правни факултет у Нишу, преузето са http://www.prafak.ni.ac.rs/files/nast_mat/Kompjuterski_kriminal.pdf приступљено дана 20.06.2022. године.
[5]The Criminal Justice Resource Manual on Computer crime, (1979), https://www.ojp.gov/pdffiles1/Digitization/118214NCJRS.pdf приступљено дана 18.07.2022 године.

2. ужу, по којој је компјутерски криминалитет посебан вид инкриминисаних понашања код којих се рачунарски систем (схваћен као јединство физичких јединица односно хардвера и програма тј. софтвера) појављује или као средство извршења или као објекат кривичног дела, и то уколико се дело на други начин или према другом објекту не би уопште могло извршити или би оно имало битно другачије карактеристике.[6]

Зато би, у светлу наведног, рачунарски криминалитет било најадекватније одредити као „облик криминалног понашања код кога се коришћење компјутерске технологије и информатичких система испољава као начин извршења кривичног дела, или се компјутер употребљава као средство или циљ извршења, чиме се остварује нека, у кривичноправном смислу релевантна последица.“[7]

Упркос различитим и широко постављеним дефиницијама, све формулације компјутерског криминалитета имају одређене заједничке елементе:

1. компјутерски криминалитет обухвата друштвено опасна понашања којима се крше правне норме и за која су прописане кривичне санкције,
2. карактерише их посебан начин и средство извршења - уз помоћ или посредством рачунара,
3. специфичан објекат заштите - рачунарски подаци, информациони систем у целини или његови делови,
4. намера учиниоца да себи или другоме обезбеди материјалну или нематеријалну корист, или да некоме нанесе штету.[8]

На крају, можемо закључити да не постоји јасна и општеприхваћена дефиниција која се усталила временом и која би обухватила све старе, нове и потенцијалне будуће врсте рачунарског криминалитета али да горенаведене интерпретације представљају добру полазну тачку.

[6]Игњатовић Ђорђе (2016): Криминологија, Правни факултет Универзитета у Београду, Београд, стр. 122.
[7]Лилић Стеван, Прља Драган (2011), Правна информатика вештина, Правни факултет Универзитета у Београду, Београд, стр. 104
[8]Константиновић Вилић, С., Николић Ристановић, В., (2018), Криминологија, Издавачко графичко предузеће, „Прометеј“, Београд, стр. 174.

2. Карактеристике рачунарског криминалитета

Прва генерација рачунарског криминалитета обухвата традиционални криминалитет, где се рачунари појављују само као оруђе, и њега називамо сајбер криминалитетом ниже класе јер би се циклус традиционалног криминалитета наставио на различите начине и када информациона технологија не би била ангажована приликом извршења кривичних дела. Друга генерација обухвата радње које се обављају путем интернета те отуда назив хибридни сајбер криминалитет (појава интернета изнедрила је нове могућности за традиционалне криминалне делатности у мери глобалних мрежа). Трећа генерација сајбер криминалитета је позната као прави сајбер криминалитет јер настаје искључиво као резултат технологије. Ова врста криминала не би уопште постојала уколико би интернет нестао (типичан пример треће генерације сајбер криминалитета су појаве попут фишинга или уцењивачког софтвера тј. ransomware-a). [9]

Међународна полицијска организација (Интерпол) је још 1982. године констатовала следеће: „Данас, у савременом свету постоји још један велики усавршени фронт који је присутан у светским размерама. Велики криминалитет и организације криминалаца се све више оријентишу ка акцијама крађи где је објекат рачунар. Електроника се злоупотребљава. Не бележи се пад класичних пљачки, али се из године у годину повећава нова врста криминалитета где се електроника користи као средство којим се криминалци служе како би се домогли милионских сума новца”.[10]

Из наведеног се закључује да је још од самог настанка овог облика криминалитета, његова основна одлика била жеља за брзим и лаким профитирањем, без улагања великих средстава приликом припремања и извршења кривичних дела, али и деловање како појединаца тако и организованих криминалних група (организоване криминалне групе имају строгу хијерархију и структуру као и начин поделе послова међу члановима, у зависности од нивоа стручности за обављање одређене врсте послова код кривичних дела ове природе). Такође, многи аутори заступају став да ова врста криминалитета спада у подврсту криминалитета белог оковратника где извршилац злоупотребљава свој

[9]Tonkolu, Demo, A.,,Investigating self efficienc of cybercrime on social media among university students“ PhD diss, Near East University, 2019. стр 30-31.
[10]Матијашевић, Ј. (2012), Високотехнолошки криминал у функцији организованог криминалитета, Организовани криминалитет, изазов 20. века, стр. 399-403.

престижни статус у друштву ради прибављања личне имовинске користи или користи за криминалну групу.

Компјутерски криминалитет има својство криминалитета транснационалног типа, са све већим интензитетом. Као такав, веома тешко се открива због лаког уништавања доказа али и отежаности идентификације места и времена извршења таквих и сличних незаконитих радњи. Оно што је од значаја за његово откривање је посебан приступ истражних органа, њихова стручност и мултидисциплинарни аспект предвидивости кривичних дела којим се он може остварити. Поред изузетних специјалистичких знања истражних органа у области информационих технологија, неопходна је и сарадња на међународном нивоу и повезаност истих у превенцији ове специфичне криминалне активности. Вршењем ових кривичних дела тежи се остварењу различитих циљева, од профита и наношења штете другоме до постизања осећаја "задовољства" упадањем у обезбеђени рачунарски систем до стварања друштвених нереда.

Једна од карактеристика рачунарског криминалитета је и високи степен анонимности што је управо и један од фактора који му даје карактеристичан облик. Иако анонимност на интернету може имати предности нпр. у диктаторским режимима који традиционално желе да остваре контролу над својим грађанима цензуром и надзором, сајбер криминалцима са друге стране, пружа одличан мотив јер на тај начин, из било ког дела света могу вршити најразноврснија кривична дела, а све што им је за потребно је – рачунар. Због природе овог феномена тешко је прикупити доказе јер сајбер криминалци често делују у више земаља што отежава проналажење њихове локације и утврђивање њихове одговорности.

Како се сајбер криминалитет ширио, тако се развијао и професионални екосистем који подржава појединце и групе које желе да профитирају од сајбер криминалних активности. Овај облик криминалитета има и високу тамну бројку (која се према неким проценама креће од 90% до 99%)[11] односно висок степен неоткривених и неевидентираних кривичних дела и починилаца истих, првенствено због компликоване технологије која отежава откривање и доказивање кривичних дела, неоспособљености истражитеља али и због тога што жртве не воде рачуна о мерама осигурања и заштите,

[11]Димовски, Д. (2019), Компјутерски криминалитет, Правни факултет Универзитета у Нишу, Зборник, LV, стр. 195-212., стр. 209-210, стр. 207.

те се већина не осећа угроженим услед ових радњи.[12]

Растућа зависност од дигиталних система - повећана током пандемије вируса „КОВИД-19" довела је до промена у готово свим сферама друштва. Индустрије су доживеле бржу дигитализацију, радници су прешли на рад од куће у областима које такав рад дозвољавају, а платформе и уређаји који олакшавају овај прелазак су се умножиле. Истовремено, претње у сфери сајбер безбедности су порасле више него икад. Само у току 2020. године, напади малвера и рансомвера порасли су за 358% и 435% па државе и истражни органи нису били у стању да адекватно реагују на ове опасности. Са једне стране, сајбер криминалци су кроз своје активности почели да користе методе напада које су све агресивније док је са друге, хронични недостатак професионалаца за сајбер безбедност довео до повећања ризика за све кориснике интернета.[13]

Савременији сајбер алати такође су омогућили криминалцима да ефикасније нападају мете по свом избору, чиме је створена могућност за извршење више циљаних напада који могу довести до још веће финансијске, друштвене и репутационе штете у будућности, док је све софистицираније употреба шпијунских технологија, на пример, омогућила циљане нападе на новинаре и активисте за људска права широм света. Криминалци усавршавањем технологија могу приступити „квалитетнијим'' и осетљивијим информацијама, док им технологије које користе вештачку интелигенцију и дубоко учење, попут дипфејка омогућавају да побољшају своје технике у креирању друштвеног инжењеринга, крађи идентитета, ширењу дезинформација и лажних вести - посебно у времену велике друштвене нестабилности.[14]

[12]Константиновић Вилић, С., Николић Ристановић, В., (2018), Криминологија, Издавачко графичко предузеће, „Прометеј“, Београд, стр. 174.
[13]The Global Risks Report 2022, 17th Edition, World economic forum, стр. 9, https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf приступљено дана 17.12.2022.
[14]Ibid.

3. Облици рачунарског криминалитета

Једна од првих подела у литератури јесте она која рачунарски криминалитет дели на:

1. ,,Злочине против машине'' које такође називамо кривичним делима против рачунарског интегритета (компјутерско хаковање, ДоС и ДДоС напади, рачунарска шпијунажа, рачунарски вируси),
2. Дела где се рачунар користи као средство извршења (пиратерија, превара и сл.),
3. злочине ,,у машини" где се злоупотребљава одређени садржај или материјал (порнографија, он-лајн узнемиравање и сл. појаве)[15]

Са извесним изменама ову класификацију је 2013. године преузела и Европска Комисија која наводи да постоје:

1. деликти који су својствени рачунарима и информационим системима попут малвера и поменутих ДоС напада,
2. традиционални деликти попут преваре, фалсификовања и крађе идентитета који се извршавају посредством рачунара и
3. деликти који су повезани са садржајем попут навођења на расну мржњу.[16]

Из наведеног се може закључити да термин ,,рачунарски криминалитет" описује веома широку категорију криминогеног понашања. Неке од ових активности исте су као и кривична дела која се не односе на рачунар, као што су крађа или превара, осим што се за њихово извршење користи рачунар. Други, попут хаковања, су јединствено и нераскидиво повезани са рачунарима. Додатно, потребно је сагледати и основна обележја која ову врсту криминалитета чине специфичном али која га и разликују од других типова криминалитета. На крају, традиционална кривична дела се можда неће увек процесуирати адекватно пре свега због недостатка доказа или недостатка посебних одредби у случају транснационалног криминала док се кривична дела повезана са рачунаром ретко процесуирају због потешкоћа повезаних са самом природом интернета и електронских

[15]Wall, D.,,What are Cybercrimes, The centre for crime and justice studies'', no. 58. Winter 2004/05, стр. 20-21, стр. 20.
[16]Phillips, Kirsty, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele, and Mary P. Aiken. 2022. "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies" Forensic Sciences 2, no. 2: 379-398. стр. 384-385.

доказа који захтевају непосредан приступ подацима, те сарадњу између органа за спровођење закона и провајдера. Због тога је приступ електронским доказима - у вези са сајбер криминалитетом али и другим врстама кривичних дела од суштинског значаја за органе кривичног правосуђа.[17]

3.1. Појавни облици рачунарског криминалитета

Као најчешће појавне облике рачунарског криминалитета издвајамо:

Компјутерске крађе јављају се као један од најчешћих облика компјутерског криминалитета и могу се реализовати на два начина. Први начин подразумева физички улазак у просторије у којима се налази рачунарска опрема и њено одношење из истих, док се други односи на ,,упад'' у рачунарски систем и противправно присвајање разних информација попут личних података, лозинки и др. Пораст ове врсте рачунарског криминалитета везује се за пораст електронске трговине.[18] Као најопаснији вид компјутерске крађе издваја се крађа идентитета која представља својеврсни облик хаковања где починилац приступа осетљивим информацијама жртве попут ЈМБГ-а, информација о банковном рачуну или броју платних картица, док се као подоблик крађе идентитета јавља синтетичка крађа идентитета[19] односно крађа личних података који се могу приписати различитим особама, а који се потом комбинују како би се направио потпуно нови лажни идентитет.

Компјутерске преваре се врше са циљем прибављања противправне имовинске користи за себе или другог или у циљу наношења штете другоме. Могу се извршити на различите начине, уношењем нетачних података или пропуштањем да се унесу тачни подаци. Сматра се да је овај облик рачунарског криминалитета међу најраширенијим и да је по својој природи најближи привредном криминалитету. Адаптацију криминалаца на

[17]Kleijssen, Jan & Perri, Pierluigi. (2017). Cybercrime, Evidence and Territoriality: Issues and Options. 10.1007/978-94-6265-207-1_7, https://rm.coe.int/cybercrime-evidence-and-territoriality-issues-and-options/168077fa98, стр. 149.
[18]Константиновић Вилић, С., Николић Ристановић, В., (2018), Криминологија, Издавачко графичко предузеће, „Прометеј“, Београд, стр. 175.
[19] https://www.mcafee.com/learn/5-common-types-of-identity-theft/ приступљено дана 29.08.2022.

нове технологије уочавамо на примеру „Нигеријске преваре 419" која је њен најпознатији облик и која циркулише још од давне 1588. године када је била позната под називом "шпански затвореник" те представља њену модерну верзију која захтева рачунар. Врши се слањем лажних порука жртви, најчешће путем електронске поште, о наводном добитку на игри за срећу, различитим пословним понудама или наследству непознатих и преминулих рођака. Како би превара била успешна, од жртве се захтева да унапред уплати одређену суму новца као би након уплате добила првобитно обећану награду.

Неовлашћено прибављање информација уз помоћ компјутера обухвата компјутерско хаковање и компјутерско прислушкивање. Основно обележје компјутерског хаковања је нарушавање система заштите и неовлашћени упад у туђе информационе системе, што је у класичном смислу еквивалентно насилном упаду у туђи објекат.[20] Међутим, не односе се све врсте хаковања на недозвољена дела. Неке организације и компаније изводе тзв. „етичко хаковање" на сопственим системима или са дозволом да истражују системе других у потрази за рањивостима. Ово се третира другачије од злонамерног хаковања тј. чина уласка у нечији рачунар без његовог знања и пристанка како би се узео неки податак или оставио вирус. Компјутерско прислушкивање постоји када се тајно, уз помоћ техничке опреме, снима и прати садржај нечијег компјутерског монитора или се прикључивањем на тај монитор обезбеђује контрола и праћење садржаја који се на њему емитују[21] Овде је значајно поменути и специфични софтвер „keylogger" који има способност да бележи све што се откуца на тастатури и да наведени садржај чува у лог фајлу који је најчешће криптован. Употреба овог софтвера може бити легитимна и малициозна. Могу га користити родитељи како би пратили онлајн активности своје деце, послодавци да прате активности запослених, односно да ли запослени користе службене уређаје у пословне сврхе (изузетно је дискутабилно да ли је овакво коришћење легално јер се нарушава приватност запосленог) или органи реда за анализу и праћење инцидената повезаних са употребом рачунара. На крају, могу га користити и злонамерни појединци ради крађе корисничких имена, лозинки, информација са платних картица и других приватних информација или уопште за нелегално праћење активности корисника [22]

[20]Петровић С. оп.цит. стр. 178
[21]Константиновић Вилић, С., Николић Ристановић, В., (2018), Криминологија, Издавачко графичко предузеће, „Прометеј", Београд, стр. 176
[22] https://www.it-klinika.rs/blog/sta-je-keylogger приступљено дана 06.07.2022. године

Уцењивачки софтвер (ransomware) је врста малициозног софтвера који ограничава приступ рачунарском систему или похрањеним подацима и тражи откупнину од жртве. Њега криминалци користе као дигитални механизам за изнуду (где наплаћују садржај који су претходно кориснику закључали на рачунару) будући да овај софтвер блокира рачунарски систем жртве док откуп не буде плаћен.[23] „Ransomware" је често дизајниран да се шири по мрежи и таргетира базе података и сервере датотека па тако може брзо парализовати и читаву компанију. Ради се о растућој претњи која доводи до тога да се сајбер криминалцима исплаћују огромне суме новца, а компанијама, владиним установама и другим субјектима наноси значајна штета.[24] Током 2020. године забележен је пораст уцењивачког софтвера од чак 435% првенствено стварањем и усавршавањем софтвера на бази вештачке интелигенције који је омогућио да овакве нападе изводе чак и криминалци који немају потребна информатичка знања и способности. Савремени начини трансфера средстава попут крипто валута одиграли су велику улогу и омогућили криминалцима да дођу до новчаних средстава уз готово занемарљив ризик по свој идентитет, без предострожности и провера које захтева рецимо класично банкарство.[25]

Рачунарска саботажа је кривично дело које чини лице које унесе, уништи, избрише, оштети, измени, прикрије или на други начин учини неупотребљивим рачунарски податак или програм или оштети рачунар или други уређај за електронску обраду и пренос података са намером да онемогући или знатно омете поступак електронске обраде и преноса података који су од значаја за државне органе, јавне службе, установе, предузећа или друге субјекте.[26] Рачунарска саботажа има два облика: физички и логички. Физичка саботажа се огледа у физичком оштећењу или уништењу рачунара и других уређаја за обраду података, док се логичка састоји у брисању, модификацији и спречавању коришћења информација садржаних у меморији информатичких уређаја.[27]

Компјутерски тероризам се дефинише као акт уништавања или ометања

[23]https://smartlife.mondo.rs/tech/uredjaji/a17963/Sajber-napad-Kako-otkljucati-zakljucane-fajlove-Sta-je-ransomware-napad-Sajber-napadi-u-Srbiji.html приступљено дана 07.07.2022. године.
[24]https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf, стр. 11 приступљено дана 10.07.2022- године.
[25]The Global Risks Report 2022 17th Edition, world economic forum, The Global Risks Report 2022 стр. 47, https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf приступљено дана 17.12.2022.
[26]Члан 299. Кривичног законика, Сл. гласник РС, бр. 85/2005, 88/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 и 94/2016.
[27]Димовски, Д. (2019), Компјутерски криминалитет, Правни факултет Универзитета у Нишу, Зборник, LV, стр. 195-212., стр. 201.

рачунарских система у циљу дестабилизације једне државе или вршење притисака на њену владу[28] и обухвата све намерно предузете и политички мотивисане нападе на рачунарске информације, рачунарске системе и мреже са циљем стварања опасности за живот или здравље људи, угрожавање јавне безбедности, застрашивање, изазивање немира или војних конфликата.[29] За разлику од других форми тероризма, компјутерски тероризам је поуздан, ефикасан, изузетно профитабилан и веома тежак за спречавање. Због тога што постоји низак ризик хватања починилаца, могућност изазивања велике штете без губитка живота (својствено традиционалном тероризму) и лака могућност врбовања, овај облик тероризма је атрактиван за ектремне појединце и терористичке организације. Откривање извршилаца је нарочито тешко због високог степена дигиталне анонимности па је готово немогуће утврдити да ли је теророристички напад изведен од стране непријатељски настројене државе, неке терористичке организације или појединца[30]

3.2. Савремени облици рачунарског криминалитета

Пиратерија (софтвера) је неовлашћено коришћење, копирање или дистрибуирање материјала заштићеног ауторским правима, без дозволе првобитног власника. У многим јурисдикцијама, само дељење материјала сматра се незаконитим, док примање не мора бити противзаконито. Међутим, у стварности многи „peer-to-peer (p2p)“[31] системи захтевају од корисника да деле материјал са другима за време његовог преузимања, што евенуално може резултирати обликом колаборативне пиратерије. Губици нанети овом нелегалном активношћу су огромни. Истраживање Привредне коморе САД-а показало је да је америчка економија само у 2019. години, као директну последницу пиратерије имала губитке од 29.2 милијарди долара.[32] те да у пиратерији преовлађују „peer-to-peer file sharing“ софтвери као што је „BitTorrent“ са уделом од чак 80%.

[28]Galley, P. (1996) Computer terrorism:What are the risks? Science, Tehnology and Society, Swiss Federal Institute of Tehnology.
[29]Константиновић Вилић, С., Николић Ристановић, В., (2018), Криминологија, Издавачко графичко предузеће, „Прометеј“, Београд, стр. 176.
[30]Петровић Р. Слободан, „Кибер - тероризам – Реалност или фикција“ часопис „Безбедност“ 2000. Вол. 42, бр. 5-6, стр. 643-675. стр. 665.
[31]Систем комуникација путем интернета који се користи за дељење датотека.
[32]Blackburn, D., Eisenach, J., Harrison, D., (2019), Impacts of digital video piracy on the U.S. economy, стр.1.

Сајбер прогањање односи се на поступке којима појединац, група или организација користећи информационо-комуникационе технологије узнемирава једну особу или више појединаца. Оваква понашања укључују претње и лажне оптужбе, крађу идентитета, крађу или уништавање података, електронско праћење и надгледање, намамљивање малолетника у сврху сексуалне експлоатације и сличне активности. Под узнемиравајућим поступцима подразумевамо оне поступке који би и код друге особе у идентичној ситуацији изазвали разуман страх.[33] Уобичајено је да починилац има контакт у стварном свету са жртвом али користи интернет како би је прогањао уместо да то чини у физичком смислу. Иако су прогањање и сајбер прогањање неминовно повезани, термини нису синоними и не треба их третирати као такве. Сајбер прогањање представља нови облик девијантног понашања који се може разликовати од ,,офлајн прогањања" по мотивацији починиоца, територији (починиоци коришћењем интернета нису географски ограничени па могу прогањати жртву која живи и на другом делу света) као и чињеници да услед распрострањености интернета починиоци имају приступ жртвама са којима чак нису ни имали претходни контакт или познанство.[34] Жртва сајбер прогањања изложена је великом броју онлајн порука, било путем друштвених мрежа, мејлова или апликација за комуникацију.[35]

Дечја порнографија/злостављање - педофили су временом увидели потенцијал нових технологија у производњи и дистрибуцији дечје порнографије. Још 1986. године „Комисија за порнографију" америчког државног тужиоца приметила је да педофили користе рачунарске мреже како би успоставили контакт и разменили различите информације између себе због чега је препоручено доношење посебног закона који би забранио такве активности.[36] За разлику од класичних случајева сексуалног експлоатисања деце, овај вид сајбер криминалитета састоји се у злоупотреби односно искоришћавању рачунара и рачунарских мрежа ради производње, продаје, размене,

[33]Bocij, P., Griffiths, M.D. & McFarlane, L. (2002). Cyberstalking: A new challenge for criminal law, стр. 12.
[34]Bocij, Paul & McFarlane, Leroy. (2003). Cyberstalking: The Technology of Hate. The Police Journal. 76. 204-221., стр. 21-22.
[35]Интересантан је пример америкаца Дезмонда Синга који је користио преко стотину профила на друштвеним мрежама, као и различите бројеве телефона и друге облике комуникације како би слао поруке жртви у виду претњи смрћу, наношења телесних повреда, расних увреда и др. Прогонитељ је такође правио и лажне профиле на друштвеним мрежама, узимајући идентитет жртве, на којима је објављивао њене личне податке попут броја телефона, датума рођења, назива школе коју је похађала и сл. Сајбер прогањање жртве почело је када јој је починилац упутио поруку на једној друштвеној мрежи у којој је исказао романтично интересовање након чега га је жртва замолила да је више не контактира.
[36]Clough, J., Principles of Cybercrime (2015), Cambridge University Press, стр. 289 – 374.

поседовања или дистрибуирања порнографског материјала у којима су главни учесници малолетници и деца. Под окриљем Савета Европе донета је и Конвенције о заштити деце од сексуалне експлоатације и злостављања која је допринела ефикасности у кривичним поступцима у којима се деца јављају као жртве сексуалне експлоатације и злостављања и коју је Република Србија ратификовала 2010. године.[37]

Дипфејк (deepfake) је врста синтетичког медија који се први пут појављује током деведесетих година прошлог века. Данас, поткрепљен усавршеним софтверима и алатима вештачке интелигенције остварује свој пун потенцијал. Првобитно замишљена као технологија која би се користила у области дигиталне уметности, сајбер криминалцима је послужила као плодно тле за извршење кривичних дела код којих је идентитет једне особе од значаја. Криминалци посредством алата вештачке интелигенције, заменом лица и представљајући се као неко други, извршавају најразноврснија кривична дела попут преваре, уцене или крађе личних података. Користи се и за низ друштвено штетних појава попут осветничке порнографије, друштвеног инжењеринга или ширења лажних вести.

II. УЛОГА ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ У САЈБЕР КРИМИНАЛУ

„Предлажемо да се у периоду од два месеца и тимом од десет људи, током лета 1956. године, одржи студија о вештачкој интелигенцији, на Дартмут колеџу, у Хановеру, држави Њу Хемпшир. Студија треба да се настави на основу претпоставке да се сваки аспект учења или било која друга карактеристика интелигенције може у принципу тако прецизно описати да се може направити машина која ће све то симулирати. Покушаћемо да пронађемо начин на који би машине научиле да користе језик, формирају апстракције и концепте, решавају врсте проблема које су за сада резервисане само за људе и на крају – побољшају саме себе“.[38]

Од 1956. године и пројекта Дартмут, који се често наводи као покретачки догађај у

[37]У Србији од 2010. године траје полицијска акција под називом „Армагедон“ која има за циљ проналажење сексуалних предатора на интернету и у којој је од поменуте године ухапшено преко 200 лица. У акцији учествују заједно Одељење за сузбијање високотехнолошког криминала, Више јавно тужилаштво у Београду, Посебно одељење за борбу против високотехнолошког криминала и полицијске снаге.

[38]McCarthy, John, Marvin L. Minsky, Nathaniel Rochester, and Claude E. Shannon. “A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955 Dartmouth AI Project Proposal; http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf приступљено дана 15.10.2022.

стварању вештачке интелигенције као области рачунарске науке, прошло је скоро 70 година. Иако је ВИ усавршена у разним областима где налази своју примену свакодневно, у другим је још увек у зачетку те је остављен простор да достигне свој пун капацитет. Очекивања су међутим, велика.

Од вештачке интелигенције се између осталог очекује да постави темеље за бољи квалитет живота, понуди нове могућности за запослење, бољи квалитет услуга у разним областима као и нове и одрживе моделе пословања. У медијској индустрији нпр. алати вештачке интелигенције користе се у различитим областима попут анализе садржаја, стварања, ширења, промоције, предвиђања, па чак и усклађености пословања *(compliance).* Но, њена употреба није ограничена само на индустрију забаве, већ обухвата много шири спектар медија, попут новинарства, оглашавања и телекомуникација.[39]

Вештачка интелигенција се генерално сматра доменом рачунарске науке који укључује когнитивно рачунарство, машинско учење (machine learning), дубоко учење ***(deep learning),*** рачунарски вид ***(computer vision),*** обраду природног језика ***(natural-language processing)*** и роботику,[40] односно подобласт рачунарске науке која обухвата теорију и развој компјутерских система способних за обављање задатака који обично захтевају људску интелигенцију попут визуелне перцепције, препознавање говора, доношење одлука и превођење језика.[41] Вештачка интелигенција развија се и допуњава муњевитом брзином па неминовно уводи промене у различите области наших живота као што су здравствена заштита (нпр. вештачке интелигенције овде може бити од користи у погледу постављања прецизније и брже дијагностике која би потом омогућила бољу превенцију болести), повећање ефикасности у пољопривреди, ублажавање ефекта климатских промена, унапређење ефикасности производних система, јачање система безбедности, између осталог. Истовремено, вештачка интелигенција са собом носи и низ потенцијалних ризика, попут нетранспарентног доношења одлука, родно засноване или дискриминацију друге врсте, задирања у наш приватни живот и на крају -

[39]Artificial Intelligence in the audiovisual industry, Summary of the EAO workshop, Strasbourg, 17 December 2019**,** European Audiovisual Observatory, Strasbourg, 2019 стр. 1-40 https://rm.coe.int/summary-workshop-2019-bat-2/16809c992a приступљено дана 15.10.2022.

[40]Nils J. Nilsson, Principles of Artificial Intelligence (Palo Alto: Tioga, 1980), стр. 2

[41]https://www.forbes.com/sites/bernardmarr/2018/02/14/the-key-definitions-of-artificial-intelligence-ai-that-explain-its-importance/?sh=7a093cb84f5d приступљено дана 19.10.2022.

коришћење у криминалне сврхе.[42]

Са аспекта криминалитета, негативна страна ове технологије огледа се у томе да су криминалци отпочели са стварањем злонамерних софтвера који су базирани на ВИ, док они који су нарочито мотивисани профитом развијају (прокси) системе вештачке интелигенције којима прикривају своју умешаност у кривична дела чиме избегавају или умањују ризик приликом извршења истих.[43] Када се вештачка интелигенција користи злонамерно она може довести до угрожавања дигиталне безбедности док би рачунари који су до сада били само средство у рукама криминалаца потенцијално могли постати вешти у хаковању и друштвеном инжењерингу на исти начин као и људски сајбер криминалци. Способност откривања сајбер напада од злонамерних софтвера вештачке интелигенције заснива се на претходном испитивању ових технологија и њиховој примени на постојеће криминалне обрасце и активности. Криминалци су одавно показали да врло брзо усвајају нове технологије па је и напредак у области ВИ омогућио и нове врсте напада.[44]

Коришћењем технологија ВИ, сајбер криминалци не само да су пронашли ново средство које ће користити ради извршења противправних активности, већ су пронашли и нове могућности за креирање и реализовање напада на владе, компаније и појединце. Иако нема довољно доказа да криминалне групе имају јаку техничку експертизу у управљању и манипулацији системима ВИ и машинског учења у криминалне сврхе, посредно се може закључити да су схватили њихов велики потенцијал. Упркос експанзији технологије ВИ у овој „бранши", криминалне групе и даље свакодневно регрутују искусне хакере како би злоупотребљавали компјутерске системе или вршили хакерске нападе и друге криминалне активности повезане са рачунаром, из било ког дела света.[45] Регрутација хакера се обавља најчешће путем огласа на дарк нету[46] у којима се између осталог тражи њихова вештина у погледу креирања малвера и фишинг страница за крађу идентитета или угрожавање корпоративне инфраструктуре. Поред програмера који су најтраженији, путем огласа се још траже и ИТ стручњаци који би спроводили нападе путем интернета,

[42]WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust Brussels, 19.2.2020 стр. 1 https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf приступљено дана 19.10.2022.
[43]Marc Goodman, Future Crimes: Inside the Digital Underground and the Battle for Our Connected World (New York: Anchor Books, 2016), стр 588, стр. 48, Kindle.
[44]Brundage, Miles, et al. "The malicious use of artificial intelligence: Forecasting, prevention, and mitigation (2018), The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation стр. 101, стр. 19.
[45]Velasco, C. Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. ERA Forum 23, 109–126 (2022). https://doi.org/10.1007/s12027-022-00702-z стр. 111
[46]Део интернета за који је потребно инсталирање специјалног софтвера како би му се приступило.

веб апликација или мобилних уређаја. „Плата“ која им се нуди у овим огласима креће се у распону од 200 до 20.000 америчких долара у зависности од вештине која се тражи. [47]

Када се говори о дезинформацијама примећује се стални глобални тренд њиховог промовисања уз подршку технологије ВИ познатије као „ботови“. Ботови се углавном користе за ширење лажних вести и садржаја широм интернета, а највише путем друштвених мрежа па је крајњи ефекат ове појаве дезинформисање и обмањивање становништва, посебно млађих генерација које још увек не могу лако да разликују легитимне изворе информација од лажних вести. Надаље, употреба ботова потенцијално може довести до нарушавања већ пољуљаног поверења у медије и постављање питање кредибилитета истих, а као најгори сценарио наводи се дестабилизације демократских и владиних институција. [48]

Упркос наведеном, ВИ има и своје предности, између осталог већ је коришћена од стране полиције са циљем идентификације и лоцирања нестале деце, скенирања недозвољених сексуално експлицитних огласа на интернету, ометања ланаца трговине људима или како би се открили финансијске трансакција које указују на могућност прања новца. Осим у полицијској делатности, ова технологија своју примену може наћи и у судовима, где може помоћи у ефикаснијем истраживању судске праксе како би се лакше и брже пронашле раније донете пресуде, чиме би се пружила подршка правницима у управљању предметима са циљем обезбеђивања ефикасног и благовременог судског поступка. У поправним установама, ВИ може се користити ради успостављања анализе понашања затвореника и смањења насиља у затворима.[49]

Како би се донекле поставио оквир у етичком коришћењу ВИ од стране технолошких гиганта, компанија „Гугл“ као један од лидера у овој области је 2018. године објавила водич о својим принципима и циљевима који укључују: друштвену корист и одговорност, избегавање стварања или јачања неправедне пристрасности, изградњу и тестирање безбедности, одговорност према грађанима која укључује дизајнирање принципа приватности и поштовање високих стандарда научне изврсности. Сматра се да

[47] https://n1info.rs/biznis/natrazeniji-poslovi-u-svetu-sajber-kriminala-zarada-od-200-do-20-000-dolara/ приступљено дана 15.02.2023.
[48] Velasco, C. Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. ERA Forum 23, 109–126 (2022). https://doi.org/10.1007/s12027-022-00702-z стр. 112
[49] The new age of technology, The United Nations Interregional Crime and Justice Research Institute, https://unicri.it/topics/ai_robotics, приступљено дана 08.01.2023.

је ово добар почетак уколико се ови принципи схвате озбиљно, али би људско доношење одлука засновано на етичким принципима требало да буде у основи стварања сваког софтверског пројекта а нарочито оног на бази вештачке интелигенције.[50]

Још један тренд и технологија ВИ која је почела широко да се користи у многим индустријама је дипфејк. Злоупотреба ове технологије нарочито када се користи за лажно представљање политичара, познатих личности или нпр. извршних директора великих компанија, а у комбинацији са техникама друштвеног инжењеринга и аутоматизацијом система, употребљава се за вршење криминалних активности и сајбер напада. Као и свака технологија и дипфејк се брзо шири и тренутно је експлоатишу сајбер криминалци на глобалном нивоу.[51]

III. ПОЈАМ И ПОДЕЛА ДИПФЕЈКА

Као један од првих примера манипулације фотографијом често се наводи 1860. година[52] и портрет Абрахам Линколна, у то време кандидата Републиканске странке за изборе. Портрет будућег председника САД-а измењен је тако што је слика његове главе залепљена на слику тела бившег потпредседника САД-а, Џона Калхуна[53] (који је важио за привлачног човека) од стране познатог фотографа у Вашингтону.

Из наведеног може се закључити да манипулација аналогним и дигиталним садржајем није новост, а да је чин „дотеривања“ садржаја стар колико и сама медијска индустрија. Међутим, недавни развој у области дубоког учења помогнут новим и јавно доступним алатима означио је почетак следеће фазе уређивања садржаја.[54]

Дипфејк настаје коришћењем технологије која се ослања на вештачку интелигенцију (ВИ), односно на:

[50]Wagner, T. and Blewer, A. (2019) “The Word Real Is No Longer Real”: Deepfakes, Gender, and the Challenges of AI-Altered Video. Open Information Science, Vol. 3 (Issue 1). https://doi.org/10.1515/opis-2019-0003, стр 32-46, стр. 41.
[51]Velasco, C. Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. ERA Forum 23, 109–126 (2022). https://doi.org/10.1007/s12027-022-00702-z стр. 113.
[52] Прва фотографија настала је 1826. године
[53] Више на https://www.atlasobscura.com/articles/abraham-lincoln-photos-edited
[54] Kietzmann, Jan, Linda W. Lee, Ian P. McCarthy, and Tim C. Kietzmann. "Deepfakes: Trick or treat?." Business Horizons 63, no. 2 (2020): 135-146.стр. 145

1. рачунарске моделе људског понашања и мисаоних процеса који су дизајнирани да раде рационално и интелигентно односно да симулирају људско понашање и
2. машинско учење које представља грану вештачке интелигенције која омогућава рачунарским системима да уче директно из примера, података и искустава као и да спроводе сложене процесе учећи из података уместо да прате унапред програмирана правила.

Посебно је важно нагласити да дипфејк представља најнапреднији и најреалнији облик општег кретања ка ономе што називамо синтетичким медијима. ***Синтетички медији*** се односе на садржај који је у потпуности или делимично креиран или којим се манипулише коришћењем вештачке интелигенције или других технологија, па би сходно томе дипфејк можда и требало третирати као најјаснији пример и напредни облик синтетичких медија.[55]

У светлу наведеног, дипфејк се може дефинисати као изманипулисан или синтетички аудио или визуелни медиј који изгледа аутентично и на коме су представљени људи који изгледају као да говоре или раде нешто што никада нису рекли или урадили, произведен коришћењем техника вештачке интелигенције, укључујући машинско и дубоко учење.[56]

У погледу назива, име је мешавина израза „*дубоко учење*“ (deep learning) и „*лажно*“ (fake) чиме се подразумева да се технологија дубоког учења користи за креирање лажних слика, видео снимака и аудио записа. Као што име сугерише, главни технолошки састојак у креирању дипфејка је *дубоко учење*[57] - техника вештачке интелигенције која се користи за тренирање *дубоких неуронских мрежа* (deep neural networks) које подсећају на неуроне у људском мозгу. ДНМ се састоје од великог скупа међусобно повезаних вештачких неурона које обично називамо јединицама. Идентично као неурони у мозгу, свака јединица сама по себи обавља рачунања која су прилично једноставна док све јединице заједно могу да обављају сложене нелинеарне операције попут препознавања одређене

[55]van der Sloot, B., & Wagensveld, Y. (2022). Deepfakes: Regulatory challenges for the synthetic society. Computer Law & Security Review, 46, 1-15. https://doi.org/10.1016/j.clsr.2022.105716 приступљено дана 20.10.2022.
[56] Tackling deepfakes in European policy, European Parliamentary Research Service, Brussels, 2021, стр. 1.
[57]Дубоко учење је име за приступ вештачкој интелигенцији који се зове неуронске мреже. Неуронске мреже су први пут предложили 1944. године два истраживача са Универзитета у Чикагу - Ворен Мекалоу и Волтер Питс који су 1952. године на чувеном универзитету МИТ (Масачусетски технолошки институт) основали прво одељење за когнитивне науке.

особе у виду пиксела на екрану.[58]

Постоји неколико метода за креирање дипфејка али они који су најчешћој употреби ослањају се на коришћење дубоких неуронских мрежа (ДНМ) и ту се најчешће мисли на аутокодере који користе технику замене лица (face swap). Да би један дипфејк настао потребно је одабрати видео који ће бити коришћен као основа за дипфејк, а затим колекцију видео снимака или фотографија особе које је потребно уметнути у снимак односно заменити. *Аутокодер* је је врста неуронске мреже која користи дубоко учење тј. посебна врста алгоритма дубоког учења[59] који има задатак да проучава видео снимке са циљем разумевања како једна особа изгледа из различитих углова и у различитм условима околине, а потом да замени ту особу појединцем у циљаном видео снимку тако што ће пронаћи заједничке карактеристике.[60] На основу задатог, великог скупа улазних слика (нпр. све приказују једну особу), аутокодер је обучен да препозна кључне карактеристике људског лица и затим поново креира улазне слике као његов излаз. У овом процесу он региструје да ли су нпр. очи отворене или затворене, позицију главе, емоционални израз лица, израз очију, боју коже или амбијент.[61] Састоји се од три компоненте: енкодера, кода и декодера. Постоје различите врсте аутокодера: аутокодери за уклањање шума, дубоки аутокодери, контрактивни аутокодери, конволуцијски аутокодери итд. [62]

Осим ДНМ-а и аутокодера, као нова и софистицираније метода за креирање дипфејка користи се и **ГАН** технологија (генеративне супарничке мреже или генеративне адверсаријске мреже). ГАН се састоји од две неуронске мреже за које се може рећи да играју игру једна са другом: дискриминатора и генератора. Дискриминатор покушава да утврди да ли је информација коју је добио стварна или лажна. Генератор, са друге стране покушава да створи податке за које дискриминатор мисли да су прави. Дискриминатор је у стању да врло прецизно одреди који су то подаци лажни, а под условом да има довољно времена и да је довољно увежбан генератор може да створи фалсификат који ће

[58] Kietzmann, Jan, Linda W. Lee, Ian P. McCarthy, and Tim C. Kietzmann. "Deepfakes: Trick or treat?." Business Horizons 63, no. 2 (2020): 135-146. Стр. 138
[59] https://bdtechtalks.com/2020/09/04/what-is-deepfake/ приступљено дана 20.10.2022.
[60] https://www.businessinsider.com/guides/tech/what-is-deepfake приступљено дана 20.10.2022.
[61] Kietzmann, Jan, Linda W. Lee, Ian P. McCarthy, and Tim C. Kietzmann. "Deepfakes: Trick or treat?." Business Horizons 63, no. 2 (2020): 135-146. стр 138-139
[62] https://recfaces.com/articles/what-is-deepfake#2 приступљено дана 20.10.2022.

преварити чак и дискриминатора тј. дискриминаторску мрежу.[63] Дакле, сврха генератора је да превари дискриминатора. Што је генерисане податке теже разликовати од стварних података, то је систем ВИ боље обучен. ГАН-ове је теже обучити јер захтевају више ресурса и чешће се користе за генерисање фотографија, а мање видео записа. [64]

Иако дипфејк видео снимци обично захтевају велики скуп слика и података да би се направио један нови материјал, неминовно је да ће се количина садржаја потребног да се направи добар дипфејк смањивати усавршавањем система вештачке интелигенције. Тако је нпр. софтвер који је развила компанија „Самсунг“ односно лабораторија ове компаније у Русији створила дипфејк снимак од само једне слике као извора. Истраживачи ове компаније успели су да генеришу дипфејк запис Мона Лизе, чувене слике Леонарда Да Винчија где се она може видети како се смеје, разговара и гестикулише. [65]

Утицај и значај дипфејка су нарочито важни јер упркос томе што је поверење у фотографију као извор информација срозано, у последњих неколико деценија управо захваљујући експанзији технологија и алата који се користе са циљем манипулације сликама, ми се још увек поуздамо у фотографске доказе, а још више верујемо видео записима које гледамо.[66] Реалистична природа дипфејка чини их метом генерације (педо)порнографског материјала, лажних вести, лажног надзора и кривичних дела попут преваре о чему ће бити речи касније у раду[67]

1. Подела дипфејка

Дипфејк се може поделити на 4 главне категорије:

1. **фото** - који обухвата замену лица или тела (*face/body swapping*),

[63]Farago, Tunde. "Deep fakes–an emerging risk to individuals and societies alike." Tilburg University (2019), стр. 1-61, стр. 14.
[64]https://recfaces.com/articles/what-is-deepfake#2 приступљено дана 20.10.2022.
[65]Више на https://www.cnet.com/tech/computing/samsung-ai-deepfake-can-fabricate-a-video-of-you-from-a-single-photo-mona-lisa-cheapfake-dumbfake/ и https://www.cnet.com/tech/computing/samsung-ai-deepfake-can-fabricate-a-video-of-you-from-a-single-photo-mona-lisa-cheapfake-dumbfake/
[66] Kietzmann, Jan, Linda W. Lee, Ian P. McCarthy, and Tim C. Kietzmann. "Deepfakes: Trick or treat?." Business Horizons 63, no. 2 (2020): 135-146., стр 136.
[67]D. Güera and E. J. Delp, "Deepfake Video Detection Using Recurrent Neural Networks," 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), 2018, pp. 1-6, doi: 10.1109/AVSS.2018.8639163. стр. 1-5, стр. 1 https://gangw.web.illinois.edu/class/cs598/papers/AVSS18-deepfake.pdf приступљено дана 01.11.2022

2. **аудио** - подразумева само замену гласа (у најширем смислу овде се може уврстити и тзв. *„text-to speech“* технологија односно *синтеза говора* - систем који има могућност да конвертује писани текст у говор),
3. **видео** (долази до замене лица, тзв. *„morphing“* или *full-body puppetry*) и,
4. **аудио-видео**, који користи комбинацију горе наведених техника.[68]

У погледу садржаја који се ствара, већина дипфејк снимака може се поделити на: **политичке**, **порнографске**, **комерцијалне** и **креативне**. Политички и порнографски дифејк садржаји се свакако сматрају друштвено опаснијим појавама узимајући у обзир озбиљност и далекосежност последица до којих могу довести у погледу државне безбедности или сигурности и добробити појединца. Комерцијални дипфејкови користе се у маркетиншке сврхе, док се креативни употребљавају као вид уметничког изражавања због чега се генерално сматрају појавама које су друштвено корисне. Порнографски дипфејк садржаји могу довести до понижења, експлоатације, физичког, менталног или финансијског злостављања најчешће жена и девојака о чему ће бити речи касније, а политички до поларизације друштва, опадања и губитка поверења у институције, а као најозбиљнија последица наводи се претња по националну безбедност и међународне односе. [69]

Политички дипфејк видео снимци најчешће настају на основу јавних говора политичара, вести или друштвено значајних догађаја на којима су исти учествовали. Креативни дипфејк видео снимци настају у циљу сатире или пародије, најчешће на познате личности, док је сврха комерцијалних оглашавање и промотивна делатност великих и малих компанија. Нажалост, као најчешћа врста дипфејк видео снимака а често и као синоним за сам дипфејк, јављају се они са порнографским садржајем где се лица познатих глумица, а све више обичних жена и девојака посредством вештачке интелигенције монтирају на лица глумица у порно филмовима. [70]

[68]Kietzmann, Jan & Lee, Linda & McCarthy, Ian & Kietzmann, Tim. (2019). Deepfakes: Trick or treat?. Business Horizons. 63. 10.1016/j.bushor.2019.11.006. стр. 8

[69] Meskys, Edvinas and Kalpokiene, Julija and Jurcys, Paulius and Liaudanskas, Aidas, Regulating Deep Fakes: Legal and Ethical Considerations (December 2, 2019). Journal of Intellectual Property Law & Practice, Volume 15, Issue 1, January 2020, стр. 24–31., Available at SSRN: https://ssrn.com/abstract=3497144 стр 5

[70] Ibid. стр. 5

1.1. Фото дипфејк

Из техничког угла, свакако је лакше модификовати једну фотографију него видео снимак. Слика је статична и не садржи елементе који чине део физиономије или анатомије једне особе, попут гласа или нпр. покрета што је случај са видео записом. У погледу манипулације видео снимком, постоје додатне потешкоће попут резолуције видео записа или дигиталног формата. За манипулацију сликама, традиционално су се користиле разноврсне технике, од којих је најпознатија морфинг (*morphing*) техника која се појавила још 70-их година. Она подразумева модификацију слике путем метаморфозе, где се слика А трансформише у слику Б и обрнуто па омогућава да се лице једне особе интегрише у лице друге.[71]

Напредовање технологије и појава вештачке интелигенције допринели су да се овај процес убрза и усаврши, при чему за стварање дипфејк слика предњаче модели дубоког учења. Манипулација лицем на фотографији може се широко груписати у две категорије: генерисање (стварање) лица и уређивање/срећивање атрибута лица. Генерисање лица укључује синтезу фотореалистичних слика људског лица које не постоји у стварном животу. Насупрот томе, уређивање атрибута лица подразумева промену постојећег изгледа или експресије лица модификовањем одређених области на лицу. То укључује нпр. уклањање/стављање наочара, промену погледа, уклањање бора и ожиљака па чак и неке измене вишег нивоа, као што су старост и пол. Манипулација експресијом лица се изводи најчешће помоћу алата као што је „Face2Face“ и тада се само израз лица једне особе пребацује на другу. Замена лица обично се изводи комбинованим техникама компјутерске графике са методама дубоког учења које захтевају претходну обуку ових алата. Код синтезе лица циљ је стварање непостојећег, али реалног изгледа. Синтеза лица заснована на вештачкој интелигенцији се већ користи у злонамерне сврхе тако што се слике настале на овај начин, у комбинацији са лажним дигиталним идентитетом употребљавају за креирање налога на друштвеним мрежама где се потом користе за ширење дезинформација [7273] или извршење других кривичних дела попут преваре.

[71]Boté-Vericad, Juan-José; Vállez, Mari (2022). Image and video manipulation: The generation of deepfakes. In: Freixa, Pere; Codina, Lluís; Pérez-Montoro, Mario; Guallar, Javier (ed.). Visualisations and narratives in digital media. Methods and current trends, Barcelona: DigiDoc-EPI. https://doi.org/10.3145/indocs.2022.8 стр. 116-127, стр. 119, приступљено дана 27.02.2023.

[72]H. Khalid and S. S. Woo, "OC-FakeDect: Classifying Deepfakes Using One-class Variational Autoencoder," 2020

Што се тиче квалитета слике, технике дубоког учења успешно се користе како би се побољшале перформансе компресије слике у чему велику улогу има примена аутокодера који су у стању да извуку више компресованих репрезентација слика са минималним губитком.[74]

Широко доступне апликације за паметне телефоне као што је „FaceApp“ способне су да аутоматски генеришу изузетно реалне трансформације лица на фотографијама. На овај начин је нпр. могуће једној особи променити фризуру, лице па чак и пол. Будући да је прављење лажних фотографија и видео записа главни арсенал дипфејка, слике и видео снимци се појављују као његов најчешће коришћени облик, нарочито када се узме у обзир да живимо у свеприсутном свету друштвених медија, где слике и видео снимци имају моћ да објасне или разјасне одређене догађаје и приче боље од обичног текста,[75] а свакако путују и преносе се брже.

1.2. Аудио дипфејк

Дипфејк технологија усавршила се у тој мери да је сада могуће произвести све врсте клонираног материјала од гласа до видео снимака. Напредак у алгоритмима за говор на бази вештачке интелигенције, нарочито у области синтезе и клонирања гласа (voice cloning), показали су потенцијал у погледу креирања изузетно реалистичних а ипак лажних гласова који се готово и не разликују од правог тј. аутентичног говора. Ова појава јавља се као нарочит проблем за ону врсту технологија код којих се као мера предострожности захтева гласовна провера односно аутентификација.[76]

Аудио-фејкови стварају се тако што програм прво слуша и детектује аудио снимке говора одређене особе. У зависности од техника за синтезу гласа које се у овом процесу користе, софтвер мора да слуша глас одређено време, а у појединим случајевима само 10

IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Seattle, WA, USA, 2020, стр. 2794-2803, стр. 2794. doi: 10.1109/CVPRW50498.2020.00336. приступљено дана 22.10.2022.

[73]Masood, M., Nawaz, M., Malik, K.M., Javed, A., Irtaza, A. and Malik, H., 2022. Deepfakes Generation and Detection: State-of-the-art, open challenges, countermeasures, and way forward. Applied Intelligence, стр.1-53. Стр. 12 -13

[74]Güera, D. and Delp, E.J., 2018, November. Deepfake video detection using recurrent neural networks. In 2018 15th IEEE international conference on advanced video and signal based surveillance (AVSS) стр 1-6, стр. стр. 2

[75]Nassif, Ali & Nasir, Qassim & Abu Talib, Manar & Gouda, Omar. (2022). Improved Optical Flow Estimation Method for Deepfake Videos. Sensors. стр. 1.

[76]Masood, Momina & Nawaz, Marriam & Malik, Khalid & Javed, Ali & Irtaza, Aun. (2021). Deepfakes generation and detection: state-of-the-art, open challenges, countermeasures, and way forward стр. 1-43, стр 16,

до 20 секунди. Потом се издвајају кључне информације о јединственим аспектима гласа жртве. Креатор (нападач) бира фразу коју ће дипфејк изговорити, а затим, користећи модификовани алгоритам за претварање текста у говор, генерише аудио узорак који звучи као да жртва изговара изабрану реченицу.[77]

Технологија клонирања гласа такође је позната и као аудио-графички фејк, синтеза говора или конверзија/замена гласа. Софтверске методе за клонирање гласа помоћу вештачке интелигенције могу да генеришу синтетички говор који је јако сличан људском гласу чијем се постизању на крају крајева и тежи. Технологија на истој бази - „text-to speech“ постала је саставни део свакодневне потрошачке електронике (пласирана од стране компанија „Гугл“, „Епл“ и „Амазон“) и нашла је своју примену нпр. кроз системе за навигацију, а квалитет гласовних клонова се брзо побољшао, углавном услед појаве ГАН-ова. Међутим, није само тон гласа оно што га чини убедљивим па садржај аудио снимка такође мора одговарати стилу и речнику лица чији се говор имитира,[78] стога стварање аутентичног аудио дипфејка захтева додатне напоре будући да сваки глас има одређену личну карактеристику.

Први забележени случај аудио-дипфејка генерисаног вештачком интелигенцијом у циљу извршења кривичног дела одиграо се 2019. године како би се преварио директор једне енергетске компаније са испоставом у Великој Британији. Директор је веровао да разговара телефоном са својим шефом, главним извршним директором немачке матичне компаније, па је следио наређења да одмах пребаци 220.000 евра на банковни рачун мађарског добављача сировина. Међутим, глас је припадао преваранту који је користио гласовну верзију дипфејка, а покушај преваре откривен је када је директор испоставе схватио да позиве добија из Аустрије а не Немачке где се извршни директор налазио.[79]

Због наведеног примера, сматра се да ће аудио-фејкови и синтетизовани гласови вероватно постати део техника које ће сајбер криминалаци користи у будућности. Ситуацију довољно отежава и чињеница да су различити алати за синтезу гласа отвореног кода и јавно доступни што омогућава свакоме ко има приступ интернету да их релативно

[77] https://theconversation.com/deepfake-audio-has-a-tell-researchers-use-fluid-dynamics-to-spot-artificial-imposter-voices-189104 приступљено дана 15.01.2023.
[78] Das, Djurre & van Boheemen, Pieter & Linda, Nierling & Jahnel, Jutta & Karaboga, Murat & Fatun, Martin & Huijstee, Mariëtte. (2021). Tackling Deepfakes in European policy стр. 2.
[79] https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/?sh=57ae3f7d2241 приступљено дана 15.01.2023.

лако креира.[80] Могућност имитације гласа може помоћи сајбер криминалцима да изведу нпр. убедљиви телефонски фишинг напад против појединца или компаније. У комбинацији са визуелним дипфејковима, аудио-фејкови имају потенцијал да створе потпуну и реалну имитацију једне особе .[81]

Добра страна ове технологије јесте у томе што је синтетички глас прилично широко прилагођен за развој различитих апликација у области синхронизације за ТВ и филмску индустрију, личне асистенте на бази вештачке интелигенције или персонализоване синтетичке гласове за гласовно хендикепиране особе.[82] Ту се користи за рекреацију гласова особа које су глас изгубиле због болести или услед других фактора. Ова могућност ствара потенцијал да персонализовани компјутерски гласови нађу своју примену и у медицини као замена за глас[83] о чему ће бити речи касније.

1.3. Видео дипфејк

Дипфејк видео подразумева манипулисање тј. модификацију постојећег видео снимка променом покрета или израза лица особе на снимку. За овај процес могу се користити различити алати и технике попут замене лица примарне особе (мете) синтетичким путем, аутокодерима или коришћењем ГАН-ова како би се креирали нови кадрови који се убацују у оригинални снимак. Поред ових користе се и традиционалне, сада већ усавршене технике као што су „morphing“ или тзв. „puppet-master“.

Иако ови видео снимци могу бити тешки за откривање будући да изгледају јако уверљиво, углавном их је лако направити. Широк спектар јавно доступних слика и видео записа на интернету допринео је да се постоји довољно материјала за креирање дипфејк видео снимака тако да скоро свако може да генерише ову врсту садржаја комбиновањем доступних података са бесплатним софтверима отвореног кода као што је нпр.

[80] https://www.darkreading.com/attacks-breaches/deepfake-audio-scores-35-million-in-corporate-heist приступљено дана 15.10.2023.
[81] https://www.scip.ch/en/?labs.20210318 приступљено дана 15.01.2023.
[82] Masood, Momina & Nawaz, Marriam & Malik, Khalid & Javed, Ali & Irtaza, Aun. (2021). Deepfakes generation and detection: state-of-the-art, open challenges, countermeasures, and way forward Стр 1-43. стр 16.
[83] https://www.scip.ch/en/?labs.20210318 приступљено дана 15.01.2023

апликација „FaceApp“. [84]

Процес стварања дипфејк видео снимка посредством аутокодера почиње тако што креатор мења лице једне особе и замењује га другим, користећи алгоритам за препознавање лица и рачунарску мрежу дубоког учења која се зове варијациони аутокодер. Ови алати су обучени да кодирају слике у нискодимензионалне репрезентације, а потом декодирају те репрезентације назад у слике.[85] Потребна су два сета слика за обуку. Први, који има само узорке оригиналног лица које ће бити замењено, а које се може издвојити из циљаног видео записа којим ће се манипулисати и који се може додатно проширити сликама из других извора за верније резултате и други, који садржи жељено лице које ће бити замењено у циљаном видео снимку. Како би се олакшао процес обуке аутокодера, најлакша замена лица би имала и оригинално лице и циљано лице приказано под сличним углом и осветљењем. Међутим, то обично није случај. Вишеструки прикази кадрова, разлике у условима осветљења и слични недостаци отежавају аутокодерима да направе реалистична лица у свим условима.[86]

Ови проблеми превазиђени су усавршавањем ГАН модела где се замена лица на видео снимку са једне особе на другу врши посредством алгоритма вештачке интелигенције чак и у реалном времену. ГАН модели су развијени уз коришћење неколико хиљада слика, тако да је могуће креирати реалистична и уверљива лица која се потом могу издвојити и убацити у оригинални видео на такав начин да створени садржај делује готово потпуно реално, а уколико се тежи ка још већој аутентичности она се може постићи путем одговарајуће постпродукцијске обраде. [87]

Традиционални приступ замене лица генерално се састоји од три корака. Прво, ови алати откривају лице изворне слике, а онда бирају слику лица кандидата из „каталога“ лица која је слична улазном изгледу слике. Друго, у процесу се замењује очи, нос и уста и додатно прилагођава осветљење и боја слике лица мете како би одговарала изгледу улазних слика где се два лица неприметно спајају. Трећи корак рангира комбиновану

[84]Nassif, Ali & Nasir, Qassim & Abu Talib, Manar & Gouda, Omar. (2022). Improved Optical Flow Estimation Method for Deepfake Videos. Sensors. 22. 2500. 10.3390/s22072500. стр. 1
[85] https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained приступљено дана 27.02.2023.
[86]Güera, D. and Delp, E.J., 2018, November. Deepfake video detection using recurrent neural networks. In 2018 15th IEEE international conference on advanced video and signal based surveillance (AVSS) стр. 1-6, стр. 3
[87]Awotunde, J.B.; Jimoh, R.G.; Imoize, A.L.; Abdulrazaq, A.T.; Li, C.-T.; Lee, C.-C. An Enhanced Deep Learning-Based DeepFake Video Detection and Classification System. Electronics 2023, 12, 87. https://doi.org/10.3390/electronics12010087 стр. 2

замену две особе израчунавањем подударања преко региона преклапања. Овај приступ може понудити добре резултате под одређеним условима, али има два велика ограничења. Прво, потпуно мења улазно лице циљним лицем, а изрази слике улазног лица се губе. И друго, синтетички резултат може да изгледа веома ригидно, а замењено лице често делује неприродно.[88]

Техника морфирања се традиционално користила као алат у области анимације како би се створили специјални филмски ефекти. Термин „*morphing*“ користи се да опише технику обраде слике у којој се долази до специфичне трансформације која претвара једну слику у другу. На пример, ако постоје две слике, А и Б, може се генерисати нова слика која трансформише слику А у Б, и обрнуто. Такође је могуће генерисати нову слику овом техником која је заснована на више од две слике.[89]

На крају, техником луткар-мајстор или „*puppet-master“* дипфејк видео настаје опонашањем или анимирањем израза циљане особе, као што је покрет очију, израз лица или покрет главе. Ствара се тако што извођач седи испред камере и глуми или изводи садржај који жели да његова „лутка" или циљана особа каже или уради. Ови дипфејк видео снимци имају за циљ да замене израз изворне особе али и покрете целог тела.[90]

1.4. Аудио-видео дипфејк

Визуелни и аудио модалитети често се преплићу и допуњују једно друго чиме се обезбеђује квалитетнија репрезентација аудио-визуелног садржаја. У ту сврху креатори таквог садржаја обучавају своје моделе заједно са оба модалитета како би створили што уверљиивији дипфејк садржаји.[91]

[88]Masood, M., Nawaz, M., Malik, K.M., Javed, A., Irtaza, A. and Malik, H., 2022. Deepfakes Generation and Detection: State-of-the-art, open challenges, countermeasures, and way forward. Applied Intelligence, стр.1-53. стр. 7-8

[89]Steyvers, Mark. (1999). Morphing techniques for manipulating face images. Behavior research methods, instruments, & computers: a journal of the Psychonomic Society, Inc. 31. 10.3758/BF03207733. стр. 359-369 стр. 360.

[90]Masood, M., Nawaz, M., Malik, K.M., Javed, A., Irtaza, A. and Malik, H., 2022. Deepfakes Generation and Detection: State-of-the-art, open challenges, countermeasures, and way forward. Applied Intelligence, стр.1-53. стр. 1-2

[91]Zhou, Y. and Lim, S.N., 2021. Joint audio-visual deepfake detection. In Proceedings of the IEEE/CVF International Conference on Computer Vision, стр.14800-1480, стр. 14801.

Ова врста дипфејка интегрише различите врсте садржаја па тако овај облик може садржати слике, видео или аудио записе. Када се овај скуп елемената комбинује заједно, омогућава стварање аудио-видео дипфејка међутим, чак и ако се ови елементи третирају одвојено, могу се јавити као део дипфејк видеа. Стога, по питању морфологије дипфејка, он може обухватати слике, аудио и видео записе. Додатно, могу се још користити и технике анимације. Прилагођавање које се постиже аудиовизуелном технологијом подразумева манипулацију одређеним карактеристикама једне особе, укључујући њихово лице, глас, покрете усана или држање тела. Иако постоје апликације које дозвољавају да дипфејк буде генерисан јефтино, стварање једног аудио-видео записа који изгледа истински аутентично изискује прилично велике трошкове будући да углавном захтева учешће стручњака из различитих области, укључујући лингвисте, видео монтажере или аниматоре. [92]

Поред поменутих алата вештачке интелигенције који се користе за креирање дипфејк фотографија или видео снимака појединачно, једна од основних техника која се користи за креирање аудио-видео дипфејка јесте већ поменути морфинг, који се састоји од идентификације образаца између две фотографије и динамичке трансформације једне слике у другу. Како је технологија еволуирала и како су се њени резултати побољшали, додавањем 3Д елемената овој техници постигнути су још реалистичнији ефекти. Још једна од традиционалних техника у употреби је тзв. савијање или „*warping*“, које омогућава промену облика дела слике (коју треба дигитално модификовати најчешће са креативном наменом) где се исправљају могуће дисфункције слике или се лик односно лице на слици искривљује односно деформише. Ова техника има различите примене и најчешће укључује стварање карикатура преувеличавањем одређених личних атрибута али се може користити и у области здравствене заштите, тачније у радиотерапији, за корекцију панорамских слика начињених спортским камерама као и за постпродукцију слика, у виду естетских побољшања фотографија.[93]

Просечан корисник интернета може путем апликација на бази вештачке

[92]Boté-Vericad, Juan-José; Vállez, Mari (2022). Image and video manipulation: The generation of deepfakes. In: Freixa, Pere; Codina, Lluís; Pérez-Montoro, Mario; Guallar, Javier (ed.). Visualisations and narratives in digital media. Methods and current trends Barcelona: DigiDoc-EPI. https://doi.org/10.3145/indocs.2022.8 ,стр. 116-127, стр. 118-119.
[93] Ibid. стр. 120.

интелигенције као што су „FakeApp'', „Faceswap'' или „ЗАО“ (ZAO) које су лако и јавно доступне, креирати аудио-видео дипфејк у року од само неколико секунди, нарочито узимајући у обзир постојање софтвера и програма отвореног кода доступних на интернету и водиче за ове алате доступне на платформи „YouTube“. Нпр. апликација „Face2Face“ бележи изразе лица једне особе у реалном времену док се та особа гледа на веб или камери мобилног телефона и модификује њено лице у жељени садржај такође у реалном времену. Како би аудио-видео снимак био што уверљивији и реалнији потребно је уградити адекватни и уверљиви звучни садржај. Добар пример за то је процес под називом *„Synthesizing Obama“*[94] који се користи за модификовање покрета уста. Ови радови су за сада фокусирани само на манипулацију главе и лица али свакако ће се проширити и на манипулацију целог тела једне особе. [95] Техника која се користи у овом поступку назива се синхронизација усана или *„lip sync“* и она укључује модификовање покрета уста говорника како би изговарао одређене речи. Најчешће се користи када једна особа говори и када је камера фокусирана искључиво на њој[96] те је комбинација оваквих аудио техника са визуелним дипфејком у стању да произведе поптпуно аутентични аудио-видео садржај једне особе.

IV. ЗЛОУПОТРЕБА ДИПФЕЈК ТЕХНОЛОГИЈЕ

1. Лажне вести и дезинформације

У ери званој *пост-истина*[97], поуздано новинарство је од круцијалног значаја за добробит сваког друштва. Чињеница да се технологије развијају муњевитом брзином не значи да једно друштво треба да буде изоловано од вредности које су историјски од

[94]Више на https://www.youtube.com/watch?v=9Yq67CjDqvw

[95]Masood, M., Nawaz, M., Malik, K.M., Javed, A., Irtaza, A. and Malik, H., 2022. Deepfakes Generation and Detection: State-of-the-art, open challenges, countermeasures, and way forward. Applied Intelligence, стр.1-53, стр. 5.

[96]Boté-Vericad, Juan-José; Vállez, Mari (2022). Image and video manipulation: The generation of deepfakes. In: Freixa,Pere; Codina, Lluís; Pérez-Montoro, Mario; Guallar, Javier (ed.). Visualisations and narratives in digital media. Methods and current trends, Barcelona: DigiDoc-EPI. https://doi.org/10.3145/indocs.2022.8 стр. 116-127, стр.121.

[97]Идеја да конкретна чињеница има мањи значај или утицај на обликовање јавног мњења у односу на емоције и лична уверења.

значаја целом човечанству. Уместо тога, потребно је да се те вредности служе технолошким могућностима овог доба.[98]

Феномен који називамо „*лажне вести*“ или „*онлајн дезинформације*“ су обмањујуће, лажне или погрешне информације односно садржај који се пласира са намером да утиче на политички дискурс или изборе,[99] док су кампање дезинформација операције и процеси који намерно шире лажне информације у циљу обмане.[100]

Данас је већ лако замислити ситуацију у којој долази до пуштања лажног упозорења за хитне случајеве које нас обавештава о предстојећем нападу или прекиду избора због објављивања лажног аудио или видео записа једног од кандидата за изборе.[101] У том контексту, није тешко предвидети како ће се лажне вести проширити на „дипфејк лажне вести“ у будућности. Како дифејк постаје широко распрострањен, јавност ће све више имати потешкоћа да поверује чак и у оно што види и чује због чега постоји опасност од фрагментације поверења неопходног за ефикасно функционисање једне демократске државе[102] У мају 2018. године, белгијска Социјалистичка партија постала је прва политичка странка која је користила дипфејк технологију како би утицала на јавну дебату. Странка је на свом профилу, на друштвеној мрежи „Фејсбук“ објавила видео снимак који наводно приказује председника САД-а, Доналда Трампа како охрабрује Белгију да се повуче из Париског споразума о климатским променама. Иако је и сама странка навела да је спорни видео дизајниран у циљу изазивања дебате, а не обмане и упркос чињеници да је врло брзо био разоткривен од стране интернет заједнице као лажан,[103] врло јасно се могу сагледати последице које дипфејк садржај може изазвати нарочито у политичко

[98]Temir, Erkam (2020). Deepfake: New Era in The Age of Disinformation & End of Reliable Journalism. стр. 1009-1024, стр. 1018.
[99]The European Data Protection Supervisor - EDPS Opinion on online manipulation and personal data. Mart 2018, стр. 3.
[100]Facing reality? Law enforcement and the challenge of deepfakes, An Observatory Report from the Europol Innovation Lab, https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf стр 11. Приступљено 16.01.2023.
[101]Facing reality? Law enforcement and the challenge of deepfakes, An Observatory Report from the Europol Innovation Lab, https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf стр 11, приступљено 16.01.2023
[102] Danielle K. Citron & Robert Chesney, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 California Law Review стр. 1753-1820, стр. 1786.
[103]Smith, Hannah, and Katherine Mansted. “What’s the Problem?” Weaponised Deep Fakes: National Security and Democracy, Australian Strategic Policy Institute, 2020, pp. 04–04. JSTOR, http://www.jstor.org/stable/resrep25129.4. Стр. 13, приступљено 09.01.2023.

осетљивим тренуцима за једну земљу или међународну заједницу па је логично претпоставити да ће са порастом дипфејкова несумњиво доћи до продубљивања неповерења у друштву и да ће се исти све више користити како би се утицало на изборни процес или политичке исходе.[104]

Интеракција између дигитализације и растућих сајбер претњи носи и нематеријалне последице. Данас је неповерење према новинарству (из различитих разлога) високо па проблеми које стварају дипфејкови нису мали, а готово да не постоји друштво које је толико напредно и свесно и које би са резервом узимало сваку фотографију или сваку вест. Са аспекта новинарства посебно је забрињавајуће што не само тзв. корисници медија, већ и познате новинске агенције често праве овакве омашке[105] те не разликују или не проверавају колико је један садржај заиста аутентичан. Деловање ботова и креирање дипфејк садржаја од стране система заснованог на алгоритму и вештачкој интелигенцији стога може утицати на способност појединца да изгради ставове који су базирани на поузданим информацијама. На овај начин манипулише се појединцима и угрожава њихово право да буду информисани како би могли да учествују у процесима демократског одлучивања али и у осталим процесима који могу бити од значаја за једну државу.[106]

Како данас просечан корисник интернета углавном није у стању да разликује између онога што је стварно и онога што је лажно, пристојан дипфејк садржај може проћи као аутентичан. На пример, дипфејк видео снимак председнице Представничког дома САД-а, Ненси Пелоси на коме је приказана у алкохолисаном стању прегледан је више од два милиона пута само првог дана од његовог објављивања на интернету. Додатно, лажне вести могу веома брзо постати видљивије и широко познате захваљујући алгоритамском појачавању и филтерима који помажу ширење оваквог садржаја на итернету.[107] Осим тога, потребно је бринути и о феномену који називамо „дивиденда лажова“ *(the liar's dividend)* – који се јавља када се лице које изговара или пласира одређену лажну информацију, брани

[104]The Global Risks Report 2022 17th Edition, world economic forum, The Global Risks Report 2022 стр. 49, https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf приступљено дана 17.12.2022
[105]Temir, Erkam. (2020). Deepfake: New Era in The Age of Disinformation & End of Reliable Journalism. 10.18094/JOSC.685338. стр 1009-1024, стр. 1016,
[106]Прља, Д., Гасми, Г., Корађ, В., 2022. Људска права и вештачка интелигенција, Институт за упоредно право Београд, стр. 82
[107]Farago, Tunde. "Deep fakes–an emerging risk to individuals and societies alike." Tilburg University (2019). стр. 15.

ставом да је у питања лажна вест у случају да медији или новинари открију да је информација коју је пласирало ово лице заиста била лажна. [108]

Постојећа решења за овакве друштвене и политичке феномене фокусирала су се на мере транспарентности чиме се у крајњој линији открива извор информација, а занемарује одговорност лица која у таквом екосистему профитирају од несумњиво штетног деловања. Смањење доступног интимног простора, као резултат неизбежног надзора компанија и влада над нама, представља застрашујући утицај на способност и вољу људи да се слободно изразе и формирају односе, укључујући можда и најбитнију грађанску сферу, која је неопходна за здравље сваке демократије.[109]

2. Дипфејк у судским поступцима

Како методе које се користе за креирање дипфејкова брзо напредују, за судове ће постати изазов да одвоје праве доказе од лажних, а све већа употреба технологије ВИ резултираће повећањем лажног доказног материјала у правним и судским поступцима.

На суду се обично верује да су аудио-визуелни докази аутентично представљање одређеног догађаја. Да ли је предметни снимак добијен из телефона осумњиченог, преузет са друштвених мрежа или добијен са надзорне камере продавнице у близини места извршења кривичног дела - аутентичност приказане сцене обично се не доводи у питање. Са порастом дипфејкова ово ће се несумњиво променити. [110]

Дипфејк садржај може утицати и на грађанске и на кривичне поступке. Међутим, док грађански поступци могу чешће настати поводом процеса креирања дипфејкова, у кривичним поступцима дипфејк се може користити као алат за извршење неког другог

[108]Покушај откривања лажи може имати потенцијално погубан утицај по јавно мњење јер је често једном изречену лаж тешко доказати, што даље може учврстити веровање јавности да је лице које износи лажи кредибилно те да се против њега води организована медијска хајка.
[109]The European Data Protection Supervisor - EDPS Opinion on online manipulation and personal data. Mart 2018, стр. 3
[110]Facing reality? Law enforcement and the challenge of deepfakes, An Observatory Report from the Europol Innovation Lab, https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf стр 14, приступљено дана 12.01.2022

кривичног дела, попут преваре или дечје порнографије. [111]

У поступку из британске суднице који се водио поводом старатељства над децом, мајка деце навела је да је њен бивши муж насилан, а као доказ је приложила аудио запис на коме се могло чути како јој исти прети. Адвокат супруга је, ангажовањем форензичких стручњака открио да је мајка деце садржај модификовала користећи софтвер и водиче доступне на интернету како би креирала дипфејк односно да је у питању била јефтинија и мање софистицираније варијанта дипфејка.[112] Опасности оваквог поступања су двојаке, по суд, доношење одлука на основу манипулисаног аудио/видео садржаја доводи до погрешне и крајње неправичне одлуке, са друге стране, невина особа била би окарактерисана као насилна и агресивна што може довести до репутационе штете и низа других друштвених и пословних непогодности за лице коме се то дешава.

У погледу будућности судских поступака, дипфејк ће несумњиво дотаћи све који учествују у суђењу: адвокати ће покушати да уведу или искључе видео записе као доказ, вештаци и сведоци ће сведочити о аутентичности, а судије ће ценити доказе и одлучивати о томе да ли је један видео материјал прихватљив у циљу доношења пресуде. [113]

Такође, неће се сви поступци завршити као онај из британске суднице јер је манипулисане доказе тешко открити будући да њихова детекција захтева технолошке и процедуралне мере у циљу потврде аутентичности материјала. Осумњичени са друге стране може тврдити да је одређени доказ лажан што може ометати ефикасно кривично гоњење. Тужилаштво ће, уместо да доказује да је окривљени извршио кривично дело, сада морати да утврђује да ли су докази аутентични. Додатно, аутентификација аудио-визуелног материјала може довести до великих трошкова за учеснике у поступку који ће да плаћају форензичке екпсперте који би утврђивали ваљаност доказа и да ли су исти на неки начин модификовани. [114]

[111] Agnes E. Venema and Zeno J. Geradts, Digital Forensics, Deepfakes, and the Legal Process, https://www.essentialresearch.eu/wp-content/uploads/2020/07/Digital-Forensics-Deepfakes-and-the-Legal-Process-Venema-Geradts2020.pdf стр. 16, приступљено дана 12.01.2022.

[112] https://www.abajournal.com/web/article/courts-and-lawyers-struggle-with-growing-prevalence-of-deepfakes приступљено дана 16.01.2023.

[113] Pfefferkorn, Riana, 'Deepfakes' in the Courtroom (October 1, 2020). Boston University Public Interest Law Journal, Vol. 29, No. 2, 2020, стр. 245-275 стр. 254,

[114] European Parliamentary Research Service, 'Tackling deepfakes in European policy', 2021 https://www.europarl.europa.eu/RegData/etudes стр 55. Приступљено дана 16.01.2023.

Један од начина на који би се судови заштитили од оваквих појава јесте употреба алата ВИ за идентификацију манипулисаних доказа. Као други наводи се сведочење под заклетвом (о томе да је материјал у поступку лажан). Ова стратегија, међутим, може бити ризична нарочито када се као сведоци позивају појединци за које је познато да имају проблема са кредибилитетом, [115] чак и када је њихово сведочење истинито или лица која су по закону искључена или ослобођена од дужности сведочења.

Најзад, постоји шири утицај који превазилази појединачне судске случајеве јер живимо у времену у коме већина људи конзумира више лажних него истинитих информација. Како постаје све теже проценити шта је истинито, судови би требало да почну да доводе у питање аутентичност сваког аудио/видео доказа. Људи ће, са друге стране почети да сумњају и у непромењен садржај јер сада знају да су реалистични дипфејкови могући што ће у крајњој линији имати потенцијално корозивно дејство и на правосудни систем који је већ рањив што може угрозити владавину права и закона.[116]

Како се одређена кривична дела сада чешће врше дигиталним алатима, утицај дигиталне технологије, сложена природа доказа и способност судија да их разумеју захтевају ново разматрање. И док често дипфејк материјал неће бити једини доказ који ће бити представљен у судници, неминовно ће постати још један аспект у даљој дигитализацији наших живота, у кривичним делима која су почињена и на крају у систему кривичног правосуђа.[117]

У светлу наведеног, можемо закључити да манипулација садржајем може резултирати доношењем судских одлука које се темеље на овим доказима због чега лица која управљају поступком морају узети у обзир рањивост манипулације друштвеним подацима и истовремено бити свесна колико је лако модификовани материјал представити као лажни доказ који може довести до погрешне судске одлуке. Управо због тога, дипфејк захтева нашу пуну пажњу и подразумева да фотографије, аудио и видео записи морају да прођу кроз процес аутентификације пре него што се нађу представљени као доказ на

---

[115]Pfefferkorn, Riana, 'Deepfakes' in the Courtroom (October 1, 2020). Boston University Public Interest Law Journal, Vol. 29, No. 2, 2020, Available at SSRN: https://ssrn.com/abstract=4321140 стр 245-275, стр.262,

[116]European Parliamentary Research Service, 'Tackling deepfakes in European policy', 2021 https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pd стр. 55. приступљено дана 16.01.2023.

[117]https://www.essentialresearch.eu/wp-content/uploads/2020/07/Digital-Forensics-Deepfakes-and-the-Legal-Process-Venema-Geradts 2020.pdf стр. 17. приступљено дана 16.01.2023.

суду односно да њихова истинитост претходно мора бити утврђена.[118]

3. Дипфејк у пословном окружењу

Још једна негативна последица експанзије дипфејк технологије јесте да се она може користити за саботажу пословних конкурената. У хипотетичком сценарију на дипфејк видео снимку можемо видети како се извршни директор конкурентске компаније понаша непримерено, купује психоактивне супстанце, унајмљује малолетне девојке ради проституције, изговара расне увреде или даје мито државном службенику. На овај начин се циљано могу ометати компаније које се налазе у процесу преговарања ради спајања или оне које су у поступку наметања за велике државне уговоре и тендере. Не само велике компаније већ би и мали привредници и њихове делатности и пословне прилике могле бити осујећене чак и ако се видео снимци евентуално разоткрију као лажни. [119]

Осим саботаже конкурената, дипфејк се такође може користити како би се остварила одређена финансијска добит или са како би се манипулисало тржиштем. Нпр. након што је лажна порука кружила апликацијом „Вотсап“ током 2019. године, у којој је било наведено да је британска Метро банка изгубила на ликвидности, њени корисници су масовно похрлили у исту како би повукли свој новац и драгоцености што је на крају резултирало падом профита банке за 9%. [120]

Осим у области пословања, дипфејк може нарушити и поверење у велики број јавних и приватних институција и установа које могу имати проблема да задрже поверење својих корисника. Лако је замислити, посебно у тренутној политичкој клими, лажни, дипфејк видео који показује службенике граничне полиције који се расистички опходе према мигрантима или се насилно понашају према детету задржаном на граници. Нарочито у местима где већ постоји јак наратив неповерења или екстремистичких

[118]Celebi, Naciye, Qingzhong Liu, and Muhammed Karatoprak. "A Survey of Deep Fake Detection for Trial Courts." (2022). Стр. 227-238, стр. 230.
[119] Danielle K. Citron & Robert Chesney, Deep Fakes: A Loomincg Challenge for Privacy, Democracy, and National Security, 107 California Law Review стр. 1753-1820. стр. 1775.
[120]van der Sloot, B., & Wagensveld, Y. (2022). Deepfakes: Regulatory challenges for the synthetic society. Computer Law & Security Review, 46, 1-15. https://doi.org/10.1016/j.clsr.2022.105716 приступљено 17.11.2022.

схватања, провокативни дипфејк материјал ће наћи публику која га радо чека. Приватни сектор је једнако рањив. Уколико једна институција има значајну улогу у друштву, било на националном или локалном нивоу, представља потенцијалну мету. Штавише, такве институције су због својих активности већ подложније нападима, па би ускоро могле и да се суоче са насртајима у виду дипфејкова. Неће остати имуне ни верске институције као и субјекти који су на било који начин политички ангажовани.[121] Додатно, сексуално експлицитни дипфејк видео снимци се могу замислити у великим корпорацијама као средство за сексуалну експлоатацију или дискриминацију на радном месту.[122]

Треба напоменути да дипфејк неће имати само утицај на међународну политичку сферу где може нпр. довести до затегнутих дипломатских односа између две државе или подстаћи оружани сукоб. Осим општег неповерења у поузданост видео снимака, дипфејк може довести и до невољности или одбијања међународне заједнице да интервенише у одређеним подручјима јер им је нпр. достављен видео или аудио материјал који наводно приказује извршење геноцида или других масовних кршења људских права, а чија је аутентичност тешко проценљива.[123]

Актуелно је и пружање услуга које су дизајниране искључиво са циљем манипулације јавног мњења у корист клијената, јавних и приватних, или са циљем наношења штете пословним конкурентима као што је већ поменуто. Преваре, нарочито у сфери банкарства ће постати лакше и учесталије, али неће остати имуне и друге области чији је процес рада убрзаном дигитализацијом почео да се све више обавља на даљину.[124] Компаније би, услед експанзије дипфејка, осим трошкова за куповину алата и софтвера којима се штите од малициозних материјала и напада, имале и додатне трошкове ради уклањања таквог садржаја, док ће се истовремено правни трошкови и трошкови

[121] Danielle K. Citron & Robert Chesney, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 California Law Review стр. 1753-1820, стр. 1779.
[122] Meskys, Edvinas and Kalpokiene, Julija and Jurcys, Paulius and Liaudanskas, Aidas, Regulating Deep Fakes: Legal and Ethical Considerations (December 2, 2019). Journal of Intellectual Property Law & Practice, Volume 15, Issue 1, January 2020. стр. 6. https://ssrn.com/abstract=3497144 приступљено 18.11.2022.
[123]de Ruiter, A. The Distinct Wrong of Deepfakes. Philos. Technol. 34, (2021). https://doi.org/10.1007/s13347-021-00459-2, стр. 1311–1332, стр. 1317.
[124] The Global Risks Report 2022 17th Edition, world economic forum, The Global Risks Report 2022 стр. 49, https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf приступљено дана 16.01.2023.

управљања кризним ситуацијама такође нагомилати. Чак и када компанија докаже да је била жртва дипфејка штета по њен имиџ већ ће бити учињена, а она потенцијално може остати без прихода и корисника. [125]

4. Преваре и крађе идентитета посредством дипфејка

Несумњиво је да ће појединци и компаније убрзаним ширењем дипфејка постати жртве преваре док ће истовремено трпети штету од лажних вести учињених путем ове технологије. Видео снимци у којима се нпр. намерно наводе лажне процене зараде компанија могу да угрозе цене акција, док би лажни видео снимци директора у компромитујућим ситуацијама свакако утицали на њега као појединца али и на репутацију и профит његове фирме. Појавиле су се и алгоритамске уцене у којима се менаџерима компанија нуди избор – да плате одређени новчани износ како би спречили даље ширење дипфејка или трпе веома јавне последице.[126]

Дипфејк је потенцијално опасан у бројним индустријама, међутим, индустрије које раде са великим количинама личних информација и података су посебно рањиве. Сајбер криминалци користе дипфејк како би украли идентитет, извршили превару, остварили лажна потраживања или украли личне налоге. Уколико ови покушаји преваре буду успешни, могу се користити за стварање лажних (синтетичких) идентитета у великим размерама, што криминалцима може омогућити да нпр. оперу новац стечен криминалним активностима на начине које раније нису били могући. Тако је почетком 2020. године, менаџер једне банке у Хонг Конгу добио позив од лица које се представило као клијент банке, са захтевом да одобри трансфер средстава за предстојећу аквизицију. Криминалци су користећи софтвер вештачке интелигенције који је опонашао глас клијента, преварили банку за суму од 35 милиона долара, а новцу се након преноса није моглоући у траг.[127]

Ситуација се додатно погоршала појавом софтвера и апликација које могу изменити лик особе у реалном времену нпр. приликом видео или конференцијског позива што

[125] https://www.marshmclennan.com/insights/publications/2020/october/digital-deception--is-your-business-ready-for-deep-fakes-.html приступљено дана 16.01.2023.
[126] Kietzmann, Jan, Linda W. Lee, Ian P. McCarthy, and Tim C. Kietzmann. "Deepfakes: Trick or treat?." Business Horizons 63, no. 2 (2020): стр. 135-146, стр. 143.
[127] https://rb.gy/vgjlcm приступљено дана 08.10.2022.

просечној особи може деловати прилично уверљиво па су захваљујући појави ових алата сајбер криминалци добили додатну заштиту приликом остваривања и извршења кривичних дела.

На овај начин ће се „дигитално лажно представљање у реалном времену“ користити не само за извршење превара где се нпр. захтева хитни банкарски трансфер средстава (криминалцима) већ и са много малициознијим намерама где се нпр. објављује банкрот једне компаније како би се потенцијално дестабилизовало једно тржиште.[128]

Још једна технологија од које су сајбер криминалци имали користи је ГАН. Његова употреба нарочито за креирање дипфејка постала је лака и доступна током последњих година. ВИ може имати и разорни ефекат по националну безбедност једне државе и њене институције. Релативно је познато да шпијуни често користе платформу „Линкдин“ како би ступили у контакт са својим метама међутим, иако могу искористити насумичне фотографије било које особе како би креирали свој налог, коришћење вештачке интелигенције и синтетичког идентитета постаје нешто што ћемо тек виђати у будућности. Тако се рецимо лажни профил на овој мрежи, са именом Кејти Џоунс, повезао са бројним политичким стручњацима у Вашингтону попут владиних личности као што су помоћник сенатора, заменик помоћника државног секретара или економиста који је у том тренутку био потенцијални кандидат за радно место у Федералним резервама САД-а[129]

Стручњаци који су прегледали активности профила Кејти Џоунс навели су да је њена профилна слика направљена од стране софтвера ВИ, конкретно путем поменутог ГАН-а, те да права особа са таквим ликом највероватније не постоји, односно да се ради о јединственом случају синтетичке крађе идентитета посредством вештачке интелигенције.

Иако (за сада) ретки, овакви случајеви показују пун потенцијал коришћења технологије ВИ са циљем стварања лажног идентитета који осим очигледних последица за појединца, може имати импликације и по безбедност једне државе. Тако је нпр. пензионисани официр америчке обавештајне службе „ЦИА“ осуђен на 20 година затвора због преношења детаља познанику на друштвеној мрежи о тајним операцијама које је ова агенција обављала у Пекингу, а познанство је почело када га је кинески агент који се

[128] de Ruiter, A. The Distinct Wrong of Deepfakes. Philos. Technol. 34, (2021). https://doi.org/10.1007/s13347-021-00459-2, стр. 1311–1332, стр. 1318.
[129] https://rb.gy/ebwkdv приступљено дана 09.10.2022.

представљао као регрутер контактирао управо на платформи „Линкдин“.[130]

5. Дипфејк порнографија

Од Мерилин Монро чије су голишаве фотографије објављене на насловној страни магазина „Плејбој“ без њене сагласности давне 1953. године до Ванесе Вилијамс која је изгубила титулу „Мис Америка“ због процурелог видео снимка сексуалног односа 1984. године, порнографски материјал пласиран без сагласности учесника у њему (non-consensual pornography)[131] је дуго утицао махом на жене и то много пре ере интернета. [132]

Традиционална „фотошоп“ *(„Adobe Photoshop“)* технологија која је била доступна деценијама полако пада у заборав, а вештачка интелигенције која се користи за стварање видео записа (у првом реду дипфејкова) који су много више софистицираније постаје актуелна.[133] Иако је донедавно употреба дипфејк технологије била ограничена углавном на заједницу која се бави развојем вештачке интелигенције можемо рећи да је историја порнографског дипфејка - историја самог дипфејка. Тако је 2017. године корисник платформе „Редит“ познат по корисничком имену “***deepfakes***” развио исту технологију уз помоћ бесплатног и отвореног кода компаније „Гугл“ на бази машинског учења под називом „TensorFlow“. Своју креацију одмах је употребио како би ставио лица познатих особа на тела глумица у порно филмовима. Бројни медији су потом известили о овом феномену, називајући га дипфејк. Иако је „Редит“ забранио овакве видео снимке, пре свега због кршења права на приватност, а затим и постојања порнографских снимака који су настали без сагласности глумица, штета је већ била учињена а дипфејк пуштен у свет.

Већ јануара 2018. године направљена је бесплатна и усавршена апликација за креирање дипфејк садржаја под називом „FakeApp“ чиме је креирање истих постало лако доступно свакоме ко има приступ интернету и фотографијама особа које жели да види у

[130] https://apnews.com/article/ap-top-news-artificial-intelligence-social-platforms-think-tanks-politics-bc2f19097a4c4fffaa00de6770b8a60d приступљено дана 17.01.2023

[131] Онлајн дистрибуција сексуално експлицитних фотографија или видео записа без пристанка појединца на сликама или видео снимку.

[132] Sophie Maddocks (2022) Feminism, activism and non-consensual pornography: analyzing efforts to end “revenge porn” in the United States, Feminist Media Studies, 22:7, 1641-1656, DOI: 10.1080/14680777.2021.1913434 приступљено дана 20.01.2023.

[133] McGlynn, C., Rackley, E., Johnson, K., Henry, N., Flynn, A., Powell, A., ... & Scott, A. (2019). Shattering lives and myths: a report on image-based sexual abuse. стр 2.

својој креацији,[134][135] а као прве мете дипфејка јавиле су се познате личности попут глумица Еме Вотсон и Скарлет Јохансон, певачице Кејти Пери али и политичари као што су амерички председници Барак Обама и Доналд Трамп.[136]

Ови примери истичу важну тачку - родну димензију искоришћавања путем технологије дипфејка. По свој прилици, већина жртава лажних, сексуално експлицитних видео снимака ће бити женског пола. Ово је свакако случај и са сајбер прогањањем и осветничком порнографијом, а вероватно ће и надаље бити случај са дипфејк видео записима порнографске природе. Лако се може замислити оваква врста видео материјала у коме се жена подвргава насилним, понижавајућим сексуалним чиновима па можемо закључити да неће сви дипфејк снимци бити дизајнирани првенствено, или уопште за творчево сексуално или финансијско задовољство већ да ће многи од њих бити креирани и као оружје за застрашивање или наношење бола жртви. С обзиром на стигму која постоји око сексуално експлицитних слика, посебно за жене и девојке, појединци приказани у оваквим садржајима осим очигледних последица, такође могу да пате од штетних нуспојава овог феномена нпр. на тржишту рада. [137]

Извештај компаније за сајбер безбедност „Deeptrace“ показао је да током 2019. године идентификован 14.678 дипфејк видео снимак на бројним интернет платформама и порно сајтовима, што је било повећање од 100 % у односу на претходна мерења од 7.964 таквих видео снимка обављених у децембру 2018. године. Истраживање је такође открило да су већина субјеката ових видео снимака, пуних 96 % - жене, углавном познате личности, и да је исти проценат дипфејк видео снимака било порнографске природе и без пристанка учесника у њима. Четири најпосећенија веб-сајта посвећена дистрибуцији оваквог материјала забележила су укупно 134 милиона прегледа на таквим видео

[134] Farago, Tunde. "Deep fakes–an emerging risk to individuals and societies alike." Tilburg University (2019). Стр. 1-61, стр. 12-13,
[135] Meskys, Edvinas and Kalpokiene, Julija and Jurcys, Paulius and Liaudanskas, Aidas, Regulating Deep Fakes: Legal and Ethical Considerations (December 2, 2019). Journal of Intellectual Property Law & Practice, Volume 15, Issue 1, January 2020, Pages 24–31., SSRN: https://ssrn.com/abstract=3497144 стр 3-4, приступљено дана 16.01.2023.
[136] Kietzmann, Jan, Linda W. Lee, Ian P. McCarthy, and Tim C. Kietzmann. "Deepfakes: Trick or treat?." Business Horizons 63, no. 2 (2020): стр. 135-146., стр. 136.
[137] Danielle K. Citron & Robert Chesney, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 California Law Review стр. 1753-1820, стр. 1773
[138] https://www.vox.com/2019/10/7/20902215/deepfakes-usage-youtube-2019-deeptrace-research-report приступљено дана 19.01.2023

„Sensity“, која детектује и прати дипфејкове на интернету, пронашла 85.047 таквих видео снимака на популарним веб сајтовима, са тенденцијом удвостручења на сваких шест месеци. У истраживању из септембра 2019. године иста компанија открила је да 96% лажних видео снимака укључује порнографију без сагласности, а да многи од њих као жртве дипфејк порнографије укључују познате или истакнуте личности. Будући да се овакав материјал углавном креира, поставља и дели анонимно на интернету, долази до потешкоћа у проналажењу откривању њиховог креатора.[139]

Ова технологија се међутим, не користи само на штету глумица и високо позиционираних жена већ и новинарки и активисткиња са циљем вршења притиска на њих што показује пример индијске новинарке Ране Аиуб (Rana Ayyub) која се нашла на мети креатора дипфејка због својих репортажа[140] у априлу 2018. године, а који су је приказали у сексуално експлицитном видео снимку у коме никада није учествовала. У року од 48 сати, дипфејк видео се у Индији толико проширио да су профили новинарке на друштвеним мрежама „Фејсбук“ и „Твитер“ били преплављени претњама смрћу и силовањем. Откривена је њена кућна адреса док се у коментарима тврдило да је доступна за анонимни секс. Овакав догађај је до те мере уздрмао новинарку да је недељама била уплашена да напусти своју кућу из страха од остваривања ових претњи.[141]

Због тога је идеја да се лица могу заменити на било ком делу медијског садржаја (а посебно садржаја за одрасле) посебно забрињавајућа. Потреба за овом појавом, нарочито у оквиру дихотомије мушког задовољства и потрошње, мора се сагледати и у оквиру реторике око родне и визуелне информатичке писмености. Дакле, није довољно само одвраћање и забрана производње и дистрибуције порнографских дипфејкова, већ дуго закаснела дискусија о томе зашто појединци траже и желе да виде ове садржаје у било ком својству.[142] Једном реченицом, не можемо извадити род из порнографије, нити извући

[139] Facing reality? Law enforcement and the challenge of deepfakes, An Observatory Report from the Europol Innovation Lab, https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf стр 11

[140] https://www.indiatoday.in/trending-news/story/journalist-rana-ayyub-deepfake-porn-1393423-2018-11-21 приступљено дана 20.01.2023

[141] All’s Clear for Deepfakes? Think Again, Farid Hany, Chesney Robert, Citron Danielle, May 11, 2020, https://www.ischool.berkeley.edu/news/2020/alls-clear-deepfakes-think-again приступљено дана 22.01.2023.

[142] Wagner, T. and Blewer, A. (2019) “The Word Real Is No Longer Real”: Deepfakes, Gender, and the Challenges of AI-Altered Video. Open Information Science, Vol. 3 (Issue 1). https://doi.org/10.1515/opis-2019-0003 стр. 32-46, стр. 45.

друштво из рода. Као друштвени феномен, порнографски дипфејк је омогућен првенствено од стране мушких потрошача, произвођача, технологије и мизогиније. Штавише, он врло вероватно игра улогу у машинерији која систематски редукује жене (као колективни идентитет) на сексуалне објекте. Стога би било адекватније рећи да је овај феномен високо родно одређен. Иако сваки дипфејк видео можда неће утицати на сваку жену која се појављују у оваквом садржају, феномен као такав је у свом тренутном облику, неодвојив од систематског деградирања жена као колективног идентитета.[143] Осим напретка у области вештачке интелигенције, дипфејкови нам показују прилично јасно жељу да се жене, било оне познате или се налазиле на неки други начин на позицији моћи - ставе у положај експлоатације без сагласности, најчешће сексуалне природе. Такође, можда већи проблем представља брза и широка дистрибуција овог садржаја која се углавном врши преко анонимних извора због чега је врло тешко доћи до креатора оваквог материјала.[144]

Поред доступности и софистицираности технологије, глобално повезивање игра важну улогу у домену дипфејк порнографије јер у првом реду, а највише путем друштвених мрежа, олакшава дистрибуцију овог садржаја. Будући да постоји огромна количина материјала који се дистрибуира путем интернета, мање је контроле па овакав садржај лако може доћи до велике публике остављајући свуда своје трагове и практично онемогућавајући потпуно брисање са интернета[145]

Због стигме која окружује сексуално експлицитни садржај, дипфејк порнографија може имати негативан последице по углед једне особе, а штета по репутацију се може манифестовати на различите начине. Друштво може осудити жртву јер постоје њене интимне слике на интернету које сви могу видети, чак и када се зна да је спорни садржај лажан или на неки начин модификован. Ово може утицати на интимне односе, јер се (потенцијални) партнери можда не могу помирити са чињеницом да постоје сексуално експлицитне слике њиховог партнера на интернету. Такође, може доћи и до смањења

[143] Ohman, Carl. (2020). Introducing the pervert's dilemma: a contribution to the critique of Deepfake Pornography. Ethics and Information Technology. 22. 10.1007/s10676-019-09522-1. Стр. 133-140, стр. 137.
[144] Wagner, T. and Blewer, A. (2019) "The Word Real Is No Longer Real": Deepfakes, Gender, and the Challenges of AI-Altered Video. Open Information Science, Vol. 3 (Issue 1). https://doi.org/10.1515/opis-2019-0003 стр. 32-46, стр. 38.
[145] Regulating Deepfake Technology Legislative possibilities in the Netherlands to obstruct the use of deepfake technology for the creation of non-consensual pornography, Daphne Stevens, Tilburg Law School стр. 11.

изгледа за запослење јер компаније могу да одбију да дају посао особи чије сексуално експлицитне слике постоје на интернету. [146]

Из етичке и нормативне перспективе, дипфејк порнографски видео снимци се пре свега сматрају новим обликом задирања у сексуалну приватност која има непроцењиву функцију у друштву јер се њоме олакшава и постиже развој идентитета, интимност и једнакост, па овакви садржаји могу имати додатне негативне последице у виду сексуалног понижавања и експлоатације, физичког, психичког или финансијског интегритета појединца а нарочито када се јавља у облику осветничке порнографије. [147]

Када већ говоримо о осветничкој порнографији, дипфејк технологија је нераскидиво повезана са истом.[148] ***Осветничка порнографија*** и њен често коришћен синоним - порнографија без сагласности (*non-consensual pornography*) подразумева дистрибуцију сексуално експлицитних слика појединаца без њиховог пристанка. Ово укључује слике које су добијене без пристанка (нпр. скривени снимци или снимци сексуалних напада) као и слике првобитно добијене уз сагласност, обично у контексту приватне или интимне везе (нпр. слике које су споразумно дате интимном партнеру који их касније дистрибуира без пристанка друге стране).[149] Жртве ове појаве боре се са анксиозношћу, а неке пате и од напада панике. Осветничка порнографија се често јавља и као облик насиља у породици јер интимне слике могу настати као резултат принуде насилног партнера, а у бројним случајевима злостављачи прете својим партнерима да ће учинити јавим и доступним њихове интимне слике или видео записе уколико покушају да напусте везу. Иако осветничка порнографија може утицати и на мушкарце и жене, емпиријски докази показују да првенствено погађа жене и девојке односно да као појава представља један облик сајбер узнемиравања и сајбер прогањања чије су жртве претежно жене.[150]

[146] Ibid, стр. 14
[147] Meskys, Edvinas and Kalpokiene, Julija and Jurcys, Paulius and Liaudanskas, Aidas, Regulating Deep Fakes: Legal and Ethical Considerations (December 2, 2019). Journal of Intellectual Property Law & Practice, Volume 15, Issue 1, January 2020, Pages 24–31., Available at SSRN: https://ssrn.com/abstract=3497144 стр. 6
[148] Ibid, стр. 5
[149] Citron, Danielle Keats and Mary Anne Franks. "Criminalizing Revenge Porn." Wake Forest Law Review 49 (2014): 345. стр. 1.
[150] Ibid, стр. 4-5

V. ПОЗИТИВНА ПРИМЕНА ДИПФЕЈК ТЕХНОЛОГИЈЕ

„ Ако једног дана (можда) умрем, иако је то мало вероватно, надам се да ће људи по кафићима Фигуераса рећи: Дали је умро, али не сасвим"

-Салвадор Дали

1. Уметност

Иако се због озбиљности и далекосежности последица које узрокује стварање и објављивање дипфејка углавном ставља акценат на његове негативне стране, било би сасвим неправедно не поменути области у којима дипфејк може бити од користи - од образовања преко медиине до уметности.

У области уметности ова технологија до сада се могла видети само у високобуџетним холивудским филмовима где је раније била позната под именом „компјутерски генерисане слике“ (*computer-generated imagery или CGI*). Међутим, бржи процесори, графичке картице високих перформанси и паметнији алгоритми учинили су је доступнијом обичном кориснику па сада свако са елементарним информатичким знањем може преузети апликацију за креирање дипфејка, пратити водич за његово стварање а видео снимци креирани на овај начин могу се користити у најразноврсније сврхе.[151]

У филму се дипфејк може користити за процес преокретања старења и креирање млађе верзије глумаца али се њиме могу уређивати и филмске сцене у случајевима када не постоји могућност да глумац (физички) учествује у њима. На пример, након што је глумац Пол Вокер преминуо сцене у којима је требало да учествује креиране су тако што су његове слике из времена док је био жив модификоване методама компјутерске графике чиме је омогућено да се филм без његовог присуства заврши.[152] Такође, гледаоци филмова „Ратови звезда“ су у филму „Rogue One: A Star Wars Story“ могли видети посредством дипфејк технологије лик принцезе Леје из оригиналне триологије (снимане током седамдесетих и осамдесетих година) иако је глумица Кери Фишер имала близу

[151] Maras, Marie-Helen & Alexandrou, Alex. (2018). Determining Authenticity of Video Evidence in the Age of Artificial Intelligence and in the Wake of Deepfake Videos. International Journal of Evidence and Proof. 23. 10.1177/1365712718807226. Стр. 256

[152] https://www.looper.com/184468/the-truth-about-recreating-paul-walker-for-fast-and-the-furious/ приступљено дана 28.01.2022.

60 година када је наставак овог филма сниман.[153]

Још један пример најсавременије употребе технике засноване на вештачкој интелигенције и дипфејку у уметничке сврхе је пројекат *„Дали живи“* у Дали музеју („Salvador Dalí Museum“) на Флориди. Осим колекције Далијевих радова које овај музеј поседује, посетиоцима је омогућено и да доживе његову ексцентричну личност. Овај пројекат даје гостима музеја прилику да са сликаром који је преминуо 1989. године, комуницирају на један изузетно реалистичан начин па тако имају јединствену прилику да сазнају више о Далијевом животу и раду од особе која га је најбоље познавала - самог уметника. На крају обиласка музеја дипфејк Дали чак пита посетиоце да ли желе селфи са њим који им касније може прослеђен путем мејла.[154][155] За овај пројекат коришћено је више од 6000 кадрова и преко 1000 сати машинског учења како би се обучио алгоритам ВИ да овлада Далијевим лицем и његовим јединственим цртама. Процес је употпуњен и софистицираним звучним инжењерингом па тако дипфејк Салвадор Дали може изговорити потенцијалних 190.512 комбинација реченица, а посетилац може доживети широк спектар одговора, расположења и емоција.

2. Образовање

Дипфејк технологија ствара низ могућности и у сфери образовања, у првом реду за наставнике и професоре, укључујући способност да се студентима пруже информације о битним догађајима на један савремен и убедљив начин, у односу на традиционална предавања. Употребом вештачке интелигенције могуће је произвести видео записе о историјским личностима које се обраћају и предају директно студентима[156] па би овакво јединствено и интерактивно искуство удахнуло иначе монотоним предавањима једну сасвим нову димензију.

Један од позитивних примера коришћења ове технологије налази се Музеју

[153] https://www.technologyreview.com/2018/10/16/139739/how-acting-as-carrie-fishers-puppet-made-a-career-for-rogue-ones-princess-leia/ приступљено дана 28.01.2023.
[154] https://thedali.org/press-room/dali-lives-museum-brings-artists-back-to-life-with-ai/ приступљено дана 28.01.2023
[155] више на https://youtu.be/mPtcU9VmIIE
[156] Danielle K. Citron & Robert Chesney, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 California Law Review. Стр. 1753-1820 стр. 1769.

холокауста, у близини Чикага где посетиоци могу непосредно разговарати за особама које су преживеле холокауст управо захваљујући вештачкој интелигенцији. Након опширних разговора са 15 преживелих, истраживачи су креирали њихове холограме који раде на принципу технологије личних асистената попут „Сири“ или „Алекса“ које користе компаније „Епл“ и „Амазон“. На самом почетку егзибиције посетиоцима се приказује кратак филм у коме свако од преживелих приповеда своју причу након чега посетилац има прилику и да поставља питања о њиховом искуству током Другог светског рата. [157]

Овакве могућности од изузетног су значаја будући да је од окончања Другог светског рата протекло близу 80 година те да постоји занемарљив број преживелих. Додатним протоком времена многа драгоцена сведочанства жртава холокауста и других злочина потенцијално могу нестати па новим генерација коришћење оваквих технологија и у ове сврхе представља један од начина на које могу веродостојно сазнати[158] (директно од преживелих) о историјским догађајима, уместо што би то учинили посредно путем филмова, књига или новина.

3. Медицина

Не само у области образовања и уметности, основна технологија машинског учења и дипфејка имаће делотворан утицај и у сфери медицине. Једна таква могућност је коришћење технике дубоког учења за синтезу реалистичних података који ће помоћи истраживачима да развију нове начине лечења болести без уобичајених стварних података о пацијентима. Рад у овој области, између осталог већ су обавиле клиника „Мејо“(„Mayo Clinic“) и компанија „Енвидиа“ („NVIDIA“) која се бави производњом графичких процесора, а које су 2018. године сарађивале на коришћењу ГАН-а за креирање „лажних“ снимака мозга са магнетне резонанце.[159] Истраживачи су обучавали алгоритме на медицинским снимцима од којих је само 10% било стварно и дошли до закључка да су ови алгоритми постали једнако добри у уочавању тумора као и алгоритми обучени само на

[157] https://www.timesofisrael.com/at-this-holocaust-museum-you-can-speak-with-holograms-of-survivors/ приступљено дана 19.01.2023.
[158] више на https://www.ilholocaustmuseum.org/exhibitions/the-journey-back-a-vr-experience/
[159] ГАН технологија је искоришћена и за креирање синтетичких медицинксих података ради истраживања, детекције и третмана болести јетре.

стварним односно постојећим снимцима мозга. Овакве апликације су вероватно само почетак улоге дубоког учења у медицини.[160]

Поред горенаведене сврхе, употреба дипфејк генерисане слике такође се може користити за идентификацију и помоћ у истраживањима у случајевима када нема довољно стварних података за даљу анализу и упоређивање. [161]

Можда најважније, (аудио) дипфејк технологија делује обећавајуће у погледу враћања способности говора особама које пате од болести узроковане дегенерацијом моторних неурона и одређених облика парализе попут амиотрофичне латералне склерозе или Лу Геригове болести[162] будући да је један од најразорнијих и крајњих исхода ове болести губитак способности говора. Идентично процесу стварања аудио дипфејка, овим пацијентима се говор може „вратити" коришћењем вештачке интелигенције у комбинацији са техником званом **гласовно банкарство** (*voice banking*)[163]. Аудио снимке говора пацијента (пре него што се болест сасвим развила) лекари могу искористити као узорке како би створили синтетички глас који особа са овом болешћу може касније користити у комуникацији у случају да се њено стање погорша.[164]

[160]https://www.forbes.com/sites/simonchandler/2020/03/09/why-deepfakes-are-a-net-positive-for-humanity/?sh=6638d6812f84 приступљено дана 22.01.2023

[161]Traboulsi, Nicole. "Deepfakes: Analysis of Threats and Countermeasures." PhD diss., California State University, Fullerton, 2020.стр. 29.

[162] Danielle K. Citron & Robert Chesney, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 California Law Review стр. 1753-1820 стр. 1771.

[163]Гласовно банкарство је процес стварања персонализованог синтетичког гласа односно синтетичке копије природног гласа особе. Како би синтетички глас настао потребно је прикупити а потом и снимити одређени скуп фраза, најчешће између 350 и 1600.

[164]https://www.engadget.com/2019-12-18-rolls-royce-quips-als-mnd-speech-ai.html?guccounter=2 приступљено дана 19.12.2022.

VI. ОТКРИВАЊЕ, МОГУЋА РЕШЕЊА И БУДУЋНОСТ ДИПФЕЈКА

1. Детекција дипфејка

Осим што пружа могућност креирања дипфејка, иста технологија би такође могла да буде искоришћена у поступку њиховог откривања. Тренутно (и углавном) још увек можемо да уочимо модификоване садржаје због малих грешака које видимо на њима попут недостатака трептања или недоследности између говора и покрета уста. Међутим, како ова технологија еволуира и испоручује снимке који су све квалитетнији, постаје све теже уочљиво када су одређени медији лажни. Управо из тог разлога важно је креирати и користити мере детекције које су у стању да открију овакве садржаје, чак и када су неприметни голим оком. Штавише, технологија детекције мора ићи у корак са иновацијама у дипфејку, а једном када се створи требало би је стално обучавати и ревидирати како је не би надмашио развој дипфејк технологије.[165]

Постоје два различита приступа детекцији дипфејк материјала: *ручно* и *аутоматско* откривање. Ручну детекцију обавља особа која је квалификована да прегледа видео материјал и потражи недоследности или знаке који могу указивати на модификовани садржај. Овај приступ је изводљив када се ради о малим количинама сумњивих материјала међутим, није компатибилан се аудио-визуелним материјалима који се користе данас па овај поступак не представља адекватно решење на друштвеном нивоу.[166] Аутоматска детекција претпоставља постојање софтвера такође на бази вештачке интелигенције који са одређеним процентом може показати да ли је представљеним садржајем на неки начин манипулисано. Нпр. софтвер би нам рекао да је вероватноћа да је одређени видео аутентичан/није модификован износи 73%. Проблем са овим приступом је да ли се може прихватити „проценат истине“ односно у ком проценту истине судија или нпр. новинар могу да прихвате поузданост извора?[167]

Методе које се користе за детекцију дипфејка ослањају се на углавном на визуелне

[165]Regulating Deepfake Technology Legislative possibilities in the Netherlands to obstruct the use of deepfake technology for the creation of non-consensual pornography, Daphne Stevens, Tilburg Law School, стр. 33.
[166] Das, Djurre & van Boheemen, Pieter & Linda, Nierling & Jahnel, Jutta & Karaboga, Murat & Fatun, Martin & Huijstee, Mariëtte. (2021). Tackling Deepfakes in European policy. стр. 17.
[167] van der Sloot, B., & Wagensveld, Y. (2022). Deepfakes: Regulatory challenges for the synthetic society. Computer Law & Security Review, 46, 1-15.

објекте створене приликом постављања лажног лица на циљно лице. Они су значајни јер представљају информације које недостају и које ДНМ нису уочиле у подацима о обуци нпр. јер је један објект скривен иза другог[168] (нпр. уво је скривено иза прамена косе).

Упркос негативним аспектима, вештачка интелигенција направила је значајан напредак у анализи аудио и видео садржаја. Узмимо за пример платформу „Јутјуб“ која може аутоматски да генерише превод из звука са неког видео снимка, скенира кључне речи и категорише садржај. Ова иста технологија може се користити нпр. за откривање фишинг напада тако што ће их аутоматски детектовати и блокирати, док методе аутентификације попут блокчејна, могу бити кључни фактор у борби против дипфејк напада. Блокчејн[169] се у ову сврху може користити на неколико начина. Првенствено може тражити од корисника да пружи доказ о свом идентитету пре него што му дозволи да шири садржај под својим именом док се блокчејн апликације могу користити како би се проверило да ли је садржај у некој датотеци фалсификован или модификован у односу на његову оригиналну верзију[170]

Тренутне методе детекције дипфејка не могу открити сваки модификовани садржај али како се технологија буде развијала у будућности и уз одговарајући безбедоносни кадар, организације би могле да релативно успешно открију дипфејкове и смање утицај будућих напада заснованих на идентитету и то са високим степеном ефикасности. Овде је акценат је на финансијским институцијама које нарочито морају бити обазриве приликом укључивања нових клијената како би спречиле покушаје лажног представљања, синтетичке идентитете или преваре.[171]

Већина предложених метода детекције, као и сам дипфејк, засноване су на вештачкој интелигенцији и машинском учењу међутим, биће потребно доста времена за обуку ових модела. Слично процесу креирања дипфејка, алгоритми за откривање морају проћи кроз фазу обуке која може резултирати прикупљањем велике количине корисничких личних података и који потенцијално могу нарушити приватност корисника.[172]

На крају, будући да су дипфејкови усавршени коришћењем технологије генеративних

[168] Nassif, Ali & Nasir, Qassim & Abu Talib, Manar & Gouda, Omar. (2022). Improved Optical Flow Estimation Method for Deepfake Videos. Sensors. Стр. 2.
[169] Блокчејн је назив за базу података која се не налази на једном месту, већ се састоји од мањих база које су међусобно повезане и које садрже информације о дигиталним трансакцијама.
[170] https://www.darkreading.com/operations/preparing-for-the-next-cybersecurity-epidemic-deepfakes приступљено дана 25.01.2023
[171] https://venturebeat.com/security/deepfakes-arent-going-away-future-proofing-digital-identity/ приступљено дана 25.01.2023
[172] https://www.infosecurity-magazine.com/next-gen-infosec/data-protection-wake-deepfakes/ приступљено дана 25.01.2023

адверсаријских мрежа, а како је ГАН дизајниран да стално учи и побољшава своје перформансе, питање је само тренутка када ће дипфејк бити толико убедљив да ћемо га као таквог тешко препознати. [173]

2. Могућа решења

Било која технологија која се може користити за генерисање лажног или обмањујућег садржаја, од фотошопа до дипфејка, може бити злоупотребљена. Иако дипфејк није увек малициозне природе неминовно се мора поставити питање да ли је исти морално погрешан сам по себи. Једна технологија може се сматрати морално погрешном уколико крши моралне норме или има негативне последице које превазилазе њене позитивне ефекте, или нпр. промовише порок, подрива међуљудске односе и фундаменталне друштвене вредности попут поверења и међусобног поштовања. Како деипфејк има и своје добре стране, можемо га квалификовати као морално проблематичан јер технологија која „обмањује" стварањем аудио/видео материјала који није оригиналан у најмању руку јесте морално сумњива будући да обмана крши норме истинитости, може инспирисати лажна уверења или се бити штетна за друштвене односе и поверење.[174]

Мере које укључују одговорна овакве злоупотребе укључују три линије напора:

1. улагање и примену технологија за откривање дипфејка,

2. промену понашања на интернету, укључујући мере политике које оснажују дигиталне кориснике да се критички баве садржајем који им се пласира и које јачају поуздане канале комуникације и

3. креирање и спровођење стандарда дигиталне аутентификације.[175]

Осим што платформе друштвених мрежа предузимају мере у циљу сузбијања дипфејка, важно је подићи свест јавности о овом феномену а нарочито о дипфејк осветничкој порнографији. Можда и најбитније, потребно је да људи постану свесни да није све што виде стварно. На овај начин појединци би могли да се боље заштите јер би били свесни да и

[173] Celebi, Naciye, Qingzhong Liu, and Muhammed Karatoprak. "A Survey of Deep Fake Detection for Trial Courts." (2022). стр. 227-238, стр 230.
[174] de Ruiter, A. The Distinct Wrong of Deepfakes. Philos. Technol. 34, (2021). https://doi.org/10.1007/s13347-021-00459-2, стр. 1311–1332, стр.1318-1319.
[175] Smith, Hannah, and Katherine Mansted. "What's the Problem?" Weaponised Deep Fakes: National Security and Democracy, Australian Strategic Policy Institute, 2020, pp. 04–04. JSTOR, http://www.jstor.org/stable/resrep25129.4. приступљено дана, 09.01. 2023.

сами могу постати жртве. Такође, органи за спровођење закона морају проћи кроз адекватне обуке како би били у стању да препознају и открију модификоване садржаје због чега је јако важна редовна едукација о стању технологије и дешавањима у погледу њеног откривања и детектовања. Ово би им омогућило да се нпр. лакше носе са случајевима дипфејк порнографије јер би знали на шта је потребно обратити пажњу приликом истраживања дипфејка као и које технологије би требало да користе ради његовог откривања.[176]

Будући да са развојем дипфејка напредују и методе за његово откривање, тренутно је нпр. могуће да се онлајн и дигитални садржај верификује коришћењем алгоритама машинског учења, дигиталних кључева или биометријском аутентификацијом попут отиска прста што у некој мери отежава постављање и ширење оваквог садржаја на интернету.

Иако се питање одговорности редовно поставља, врло је тешко идентификовати особу који је креирала или објавила дипфејк. Такође, постоји и сложен проблем уклањања видео записа након његовог објављивања на интернету. Када се видео једном објави на мрежи, тешко га је уклонити, а обично је емоционална и штета по имиџ једне особе већ учињена. У идеалном случају, закон би требало да сматра одговорним појединца који је направио и објавио дипфејк садржај. Међутим, у већини случајева јако је изазовно идентификовати починиоца који га је направио из два разлога. Прво, многе веб странице и платформе као што су „Редит“ и „Твитер“ дозвољавају анонимно постављање садржаја и управо на овим платформама су дипфејк видео снимци доживели свој процват. Друго, креатори дипфејка могу користити софтвере као што је „Тор“ како би ИП *(„IP*“) адресу са које је дипфејк садржај постао доступан учинили непрегледном[177] тј. замаскирали исту.

Додатни проблем који се јавља приликом покушаја откривања креатора дипфејка је да једну ИП адресу (адресу интернет протокола) може користити више особа те да лице које је поставило ову врсту садржаја можда није стварни креатор таквог материјала, што може отежати идентификовање стварног извршиоца дела. На крају, можда и највећа препрека која се јавља узрокована је глобалним карактером интернета, а то је да особа која је објавила садржај можда није у надлежности државе у којој се води истрага или судски поступак. Ово је додатно отежано непостојањем усаглашених правила у вези са дипфејк технологијом на међународном нивоу тако да међународна истрага и сарадња могу бити и више него

[176] Regulating Deepfake Technology Legislative possibilities in the Netherlands to obstruct the use of deepfake technology for the creation of non-consensual pornography, Daphne Stevens, Tilburg Law School стр.35-36.
[177] Delfino, Rebecca. (2020). Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act. Actual Problems of Economics and Law. 14. 10.21202/1993-047X.14.2020.1.105-141. Стр. 887-938, стр. 898-899.

изазовни у овим случајевима.[178]

3. Будућност дипфејка

Појава а потом и експанзија дипфејка поставила је релевантне и сложене правне изазове у циљу њиховог откривања и регулисања. Прво и најважније, многи органи за спровођење закона широм света још увек немају потпуно способне и обучене стручњаке, правни оквир и процедуралне мере пре свега у кривичном законодавству којима би се наредило очување дигиталних доказа и истрага сајбер криминала. Друго, пошто одређени проценат ових напада обично спроводе добро организоване криминалне групе (нарочито оне који се баве стицањем финансијске добити) које се налазе у различитим јурисдикцијама, постоји јасна потреба за међународном сарадњом, а посебно за блиском сарадњом са глобалним провајдерима услуга како би се обезбедили подаци о претплатницима и интернет саобраћају. Такође, потребне су брже и ефикасније истраге, распоређивање заједничких истражних тимова на територијама различитих држава како би се ушло у траг осумњиченим лицима.[179]

С обзиром на тренд слободног објављивања софтвера за креирање дипфејка на интернету, лако је предвидети експанзију дипфејка садржаја. Тренутни тренд креирања програма који су лаки за коришћење такође чини стварање дипфејка нечим што је доступно широј јавности, а не само онима са обимним компјутерским знањем или врхунским хардвером.[180]

Са аспекта вештачке интелигенција а нарочито после појаве ГАН-а, конкуренција између стварања, откривања и превенције дипфејка постала је све жустрија. У будућности, дипфејк технологија не само да ће постати доступнија, већ ће и крериање овакве врсте садржаја постати неупоредиво лакше. Дипфејк ће наставити да еволуира и да се шири, а проблеми попут недостатка детаља у синтези ће бити превазиђени, док ће време обуке и

[178]Regulating Deepfake Technology Legislative possibilities in the Netherlands to obstruct the use of deepfake technology for the creation of non-consensual pornography, Daphne Stevens, Tilburg Law School стр. 15.
[179]Velasco, C. Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. ERA Forum 23, 109–126 (2022). https://doi.org/10.1007/s12027-022-00702-z стр. 113, приступљено дана 09.01.2023.
[180]https://www.essentialresearch.eu/wp-content/uploads/2020/07/Digital-Forensics-Deepfakes-and-the-Legal-Process-Venema-Geradts2020.pdf стр. 17, приступљено дана 09.01.2023.

генерисања садржаја бити значајно смањено. Експерти сматрају да ће управо ГАН бити главни покретач развоја дипфејка у будућности и да ће се његова употреба убрзано повећававати у секторима као што су забава, вести и образовање. Међутим, овај развој догађаја истовремено ће довести до повећања криминалних активности, ширења дезинформација, синтетичке крађе идентитета, превара, мешања у изборне процесе или до политичких тензија. [181]

Како би се штетне последице свеле на минимум и сузбило подривање поверења, ИТ стручњаци, новинари и законодавци играће кључну улогу у образовању јавности о могућим опасностима синтетичких медија. Јавност се са друге стране мора научити да верује само садржају из реномираних извора те да пронађе начине на које може имати користи од дипфејка у будућности.[182]

Како основна информациона и дигитална писменост више не представљају стручно знање а информације постоје у безброј намена и чекају да буду добро уређене - њихова злоупотреба остаје потенцијална. Тако, креирање политике у погледу дипфејка није само обавеза законодаваца већ и креатора, потрошача и дистрибутера овог садржаја. [183] Додатно, капацитет за генерисање дипфејка сигурно ће се брзо ширити без обзира на то који се напори улажу да би се овај процес успорио или зауставио и у првом реду зависи од приступа знању и технологијама као што су поменути ГАН и други облици машинског учења[184]

Органи који се баве истрагама сајбер криминала још увек нису у потпуности спремни да се баве техничким и правним димензијама вештачке интелигенције када се иста користи за извршење кривичних дела. Такође, још увек нема довољно података који би нам указали да ли су органи за спровођење закона широм света добро опремљени и обучени да прикупљају прекограничне доказе за спровођење истрага у случајевима када је систем вештачке интелигенције био укључен у извршење неког кривичног дела али ће будући рад међународних организација попут Савета Европе и Интерпола бити релевантан за креаторе политике и органе за спровођење закона као смерница у примени будућих националних

[181] https://blog.richardvanhooijdonk.com/en/the-good-the-bad-and-the-future-of-deepfakes/ приступљено дана 23.01.2023

[182] https://blog.richardvanhooijdonk.com/en/the-good-the-bad-and-the-future-of-deepfakes/ приступљено дана 22.01.2023

[183] Wagner, Travis L. and Blewer, Ashley. "“The Word Real Is No Longer Real”: Deepfakes, Gender, and the Challenges of AI-Altered Video" Open Information Science 3, no. 1 (2019) стр. 32-46, стр. 44.

[184] Danielle K. Citron & Robert Chesney, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 California Law Review, стр.1753-1820, стр. 1763.

политика о вештачкој интелигенцији. Стварање националних радних група за борбу против сајбер криминала (састављених од органа за спровођење закона, представника правосуђа, стручњака из области технологије ВИ и провајдера) може бити први корак у борби против незаконитог понашања у вези са злоупотребом дипфејка и злоупотребом технологија на бази вештачке интелигенције.[185]

VII. НОРМАТИВНО ПРАВНИ ОКВИР ДИПФЕЈК ТЕХНОЛОГИЈЕ

1. Међународне конвенције

1.1. Конвенција из Будимпеште

Свакако најзначајнији документ у области успостављања стандарда приликом сузбијања високотехнолошког криминалитета јесте *Конвенција Савета Европе о високотехнолошком криминалу* (колоквијално Будимпештанска конвенција)[186] усвојена 23. новембра 2001. године а ступила на снагу 1. јула 2004. године. Њен примарни циљ је усклађивање односно хармонизација националних законодавстава када је реч о материјалним одредбама, затим увођење адекватних инструмената у национална законодавства када је реч о процесним одредбама и на крају установљавање брзих и ефикасних институција и процедура међународне сарадње.[187] У преамбули ове конвенције наглашено је да државе чланице Савета Европе, као и друге државе потписнице имају циљ спровођења заједничке политике у борби против овог глобалног проблема. Први Додатни протокол уз Конвенцију о високотехнолошком криминалу ступио је на снагу 1. марта 2006. године.[188] Он је унео

[185] Velasco, C. Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. ERA Forum 23, (2022). стр. 109–126, стр. 125-126
[186] https://rm.coe.int/1680081561 приступљено дана 03.08.2022. године
[187] Бјелајац, Ж., Матијашевић, Ј., Димитријевић, Д. (2012), Значај успостављања међународних стандарда у сузбијању високотехнолошког криминала. LXIII. 66-84., стр. 71-73.
[188] https://ccdcoe.org/uploads/2018/11/CoE-030128-AdditionalProtocol-1.pdf приступљено дана 06.08.2022. године

новине које се односе на инкриминацију дела расистичке и ксенофобичне природе те инкриминацију у случајевима минимализације, порицања, одобравања и оправдања геноцида и злочина против човечности. Дана 12. маја 2022. године постао је отворен за потписивање и Други додатни протокол уз Конвенцију који је између осталих потписала и Србија. Новине у Другом додатном протоколу односе се на појачану сарадњу и откривање електронских доказа као и појачану прекограничну сарадњу како у хитним случајевима тако и у циљу спровођења заједничких истрага. Овај протокол је у одељку пет регулисао и поступке који се примењују на међународну сарадњу у случају када не постоји важећи међународни споразум и одредио да нпр. сведоци и вештаци могу давати исказе путем видео-конференције. Иако је једна од главних замерки Конвенције била непостојање одредаба које би предвиђале обавезу држава потписница да оснују посебне органе који би се бавили високотехнолошким криминалом,[189] у чл. 12. Другог додатног протокола наведена је могућност да надлежни органи двеју или више страна уговорница (на основу узајамног споразума) могу основати заједнички истражни тим на својим територијама и управљати тим тимом како би се олакшале кривичне истраге или поступци онда када се сматра да је појачана сарадња нарочито корисна, а да су поступци и услови рада заједничких истражних тимова, као што су њихова конкретна сврха, састав, функција, трајање, организација и остале активности, предмет договора између тих надлежних органа. Протокол би званично требало да ступи на снагу када буде ратификован од стране пет држава.[190]

Упркос томе да Будимпештанска конвенција садржи само минимум дефиниција, она ипак криминализује известан број непожељних понашања и квалификује многа кривична дела у вези са садржајем која могу бити применљива и на деликте извршене коришћењем система вештачке интелигенције. ВИ и сајбер криминалитет су феномени којима је потребна даља анализа и детаљна дискусија међу државама потписницама ове конвенције, нарочито узимајући у обзир пораст случајева злоупотребе технологија вештачке интелигеније од стране сајбер криминалаца и извршење кривичних дела против појединаца у сајбер простору. Питања попут одговорности за понашање учињено употребом алгоритама и машинског

[189]Димовски, Д. (2019), Компјутерски криминалитет, Правни факултет Универзитета у Нишу, Зборник, LV, стр. 195-212, стр. 199.
[190]Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, Council of Europe Treaty Series – No. 224.

учења захтевају додатну дискусију и појашњење будући да се регулисање кривичне одговорности у овим сферама значајно разликује у правним системима многих земаља[191]

1.2. Ланзарот конвенција

Иако се директно не бави вештачком интелигенцијом и дипфејком, битно је поменути и *Конвенцију о заштити деце од сексуалне експлоатације и сексуалног злостављања* (тзв. Ланзарот конвенција)[192] која је ступила на снагу 1. јула 2010. године. Конвенција је покушала да изврши хармонизацију националних законодавстава у погледу материјалног кривичног права у оним случајевима у којима се елементи рачунарске технике користе у циљу дистрибуције, размене и складиштења недозвољеног садржаја[193] нарочито узимајући у обзир повећан обим злоупотребе рачунара у недозвољене сврхе. Такође је одредила да би свака уговорна страна требало да предузме неопходне законодавне или друге мере како би подстакла и подржала успостављање информативних сервиса попут телефонских или интернетских линија за помоћ, ради пружања савета позиваоцима, укључујући и поверљиве позиве и уз дужно поштовање њихове анонимности.

Комитет ове конвенције још увек није у потпуности истражио како се одредбе материјалног и процесног кривичног права могу применити у контексту коришћења система вештачке интелигенције или дипфејка у сврхе повезане са децом и криминалом. Иако за сада деца нису примарне жртве дипфејка несумњиво је да ће се ширењем доступности алата за прављење таквих садржаја појавити и дипфејк снимци са децом као главним актерима. Имајући у виду осетљивост ове популације и постојање потребе за посебном заштитом, државе чланице би требало да поведу разговоре како би се не само делило знање о актуелним трендовима међу државама, већ и како би се идентификовало незаконито понашање, злостављање, експлоатација деце путем система вештачке интелигенције[194] и дечја дипфејк порнографија а све са циљем превенције злочина и додатном заштитом деце на интернету.

---

[191] Velasco, C. Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. ERA Forum 23, (2022). https://doi.org/10.1007/s12027-022-00702-z стр. 109–126, стр. 118-119.

[192]Council of Europe, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No. : 201, Lanzarote, the 23 October 2007.

[193]Матијашевић, Ј. оп. цит. стр. 228.

[194] Velasco, C. Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. ERA Forum 23, (2022). https://doi.org/10.1007/s12027-022-00702-z стр. 109–126, стр. 119.

1.3. Истанбулска конвенција

Под окриљем Савета Европе донета је *и Конвенција о спречавању и борби против насиља над женама и насиља у породици* или Истанбулска конвеницица која је потписана 2011. године а ступила на снагу и почела да се примењује од 2014. године. Србија је у октобру 2013. године, донела закон о потврђивању ове Конвенције али је приликом ратификације изразила резерве у односу на два члана Конвенције - члан 30 ст. 2, који се односи на накнаду штете жртвама које нису у могућности да ову накнаду остваре из других извора и члана 44 став 1, тачка е) који се односи на надлежност када је кривично дело почињено од стране лица које борави на територији државе потписнице, док не изврши усаглашавање унутрашњег кривичног законодавства са наведеним одредбама Конвенције.[195]

Конвенција се односи на све видове насиља над женама, укључујући насиље у породици, које жене погађа несразмерно више. На самом почетку Конвенција узима историјски контекст неједнакости између жена и мушкараца и препознаје да је насиље над женама манифестација оваквог односа те да је кључни елемент у превенцији насиља над женама постизање de jure и de facto једнакости између жена и мушкараца. Као главни циљеви Конвенције наводе се: заштита жена од свих видова насиља и спречавање, допринос сузбијању свих облика дискриминације над женама и промоција суштинске једнакости између жена и мушкараца, израда свеобухватног оквира, политика и мера заштите и помоћи свим жртвама насиља над женама и насиља у породици, промоција међународне сарадње у погледу елиминисања насиља над женама и насиља у породици и пружање подршке и помоћи организацијама и органима унутрашњих послова у делотворној сарадњи са циљем елиминисању насиља над женама и насиља у породици.[196]

Истанбулска конвенција не садржи посебне одредбе у контексту дипфејка или насиља почињеног коришћењем информационих технологија, међутим експертска група за борбу против насиља над женама и насиља у породици (*ГРЕВИО*) тренутно анализира приступе за проширење примене ове Конвенције у смеру вршења незаконитих радњи и понашања

[195] Истанбулска конвенција у Србији – пракса и изазови родне равноправности, Комитет правника за људска права – YUCOM, стр 9 https://www.yucom.org.rs/wp-content/uploads/2019/03/Istanbulska-konvencija-u-Srbiji-praksa-i-izazovi.pdf , приступљено дана 29.01.2023.

[196] https://ravnopravnost.gov.rs/wp-content/uploads/2012/11/images_files_zakon%20o%20potvrdjivanju%20konvencije%20saveta%20evrope%20o%20sprecavanju%20i%20borbi%20protiv%20nasilja%20nad%20zenama%20i%20nasilju%20u%20porodici.pdf , https://rm.coe.int/1680462540 приступљено дана 30.01.2023.

коришћењем рачунарских и информационих система у оквиру националних правних оквира држава чланица. Током 2021. године усвојена је Општа препорука о дигиталној димензији насиља над женама која се односи између осталог на примену општих одредаба Истанбулске конвенције у вези злочина почињених над женама у сајбер простору када су и предложене конкретне радње које треба предузети, а на основу четири стуба Истанбулске конвенције: превенција, заштита, кривично гоњење и координиране политике,[197] и које се између осталог ослања и на Конвенцију из Будимпеште о високотехнолошком криминалу.

2. Европска Унија

2.1. Општа уредба о заштити података о личности (ГДПР)

Као кровни документ Европске Уније у области личних података, 27. априла 2016. године донета је *Општа уредба о заштити података о личности* која је почела да се примењује од 2018. године. Уредба је у члану 4. лични податак одредила као сваки податак који се односи на физичко лице чији је идентитет одређен или се може одредити, а физичко лице чији се идентитет може одредити као лице које се може идентификовати посредно или непосредно, посебно помоћу идентификатора попут имена, идентификационог броја, података о локацији, мрежног идентификатора или помоћу једног или више фактора својствених за физички, физиолошки, генетски, ментални, економски, културни или друштвени идентитет тог физичког лица.[198]

Поставља се питање - да ли садржај који је претходно модификован употребом вештачке интелигенције и машинског учења - лични податак? Са једне стране сматра се да оваква врста материјала никако не може представљати личне податке будући да се након модификације садржаја лични подаци из новонасталог садржаја не могу приписати само једној одређеној особи. Са друге стране лични подаци судећи по Директиви не морају бити објективне природе већ се и информације попут личног мишљења, судова или процена могу

[197] Velasco, C. Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. ERA Forum 23, (2022). https://doi.org/10.1007/s12027-022-00702-z, стр. 109–126, стр 120, приступљено дана 30.01.2023.
[198] https://gdpr-info.eu/ приступљено дана 30.01.2023.

сматрати личним податком. У том контексту дипфејк би свакако могли посматрати ширем смислу као креацију која садржи личне податке једног или више лица.

У светлу наведеног, скоро свака радња која се односи на личне податке, укључујући прикупљање и мењање (који су од темељног значаја за креирање дипфејка садржаја) може се сматрати обрадом личних података, а како се дипфејк креира између осталог путем софтвера комбиновањем великог броја личних података попут слика, гласова или видео снимака, нема сумње да се лични једног лица обрађују барем док се креира лажни садржај.[199]

Иако обрада података о личности не представља апсолутно право већ се посматра у складу са функцијом коју има у једном друштву и у складу са начелом пропорционалности, Уредба изричито предвиђа да обрада увек мора бити законита односно почивати бар на једном од шест правних основа од којих се само обрада која потребна ради легитимног интереса чијем остварењу тежи руковалац података или треће лице и обрада података на основу пристанка лица чији се подаци обрађују у одређене сврхе, могу посматрати у контексту дипфејка.

У погледу процеса настанка дипфејк материјала и под условом да смо већ одредили дипфејк као садржај који има личне податке, а сходно горе наведеним условима обраде, и са аспекта легитимног интереса, креатор дипфејка би могао да се позива и на своја лична мишљења или слободу говора уколико је створио дипфејк садржај познате особе који је креативне или рецимо сатиричне природе. По питању другог правног основа, односно сагласности лица, она би морала бити прибављена не само од особе која се појављује у првобитном тј. оригиналном садржају већ и од особе које се налази у дипфејку будући да се лични подаци оба лица обрађују.

Чињеница да су информације пренете путем дипфејка нетачне не утиче на применљивост Уредбе, све док се особа у дипфејку може на неки начин препознати. Дакле, чак и када изгледа да једна особа ради или говори ствари које никада није урадила или рекла, то се и даље третира као лични податак јер се подаци односе на ту особу што практично значи да без обзира да ли је видео, аудио или други материјал о некој особи измењен путем технологија вештачке интелигенције - није релевантно, већ је једино битно да ли се особа може разумно идентификовати. Додатно, Уредба се у принципу не примењује на преминуле особе тако да уколико неко направи дипфејк филм порнографске садржине у коме су главни

[199] https://www.mondaq.com/turkey/privacy-protection/863064/deepfake-an-assessment-from-the-perspective-of-data-protection-rules приступљено дана 30.01.2023.

актери две давно преминуле личности, то не спада у оквир заштите података.[200]

2.2. Директива о електонској трговини (e-Commerce Directive)

Иако донета много пре настанка дипфејка значајно је поменути и *Директиву о електонској трговини* (EU Directive on electronic commerce)[201] донету 2000. године. Директиваје донета са циљем отклањања препрека у погледу онлајн услуга унутар тржишта ЕУ, обезбеђења правне сигурност за пословање и грађане, а како би понудила флексибилне и истовремено балансиране правне оквире грађанима којима би се осигурала и побољшала међусобна конкуренцију између европских провајдера услуга. Директива је такође одредила да провајдери нису у обавези да прате саобраћај који се одвија преко њихових сервиса односно канала али и истовремену обавезу уклањања садржаја за који се утврди да је противправан. Један од проблема у вези са дипфејком јесте да се по Директиви веб сајтови који су домаћини оваквог садржаја неће сматрати одговорним уколико немају знања о постојању нелегалног материјала или информација, или када је провајдер у случују да му је било познато постојање нелегалних активности, благовремено реаговао како би отклонио или онемогућио приступ таквим информацијама. У светлу наведеног можемо закључити да Директива прихвата могућност уклањања дипфејк садржаја уклико се нађе да је такав материјал био незаконит али је проблематично што из ње не можемо сазнати шта се конкретно подразумева под незаконитом активношћу због чега и постоји потреба за усклађивањем са новим технологијама на бази вештачке интелигенције.

2.3. Закон о дигиталним тржиштима и закон о дигиталним услугама

Као замену сада већ застареле Директиве о електронском пословању на територији ЕУ, а у корак са убрзаном дигитализацијом друштва, Европска Комисија је 2020. године предложила два законска решења у виду *Закона о дигиталним тржиштима* и *Закона о дигиталним услугама* (Digital markets act и Digital services act) који су почели да се примењују у државама чланица од 1. јануара 2024. године. Ови закони имају два главна циља: стварање

[200] van der Sloot, B., & Wagensveld, Y. (2022). Deepfakes: Regulatory challenges for the synthetic society. Computer Law & Security Review, 46, 1-15.
[201] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN приступљено дана 30.01.2023.

безбедног дигиталног простора у коме би основна права свих корисника дигиталних услуга била заштићена и успостављање простора у коме ће се неговати иновације, раст и конкурентонст како на простору ЕУ тако и на глобалном нивоу.

Закон о дигиталним услугама[202] под дигиталним сервисима подразумева широк спектар интернет сервиса од инфраструктуре за интернет до онлајн платформи, а један од основних циљева овог закона односи се на доношење мера ради спречавања незаконите трговине и размене роба и услуга на интернету али и спречавање ширења дезинформација. Како се ово законско решење имплементира и на садржај на друштверним мрежама где између осталог и циркулише дипфејк материјал, створена је обавеза за провајдере да на основу пријава обришу или склоне садржај за који се утврди да је незаконит.

Закон о дигиталним тржиштима[203] је са друге стране унео одређени ред у погледу модерирања садржаја, одабира огласа или препоруке садржаја од стране алгоритама. Њиме су се ускладиле обавезе онлајн платформи и провајдера информационих услуга у борби против незаконитог садржаја који постављају корисници како би се заштитила основна људска права. Тако се члан 24б овог акта директно односи на онлајн платформе које се првенствено користе за ширење порнографског садржаја креираног од стране корисника, те им закон налаже низ организационих и техничких захтева. Закон такође предвиђа низ обавеза за велике компаније и онлајн платформе у погледу њиховог понашања према корисницима као и листу обавеза које би морале да имплементирају у свакодневном пословању како би се осигурало њихово фер и коректно учешће на тржишту ЕУ.

Закон о дигиталним услугама није конкретно обухватио проблем родне природе злостављања и узнемиравања на интернету као ни садржај осветничке порнографије који је широко доступан на интернету. Брзо уклањање слика са које су настале без сагласности лица на њима може значајно смањити штету и виктимизацију које доживљавају жртве али упркос томе пријављују се значајна кашњења у уклањању материјала са порнографских сајтова или се пријаве потпуно игноришу. Стога је дошло време да се размотри шта се још може учинити како би се смањила распрострањеност злоупотребе интимних слика, посебно на порнографским сајтовима[204] и којим инструментима је то могуће постићи.

Европски парламент ратификовао је додатне амандмане на Закон о дигиталним

[202] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065 приступљено дана 01.02.2023.
[203] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1925 приступљено дана 01.02.2023.
[204] https://inforrm.org/2022/02/03/pornography-platforms-the-eu-digital-services-act-and-image-based-sexual-abuse-clare-mcglynn-and-lorna-woods/ приступљено дана 01.02.2023.

услугама а који се односи на ширењем дипфејка. Амандман 339. предлаже потпуно нови члан 30а, под називом „Дипфејк“ и наводи да у случају када интернет платформа буде обавештена да је један садржај генерисан или манипулисан и да значајно подсећа на постојеће особе, објекте, места или друге ентитете или лажно изгледа - провајдер такав садржај мора означити на начин који објашњава да је садржај неаутентичан и да је јасно видљив за примаоца услуга односно крајњег корисника. Други амандман односи се на постојећи члан 63. где се конкретнно наводи да би велике интернет платформе требало да означе све познате дипфејк видео записе, аудио или друге датотеке.[205][206]

2.4. Закон о вештачкој интелигенцији (Artificial Intelligence Act)

Након бројних амандмана и расправа процес који је трајао од 2021. године званично је приведен крају 21. маја 2024. године када је Савет ЕУ усвојио је први закон на нивоу Европске Уније који регулише системе вештачке интелигенције и поставља правила за безбедно стављање робе која садржи компоненте ВИ на тржиште ЕУ. Можда и најбитнија новина коју овај акт садржи односи се на екстериторијалну примену и прилично високе казне[207] за субјекте који крше одредбе закона.[208]

Предлог је и одговор на изричите захтеве Европског парламента и Европског Савета, који су више пута позивали на законодавне мере како би се обезбедило функционално унутрашње тржиште за системе вештачке интелигенције. Главни циљеви овог закону су:

1. да су системи ВИ који се стављају и употребљавају на тржишту ЕУ, сигурни и усклађени са постојећим правом о темељним правима и вредностима ЕУ,
2. правна сигурност којом би се олакшала улагања и иновације у области ВИ,
3. побољшање управљања и делотворније одредбе постојећих прописа о темељним правима и сигурносним захтевима примењивима на системе ВИ и
4. олакшавање развоја јединственог тржишта за законите, сигурне и поуздане примене ВИ, те спречавање фрагментације тржишишта.

[205] https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.html приступљено дана 26.02.2023
[206] https://www.unite.ai/european-and-uk-deepfake-regulation-proposals-are-surprisingly-limited/ приступљено дана 26.02.2023.
[207] За кршење одредби Закона предвиђена је казна од 35 милиона еура или 7% годишњег профита компаније у зависности од тога који је износ виши.
[208] https://www.sidley.com/en/insights/newsupdates/2022/12/proposal-for-eu-artificial-intelligence-act-passes-next-level#:~:text=Following%20multiple%20amendments%20and%20discussions,)%20on%20December%206%2C%202022. приступљено дана 01.02.2023.

У случају када се систем ВИ употребљава за манипулисање сликовним, аудио или видео садржајем у коме постоји знатна сличност са аутентичним садржајем, постоји обавеза наглашавања да је тај садржај створен на такав начин, изузев када се креира у дозвољене сврхе (нпр. слобода изражавања). За ове системе у које осим *четботова* (који имају способност генерисања текста) спада и дипфејк предлажу се само минималне обавезе у погледу транспарентности у погледу обележавања. Ово се најчешће остварује стављањем воденог жига (*тзв. „watermark''*) на садржај међутим, док би по Закону овој обавези били подвргнути субјекти који стављају на тржиште системе ВИ који на овај начин могу да манипулишу садржајем, поставља се питање колико је Закон заиста делотворан према лицима која не спадају у ову категорију попут сајбер криминалаца или малициозних појединаца, те да ли је нпр. уопште разумно очекивити од особе која путем интернета поставља и шири дипфејк садржај порнографске природе - да исти обележи као дипфејк?

Осим за дипфејк ове обавезе примењују се и за системе који комуницирају са људима, служе за откривање емоција или одређивање повезаности са (друштвеним) категоријама на темељу биометријских података [209] па корисници у сваком тренутку морају бити обавештени да се интеракција коју обављају дешава са системом вештачке интелигенције.

2.5. Активности Европског Парламента

Под окриљем Европског парламента 2019. године успостављен *је Центар за вештачку интелигенцију (C4AI)* док је у оквиру самог парламента формиран и комитет који анализира утицај законадавне политике на области попут сајбер безбедности и одбране[210]

Као резултат постојећих опасности и ризика које представља коришћење система ВИ широм Европе, Европски парламент је 6. октобра 2021. усвојио резолуцију којом позива на трајну забрану система вештачке интелигенције који дозвољавају коришћење аутоматског препознавања појединаца од стране органа за спровођење закона на јавним местима. (*EP Resolution on AI in Criminal Law and Policing)*[211] Даље, Резолуција захтева мораторијум на примену система за препознавање лица у циљу спровођења закона и забрану предиктивног

[209] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 приступљено дана 30.01.2023.
[210] https://www.sidley.com/en/insights/newsupdates/2022/12/proposal-for-eu-artificial-intelligence-act-passes-next-level#:~:text=Following%20multiple%20amendments%20and%20discussions,)%20on%20December%206%2C%202022. приступљено дана 01.02.2023
[211] https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html приступљено дана 01.02.2023.

рада полиције на основу података о понашању и друштвених поена како би се осигурала заштита основних права европских грађана.

Комитет Европског парламента о вештачкој интелигенцији у дигиталном добу - *АИДА комитет* (Special Committee on Artificial Intelligence in a Digital Age) одржао је дводневно јавно саслушање са комитетом за спољне послове - *АФЕТ* (The Committee on Foreign Affairs) комитетом током марта 2021. Године, а тема је била ВИ и управљање у глобалном окружењу. Такође је поменута важност вештачке интелигенције за сајбер безбедност и област одбране. Дијалог и ангажовање различитих комитета Европског парламента о политици вештачке интелигенције кључни су за будућу имплементацију политика у области дипфејка, криминала и области правосуђа која се тиче коришћења и примене система ВИ. Због тога би Европски парламент требало да настави да промовише даље дијалоге и активности са другим међународним организације као што су Савет Европе и Организација за економску сарадњу и развој (OECD) а да националним парламентарцима помогне у разумевању димензија и импликација креирања прописа и политика о вештачкој интелигенцији посебно у циљу борбе против сајбер криминалитета[212]

Конкретно помињање дипфејка може се наћи на различитим парламентарним активностим, попут Резолуције из фебруара 2019. године којом се позива на означавање произвођача дипфејк материјала или синтетичких видео снимака. Позив на увођење строгих ограничења (или друге заштитне мере попут темељних истрага о непријатељским кампањама) о употреби дипфејка у контексту избора могу се наћи у скоро свим оваквим активностима. Парламент је у свом извештају за 2020. годину о правима интелектуалне својине за развој вештачке интелигенције, позвао на повећано подизање свести и медијску писменост, како би се сузбила могућност масовних манипулација кроз дипфејк. Најсвеобухватнији документ у вези са расправом по питању дипфејка је Резолуција од 19. маја 2021.године *„Вештачка интелигенција у образовању, култури и аудиовизуелном сектору.“*[213] Ова Резолуција садржи различите предлоге који се односе на будућа поступања попут важност подизања свести о ризицима дипфејка и унапређења дигиталне писмености, потешкоћа у откривању и означавању лажних и манипулисаних садржаја. Истовремено позива на увођење одговарајућег правног оквира за регулисање стварања, производње или

[212] Velasco, C. Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. ERA Forum 23, (2022). Стр. 109–126, стр. 123-124.
[213] https://www.europarl.europa.eu/doceo/document/TA-9-2021-0238_EN.html приступљено дана 02.02.2023.

дистрибуције дипфејка нарочито када се користи у злонамерне сврхе.[214]

3. Међународне организације

3.1. Светска организација за интелектуалну својину

Светска организација за интелектуалну својину (WIPO) је 2019. године а потом и 2020. године донела нацрт односно ревидирану верзију нацрта питања о политици интелекталне својине и вештачкој интелигеницји. *(Draft Issues Paper On Intellectual Property Policy And Artificial Intelligence*[215] и *Revised Draft Issues Paper On Intellectual Property Policy And Artificial Intelligence).*[216]

Организација раније није дефинисала концепт ВИ, међутим, након што су бројни поднесци и коментари истицали недостатак дефиниције, овај акт је сада вештачку интелигенцију дефинисао као „дисциплину рачунарске науке која има за циљ развој машина и система који могу да извршавају задатке који захтевају људску интелигенцију, уз ограничену или никакву људску интервенцију".

Наравно поставља се и питање проналазаштва и власништва, које се примењује на сва права интелектуалне својине па се поставља питање да ли би законска решења требало да захтевају да се људско биће именује као проналазач или би закон требало да дозволи да се апликација ВИ именује као проналазач? Као један од могућих проблема наводи се и дипфејк технологије односно технологије које генеришу или стимулишу људске атрибуте попут гласа и изгледа.

У погледу дипфејка, нарочито оног који је створен без пристанка особе приказане у њему постоје позиви да се ова технологија забрани или ограничи. Са друге стране, указује се на могућност стварања аудиовизуелних дела која могу дозволити ангажовање популарних или познатих извођача након њихове смрти па акт поставља низ питања попут: да ли је ауторско право уопште одговарајуће средство за регулисање дипфејка, затим уколико дипфејк садржај има користи од ауторских права, коме ће ауторска права у дипфејку

[214] Tackling deepfakes in European policy, European Parliamentary Research Service, Brussels, 2021, стр. 44.
[215] https://www.wipo.int/meetings/en/doc_details.jsp?doc_id=470053, приступљено дана 02.02.2023
[216] https://www.wipo.int/meetings/en/doc_details.jsp?doc_id=499504 приступљено дана 02.02.2023

припадати и на крају уколико дипфејк креатори имају користи од ауторских права, треба ли да постоји систем правичне накнаде за особе чији је лик коришћени у дипфејку? Акт закључује да етика и вештачча интелигенција морају ићи руку под руку и да је систем ВИ добар само онолико колико су добри подаци на којима је изграђен. [217]

3.2. Интерпол

На међународном нивоу, Међународна организација криминалистичке полиције (*INTERPOL*) и Агенција Европске уније за сарадњу у спровођењу закона (*EUROPOL*) подржавале су истраге које обухватају више јурисдикција у циљу спровођење закона. У својој процени претње организованог криминала на интернету од 2018. године, ЕУРОПОЛ је истакао важност сарадње са органима за спровођење закона, приватним сектором и академским кругом у борби сајбер криминалитета.[218]

Интерпол је заједно у сарадњи са *UNICRI* посредством њиховог центра за вештачку интелигенцију и роботику *(Centre for Artificial Intelligence and Robotics)* одржао други глобални састанак о вештачкој интелигенцији за органе за спровођење закона у Сингапуру 2019. године. Извештај овог сусрета допуњен је даљом анализом и увидима о недавним дешавањима од значаја у вези са употребом вештачке интелигенције. Представљени су општи принципи којих би органи за спровођење закона требало да се придржавају попут поштовања људских права, демократије, правде и владавине права, као и сродних захтева правичности, одговорности и транспарентности.

Као добра страна ове технологије истакнут је пример аустралијске федералне полиција (АФП) која је моделе дубоког учења искористила за у процесу препознавања, означавања и груписања слика и видео снимака попут материјала о сексуалном злостављању деце. Аутоматско препознавање снимака дечје порнографије ефикасно је заштитило полицијске службенике и истражитеље тако што је умањило њихову изложеност оваквим

[217]Draft issues paper on intellectual property policy and artificial intelligence, december 13, 2019 revised issues paper on intellectual property policy and artificial intelligence date: may 21, 2020

[218] Union Agency for Law Enforcement Cooperation, Internet Organized Crime Threat Assessment 2018 (The Hague: European Cybercrime Centre, 2018), https://www.europol.europa.eu/,activities-services/main-reports/internet-organised-crime-threat-assessment. приступљено дана 05.02.2023

садржајима.

Истовремено, закључило се да је криминални потенцијал дипфејка огроман и нагласило да постоји могућност изазивања друштвених и политичких немира због чега би полицијске снаге требало да буду спремне да са једне стране користе ВИ у позитивне сврхе, а са друге буду адекватно опремљене за нове и будуће претње ове технологије. Значај аудио и визуелног процесуирања материјала је нарочито истакнут због чега је упозорено на могуће злоупотребе и проблеме са којима ће се полицијске снаге суочавати ради откривања таквих технологија и кривичних дела. [219]

3.3. Европол

Европол је 2022. године донео први и детаљни извештај и анализу своје лабораторије за иновацију *(Europol Innovation Lab's Observatory*) који се фокусира на дипфејк технологију и њихов могући утицај на грађане ЕУ и органе реда. Многе организације су од тада почеле да посматрају дипфејк као још већи ризик од крађе идентитета посебно када се већина интеракција преселила на интернет од избијања пандемије „КОВИД-19". Све већа присутност лажних вести и дезинформација већ има дубок утицај на начин на који људи доживљавају ауторитет и информативне медије јер се са повећањем обима дипфејка поверења у власти и званичне чињенице - поткопава. Из ових разлога стручњаци страхују да би то могло довести до ситуације да грађани више немају заједничку стварност што се понекад назива апокалипса информација или апатија стварности.

У извештају су наведене опасности које појава дипфејка изазива у сфери пословања, дезинформација и лажних вести, крађе идентитета, осветничке порнографије и сајбер криминала као и утицај на рад полиције и правне поступке. Истовремено, разматране су и превентивне мере које се могу предузети против ове претње. У извештају се закључује да у наредним месецима и годинама постоји велика вероватноћа да ће сајбер криминалци све више користити дипфејк технологију како би олакшали извршење разних кривична дела али и са циљем стварања кампања дезинформисања како би се утицало на јавно мњење. [220]

[219]Towards responsible AI innovation second Interpol-Unicri report on artificial intelligence for law enforcement https://unicri.it/towards-responsible-artificial-intelligence-innovation приступљено дана 05.02.2023

[220] Europol (2022), Facing reality? Law enforcement and the challenge of deepfakes, an observatory report from the Europol Innovation Lab, Publications Office of the European Union, Luxembourg, приступљено дана 06.02.2023

VIII. НОРМАТИВНИ ОКВИР ДИПФЕЈКА У ПОЈЕДИНИМ ДРЖАВАМА

1. САД

Сједињене Америчке државе немају посебан акт који би на јединствен начин уредио проблем дипфејка већ је регулатива у поменутој области остављена на надлежност савезним државама. Међу првим државама које су то учиниле су Калифорнија, Тексас и Њујорк.

Сенат државе Калифорније је 12. септембра 2019. године, донео предлог закона АВ-602 *(Assembly Bill 602 - Deepfakes and Sexually Explicit Material)* чиме је омогућено право на приватну тужбу против особа које креирају или откривају туђи сексуално експлицитан садржај коришћењем „дипфејк" технологије. Конкретно, поступак може бити покренут против лица које креира или намерно открива сексуално експлицитан материјал уколико та особа зна, или би разумно требало да зна, да на такво стварање или откривање није пристала приказана особе, или када таква особа није креирала, али је намерно открила такав садржај знајући да приказана особа није пристала на његово стварање. [221]

Креатори нацрта имали су на уму да се закон примењује у две различите ситуације, прва, када је лице једне особе постављено на тело друге особе на начин који сугерише да се она ангажује на сексуално експлицитан начин, друга, где филмски стваралац високобуџетних филмова путем дипфејка дигитално мења филмску сцену како би изгледало као да се глумац бави сексуално експлицитним активностима.[222]

АБ-602 је међутим ограничен на разне начине тако што само штити особе чија су лица постављена на тела других, али не и особу (тј. тело) за коју се показало да се бави сексуално експлицитним понашањем. Затим, штити провајдере интернет садржаја од одговорности за незаконит садржај који постављају корисници његових услуге. На крају, права приказаног појединца се гасе његовом смрћу јер закон не предвиђа остваривање права из ове одредбе за преминула лица.[223]

[221] https://www.lexology.com/library/detail.aspx?g=4700f977-4845-417b-834d-b3c06390ee27 приступљено дана 065.02.2023

[222] https://www.bakerdatacounsel.com/state-legislation/if-signed-by-governor-california-bill-ab-602-will-provide-private-right-of-action-for-victims-of-sexually-explicit-deepfakes/ приступљено дана 06.02.2023

[223] https://www.bakerdatacounsel.com/state-legislation/if-signed-by-governor-california-bill-ab-602-will-provide-

Други закон који се односи на дипфејк у Калифорнији и који је почео да се примењује од 1. јануара 2023. године је AB 730 *(California Assembly Bill 730).* Овим законом постало је незаконито дистрибуирати изманипулисани садржај кандидата за изборе у року од 60 дана пре избора који има за циљ повреду угледа кандидата или обману бирача са циљем гласања за или против кандидата, осим ако материјал не садржи упозорење да је њиме манипулисано. Кандидат за јавну функцију чији се лик појављујеу дипфејку може покренути грађанску тужбу против било које особе, фирме, удружења или корпорације која је произвела, дистрибуирала, објавила или емитовала овакав садржај, а суд може досудити одштету у износу једнаком трошковима производње, дистрибуције, објављивања или емитовања материјала кампање који је прекршио овај закон, наравно поред адвокатских хонорара и трошкова поступка.[224]

Тексашки закон је веома сличан калифорнијском јер забрањује креирање и објављивање дипфејк садржаја односно његову дистрибуцију у року од 30 дана пре избора. Закон је дипфејк видео дефинисао као видео запис створен са намером да обмане, који приказује стварну особа како врши одређену радњу која се није догодила у стварности. Лице чини кривично дело уколико са умишљајем на овај начин повредити кандидата на изборима или утиче на резултат избора.[225]

У Њујорку је 30. новембра 2020. године од стране гувернера потписан нови државни закон *(Senate Bill S5959D)* који штити умрла лица од комерцијалне експлоатације или неовлашћеног коришћења њиховог имена, слике, гласа или потписа и даје само породицама тих особа право да их користе.[226][227] Закон има две главне компоненте. Прво, успоставља постмортем право на публицитет како би се заштитио лик и дело извођача од неовлашћене комерцијалне експлоатације у периоду од 40 година након њихове смрти и друго, забрањује компјутерски генерисану порнографију без сагласности односно дипфејк порнографију стварену вештачком интелигенцијом. Тако је Њујорк постао прва држава у САД-у која експлицитно проширује право на публицитет неке особе на компјутерски генерисане слике, такозване дигиталне реплике и који је увео право приватне тужбе против порнографских

private-right-of-action-for-victims-of-sexually-explicit-deepfakes/ приступљено дана 06.02.2023

[224] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB730 приступљено дана 06.02.2023

[225] https://capitol.texas.gov/tlodocs/86R/billtext/html/SB00751F.htm приступљено дана 06.02.2023.

[226] https://www.nysenate.gov/legislation/bills/2019/A5605 приступљено дана 06.02.2023

[227] Mania, Karolina. (2022). Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study. Trauma, Violence, & Abuse.

дипфејкова. Закон је резултат дугогодишњег залагања Удружења филмских глумаца (SAG-AFTRA) како би заштитили своје ликове од неовлашћене обраде и манипулације, нарочито након убрзаног напретка дигиталне технологије а имајући у виду да су глумци почели да се појављују у филмовима годинама након њихове смрти[228] захваљујући дигиталним манипулацијама попут дипфејка или рачунарски генерисаних слика („CGI'').

2. Велика Британија

Важећи закон у Великој Британији ограничен је на ширење правих слика као што су случајеви осветничке порнографије коју је држава криминализовала 2015. године. Важеће решење је да уколико починилац изнесе и објави лажни материјал који претвара идентитет његове жртве у порнографски садржај, може бити кривично гоњен само ако директно узнемирава жртву усмеравањем таквог материјала на њу, или у складу са законима који се односе на заштиту ауторска права. У првом случају, лакоћа са којом нови дипфејк садржај циркулише и привлачи пажњу и гледаоце готово неизбежно значи да ће жртву обавестити забринути пријатељи или непознате треће стране, а не особа која је креирала такав садржај па широка доступност таквог материјала омогућава заштиту креатора дипфејка. У другом случају, кривично гоњење би вероватно било изводљиво само ако је неконтролисани порнографски видео треће стране (на који се касније пребацује идентитет жртве) професионално произведен и легитимно заштићен под доменом ауторских права у Великој Британији.[229]

Према планираном амандману на Закон о безбедности на мрежи, особе које деле дипфејк слике или видео записе биће међу онима који ће по први пут бити посебно криминализоване. Влада је такође предложила пакет додатних закона ради решавања низа понашања, укључујући постављање опреме, као што су скривене камере или снимање некога без пристанка (укључујући и дипфејк). Влада Велике Британије такође планира и да имплементира неколико препорука Правне комисије како би осигурала да законодавство иде у корак са технологијом и може ефикасно да се носи са новим облицима злоупотребе.

[228] https://variety.com/2020/film/news/sag-aftra-commends-andrew-cuomo-deep-fake-videos-1234842715/ приступљено дана 06.02.2023

[229] https://www.unite.ai/european-and-uk-deepfake-regulation-proposals-are-surprisingly-limited/ приступљено 27.02.2023

Ове мере укључују укидање и замену постојећег законодавства новим прекршајима како би се закон поједноставио и олакшало кривично гоњење починилаца, увођење новог кривичног дела - дељење интимних слике без пристанка и тежа кривична дела заснована на намери да се изазове понижење или узнемиреност у циљу добијања сексуалног задовољства.[230] Оваквим решењем положај тужиоца знатно је олакшан будући да више не би морали да доказују намеру починиоца да узнемирава жртву таквим материјалом јер су у појединим случајевима, према постојећем закону, мушкарци признавали да јесу делили интимне слике жена без њиховог пристанка, али потом нису били кривично гоњени јер би се изјашњавали да нису намеравали да жртви нанесу штету. [231]

У Великој Британији проблем дипфејкова ће се решавати у светлу шире иницијативе за сузбијање осветничке порнографије и других облика злоупотребе интимних слика будући да су статистички подаци у Енглеској и Велсу показали да је једној од 14 одраслих особа неко претио да ће поделити њихове интимне слике без њиховог пристанка. Амандмани на Закон о безбедности на мрежи дефинисали су дипфејкове као произведене интимне слике које се деле без сагласности. [232]

3. Кина

Кина је 2019. године усвојила „Правилник о администрацији онлајн аудио и видео информационих услуга“ *(Regulations on the Administration of Online Audio and Video Information Services)*[233] којим је у ширем смислу забранила употребу машински генерисаних слика, аудио и видео записа у циљу креирања или ширења „гласина“. Овим актом предвиђено је да дипфејк видео или аудио садржај, или садржај креиран коришћењем алгоритама дубоког учења и технологија виртуелне реалности (VR) мора бити адекватно обележен и обавезује платформе да у супротном такав материјал самостално идентификују и уклањају а не да чекају пријаве корисника. Према овом акту, производња и ширење лажних

[230] https://www.gov.uk/government/news/new-laws-to-better-protect-victims-from-abuse-of-intimate-images приступљено дана 07.02.2023.
[231] https://www.bbc.com/news/technology-63669711 приступљено дана 07.02.2023.
[232] https://www.theverge.com/2022/11/25/23477548/uk-deepfake-porn-illegal-offence-online-safety-bill-proposal приступљено дана 07.02.2023.
[233] https://www.global-regulation.com/translation/china/160191/provisions-on-administration-of-internet-audio-video-program-services.html приступљено дана 07.02.2023.

вести је забрањена, а за спровођење ових правила одговорна је Кинеска управа за сајбер простор (Cyberspace Administration of China).[234]

Дана 28. јануара 2022. године кинеска државна канцеларија за информације о интернету објавила је Нацрт закона о управљању услугама интернет информационих сервиса дубоке синтезе *(Provisions on the Administration of Deep Synthesis Internet Information Services).*[235] Предлог је нацрт прописа за технологију дубоке синтезе односно синтетички генерисани садржај што подразумева и дипфејк. Одредбе овог закона представљављају искорак у односу на САД и ЕУ у регулативи дипфејка али и оличење напора кинеских власти да контролишу домаћи интернет садржај. Закон подразумева да интернет платформе морају добити сагласност од појединаца пре него што од њих направе дипфејк садржај и да морају потврдити аутентичност идентитета корисника због чега се исти морају регистровати на овим платформама личним документима или бројевима телефона. Креирани дипфејкови не могу се користити зарад активности које су забрањене законима и административним прописима, а пружаоци услуга дубоке синтезе морају на своју творевину додати потпис или водени жиг како би показали да је дело синтетичко и тиме избегли јавну забуну или погрешну идентификацију. Овај закон међутим, не подразумева само забрану манипулисаног садржаја попут дипфејка већ укључује и текст генерисан вештачком интелигенцијом као и нове технологија попут виртуелне реалности што указује на то да кинеска влада размишља шире о томе како ове технологије могу да утичу на стабилност њеног режима.[236]

Одредбе о дубокој синтези ступиле су на снагу 10. јануара 2023. године и јасно прописују главну одговорност пружалаца услуга дубоке синтезе и покривају неколико кључних области укључујући безбедност података и заштиту личних информација. У складу са одредбама о дубокој синтези, пружаоци услуга дубоке синтезе морају да ојачају управљање подацима предузимањем неопходних мера за заштиту личних података док су провајдери услуга дужни да успоставе и побољшају системе управљања за обуку особља, преглед алгоритама, регистрацију корисника, сигурност података, заштиту деце и заштиту личних података. У погледу транспарантности, провајдери услуга дубоке синтезе морају да успоставе смернице, критеријуме и процесе за препознавање лажних или штетних информација као и да се баве корисницима који производе лажан или штетан материјал

[234] Tackling deepfakes in European policy, European Parliamentary Research Service, Brussels, 2021, стр. 46-47
[235] https://www.chinalawtranslate.com/en/deep-synthesis/ приступљено дана 07.02.2023
[236] Hine, E., Floridi, L. New deepfake regulations in China are a tool for social stability, but at what cost?. Nature Machine Intelligence 4, 608–610 (2022).

користећи технологију дубоке синтезе. Додатно, одредбе позивају на стварање механизама за борбу против лажних вести, када се услуге дубоке синтезе користе за производњу, копирање, објављивање и ширење лажних информација а од добављача услуга дубоке синтезе се тражи да предузму низ мера у овом смеру попут вођења евиденције и пријављивања релевантним органима. Можда најважније, нове мере обавезују да се материјал и информације генерисане технологијом дубоке синтезе - означе као такве.[237]

4. Тајван

Парламент Тајвана усвојио је нацрт амандмана за сузбијање употребе сексуалних слика и видео записа који би производњу и ширење лажних или изманипулисаних слика и видео снимака ради зараде учинили кривичним делом. Нацрт измена и допуна Кривичног законика укључује и додатни члан који је посвећен дипфејку где се технологија дубоке синтезе дефинише као она која користи дубоко учење, виртуелну стварност и друге синтетичке алгоритме за производњу текста, слика, аудио, видео записа, виртуелних сцена и других мрежних информација. Оваква дефиниција укључује и технике за креирање или измену текста, технологије за креирање или промену гласовног садржаја као што је претварање текста у говор, технике за креирање или измену биометријских карактеристика на сликама и видео садржају, као што су генерисање лица, замена лица или манипулација покретима, дигитална симулација и друге технологије које креирају или мењају изглед једне особе. [238]

Нацрт амандмана предложен је након хапшења популарног тајванског јутјубера који је креирао и продавао дипфејк порнографске видео снимке десетина истакнутих жена, укључујући и политичарке. Амандман између осталог садржи одредбу која предвиђа да се за производњу сексуалног материјала који укључује слике или видео снимке другог лица без пристанка те особе, изриче максимална казна од три године затвора, док неовлашћена дистрибуција таквог материјала може резултирати затворском казном од шест месеци до пет година затвора. Уколико једно лице буде проглашено кривим за дистрибуцију таквог садржаја а ради стицања имовинске користи, запрећена је додатна казна до половине

[237] https://www.china-briefing.com/news/china-to-regulate-deep-synthesis-deep-fake-technology-starting-january-2023/ приступљено 25.02.2023.
[238] https://www.taipeitimes.com/News/front/archives/2023/01/08/2003792190 приступљено дана 28.02.2023

прописане казне. Амандман такође укључује предлог да се свако ко је осумњичен за производњу сексуалних слика или видео снимака друге особе употребом претњи или насиља, може казнити казном до пет година затвора и од једне до седам година уколико је у питању дистрибуција таквог садржаја. Особе које репродукују, дистрибуирају, емитују, испоручују, приказују или користе друге методе за приказивање сексуалних слика без пристанка укључене стране могу бити кажњене до пет година затвора уз обавезу плаћања новчане казне у износу до 16.000 америчких долара. [239]

5. Јужна Кореја

Јужна Кореја нема посебан закон који помиње или криминализује употребу дипфејк технологије међутим, постоје закони и прописи који се могу применити на решавање проблема у вези са дипфејком, као што су нпр. закони који се односе на приватност и ширење лажних информација. Влада Јужне Кореје је предузела кораке како би се позабавила овим проблем па је тако основала агенцију под називом Дигитални форензички центар који се између осталог бави и провером чињеница и промоцијом технологија ВИ за откривање дипфејка. Јужна Кореја се такође придружила међународним напорима у борби против ширења дипфејка, као што је *Глобално партнерство за вештачку интелигенцију* (ГПАИ).

Упркос чињеници да има популацију која је у самом светском врху по дигиталној писмености, злоупотребе модерних технологија су учестале и свакодневне, а као најчешће жртве јављају се познате личности. Због тога је између осталог, предложен „дипфејк закон“ као ревизија актуелног Закона о сексуалним злочинима којим се предлаже казна до седам година затвора за лица која дистрибуирају лажне видео снимке. Да би овај закон званично ступио на снагу потребно је време будући да мора проћи кроз одређене фазе од консултација са владиним одељењима до јавних расправа у циљу подизања друштвене свести о овим питањима. [240]

[239] https://www.taipeitimes.com/News/front/archives/2023/01/08/2003792190 приступљено дана 28.02.2022.
[240] https://www.koreatimes.co.kr/www/tech/2020/04/129_279851.html приступљено дана 28.02.2023

IX. НОРМАТИВНИ ОКВИР ДИПФЕЈКА У РЕПУБЛИЦИ СРБИЈИ

1. Кривични законик

Република Србија за сада нема законских решења у погледу регулисања или криминализације дипфејка али се високотехнолошком криминалу супротставља Кривичним закоником, Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала, Законом о ауторским и сродним правима, Законом о информационој безбедности, Законом о спречавању прања новца и фининасирања тероризма, Законом о електронским комуникацијама и др. Кривичним закоником[241] из 2006. године уведена су кривична дела против безбедности рачунарских података, која су набројана у глави XXVII. Објект заштите ових кривичних дела је безбедност рачунарских програма и података, а по питању кривичних санкција, прописана је казна затвора или новчана казна у зависности од тежине учињеног дела. У поменутој глави КЗ-а као појавна кривична дела против рачунарских података убрајају се:

Оштећење рачунарских података и програма (члан 298). Закон је рачунарски податак дефинисао као свако представљање чињеница, информација или концепта у облику који је подесан за њихову обраду у рачунарском систему, укључујући и одговарајући програм на основу кога рачунарски систем обавља своју функцију, а рачунарски програм као - уређени скуп наредби који служе за управљање радом рачунара и решавање одређених задатка помоћу рачунара. Оштећење рачунарског податка или програма може се извршити утицајем на хардвер или софтвер рачунара. У првом случају долази до физичког деловања на део хардвера који је и носилац предметног податка или програма док у другом случају долази до софтверског деловања путем рачунара којим се податак или програм модификују или бришу.[242] Радња овог кривичног дела састоји се у неовлашћеном брисању, измени, оштећењу, прикривању или на други начин чињењу неупотребљивим рачунарског податка или програма, што је и основни облик овог кривичног дела. Објект радње је рачунарски податак

[241]Кривични законик РС, "Сл.гласник РС, бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019

[242]Миладиновић Богавац, Ж., Чекеревац З., „Кривична дела против безбедности рачунарских података" Београд, стр. 119-126.

односно рачунарски програм. Закон је предвидео два тежа облика овог дела, први када је проузрокована штета која прелази износ од 450.000 динара и други уколико је проузрокована штета која прелази износ од 1.500.000 динара. За први тежи облик прописана је казна затвора од три месеца до три године, док је за други предвиђена казна затвора од три месеца до пет година. У погледу дипфејка, свакако да се слика, текст, видео или аудио запис могу подвести под термин „ненумерички рачунарски подаци“, а будући да дипфејк настаје управо манипулисањем фотографија, аудио или видео записа, у ширем смислу можда има основа за његово инкриминисање али се у погледу последице овог кривичног дела односно чињења неупотребљивим рачунарског податка или програма то не може рећи јер дипфејк садржај након манипулације не постаје неупотребљив. Стога, може се закључити да ово законско решење није адекватно у погледу криминализације дипфејка.

Рачунарска саботажа (члан 299) се састоји у уношењу, уништењу, брисању, оштећењу, прикривању или на други начин чињењу неупотребљивим рачунарског податка или програма или уништењу, оштећењу рачунара или другог уређаја за електронску обраду и пренос података са намером да се онемогући или знатно омете поступак електронске обраде и преноса података који су од значаја за државне органе, јавну службу, установу, предузеће или друге субјеке. Карактеристика овог кривичног дела јесте специфична намера учиниоца да онемогући или знатно омете поступак електронске обраде и преноса података који су од значаја за различите службе и организације па се с обзиром на наведено може извршити само са директним умишљајем. Рачунарска саботажа има два објекта напада. Први, рачунарски податак или програм и други, рачунар или други уређај за електронску обраду и пренос података. Последице овог кривичног дела су далекосежније и друштвено опасније од других кривичних дела против безбедности рачунарских података будући да могу довести до онемогућавања функционисања државног органа што повлачи са собом и велике губитке, материјалну штету као и штету у изгубљеном времену. По питању санкције предвиђена је казна затвора од шест месеци до пет година док тежи облик дела није законом предвиђен.

Прављење и уношење рачунарских вируса (члан 300). Законодавац је рачунарски вирус дефинисао као рачунарски програм или други скуп наредби унет у рачунар или рачунарску мрежу који је направљен да сам себе умножава и делује на друге програме или податке у рачунару или рачунарској мрежи, додавањем тог програма или скупа наредби једном или више рачунарских програма или података. Радња извршења овог кривичног дела

састоји се у прављењу односно ширењу рачунарског вируса. Основни облик састоји се у прављењу рачунарског вируса и намери његовог уношења у туђи рачунар или рачунарску мрежу, док се тежи облик састоји у уношењу рачунарског вируса у туђи рачунар или рачунарску мрежу чиме се другом проузрокује штета. За основни облик предвиђена је новчана казна или казна затвора до шест месеци, а за тежи облик превиђена је новчана казна или казна затвора до две године.

Рачунарска превара *(*члан 301) састоји се у уношењу нетачног податка, пропуштању уношења тачног податка или на други начин прикривању односно лажном приказивању податка чиме се утиче на резултат електронске обраде и преноса података у намери да се себи или другом прибави противправна имовинска корист и тиме проузрокује штета другом лицу, што представља и радњу извршења овог кривичног дела и његов основни облик. Као и код класичног кривичног дела преваре, висина прибављене противправне имовинске користи служи за одређивање тежег облика. Први тежи облик постоји у случају када је кривичним делом прибављена противправна имовинска корист која прелази износ од 450.000 динара, а други када је тај износ већи од 1.500.000 динара. За први облик прописана је казна затвора од једне до осам година, а за други затвор од две до десет година. Поред основног и два тежа облика, закон је предвидео и привилеговани облик, и то у случају када је радња из основног облика кривичног дела предузета са намером да се друго лице оштети што је санкционисано новчаном казном или казном затвора до шест месеци.

Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (члан 302). Радња овог кривичног дела састоји се у неовлашћеном укључивању у рачунар или рачунарску мрежу или у неовлашћеном приступу електронској обради података кршењем мера заштите. Мера заштите о којој се говори је најчеће лозинка односно шифра рачунара коју корисник уноси како би приступио електронској обради података. Поред основног облика законодавац је предвидео и два тежа облика, први, када се сними или употреби податак добијен приликом неовлашћеног укључења у рачунар или рачунарску мрежу или неовлашћеног приступа електронској обради података. Други, тежи облик постоји уколико је приликом извршења основног облика дошло до застоја или озбиљнијег поремећаја функционисања електронске обраде и преноса података или мреже или уколико су наступиле друге тешке последице. У првом случају учинилац ће се казнити новчаном казном или затвором до две године, а у другом казном затвора до три године.

Спречавање и ограничавање приступа јавној рачунарској мрежи (члан 303). Радњу овог кривичног дела чини свако ко неовлашћено спречава или омета приступ јавној рачунарској мрежи. Законодавац је рачунарску мрежу дефинисао као скуп међусобно повезаних рачунара, односно рачунарских система који комуницирају размењујући податке, док се под јавном рачунарском мрежом подразумева мрежа која је доступна неодређеном броју лица. Основни облик овог кривичног дела може извршити било које лице, а тежи облик може учинити само службено лице у вршењу службе. Санкција за основни облик је новчана казна или казна затвора до три месеца, док је за тежи облик предвиђена казна затвора до три године. По питању кривице, ово кривично дело може се извршити само са умишљајем.

Неовлашћено коришћење рачунара или рачунарске мреже (члан 304). Радњу овог кривичног дела врши свако ко неовлашћено користи рачунарске услуге или рачунарске мреже у намери да себи или другом лицу прибави противправну имовинску корист. У случају када извршилац вишекратно неовлашћено користи рачунарске услуге или рачунарску мрежу, постојаће само једно кривично дело, тако да у неким случајевима неће ни бити потребе за применом конструкције продуженог кривичног дела јер ће се радити о природном јединству дела.[243] Законодавац је у ставу 2. овог члана одредио да се гоњење за ово кривично дело предузима по приватној тужби.

Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података (члан 304а). Радња извршења огледа се у производњи, продаји, набављању ради употребе, увозу, дистрибуирању или на други начин стављању на располагање уређаја и рачунарских програма у сврху извршења кривичних дела прописаних у глави XXVII КЗ (ст.1. тач.1.) као и рачунарских шифри и сличних података путем којих се може приступити рачунарском систему као целини или неком његовом делу са намером да буде употребљен у извршењу неког од кривичних дела прописаних у глави XXVII КЗ (ст.1. тач.2.) У ставу 2. одређен је и привилеговани облик овог дела и то у случају када се поседује неко од средстава из ст. 1. са намером да се употреби у сврху извршења неког од кривичних дела прописаних у глави XXVII КЗ. Учинилац овог кривичног дела може бити свако лице које са умишљајем намерава да произведе, набави, прода или другоме да на употребу рачунар, рачунарски систем, рачунарски податак или програм у циљу извршења кривичних дела против безбедности рачунарских података. По питању санкција, законодавац

[243]Миладиновић Богавац, Ж., Чекеревац З., „Кривична дела против безбедности рачунарских података" Београд, стр. 119-126, стр. 124.

је прописао за основни облик казну затвора од шест месеци до три године, док је за привилеговани облик одредио новчану казну или казну затвора до три године.

Као што је на почетку поглавља наведено, дипфејк у законодавству Републике Србије као посебно кривично дело није инкримисан. Имајући у виду нарочито озбиљне последице које ова појава може изазвати, а које су између осталог наведене у овом раду, посебно оне које се односе на дипфејк осветничку порнографију, потребно је у догледно време извршити криминализација ове појаве. Иако се осветничка порнографија често користи и као средство контроле које укључује уцењивање партнера или супружника сексуално експлицитним материјалом (обичним или манипулисаним садржајем тј. дипфејком) како би се исти спречио да их напусти односно изађе из емотивне везе, квалификација оваквог поступања као кривичног дела насиља у породици била би без основа. Жртве се међутим могу позивати на кривичн дело изнуде из члана 214. ст. 1 КЗ где се наводи да ће се лице које користи силу или претњу како би принудило друго лице да нешто учини или не учини на штету своје или туђе имовине у намери да себи или другом прибави противправну имовинску корист, казнити затвором од једне до осам година и уцене, и кривично дело уцене из чл. 215. ст. 1 КЗ[244] којим је прописано да ће свако ко у намери да себи или другом прибави противправну имовинску корист па запрети другом да ће против њега или њему блиског лица открити нешто што би њиховој части или угледу шкодило и тиме га принуди да нешто учини или не учини на штету своје или туђе имовине, казнити затвором од шест месеци до пет година. Проблем код ове квалификације је да су кривична дела изнуде и уцене, кривична дела против имовине па је циљ починиоца стицање имовинске користи, те би се жртве дипфејка на ова кривична дела могле позивати само под условом да се од њих захтева нека финансијска корист што у већини ситуација, бар када је у питању дипфејк садржај или дипфејк осветничка порнографија - није случај због чега се поставља питање колико је ово законско решење заиста делотворно.

У погледу кривичноправне заштите малолетних лица од дипфејк материјала, заштита би се могла пружити на основу главе XVIII Кривичног законика која прописује кривична дела против полне слободе и инкриминише кривично дело приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију (члан 185 ст. 2). Законодавац је у ставу 6. истог члана дефинисао шта сматра предметима порнографске садржине и одредио да је то садржај настао искоришћавањем малолетног лица

[244] Кривични законик РС, "Сл.гласник РС, бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019

који визуелно приказује малолетно лице које се бави стварним или симулираним сексуално експлицитним понашањем, укључујући и свако приказивање полних органа детета у сексуалне сврхе.

У погледу спречавања ширења и дистрибуције порнографског дипфејк материјала у којима су главни актери деца, значајно је поменути и став 4. горе наведеног члана којим је инкриминисано прибављање за себе или другог, поседовање, продаја, приказивање, јавно излагање или електронски или на други начин чињење доступним слике, аудио-визуелних или других предмета порнографске садржине насталих искоришћавањем малолетног лица за где је прописана казна затвора од три месеца до три године. Такође, заштита деце и малолетних лица од приступања других лица сликама, аудио-визуелним или другим предметима порнографске садржине насталим искоришћавањем малолетног лица загарантована је ставом 5. овог члана.

Иако дипфејк видео снимци порнографског садржаја у којима су главни акери деца или малолетна лица – нису чести, то не значи да се овакав материјал у будућности неће стварати или повећавати, те ове одредбе Кривичног законика свакако иду у корист кривичноправној заштити малолетних лица. Мана оваквог законског решења јесте у томе што се кривичноправна заштита по овом основу не може пружити пунолетним лицима која су (за сада) доминантна групација која се појављује у манипулисаним односно дипфејк медијима.

2. Закон о ауторским и сродним правима

Са грађанскоправног становишта, Закон о ауторским и сродним правима[245] уредио је питање ауторских права, њихове злоупотребе и судску заштиту истих. У складу са законом, повреду ауторског или сродног права представља неовлашћено вршење било које радње која је обухваћена искључивим правима носиоца ауторског или сродног права, неплаћање прописане накнаде, као и неизвршавање других обавеза према носиоцу ауторског или сродног права. Како дипфејк настаје креирањем постојећих фотографија, аудио или видео записа, аутор ових медија на основу чл. 17. поменутог закона, има право да штити интегритет свог дела и да се супротстави изменама истог од стране неовлашћених лица, те да даје дозволу за прераду свог дела, док је чланом 18. прописано да аутор има искључиво право да

[245]Закон о ауторским и сродним правима, Сл. гласник РС, бр. 104/2009, 99/2011, 119/2012, 29/2016

се супротставља искоришћавању свог дела на начин који угрожава или може угрозити његову част или углед. Када би се дипфејком користио материјал који је заштићен ауторским правом без дозволе аутора, свакако да би постојао основ за одговорност креатора оваквог садржаја. Међутим, постоје извесна ограничења у зависности од сврхе у коју се ауторско дело користи па закон тако предвиђа да је дозвољена слободна прерада објављеног ауторског дела уколико се ради о пародији или карикатури, под условом да се не ствара забуна или да не може доћи до стварања забуне у погледу извора дела. Затим, дозвољена је прерада дела за личне потребе која није намењена и није доступна јавности и прерада у вези са дозвољеним коришћењем дела, која је проузрокована самом природом или начином тог коришћења. Додатно, како под ауторским делом подразумевамо оригиналну духовну творевину аутора поставља се питање колико је један дипфејк садржај заиста оригиналан будући да настаје комбиновањем различитих и већ постојећих медија и посредством софтвера вештачке интелигенције. Тек уколико би аутор дипфејка у своју креацију унео елементе које је сам створио попут музике или видео снимка, тада би и сам могао да буде заштићен као аутор дела. Као санкција за повреду ауторских и сродних права, одређена је прекршајна одговорност и одговорност за привредне преступе док је за односе у области права интелектуалне својине предвиђена грађанска одговорност.

3. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала

Значајно је поменути и Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала,[246] који је уредио материју образовања, организације и надлежности државних органа за борбу против високотехнолшког криминала о којима ће бити речи у следећем поглављу. Закон се примењује ради откривања, кривичног гоњења и суђења за:

1) кривична дела против безбедности рачунарских података одређена Кривичним закоником,

2) кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство извршења кривичних дела јављају

[246]Закон је ступио на снагу 25. јула 2005. године.

рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци, као и њихови производи у материјалном или електронском облику, уколико број примерака ауторских дела прелази 2000 или настала материјална штета прелази износ од 1.000.000 динара и

3) кривична дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира и уставног уређења и безбедности Републике Србије, која се због начина извршења или употребљених средстава могу сматрати кривичним делима високотехнолошког криминала.

Иако за сада дипфејк није посебно регулисан у Републици Србији, овај закон би у будућности могао представљати добру полазну тачку будући да би органи који су надлежни за решавање предмета из области вискотехнолошког криминала свакако били надлежни и за поступање у предметима поводом дипфејка. Међутим, због сложености и посебности ове технологије, надлежни органи би морали блиско да сарађују са организацијама, приватним и јавним сектором као и физичким лицима из ове сфере будући да постојећа специјалистичка знања која поседују судије и тужиоци из области високотехнолошког криминала нису довољна за ефикасну борбу против малициозне употребе дипфејк технологије.

X. НАДЛЕЖНОСТ И ПОСТУПАЊЕ ОРГАНА У ОБЛАСТИ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА, ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ И ДИПФЕЈКА И СТРАТЕШКИ ОКВИР ЗА БУДУЋНОСТ

Поменутим законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала, надлежност за поступање у предметима из ове области има Више јавно тужилаштво у Београду (за територију целе државе) односно Посебно одељење за борбу против високотехнолошког криминала у оквиру наведеног тужилаштва. На челу Посебног одељења налази се Посебни јавни тужилац,[247] кога именује Врховни јавни тужилац на период од шест година, без могућности реизбора. Посебни јавни тужилац има иста права и дужности као и главни јавни тужилац те када дође до сазнања о почињеном кривичном делу из области високотехнолошког криминала обратиће се у писменој форми Врховном јавном тужиоцу, захтевајући од њега да му пренесе или повери надлежност.

[247]Приликом избора предност имају тужиоци који имају адекватна знања из области информатичких технологија.

У оквиру Службе за борбу против организованог криминала (СБПОК) делује и специјално Одељење за сузбијање високотехнолошког криминала[248] 2019. године извршена је подела на четири одсека:

1. Одсек за сузбијање криминалитета у области интелектуалне својине,
2. Одсек за сузбијање електронског криминалитета,
3. Одсек за сузбијање недозвољених и штетних садржаја на интернету и
4. Одсек за сузбијање злоупотреба у области електронске трговине, електронског банкарства и платних картица на интернету.

Подела унутар Одељења битна је због потребе за посебно образованим кадром, који би се бавио искључиво сузбијањем горе наведених облика криминалног деловања, али која ће бити постављена тако да запослени у овом органу не буду преоптерећени и да одређени кривични предмети услед тога не буду запостављани. Специфична природа ових послова између осталог захтева и блиску сарадњу државних органа међутим, нема довољно капацитета и људства ни у полицији ни у тужилаштву.[249] Одељење има обавезу да поступа по захтевима Посебног тужилаштва за борбу против високотехнолошкох криминалитета али и по захтевима других тужилаштава када је то потребно. Остварује и сарадњу са међународним институцијама попут Интерпола и Европола у погледу размене информација и доказа, са циљем сузбијања сајбер криминалитета. На челу ове службе је старешина кога поставља министар надлежан за унутрашње послове, након прибављеног мишљења Посебног јавног тужиоца по чијим захтевима и поступа. Једна од основних замерки овако постављеној надлежности огледа се у непостојању законске одредбе која се тиче обавезе поседовања стручних знања из области информатичких технологија на страни стручних кадрова и старешина службе па се у стварности може десити да на чело овог органа буде изабрано лице које таква знања не поседује.[250]

Овако одређена надлежност биће основ и за будућа поступања поменутих органа поводом предмета у којима ће се у неком облику појављивати и дипфејк. Изван система кривичног правосуђа, за успешну борбу против ове појаве потребна је и сарадња стручњака

[248]Одељење је постало једина специјализована јединица МУП-а задужена за кривична дела високотехнолошког криминала.
[249]Анализа функционисања институција у борби против организованог високотехнолошког криминала у Србији, Београдски центар за безбедоносну политику, (март 2021), стр. 5.
[250]Димовски, Д. (2019), Компјутерски криминалитет, Правни факултет Универзитета у Нишу, Зборник, LV, стр. 195-212., стр. 209-210, стр. 204.

из различитих научних области због чега се осећа снажна потреба за професионалцима који имају колективно знање о сајбер криминологији, праву и форензици. Одељења за конвенционалну криминологију би требало да сарађују на мултидисциплинарном нивоу са одељењима за рачунарство, право и информационе технологије. На овај начин створила би се група професионалаца која би служила као својеврсна база, са мешавином теоријског и практичног знања о кривичним делима, истрагама и законима из ове области, што би са једне стране унапредило професију а са друге, било од помоћи органима за спровођење закона поводом истрага у предметима сајбер криминала.[251] Још једна значајна област којој би ови професионалци могли да допринесу односи се и на пружање подршке жртвама дипфејка где могу преузети саветодавну улогу односно деловати као ресурсни центар поводом виктимизације жртава, а који би служио да подигне свест научној и лаичкој јавности.[252]

Осим поменутих закона, Република Србија активност у овој области, између осталог спровела је и *Стратегијом за борбу против високотехнолошког криминала* донету за период од 2019. до 2023. године. Стратегија представља наставак и проширење активности којима је циљ јачање ефикасности свих субјеката у области сузбијања високотехнолошког криминала у Републици Србији. Посебно је усмерена на наставак усклађивања законодавства са међународним стандардима, унапређење капацитета носилаца борбе против високотехнолошког криминала и интерресорне сарадње у друштву, као и сарадње Републике Србије на регионалном и међународном нивоу у овој сфери.[253] Како се наводи у поменутом документу и Војска Србије је између осталог израдила Нацрт концепта сајбер одбране Војске Србије, где је представљен поглед на питање како се процењује одбрамбени, безбедносни, технолошки и друштвени утицај који ће у наредном петогодишњем периоду развоја и употребе Војске Србије остварити развој информационо-комуникационих технологија, активности и дејстава у сајбер простору и употреба офанзивних сајбер способности могућих противника на одбрану Републике Србије. Процена је заснована на резултатима предвиђања релевантних међународних субјеката о очекиваном развоју информационо-комуникационих технологија и њиховом утицају на одбрану и безбедност Републике Србије и достигнутом и очекиваном степену развоја капацитета и способности државних и недржавних субјеката за

[251] Karuppannan, Jaishankar. (2023). The Future of Cyber Criminology: Challenges and Opportunities 1., International Journal of Cyber Criminology (IJCC) ISSN: 0974, (2010) Vol 4, стр.26–31, стр.27.
[252] Ibid. стр. 28.
[253]Стратегија за борбу против високотехнолошког криминала 2019-2023. године, стр. 2, http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2018/71/1/reg приступљено дана 08.02.2023

дејства и активности у сајбер простору или из њега, а која могу бити од утицаја на мисије и задатке Војске Србије, међутим поменути документ још увек није усвојен. Већина пројеката које је Србија започела у овој области финансирана је од стране Европске Уније.

У погледу стратешког оквира за информациону безбедност, усвојена је и *Стратегија развоја информационог друштва и информационе безбедности* у Републици Србији за периодод 2021. до 2026. године, која је усклађена са Директивом о мрежној и информационој безбедности ЕУ (НИС директива), а којом су обухваћене све приоритетне области које доприносе развоју једног информационог друштва као што су електронска комуникација, е-управа, е-здравство и е-правосуђе, ИКТ у образовању, науци и култури, електронска трговина, пословни сектор и др. Стратегија је по обухвату међусекторска, и за њену израду су релевантна планска и стратешка документа у области развоја мрежа нове генерације, дигиталних вештина, вештачке интелигенције, развоја индустријске политике, паметних специјализација, туризма, културе, пољопривреде, правосуђа, високотехнолошког криминала, као и прописи у области електронског документа, електронске идентификације и услуга од поверења, информационе безбедности и електронске управе и безбедности деце на интернету. Док са једне стране је чињеница да дигитализација свакако пружа разноврсне предности за обичне грађане, са друге истовремено укључује и висок ризик за безбедност и људска права, пре свега због прикупљања велике количине података о личности, нарочито осетљивих података који се односе на грађане у дигиталном свету.[254]

Иако за сада, не постоји званична политика и методологија у погледу формирања посебних државних органа у контексту будуће борбе против дипфејка и сличних појава, Влада Србије је за почетак направила добре кораке усвојивши ***Стратегију развоја вештачке интелигенције***[255] за период 2020-2025. године којом је држава ставила до знања да жели да иде у корак са модерним технологијама и то само две године након што је то прва у свету учинила Финска.[256] Стратегијом се предвиђа развој вештачке интелигенције, чија имплементација треба да резултира економским растом, унапређењем јавних услуга, унапређењем научног кадра и развојем вештина за послове будућност. Такође је наведено да

[254]Стратегија развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године, "*Службени гласник РС*", број 86 од 3. септембра 2021.
[255]https://www.srbija.gov.rs/extfile/sr/437304/strategija_razvoja_vestacke_inteligencije261219_2_cyr.pdf, приступљено дана 08.02.2023
[256] Бјелош, Маја, Павловић, Марија, Сајбер безбедност и људска права на Западном Балкану:случај Србије, Београдски центар за безбедоносну политику, 2022, стр. 6-7, , https://bezbednost.org/publikacija/sajber-bezbednost-i-ljudska-prava-na-zapadnom-balkanu-slucaj-srbije/ приступљено дана 08.02.2023

је разлог за њено доношење нагли и брзи развој и ширење примене вештачке интелигенције, пре свега захваљујући продорима у области дубоких неуронских мрежа и пратећим технолошким напретком који је тај продор омогућио. Стратегија такође говори и о могућим проблемима и етичким изазовима, попут превенције дискриминације по било ком основу - јер се кроз податке за тренирање могу преузети предрасуде и пристрасности, изазову транспарентности - јер у машинском учењу често нису транспарентна правила по којима систем доноси одлуке, као и утицају ових алата на тржишту рада. Иако дискриминација није нова категорија, ако би се успоставила машинским учењем, она би могла бити системска, па је такве ризике потребно предупредити. Како је вештачка интелигенција напредна технологија чији домети и утицај на друштво још увек нису у потпуности познати, а не могу бити у целости ни предвиђени, важно је да се активно ради на изградњи окружења које ће, са једне стране, обезбедити поверење јавности, а са друге омогућити стварање нових прилика за развој и употребу вештачке интелигенције. Један од главних циљева ове Стратегије јесте увођење превентивних механизама који ће омогућити одговоран развој вештачке интелигенције у складу са највишим етичким и безбедносним стандардима. Кључни циљ је да се пронађе баланс између подршке развоју и употреби вештачке интелигенције и њеног одговорног развоја заснованог на основним етичким принципима. У том погледу, развој етичког оквира би требало да омогући заштиту основних људских права и заједничких вредности, али и да буде у служби даљег развој вештачке интелигенције стварањем нових прилика за побољшање живота појединаца и напретка читавог друштва. Стратегија нарочито истиче да је неопходно подстицати јавни дијалог, у виду организовања радионица, семинара, предавања и сличних активности, намењених широј јавности са циљем приближавања предности, али и указивања на изазове који настају развојем и употребом вештачке интелигенције. Додаје се да и поред квалитетног кадра који Република Србија има да понуди у овој области, исти је ипак недовољан те постоје изазови који се огледају у недовољном броју инвестиција у стартап компаније, малом броју истраживача у области вештачке интелигенције на универзитетима и институтима и недовољна сарадња универзитета са привредним сектором. Закључује се да би се кроз унапређивање образовања, модернизације законске регулативе и улагања у Фонд за иновациону делатност и Фонд за науку, направили почетни кораци за решавање ових проблема.[257]

[257] https://www.srbija.gov.rs/extfile/sr/437304/strategija_razvoja_vestacke_inteligencije261219_2_cyr.pdf

ЗАКЉУЧНА РАЗМАТРАЊА

Развој интернета и широко усвајање дигиталних технологија створили су нове могућности за криминалне активности. Како је сајбер криминалитет постао све заступљенији и софистицираније облик криминалне активности у дигиталном добу који наставља да еволуира, јасно је да традиционални и регулаторни приступи спровођења закона нису адекватни за решавање изазова које поставља. Иако су уложени значајни напори у борби против ове појаве, укључујући законодавство, стратегије и технолошке иновације, проблем је и даље сложен и вишеструк. Штавише, с обзиром на брзо развијајућу природу сајбер криминалитета, од суштинске је важности остати опрезан и прилагодљив у одговору на нове претње и рањивости будући да борба у овој области захтева континуиране напоре и вишеструки приступ свих заинтересованих страна, укључујући појединце, предузећа, владе и органе за спровођење закона. Како би се обезбедио сигурнији дигитални екосистем неопходна је и сарадња на међународном нивоу, подизање свести и образовање јавности али и промоција етичког коришћења система вештачке интелигенције.

Појава и коришћење вештачке интелигенције у комбинацији са сајбер криминалитетом, створила је додатни скуп изазова. Пре свега, сајбер криминалцима је ово омогућило да изводе софистицираније нападе, а органима за спровођење закона значајно отежало поступак лоцирања и идентификације починилаца. Док вештачка интелигенција има потенцијал да унесе револуцију у област сајбер безбедности тако што ће омогућити ефикасније откривање и реаговање на сајбер нападе и претње, она такође са собом носи ризике и изазове, укључујући потенцијал за нападе на бази софтвера које покреће вештачка интелигенција. Међутим, невезано за криминал, постоје значајна етичка и правна разматрања која се морају размотрити како би се осигурало да се ВИ користи на одговоран и доследан начин попут питања која се односе на приватност и транспарентност, између осталог. Штавише, од суштинске је важности да се уравнотеже потенцијалне користи од вештачке интелигенције са потребом за етичком и одговорном употребом, укључујући заштиту приватности појединца и спречавање дискриминаторног и пристрасног доношења одлука од стране њених софтвера и алата.

Дипфејк технологија, која користи алгоритме машинског учења - подобласти

вештачке интелигенције за креирање реалистичних синтетичких медија, појавила се као поље које брзо напредује са низом потенцијалних примена, како позитивних тако и негативних. Са једне стране, њен потенцијал је видљив у различитим индустријама попут забаве и маркетинга јер омогућава стварање дигиталног садржаја који је изгледа реалистично. Са друге стране, поставља озбиљне етичке и друштвене изазове, посебно у контексту политичких дезинформација, манипулације јавним мњењем и криминалних делатности. Како дипфејк технологија наставља да се развија и постаје приступачнија просечном кориснику интернета, неопходно је разумети њене потенцијалне користи и ризике, као и шире импликације по друштво. Овај мастер рад има за циљ да пружи свеобухватну анализу дипфејка, укључујући његову основну технологију, примену и потенцијалне утицаје, те да истражи стратегије за решавање етичких, законских и друштвених изазова које поставља када се користи.

Како се технологија вештачке интелигенције константно транформише, а сајбер криминалци се прилагођавају и најмањим променама у овој области, постојала је потреба да се у овом раду испита веза нових технологија у контексту сајбер криминалитета, њихова заједничка будућност и могућа решења. У светлу наведеног може се закључити да како ова област буде напредовала, дипфејк ће постати још софистициранији и тежи за откривање, а његова употреба нарочито у криминалне и злонамерне сврхе може изазвати озбиљне и далекосежне последице. Дипфејк порнографија се појавила као значајан и узнемирујући тренд са озбиљним импликацијама по појединце али и друштво у целини. Употреба дипфејк технологије за стварање реалистичних синтетичких порнографских садржаја без пристанка укључених појединаца поставља озбиљна етичка и правна питања, укључујући питања приватности, пристанка и сексуалне експлоатације. Доступност и дистрибуција таквог садржаја представљају додатну претњу посебно за жене и девојке које су главна мета дипфејк порнографије.

Имајући у виду да јесу уложени напори у борби против дипфејка, да су га поједине државе и законодавно регулисале, а међународна заједница најавила како ће дипфејк законски кодификовати на међународном нивоу, те да су предузете технолошке противмере великих компанија и платформи - проблем је и даље знатан. Да би се ефикасно позабавили овим проблемом, потребан је свеобухватан приступ, укључујући повећану свест и образовање јавности, јача и квалитетнија правна заштита за жртве и развој напредних

технологија за откривање и уклањање оваквог садржаја. Штавише, од суштинског је значаја препознати шире друштвене и културне факторе који доприносе производњи и ширењу нарочито дипфејк порнографије, укључујући мизогинију, сексизам и објективизацију жена.

Србија за сада нема потребно законодавство којим би извршила криминализацију дипфејка. Закон о ауторском и сродним правима свакако није адекватан у случајевима дипфејк порнографије већ је то задатак Кривичног законика РС који још увек није криминализовао ни дело осветничке порнографије упркос вишегодишњим апелима и притисцима организација које се баве заштитом права жена. Иако КЗ укључује низ одредби које се односе на безбедност рачунарских података, једино кривично дело приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију може само делимично обезбедити кривичноправну заштиту у контексту дипфејка. Негативна страна овог решења јесте да се оно може користити само у случајевима када је малолетно лице искоришћено за дипфејк порнографију. Постојећа Стратегија о вештачкој интелигенцији свакако није адекватни инструмент за регулисање ове области стога би Србија требало да прати решења недавно усвојеног Закона о вештачкој интелигенцији будући да представљају добар искорак у погледу регулисања система ВИ (на територији ЕУ), те да покуша да постојеће и будуће системе ВИ стави у прикладни законодавни оквир.

Како су постојећи механизми недовољни и неадекватни, држава мора предузети хитне мере и кораке у циљу законодавног регулисања у погледу стварања, ширење и малициозне употребе дипфејка. Технолошке компаније и платформе морају своје активности да усмере на развој начина за откривање и ублажавање негативних ефеката дипфејка попут развоја алгоритама и алата за откривање лажног и синтетичког материјала док се јавност се мора образовати о томе како да препозна овакве садржаје. Држава би додатно морала да сарађује са међународном заједницом на размени информација и знања будући да је међународна сарадња од суштинског значаја за решавање прекограничне природе дипфејк напада. У складу са наведеним, будућност дипфејка ће вероватно зависити од тога како се исти користе, као и од технолошких, регулаторних и друштвених одговора на ову појаву.

ПОПИС КОРИШЋЕНЕ ЛИТЕРАТУРЕ

1. Agnes E. Venema and Zeno J. Geradts, Digital Forensics, Deepfakes and the Legal Process,
2. Awotunde, J.B.; Jimoh, R.G.; Imoize, A.L.; Abdulrazaq, A.T.; Li, C.-T.; Lee, C.-C. An Enhanced Deep Learning-Based DeepFake Video Detection and Classification System. Electronics 2023, 12, 87.
3. Blackburn, D., Eisenach, J., Harrison, D., (2019), Impacts of digital video piracy on the U.S. economy,
4. Bocij, P., Griffiths, M.D. & McFarlane, L. (2002). Cyberstalking: A new challenge for criminal law,
5. Bocij, Paul & McFarlane, Leroy. (2003). Cyberstalking: The Technology of Hate. The Police Journal. 76.
6. Boté-Vericad, Juan-José; Vállez, Mari, Image and video manipulation: The generation of deepfakes. In: Freixa, Pere; Codina, Lluís; Pérez-Montoro, Mario; Guallar, Javier (ed.). Visualisations and narratives in digital media. Methods and current trends, Barcelona,
7. Brundage, Miles, et al. "The malicious use of artificial intelligence: Forecasting, prevention, and mitigation (2018), The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation,
8. Celebi, Naciye, Qingzhong Liu, and Muhammed Karatoprak, A Survey of Deep Fake Detection for Trial Courts,
9. Citron, Danielle Keats and Mary Anne Franks. “Criminalizing Revenge Porn.” Wake Forest Law Review 49,
10. Clough, J., Principles of Cybercrime (2015), Cambridge University Press,
11. D. Güera and E. J. Delp, "Deepfake Video Detection Using Recurrent Neural Networks," 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), 2018,
12. Danielle K. Citron & Robert Chesney, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 California Law Review,
13. Das, Djurre & van Boheemen, Pieter & Linda, Nierling & Jahnel, Jutta & Karaboga, Murat & Fatun, Martin & Huijstee, Mariëtte. (2021). Tackling Deepfakes in European policy,
14. de Ruiter, A. The Distinct Wrong of Deepfakes. Philos. Technol. 34, (2021),
15. Delfino, Rebecca. (2020). Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn’s Next Tragic Act. Actual Problems of Economics and Law,
16. Facing reality? Law enforcement and the challenge of deepfakes, An Observatory Report from the Europol Innovation Lab,
17. Farago, Tunde. "Deep fakes–an emerging risk to individuals and societies alike." Tilburg University

(2019),

18. Galley, P. (1996) Computer terrorism:what are the risks? Science, Tehnology and Society, Swiss Federal Institute of Tehnology,

19. Goodman, Marc, Future Crimes: Inside the Digital Underground and the Battle for Our Connected, World (New York: Anchor Books, 2016),

20. H. Khalid and S. S. Woo, "OC-FakeDect: Classifying Deepfakes Using One-class Variational Autoencoder," 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Seattle, WA, USA, 2020,

21. Hine, E., Floridi, L. New deepfake regulations in China are a tool for social stability, but at what cost?. Nature Machine Intelligence 4,

22. Karuppannan, Jaishankar. (2023). The Future of Cyber Criminology: Challenges and Opportunities 1.

23. Kietzmann, Jan, Linda W. Lee, Ian P. McCarthy, and Tim C. Kietzmann. "Deepfakes: Trick or treat?." Business Horizons 63, no. 2 (2020),

24. Kleijssen, Jan & Perri, Pierluigi. (2017). Cybercrime, Evidence and Territoriality: Issues and Options,

25. Maddocks, Sophie, Feminism, activism and non-consensual pornography: analyzing efforts to end "revenge porn" in the United States, Feminist Media Studies, 22:7,

26. Mania, Karolina. (2022). Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study. Trauma, Violence, & Abuse,

27. Maras, Marie-Helen & Alexandrou, Alex. (2018). Determining Authenticity of Video Evidence in the Age of Artificial Intelligence and in the Wake of Deepfake Videos. International Journal of Evidence and Proof. 23,

28. Masood, M., Nawaz, M., Malik, K.M., Javed, A., Irtaza, A. and Malik, H., 2022. Deepfakes Generation and Detection: State-of-the-art, open challenges, countermeasures, and way forward. Applied Intelligence,

29. McCarthy, John, Marvin L. Minsky, Nathaniel Rochester, and Claude E. Shannon. "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955 Dartmouth AI Project Proposal,

30. McGlynn, C., Rackley, E., Johnson, K., Henry, N., Flynn, A., Powell, A., ... & Scott, A. (2019). Shattering lives and myths: a report on image-based sexual abuse,

31. Meskys, Edvinas and Kalpokiene, Julija and Jurcys, Paulius and Liaudanskas, Aidas, Regulating Deep Fakes: Legal and Ethical Considerations , Journal of Intellectual Property Law & Practice, Volume 15, Issue 1, January 2020,

32. Nassif, Ali & Nasir, Qassim & Abu Talib, Manar & Gouda, Omar. (2022). Improved Optical Flow Estimation Method for Deepfake Videos. Sensors,

33. Nils J. Nilsson, Principles of Artificial Intelligence (Palo Alto: Tioga, 1980),

34. Ohman, Carl, Introducing the pervert's dilemma: a contribution to the critique of Deepfake Pornography. Ethics and Information Technology. 22.

35. Pfefferkorn, Riana, 'Deepfakes' in the Courtroom, Boston University Public Interest Law Journal, Vol. 29, No. 2, 2020,

36. Phillips, Kirsty, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele, and Mary P. Aiken. 2022. "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies" Forensic Sciences 2, no. 2,

37. Quinney, Richard, "Structural Characteristics, Population Areas, and Crime Rates in the United States," The Journal of Criminal Law, Criminology and Police Science, 57(1),

38. Smith, Hannah, Mansted, Katherine. "What's the Problem?" Weaponised Deep Fakes: National Security and Democracy, Australian Strategic Policy Institute, 2020,

39. Stevens, Daphne, Regulating Deepfake Technology Legislative possibilities in the Netherlands to obstruct the use of deepfake technology for the creation of non-consensual pornography, Tilburg Law School,

40. Steyvers, Mark. (1999). Morphing techniques for manipulating face images. Behavior research methods, instruments, & computers: a journal of the Psychonomic Society, Inc. 31,

41. Temir, Erkam. (2020). Deepfake: New Era in The Age of Disinformation & End of Reliable Journalism,

42. Tonkolu, Demo, A.,,Investigating self efficienc of cybercrime on social media among university students" PhD diss, Near East University, 2019,

43. Traboulsi, Nicole. "Deepfakes: Analysis of Threats and Countermeasures." PhD diss., California State University, Fullerton, 2020,

44. van der Sloot, B., & Wagensveld, Y. (2022). Deepfakes: Regulatory challenges for the synthetic society. Computer Law & Security Review, 46,

45. Velasco, C. Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. ERA Forum 23,

46. Wagner, T. and Blewer, A. (2019) "The Word Real Is No Longer Real": Deepfakes, Gender, and the Challenges of AI-Altered Video. Open Information Science, Vol. 3 (Issue 1),

47. Wall, D. ,,What are Cybercrimes, The centre for crime and justice studies'', no. 58 Winter 2004/05,

48. Zhou, Y. and Lim, S.N., 2021. Joint audio-visual deepfake detection. In Proceedings of the IEEE/CVF International Conference on Computer Vision,

49. Анализа функционисања институција у борби против организованог високотехнолошког криминала у Србији, Београдски центар за безбедоносну политику, (март 2021),

50. Бјелајац, Ж., Матијашевић, Ј., Димитријевић, Д. (2012), Значај успостављања међународних стандарда у сузбијању високотехнолошког криминала. LXIII,

51. Бјелош, Маја, Павловић, Марија, Сајбер безбедност и људска права на Западном Балкану:случај Србије, Београдски центар за безбедоносну политику, 2022,

52. Димитријевић, Предраг, Компјутерски криминал, Презентације, Правни факултет у Нишу

53. Димовски, Д. (2019), Компјутерски криминалитет, Правни факултет Универзитета у Нишу, Зборник, LV,

54. Игњатовић Ђорђе (2016): Криминологија, Правни факултет Универзитета у Београду,

55. Константиновић Вилић, С., Николић Ристановић, В., (2018), Криминологија, Издавачко графичко предузеће, „Прометеј“, Београд,

56. Лилић Стеван, Прља Драган (2011), Правна информатика вештина, Правни факултет Универзитета у Београду

57. Лутовац, С., Рачић, Ј. (2021), Компјутерски криминал као савремени облик криминалитета. Мега, тренд ревија, 18(4),

58. Матијашевић, Ј. (2012), Високотехнолошки криминал у функцији организованог криминалитета.(У Организовани криминалитет, изазов 20. века,

59. Миладиновић Богавац, Ж., Чекеревац З., „Кривична дела против безбедности рачунарских података" Београд,

60. Петровић Р. Слободан, „Кибер - тероризам – Реалност или фикција“ часопис „Безбедност“ 2000. Вол. 42, бр. 5-6,

61. Петровић, С. Р. (2012), Дилема - кибер или сајбер. Страни правни живот, 2,

62. Прља, Д., Гасми, Г., Корać, В., 2022. Људска права и вештачка интелигенција, Институт за упоредно право Београд,

ПОПИС ОСТАЛЕ ИСТРАЖИВАЧКЕ ГРАЂЕ

Закони и подзаконски акти

1. Amendments adopted by the European Parliament on 20 January 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31,

2. California Assembly Bill 602 - Deepfakes and Sexually Explicit Material,

3. California Assembly Bill 730 - Deceptive Audio Or Visual Media,

4. Council of Europe, Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28.1.2003,

5. Council of Europe, Convention on Cybercrime, 23 November 2001,

6. Council of Europe, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No. : 201, Lanzarote, the 23 October 2007,

7. Council of Europe, The Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence , November 2014,

8. Draft Issues Paper on Intellectual Property Policy and Artificial Intelligence, WIPO/IP/AI/2/GE/20/1,

9. European Parliament resolution of 19 May 2021 on artificial intelligence in education, culture and the audiovisual sector (2020/2017(INI),

10. European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters, (2020/2016(INI)

11. New York Senate Bill (S5959D),

12. Proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (ARTIFICIAL INTELLIGENCE ACT),

13. Provisions On Administration Of Internet Audio-Video Program Services (Кина),

14. Provisions on the Administration of Deep Synthesis Internet Information Services (Кина),

15. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (General Data Protection Regulation) – Општа уредба о заштити података о личности,

16. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act),

17. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act),

18. Revised Issues Paper on Intellectual Property Policy and Artificial Intelligence, WIPO/IP/AI/2/GE/20/1 REV,

19. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, Council of Europe Treaty Series – No. 224,

20. Texas Senate Bill. No. 751,

21. Закон о ауторским и сродним правима, *Сл. гласник РС*, бр. 104/2009, 99/2011, 119/2012, 29/2016,

22. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, "*Сл. гласник РС*", бр. 94/2016, 87/2018 - др. закон и 10/2023,

23. Закон о потврђивању Конвенције Савета Европе о спречавању и борби против насиља надженама и насиља у породици, *Службени гласник РС* – Међународни уговори“, број 012/13,

24. Кривични законик, *Сл.гласник РС*, бр. 85/2005, 88/2005 – испр., 107/2005 – испр.72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019,

25. Стратегија за борбу против високотехнолошког криминала за период 2019–2023. Године, *Службени гласник РС*, број 71 од 25. септембра 2018,

26. Стратегија развоја вештачке интелигенције у Републици Србији за период 2020–2025. године, *Службени гласник РС*, број 96 од 31. децембра 2019.

27. Стратегија развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. Године, *"Службени гласник РС*", број 86 од 3. септембра 2021.

Интернет извори

1. https://revisesociology.com/2016/04/03/functionalist-explanations-of-deviance/
2. https://www.ojp.gov/pdffiles1/Digitization/118214NCJRS.pdf
3. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
4. https://www.mcafee.com/learn/5-common-types-of-identity-theft/
5. https://www.it-klinika.rs/blog/sta-je-keylogger
6. https://smartlife.mondo.rs/tech/uredjaji/a17963/Sajber-napad-Kako-otkljucati-zakljucane-fajlove-Sta-je-ransomware-napad-Sajber-napadi-u-Srbiji.html
7. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf
8. http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf
9. https://rm.coe.int/summary-workshop-2019-bat-2/16809c992a
10. https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf
11. https://www.forbes.com/sites/bernardmarr/2018/02/14/the-key-definitions-of-artificial-intelligence-ai-that-explain-its-importance/?sh=6c2e7ab04f5d
12. https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf
13. https://n1info.rs/biznis/natrazeniji-poslovi-u-svetu-sajber-kriminala-zarada-od-200-do-20-000-dolara/
14. https://www.atlasobscura.com/articles/abraham-lincoln-photos-edited

15. https://bdtechtalks.com/2020/09/04/what-is-deepfake
16. https://www.businessinsider.com/guides/tech/what-is-deepfake
17. https://recfaces.com/articles/what-is-deepfake#2
18. https://www.cnet.com/tech/computing/samsung-ai-deepfake-can-fabricate-a-video-of-you-from-a-single-photo-mona-lisa-cheapfake-dumbfake
19. https://www.cnet.com/tech/computing/samsung-ai-deepfake-can-fabricate-a-video-of-you-from-a-single-photo-mona-lisa-cheapfake-dumbfake
20. https://theconversation.com/deepfake-audio-has-a-tell-researchers-use-fluid-dynamics-to-spot-artificial-imposter-voices-18910
21. https://www.scip.ch/en/?labs.20210318
22. https://www.darkreading.com/attacks-breaches/deepfake-audio-scores-35-million-in-corporate-heist
23. https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/?sh=57ae3f7d2241
24. https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained
25. https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf
26. https://www.abajournal.com/web/article/courts-and-lawyers-struggle-with-growing-prevalence-of-
27. https://www.marshmclennan.com/insights/publications/2020/october/digital-deception--is-your-business-ready-for-deep-fakes-.html
28. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf
29. https://venturebeat.com/security/deepfakes-arent-going-away-future-proofing-digital-identity/
30. https://apnews.com/article/ap-top-news-artificial-intelligence-social-platforms-think-tanks-politics-bc2f19097a4c4fffaa00de6770b8a60d
31. https://www.theverge.com/2019/6/13/18677341/ai-generated-fake-faces-spy-linked-in-contacts-associated-press
32. https://www.vox.com/2019/10/7/20902215/deepfakes-usage-youtube-2019-deeptrace-research-
33. https://www.indiatoday.in/trending-news/story/journalist-rana-ayyub-deepfake-porn-1393423-2018-11-21
34. https://www.looper.com/184468/the-truth-about-recreating-paul-walker-for-fast-and-the-furious
35. https://www.technologyreview.com/2018/10/16/139739/how-acting-as-carrie-fishers-puppet-made-a-career-for-rogue-ones-princess-leia
36. https://thedali.org/press-room/dali-lives-museum-brings-artists-back-to-life-with-ai/
37. https://www.timesofisrael.com/at-this-holocaust-museum-you-can-speak-with-holograms-of-survivors
38. https://www.forbes.com/sites/simonchandler/2020/03/09/why-deepfakes-are-a-net-positive-for-humanity/?sh=6b1c8b022f84
39. https://www.engadget.com/2019-12-18-rolls-royce-quips-als-mnd-speech-ai.html?guccounter=2
40. https://www.darkreading.com/operations/preparing-for-the-next-cybersecurity-epidemic-deepfakes

41. https://venturebeat.com/security/deepfakes-arent-going-away-future-proofing-digital-identity
42. https://www.infosecurity-magazine.com/next-gen-infosec/data-protection-wake-deepfakes
43. https://blog.richardvanhooijdonk.com/en/the-good-the-bad-and-the-future-of-deepfakes/
44. https://www.yucom.org.rs/wp-content/uploads/2019/03/Istanbulska-konvencija-u-Srbiji-praksa-i-izazovi.pdf
45. https://www.mondaq.com/turkey/privacy-protection/863064/deepfake-an-assessment-from-the-perspective-of-data-protection-rules
46. https://inforrm.org/2022/02/03/pornography-platforms-the-eu-digital-services-act-and-image-based-sexual-abuse-clare-mcglynn-and-lorna-woods/
47. https://www.sidley.com/en/insights/newsupdates/2022/12/proposal-for-eu-artificial-intelligence-act-passes-next-level#:~:text=Following%20multiple%20amendments%20and%20discussions,)%20on%20December%206%2C%202022
48. https://www.lexology.com/library/detail.aspx?g=4700f977-4845-417b-834d-b3c06390ee27
49. https://www.bakerdatacounsel.com/state-legislation/if-signed-by-governor-california-bill-ab-602-will-provide-private-right-of-action-for-victims-of-sexually-explicit-deepfakes/
50. https://variety.com/2020/film/news/sag-aftra-commends-andrew-cuomo-deep-fake-videos-1234842715
51. https://www.unite.ai/european-and-uk-deepfake-regulation-proposals-are-surprisingly-limited/
52. https://www.gov.uk/government/news/new-laws-to-better-protect-victims-from-abuse-of-intimate-images
53. https://www.bbc.com/news/technology-63669711
54. https://www.theverge.com/2022/11/25/23477548/uk-deepfake-porn-illegal-offence-online-safety-bill-proposal
55. https://www.global-regulation.com/translation/china/160191/provisions-on-administration-of-internet-audio-video-program-services.html
56. https://www.chinalawtranslate.com/en/deep-synthesis/
57. https://www.china-briefing.com/news/china-to-regulate-deep-synthesis-deep-fake-technology-starting-january-2023
58. https://www.taipeitimes.com/News/front/archives/2023/01/08/2003792190
59. https://www.koreatimes.co.kr/www/tech/2020/04/129_279851.html
60. https://bezbednost.org/publikacija/sajber-bezbednost-i-ljudska-prava-na-zapadnom-balkanu-slucaj-srbije
61. https://www.srbija.gov.rs/extfile/sr/437304/strategija_razvoja_vestacke_inteligencije261219_2_cyr.pdf
62. http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2018/71/1/reg

САЖЕТАК И КЉУЧНЕ РЕЧИ

Криминалитет као феномен има значајан утицај на појединце, заједницу и друштво у целини, а различите врсте криминалитета имају различите узроке, последице и решења. Због тога разумевање природе криминалитета захтева интердисциплинарни приступ који узима у обзир низ друштвених, економских и политичких фактора, као и сложену корелацију између понашања појединца и ширих друштвених норми и вредности.

Сајбер криминалци се стално прилагођавају новим технологијама и користе их за обављање незаконитих активности на софистицираније и ефикасније начин. Појава и свакодневна употреба вештачке интелигенције и алгоритама машинског учења допринели су да сајбер криминалци аутоматизују своје нападе и прецизније идентификују и уоче рањивости једног система, те да делују убедљивије приликом извршења традиционалних кривичних дела попут преваре или крађе.

У раду је са једне стране истражено како сајбер криминалци иду у корак са најновијим технологијама и употребљавају их за извршење најразноврснијих деликта, а са друге је испитан однос између сајбер криминалитета и дипфејка, односно синтетичког медија генерисаног коришћењем алгоритама дубоког учења. Пружен је свеобухватан преглед техничких аспеката креирања дипфејка, као и различитих врста криминалних али и потенцијално опасних понашања у чијој је основи дипфејк, као што су превара, крађа идентитета, осветничка порнографија и друштвени инжењеринг. Такође, дат је простор позитивним аспектима ове технологије у разним сферама живота. Посебно су истакнуте етичке импликације дипфејка, укључујући његов потенцијал да пољуља поверење у медије и нанесе штету појединцима и друштву.

Кроз овај рад обрађено је постојеће међународно законодавство у погледу дипфејка, недостаци у домаћем као и будуће стратегије и кораци који би требало да буду предузети од стране Републике Србије и међународне заједнице како би борба против злонамерне употребе дипфејк технологије била успешна. Додатно су истражени правни и политички оквири у погледу сајбер криминалитета и изазови регулисања и спровођења закона у информационо-технолошком пејзажу који се брзо развија.

Свеукупно, овај рад има за циљ да допринесе бољем разумевању сложеног питања дипфејк технологије у контексту сајбер криминалитета и да обезбеди свеобухватан оквир за решавање овог феномена. Досадашња истраживања нагласила су потребу за континуираним проучавањем, сарадњом и иновацијама у борби против сајбер криминалитета и дипфејка као и политичком интервенцијом са циљем решавања ове нове и растуће претње дигиталној безбедности и друштвеном поверењу.

Кључне речи: сајбер криминалитет, вештачка интелигенција, дипфејк, синтетички медији, порнографија, кривични поступак

SUMMARY AND KEYWORDS

AI generated videos (deepfakes) as a form of cybercrime

Crime as a phenomenon has a significant impact on individuals, communities and society, and different types of crime have different causes, consequences and solutions. Therefore, understanding the nature of crime requires an interdisciplinary approach that takes into account a number of social, economic and political factors, as well as the complex correlation between individual behavior and broader social norms and values.

Cybercriminals are constantly adapting to new technologies and using them to carry out illegal activities in a more sophisticated and efficient manner. The emergence and daily use of artificial intelligence and machine learning algorithms have contributed to cybercriminals automating their attacks and more precisely identifying and spotting the vulnerabilities of a system, as well as acting more convincingly when committing traditional crimes such as fraud or theft.

This paper examines how cybercriminals are keeping up with the latest technologies and use them to commit the most diverse crimes, the relationship between cybercrime, deepfake and synthetic media generated using deep learning algorithms. It also provides a comprehensive overview of the technical aspects of deepfake creation, as well as various types of crimes based on deepfake content, such as fraud, identity theft, revenge pornography and social engineering. Additionally, it gives space to the positive aspects of deepfake technology in various areas of life. In particular, the ethical implications of deepfake were highlighted, including it's potential to undermine trust in the media and harm individuals and society.

Through this work, the existing international legislation regarding deepfake was processed, shortcomings in the domestic one as well and future strategies and steps that should be taken by the Republic of Serbia and the international community in order to fight against the malicious use of deepfake technology are addressed too. Additionally, the legal and policy frameworks regarding cybercrime and the challenges of regulation and law enforcement in the rapidly evolving information technology landscape were explored.

Overall, this paper aims to contribute to a better understanding of the complex issue of deepfake technology in the context of cybercrime and to provide a comprehensive framework for addressing this phenomenon. Previous research has highlighted the need for continued study, collaboration and innovation in the fight against cybercrime and deepfakes, as well as political intervention aimed at addressing this new and growing threat to digital security and social trust.

Keywords: cybercrime, artificial intelligence, deepfake, synthetic media, pornography, criminal procedure

БИОГРАФИЈА СТУДЕНТКИЊЕ

Милица Момчиловић рођена је 26.01.1991. године у Лесковцу. Основну школу и гимназију завршила је у Лебану. Дипломирала је на Правном факултету Универзитета у Нишу 2019. године, а мастер студије на истом факултету, смер ,,Унутрашњи послови“ уписује 2020/2021. године и завршава их са просечном оценом 9,80. Као студенткиња, учесница је разних трибина, семинара и конференција, од којих издваја учествовање у регионалној школи људских права и moot court такмичењу ”Horizontal Facility for the Western Balkans and Turkey II”, спроведену под окриљем Савета Европе, ,,Internet Freedom Meet“ окупљање одржано у Тирани и организовано од стране Балканске истраживачке мреже Србије (БИРН), радионице “Climate and Tech Justice” реализоване од стране Универзитета "LUISS Guido Carli" из Рима и програма ,,Cyber School’’ организованог од стране невладине организације која са бави сајбер безбедношћу ,,Cyber Peace Institute’’ у сарадњи са компанијом ,,Мајкрософт’’. Кандидаткиња је била учесница прве школе приватности одржане од стране организације ,,Партнери Србија“ и полазница специјалистичког курса Међународног избегличког права имплементираног од стране Међународног института за хуманитарно право из Санрема. Обавезну стручну праксу обавила је у Основном јавном тужилаштву у Лебану, а правосудни испит положила маја 2023. године. Запослена је у ИТ компанији на пословима усклађености пословања (compliance). Говори енглески и служи се француским језиком.

ИЗЈАВА О ИСТОВЕТНОСТИ
ШТАМПАНОГ И ЕЛЕКТРОНСКОГ ОБЛИКА МАСТЕР РАДА

Име и презиме аутора мастер рада: Милица Момчиловић

Наслов мастер рада: Видео снимци генерисани уз помоћ вештачке интелигенције (дипфејк) као облик сајбер криминалитета

Ментор: Проф. др Дарко Димовски

Изјављујем да је електронски облик мастер рада у pdf формату истоветан штампаном облику, који сам предао/ла Правном факултету Универзитета у Нишу.

У Нишу, _____

Потпис аутора

_____

ИЗЈАВА О АУТОРСТВУ И ОДОБРАВАЊУ ОБЈАВЉИВАЊА МАСТЕР РАДА

Изјављујем да је мастер рад, под насловом:,,Видео снимци генерисани уз помоћ вештачке интелигенције (дипфејк) као облик сајбер криминалитета''
пријављен и одбрањен на Правном факултету Универзитета у Нишу:
• резултат сопственог истраживачког рада;
• да овај мастер рад у целини, нити у деловима, нисам пријављивао/ла на другим факултетима, нити универзитетима;
• да нисам повредио/ла ауторска права, нити злоупотребио/ла интелектуалну својину других лица.

Дозвољавам да се овај мастер рад чува у библиотеци и објави на сајту Правног факултета Универзитета у Нишу, са подацима о датуму одбране и комисији пред којом је рад брањен.

Аутор мастер рада: Милица Момчиловић, М 033/23-УП

У Нишу, _____

Потпис аутора

_____