УНИВЕРЗИТЕТ У НИШУ

ПРАВНИ ФАКУЛТЕТ

ДИГИТАЛНО ПАРТЕРСКО СЕКСУАЛНО НАСИЉЕ (ОСВЕТНИЧКА ПОРНОГРАФИЈА) КАО ОБЛИК КРИМИНАЛИТЕТА

Ментор:

проф др Дарко Димовски

Студент:

Данијела Вукићевић, М002/22-ИТ

Ниш, 2024. године

САДРЖАЈ

УВОД

У савременом друштву, свеобухватни напредак технологије у протеклих седам деценија створио је парадигматску трансформацију у свим аспектима људског живота. Централни протагониста ове технолошке експлозије је компјутер, чији је неоспоран значај постао неоспорно битан у различитим сферама људске делатности. Поред тога, широка доступност компјутерских технологија омогућила је масовно усвајање ових уређаја, што је резултирало њиховом свеприсутношћу у скоро сваком домаћинству. Употреба рачунара као кључног инструмента за повећање продуктивности и олакшавање приступа информацијама је укорењена у темељима савременог друштва, што их чини незамисливим без присуства ових технолошких ентитета. Међутим, уз све очигледне предности, појава рачунара и њихова даља еволуција довела је до појаве нових облика криминалних активности и иновативних методологија за њихово извршење.

Приступачност компјутерских технологија омогућава свакоме са основним знањем да учествује у незаконитим активностима, чиме се смањује баријера за улазак у сферу сајбер криминала. Исто тако, глобално усвајање интернета омогућава прелазак граница у извршењу кривичних дела, што ствара нове изазове за правосудне системе широм света. У том контексту, питање безбедности рачунарских система и интегритета података постаје кључно за очување друштвеног поретка и функционисање савременог друштва. Дакле, изазови који произилазе из технолошког напретка захтевају не само техничка решења већ и мултидисциплинарни приступ који укључује правне, етичке и друге факторе како би се на адекватан начин одговорило на растуће претње у области сајбер безбедности.

Криминалци искоришћавају значајну брзину, лакоћу и посебно анонимност коју пружају савремене технологије да би се укључили у различите незаконите активности. Поменуте активности углавном обухватају сајбер нападе на рачунарске системе и мреже, као и случајеве крађе идентитета и података, ширења дечије порнографије, лажних активности и пиратерије у домену компјутерског софтвера и сродних предмета. Земље које су постигле значајан технолошки напредак донеле су законе који се односе на ове

нове криминалне активности у различитим временским периодима, при чему су неке то чиниле раније, а друге касније.

У последње време као вид компјутерског криминалитета јавља се осветничка порнографија. С тим у вези неопходно је посветити пажњу њеним појавним облицима како би надлежни органи што пре знали како да препознају њено извршење, али и на који начин да реагују у складу са постојећим нормативним оквиром. Израз „осветничка порнографија“ се може користити за описивање ситуације у којима се интимни или експлицитни материјал неке особе дистрибуира или дели без њихове пристанке или против њихове воље, често као облик освете или за наношење штете тој особи. Овај облик злоупотребе може укључити објављивање приватних фотографија, видео снимака или другог сексуално експлицитног садржаја без дозволе особе на тим материјалима.Осветничка порнографија представља озбиљан проблем који може имати дубоке психолошке и социјалне последице на жртве и друштво у целини. Овај предмет истраживања усмерава пажњу на разумевање тих последица и њихов утицај на живот појединаца и заједнице. Предмет истраживања овог рада је утврђивања у којим областима се појављује компјутерски криминалитет са освртом на осветничку порнографију као вид компјутерског криминалитета.

Циљ истраживања овог рада да на основу анализе доступне релевантне литературе дубље разуме концепт осветничке порнографије као вида компјутерског криминалитета. Осветничка порнографија се јавља као веома озбиљан проблем савременог друштва и има веома значајан утицај на друштво. Основни циљеви истраживања обухватају посматрање феномена осветничке порнографије у контексту друштвене импликације, при чему би посебна пажња била посвећења појавним облицима и узрочношћу овог облика компјутерског криминалитета, кроз призму законодавне регулативе осветничке порнографије у домаћем и страном законодавству.

1. ПОЈАМ И ОБЛИЦИ КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА

1.1. Појам и распрострањеност компјутерског криминалитета

У савременом друштву, компјутерски криминал је постао неизбежан и значајан аспект нашег свакодневног живота. Иако његове појаве често пролазе несвесно или без директног учешћа, ваља напоменути да су информатички развијене земље, као и оне које теже таквом статусу, формирале специјализоване организације и радне групе са циљем праћења и истраживања компјутерског криминала на националном и међународном нивоу. Ово је резултат препознате важности и друштвене опасности коју компјутерски криминал представља, као и потребе за адекватним одговором и суочавањем са њим у свим сегментима друштва.

Компјутерски криминал, у светлу свог специфичног карактера и велике друштвене опасности, представља озбиљан друштвени проблем. Он се непрекидно шири и еволуира, посебно у оквиру различитих облика и видова испољавања. Због тога, постаје неопходно да друштво у целини, као и правни субјекти као што су организације и корпорације, приложе значајне напоре у борби против овог феномена. Друштво, држава и међународна заједница морају обратити пажњу на овај проблем и развити ефикасне механизме за сузбијање компјутерског криминала.

Рачунари и рачунарска технологија, као савремени алати комуникације, могу бити подложни многим облицима злоупотребе који угрожавају приватност корисника, нарушавају доступност и поузданост рачунарских мрежа и комуникационих система и служе као медиј за вршење конвенционалних криминалних активности. Приметна је корелација између степена друштвеног развоја и распрострањености различитих облика криминалних активности. Како друштво напредује, постоји све већи потенцијал за појаву и опстанак широког спектра кривичних дела. Такође, методе које се користе у извршењу ових злочина имају тенденцију да постају разноврсније и сложеније, док број и компетенција појединаца који су укључени као извршиоци такође имају тенденцију раста. Компјутерски криминал обухвата активну и пасивну употребу рачунара, као и задржавање доказа који се односе на кривично дело почињено било у компјутеру или у електронском формату. Физичка и правна, који користе рачунар или се ослањају на

његову функционалност, могу се класификовати као жртве или потенцијалне жртве таквих злочина.[1]

У литератури још увек не постоји консензусна и општеприхваћена дефиниција компјутерског криминала. Овај проблем потиче из чињенице да је компјутерски криминал релативно нов појам, са изузетном динамиком и различитим облицима извршења. Истовремено, он представља савремени облик кривичног дела који захтева постојано ажурирање и прилагођавање правних и регулаторних оквира.[2]

Компјутерски криминалитет је криминално понашање које користи компјутерску и информатичку технологију у извршењу кривичних дела или употребљава рачунар као средство за извршење криминалних радњи. Па тако, компјутерски криминалитет, може се дефинисати као облик криминалног понашања који користи компјутерску и информатичку технологију у сврху извршења кривичног дела или се сам рачунар употребљава као средство за извршење криминалне радње, на начин да се остварује нека последица.[3]

Компјутерски криминалитет је озбиљна претња која се јавља у савременом друштву. Он обухвата различите видове незаконитих радњи које се извршавају у вези са компјутерским системима. Ово може укључити акте који имају за циљ уништење, отуђење или оштећење рачунарских система или њихових делова. Такође, под обухватањем компјутерског криминалитета сматрају се и акције као што су уништење, оштећење, отуђење и неовлашћена измена софтверских и програмских производа, као и података. Ово може довести до озбиљних последица како за индивидуалце тако и за организације, укључујући финансијске губитке, губитак података и угрожавање безбедности. Додатно, компјутерски криминалитет укључује и извршавање кривичних дела путем компјутерских система, као и неовлашћено коришћење рачунарских ресурса и нарушавање сигурносних система.[4] Због тога је од кључног значаја усмерити пажњу и ресурсе на борбу против оваквих активности и унапређење система заштите и безбедности информационих технологија.

[1] Вилић, В. (2016). *Повреда права на приватност злоупотребе друштвених мрежа као облик компјутерског криминалитета.* Докторска дисертација, Ниш, стр. 93.
[2] Бошковић, М. (2020). *Криминологија*. Нови Сад: Правни факултет за привреду и правосуђе, стр. 361.
[3] Алексић, Ж., Шкулић М. (2007). *Криминалистика*. Београд: Службени гласник, стр. 385.
[4] Петровић, С. (2004). *Компјутерски криминал*. Београд: Војно-издавачки завод, стр. 61-62.

Компјутерски криминалитет представља серију кривичних дела која се извршавају коришћењем рачунарских система као средства или мете. У детаљној дефиницији оваквог криминалитета, фокус је на томе да је рачунарски систем средство које омогућује извршење дела или је сам мета кривичне радње. Без употребе компјутера, та дела би била немогућа или би имала значајно другачије карактеристике. Примери компјутерског криминалитета укључују хакерске нападе на системе, крађу личних података путем интернета, распрострањивање злонамерног софтвера као што је маливер, и финансијске преваре које се одвијају преко онлајн платформи. У свим овим случајевима, рачунар игра кључну улогу као алат за извршење или објекат кривичних радњи.[5]

Током протеклих година, разумевање компјутерског криминала је претрпело значајне промене, одражавајући еволуцију употребе рачунара. Овај облик криминала укључује неправилну употребу рачунара и њихову све већу примену у различитим сферама. С обзиром да је компјутерски криминал релативно нова појава, која се развијала упоредо са брзим напретком технологије, недостатак адекватне законске регулативе додатно отежава дефинисање ове појаве, која представља изазов за правосудни систем.

Компјутерски злочин се може описати као облик деликта који је дубоко повезан са употребом рачунара. У неким случајевима, рачунар се може користити за извршење самог злочина, док у другим може бити мета напада. С обзиром на кључну улогу коју технологија, посебно рачунари, играју у савременом пословању, јасно је да компјутерски криминал може имати озбиљне последице по привреду, инфраструктуру, комуникације, финансије и друге области. Штета која проистиче из компјутерских злочина је често већа него што би се на први поглед могло претпоставити, често превазилазећи обим штете узроковане традиционалним облицима криминала. Процене показују да финансијски губици због компјутерског криминала могу достићи стотине милиона долара.

Компјутерски криминал обухвата низ атрибута који су кључни за разумевање његове природе и утицаја. На основу дискурса који сте споменули, можемо истаћи неколико кључних атрибута. *Просторна димензија* криминалне активности односи се на географску дистрибуцију и локацијске обрасце криминалног понашања. Компјутерски криминал може бити глобалне природе, јер Интернет омогућава криминалцима да делују

[5] Игњатовић, Ђ. (1991). Појмовно одређење компјутерског криминалитета. *Анали Правног факултета*, 39(1-3), Београд: Правни факултет, стр. 142.

из различитих делова света, прелазећи националне границе. *Временска димензија* криминалне активности се односи на аспекте везане за време, као што су учесталост, трајање и временски обрасци кривичних инцидената. Компјутерски криминал може бити континуиран, с обзиром да се напади могу десити у било ком тренутку, а појединачни напади могу бити краткорочни или дугорочни, у зависности од циља и стратегије нападача. *Феномен сталне експанзије у нове секторе друштвеног живота* значи континуирани процес којим се криминалне активности инфилтрирају и утичу на различите домене друштвеног функционисања. Компјутерски криминал стално проналази нове методе и жртве, ширећи се у различите секторе као што су финансије, здравство, приватност података итд. *Детаљна карактеризација учиниоца* омогућава разумевање мотива, способности и метода коришћених у извршењу кривичних дела. Појединци, групе или организације могу бити укључени у компјутерски криминал, са различитим нивоима стручности и циљевима. Значајан *ентитет у сенци* односи се на то како се криминалне активности могу сакрити или маскирати, што их чини тешким за откривање и сузбијање. Нападачи често користе технике као што су шифровање података или анонимне мреже да сакрију свој идентитет и трагове. *Методологија коришћена у извршењу и идентификацији кривичних дела* односи се на техничке и стратешке приступе које извршиоци користе у извођењу напада, као и на процесе откривања и истраге ових радњи од стране надлежних органа. *Величина последица и обим штете* могу бити значајни, јер компјутерски напади могу изазвати озбиљне економске, социјалне и безбедносне последице. То може укључивати крађу финансијских средстава, компромитовање личних података, поремећај виталних система итд. *Вишеструка природа* рачунарске технологије указује да се исти алати и технологије који омогућавају напредак и развој друштва могу користити и у злонамерне сврхе. Компјутерски криминал користи рањивости и недостатке у технолошким системима за извођење напада.[6]

Ови атрибути су важни за разумевање сложености компјутерског криминала и развој стратегија за сузбијање и спречавање таквих активности.

Управљање и борба против компјутерског криминала захтева мултидисциплинарни приступ, укључујући сарадњу између правосудних органа, технолошких стручњака, приватног сектора и међународних организација. Неопходно је

[6] Subotin, M., Obradović, J. M. (2019). Criminological and criminal aspects of computer crime. *Pravo i digitalne tehnologije*, 37(3), 1-12.

континуирано унапређивати законодавство како би се прилагодило промјенама у технолошком пејзажу и обезбиједило ефикасно суочавање са све сложенијим облицима криминала. Поред тога, едукација и подизање свести о безбедности информација играју кључну улогу у превенцији оваквих инцидената. Кроз ове напоре, можемо радити на стварању сигурнијег и отпорнијег дигиталног окружења за све кориснике рачунара и Интернета.

За борбу против компјутерског криминалитета, потребно је да правосудне институције и технолошке компаније сарађују у развоју напредних сигурносних система, образовању јавности о безбедности на интернету и примени ефикасних закона који регулишу овај облик криминалитета. Овај приступ помаже у заштити корисника и компанија од потенцијалних штетних последица компјутерских кривичних дела.

1.2. Врсте компјутерског криминалитета

У савременом дигиталном добу, рачунарски системи и подаци представљају основну инфраструктуру која омогућава функционисање многих сегмената друштва, од приватних компанија до јавних институција. Међутим, са повећањем значаја ових система, повећава се и ризик од неовлашћеног приступа, брисања, измене или оштећења података. Законодавство Републике Србије у потпуности препознаје озбиљност ових дела, дефинишући их као кривично дело у складу са Кривичним закоником.

Кривично дело *оштећење рачунарског система или података* има за последицу угрожавање заштићеног добра, што може резултирати озбиљним последицама по појединца, предузеће или чак цело друштво. То може довести до губитка података, нарушавања приватности, финансијских губитака или поремећаја у функционисању јавних услуга.[7]

Компјутерска саботажа, позната и као рачунарска саботажа, представља серију акција које се односе на манипулацију, уништење или преусмеравање рачунарских података или програма са циљем ометања нормалног функционисања рачунара. Овај облик саботаже може обухватити различите активности, укључујући брисање важних

[7] Кривични законик Републике Србије, Службени 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, чл. 298.

информација, мењање података или програма, као и упаде у рачунарски систем ради ометања нормалног рада. Саботаже могу причинити оштећења на самом рачунару или другим уређајима за обраду података у систему. Ове активности могу имати различите циљеве, укључујући уклањање или онемогућавање приступа важним информацијама, штете компанији или организацији која користи рачунарски систем, као и крађу података за личне или финансијске користи.[8]

Са повећаном употребом рачунарских система, такође се повећава и ризик од рачунарских злочина, укључујући и прављење и уношење рачунарских вируса. Прављење и уношење рачунарских вируса представља озбиљан криминални чин који може проузроковати озбиљне последице, како за појединце, тако и за организације. Овај облик криминала се кажњава законом, а постоје различити облици и тежине овог дела, зависно од намера и последица које произилазе из напада. Особа која ствара рачунарски вирус са намером да га унесе у туђи рачунар или рачунарску мрежу чини основни облик овог кривичног дела. Сам чин прављења вируса представља основну радњу извршења овог дела. Рачунарски вируси су софтверски програми који имају способност да се реплицирају и шире штетне ефекте по систем у који су унети. Њихове врсте и карактеристике могу бити различите, а њихова сврха може бити разнолика - од крађе података до онеспособљавања система.[9]

Рачунарска превара је озбиљан проблем савременог друштва. Ова врста компјутерског криминала обухвата различите методе и технике којима се остварује финансијска корист за учиниоца или за неког другог. Мотиви за извршење овог кривичног дела могу бити различити, укључујући финансијску корист, личну корист или штету другима. Овај чин се обично спроводи уношењем нетачних података у рачунарску мрежу или систем, или неуношењем тачних података. Понекад се сам компјутерски систем манипулише или злоупотребљава да би се постигао циљ преваре. На пример, електронски системи могу бити хаковани ради добијања приступа финансијским подацима, преваре електронских плаћања или фалсификовања информација да би се стекла незаслужена корист. Овакве активности наносе штету појединцима, компанијама и друштву у целини. Поред финансијских губитака, компјутерска превара може

[8] Бошковић, М. (2020). нав. дело, стр. 368.
[9] Кривични законик, чл. 300.

проузроковати и кршење приватности, претње безбедности података, губитак пословног и јавног поверења у интернет и електронске системе.[10]

Хакинг криминалитет представља сериозну претњу за целокупну безбедност у дигиталном окружењу. Кривична дела која су повезана са хакерским активностима обухватају неовлашћени приступ рачунарским системима и базама података. Особе које се баве оваквим радњама, познате као хакери, често имају различите мотиве као што су жеља за авантуром, потврђивање својих вештина или чак само за забаву. Међутим, и покушаји хаковања из незлонамерних мотива могу имати озбиљне последице. Неупотребљивање личних података, угрожавање приватности, као и штете пословним системима, су само неки од потенцијалних ризика. Често путем хаковања се угрожавају не само рачунарски системи већ и особе или компаније које користе те системе.[11]

Спречавање и ограничавање приступа јавној рачунарској мрежи представља сериозно кривично дело које има за циљ да заштити интегритет и безбедност информационих система који су кључни за функционисање различитих институција и организација. Овај вид кривичног дела може се појавити у различитим облицима, од једноставних акта неовлашћеног спречавања или ометања приступа јавној рачунарској мрежи, до озбиљнијих случајева када је у питању злоупотреба службеног положаја. У основном облику кривичног дела, лице које неовлашћено спречава или омета приступ јавној рачунарској мрежи може бити кажњено новчаном казном или затвором до једне године. Ово се односи на случајеве када неко намерно блокира или пречи у нормалном коришћењу рачунарске мреже која је од јавног значаја. У случају да је учинилац овог дела службено лице, а као такав користи свој положај да спречи или ометне приступ јавној рачунарској мрежи, ради се о квалификованом делу. Таква злоупотреба службеног положаја може имати озбиљне последице по безбедност и функционисање рачунарских мрежа, због чега је предвиђена казна затвора до три године.[12]

Компјутерске злоупотребе, познате и као компјутерске крађе или неовлашћено коришћење рачунара и рачунарских мрежа према домаћем законодавству, представљају озбиљан проблем који често има озбиљне последице. Овај облик криминала је чест и носи са собом велике економске и имовинске губитке. Овај облик криминала укључује разне активности као што су уношење, мењање, брисање или ометање рачунарских

[10] Бошковић, М. (2020). нав. дело, стр. 368.
[11] Исто, стр. 366.
[12] Кривични законик, чл. 303.

података или програма, с намером да се оствари незаконита економска добит. Последице оваквих дела могу бити разнолике, од директних финансијских губитака до штете по репутацију појединаца или компанија. Један од најчешћих облика компјутерских злоупотреба, који такође има озбиљне последице, јесте злоупотреба крађе идентитета. Ово представља ситуацију у којој се неовлашћено користи идентитет неке особе ради остваривања користи или извршавања разних криминалних активности. То може укључивати крађу личних података попут имена, адресе, бројева личних докумената или банковних информација, што може довести до великих проблема за жртву, укључујући финансијске губитке, кршење приватности, па чак и правне проблеме.[13]

Дакле, компјутерски криминалитет представља озбиљан изазов у савременом друштву, а његове различите манифестације обухватају широк спектар активности. Једна од истакнутих манифестација је компјутерска крађа, која ставља велики акценат на сферу компјутерског криминала. Друга врста која се издваја је крађа идентитета, која представља значајан друштвени проблем због штетних последица које има на поверење у пословне трансакције и приватност појединаца. Пораст случајева крађе идентитета може се директно приписати експанзији електронске трговине, која пружа више простора за такве активности. Починиоци оваквих злочина често користе украдене идентитете за разне незаконите активности, попут отварања лажних банковних рачуна, добијања кредита или чак куповине, а све то на рачун правог власника идентитета. Људи чији су идентитети украдени најчешће нису свесни злоупотребе све док не примете необичне финансијске трансакције или не добију повезане финансијске извештаје. Раширена је и компјутерска превара, коју карактерише намерна манипулација рачунарским системима, како софтверским тако и хардверским средствима.

Ове лажне праксе имају за циљ стицање финансијске користи или наношење штете циљаним системима. Овакве активности се могу реализовати уношењем нетачних података у рачунарски систем, изостављањем тачних података или коришћењем рачунара на начин који омогућава неовлашћено понашање. Сагледавање читавог спектра лажних активности и њиховог модуса операнди захтева детаљно истраживање, с обзиром да обухвата широк спектар рудиментарних и софистицираних шема.

Напредне шеме често захтевају висок ниво стручности од стране преступника. Активности попут хаковања рачунара и прислушкивања рачунара спадају у домен

[13] Бошковић, М. (2020). нав. дело, стр. 367.

добијања информација без одговарајућег овлашћења коришћењем рачунара. Хаковање рачунара се односи на незакониту инфилтрацију у информационе системе са циљем добијања поверљивих информација или неовлашћеног приступа подацима, често са намером да се те информације измене, униште или нанесу штету.

Надаље, битно је напоменути и феномен компјутерског прислушкивања укључује скривене методе снимања визуелног садржаја приказаног на монитору рачунара појединца. Ово се може постићи коришћењем видео опреме или повезивањем на монитор за праћење приказаних информација. Важно је напоменути да се компјутерско прислушкивање разликује од неовлашћеног приступа, јер укључује праћење информација без могућности манипулисања или одабира материјала који се преноси. Неовлашћено коришћење рачунарских ресурса обухвата активности као што су личне и комерцијалне активности, коришћење рачунарског хардвера и софтвера у приватне сврхе, као и учешће у рекреативним активностима на рачунару током радног времена. Људи одговорни за ове злоупотребе су често запослени у компјутерским одељењима, укључујући оператере и програмере, који имају овлашћени приступ. Такве активности могу укључивати модификацију или уништавање рачунарских информација, ометање или ограничавање приступа овлашћеним корисницима. Мотивације за ове акције могу бити различите, укључујући личне освете, политичке факторе или незадовољство фирмом или колегама.[14]

Пролиферација компјутерског тероризма представља растућу претњу глобалном друштву. Сајбер ратовање, с друге стране, обухвата намерне и политички мотивисане акције које укључују уништавање или ометање компјутерских система, са циљем дестабилизације нација или вршења притиска на њихове владе. У данашњем свету постоји опипљив ризик да информациони ресурси и глобалне информационе мреже постану моћно оруђе које користе терористички субјекти.[15]

1.3. Појам и врсте нападача у сајбер простору

У савременом свету информационо-комуникационе технологије представљају неизоставан део нашег живота, омогућавајући нам да обављамо различите задатке и

[14] Николић-Ристановић, В., Константиновић Вилић, С. (2018). *Криминологија*. Прометеј, стр. 175.
[15] Исто, стр. 176.

комуницирамо на разнообразне начине. Међутим, уз напредак технологије, појављују се и они који је користе на штетан начин. Особе које се упуштају у нападе на рачунарске системе, у намери да угрозе њихову безбедност и нанесу штету, треба да буду осуђење и сматране одговорним за своје делатности.

Нападачи у области информационо-комуникационих технологија често користе своје знање и стручност како би проникли у рачунарске системе, крали информације, уништавали податке или ометали нормално функционисање система. Такви напади не само што могу изазвати материјалну штету, већ могу изазвати и озбиљне последице по приватност, безбедност и функционисање различитих институција и организација.[16]

За борбу против оваквих напада, неопходно је да постоје ефикасни механизми за откривање и спречавање инцидената, као и да се примене одговарајуће законске и техничке мере за заштиту информација и рачунарских система. Исто тако, образовање и освешћивање јавности о безбедносним ризицима које носи употреба информационо-комуникационих технологија може допринети смањењу броја напада и заштити корисника.

Постоји неколико начина за поделу група нападача који угрожавају безбедност рачунарских система, односно представљају претњу у сајбер простору. Једна од подела је на: *White Hat* хакере, *Black Hat* хакере, *Grey Hat* хакере и *Blue Hat* хакере.

„Бели шешири“, познати и као *White Hat* хакери, су етички нападачи рачунарских система. За разлику од *Black Hat* хакера, који имају лоше намере и углавном се баве кражом информација или оштећивањем система, бели шеширови користе своје вештине у добром духу. Они приступају системима користећи одређене технике и алате за напад, али уместо да нанесу штету или преузму информације, њихов циљ је да пронађу слабости и пропусте у заштити. Сврха ових упада у системе је да се идентификују ризици у безбедности и сигурности самог система. Уместо да злоупотребе ове пропусте, *White Hat* хакери их извештавају надлежнима или власницима система о потенцијалним проблемима. Овакво понашање има за циљ да помогне у унапређењу безбедности и заштите података, што је од кључног значаја у данашњем дигиталном друштву.[17]

[16] Вулетић, Д. (2017). Сајбер безбедност. У: *Интегрална безбедност Републике Србије*, Београд: Факултет за пословне студије и право, Факултет за стратешки и оперативни менаџмент, Универзитет „Унион-Никола Тесла“, стр. 176.
[17] Исто.

Black Hat хакери су одметници који се баве разбијањем безбедности рачунарских система. Ови нападачи су такође познати као крекери, назив који наглашава њихову тенденцију да креирају злонамерне програме као што су вируси или тројанци. Главни циљ ових злонамерних програма је да провале у рачунарски систем са намером да приступе подацима или нанесу штету систему. Хаковање са овим намерама представља озбиљну претњу по безбедност информација и функционисање рачунарских система. Последице могу бити различите, од крађе података до нарушавања рада читавих мрежа. Зато је од пресудног значаја да системи буду адекватно заштићени и да се примењују мере за одбрану од оваквих напада. На крају, циљ је разумети механизме и технике које користе *Black Hat* хакери како би развили ефикасну одбрану и заштитили рачунарске системе од таквих непријатеља.[18] Важно је савесно поступати и поштовати принципе етике у коришћењу информационих технологија, како би се избегле негативне последице које овакви напади могу изазвати.

Grey Hat хакери представљају занимљиву категорију у свету ИТ безбедности. Они су као нека врста хибридне форме између хакера *White Hat* и *Black Hat*. С једне стране, поседују значајно знање о рачунарским системима, што их сврстава у способне, искусне професионалце. С друге стране, њихове активности се понекад могу граничити са незаконитошћу. Важно је разумети да *Grey Hat* хакери генерално немају злонамерне намере. Уместо тога, њихова мотивација може бити проучавање и тестирање безбедности рачунарских система. Стога њихови упади у системе најчешће нису скакали у реализацију злонамерних циљева, већ су излазили из оквира испитивања и праћења. Међутим, важно је истаћи да *Grey Hat* хакери могу да изазову озбиљне безбедносне проблеме, посебно ако искористе безбедносне пропусте система. Иако њихови мотиви можда нису злонамерни, њихови поступци могу имати нежељене последице и угрозити безбедност података и система.[19] Стога, иако је интригантно размотрити постојање *Grey Hat* хакера у циљу подизања свести о безбедности информационих система, важно је напоменути да их треба темељно разумети и поштовати правне и етичке принципе у свом деловању. Савладавање ових принципа помаже у одржавању равнотеже између истраживања безбедности и заштите корисника и система.

Услуге *Blue Hat* хакера постале су неизоставни део стратегије компанија које велику пажњу поклањају безбедности својих система. У свету у коме су свакодневни

[18] Исто.
[19] Исто.

напади на информационе системе постали стварност, компаније се ослањају на ову елитну групу хакера да проактивно открију и поправе потенцијалне безбедносне пропусте пре него што их злонамерни актери искористе. Пример компаније која је прихватила ову филозофију је Microsoft, који не само да ангажује *Blue Hat* хакере, већ и организује *Blue Hat Microsoft Hacker Conference*, где се састају инжењери и хакери како би разменили знања и искуства о унапређењу безбедности програма. Ова сарадња не само да доприноси развоју и унапређењу безбедности у целини, већ и демонстрира ангажовање компанија као што је Microsoft у креирању безбедних и поузданих производа за своје кориснике.[20] Примена *Blue Hat* хакера је, дакле, више од реактивног мерења безбедносних претњи; представља напредну стратегију која укључује сарадњу и иновације у области безбедности информационих система. Овај приступ гарантује да компаније попут Microsoft-а остају на челу индустрије и пружају највиши ниво заштите својим корисницима.

1.4. Појам и врсте напада у сајбер простору

Пракса показује да напади на рачунарске системе углавном представљају комбинацију неколико врста напада. Вулетић (2017) наводи следеће карактеристичне врсте напада хакера на рачунарске системе:[21]

- *Denial-of-Service - DoS (напада ускраћивањем услуга).* Озбиљна претња по безбедност мреже која има за циљ да спречи легитимне кориснике да користе мрежне услуге. Ова врста напада се обично изводи преоптерећењем мрежног система циља, што доводи до прекида везе и онемогућавања приступа интернету. Постоје различити начини извођења оваквих напада, али један од најчешћих је слање великог броја захтева серверу. Ово преоптерећује сервер и омета његово нормално функционисање, што резултира недоступношћу услуга за легалне кориснике. С обзиром на ову врсту опасности, од кључне је важности да се примењују одговарајуће мере заштите, укључујући филтрирање саобраћаја и коришћење заштитних механизама који могу препознати и одбранити такве нападе.

[20] Исто.
[21] Исто, стр. 176-181.

- *Botnet*. Ботови (енгл. *bots*, скраћено од *robots*) представљају програме који се уграђују у рачунарске системе са циљем да омогуће неовлашћеним лицима да преузму контролу над системом, представљају озбиљну претњу по безбедност Интернета. Када се рачунарски системи заразе таквим програмима, они постају део бот мрежа, такође познатих као ботнет. Ови ботнети се користе за извођење различитих напада, укључујући и оне који циљају на критичну инфраструктуру земаља. Један од најпознатијих случајева коришћења ботнета у нападима на националну безбедност догодио се 2007. године у Естонији. Тада је напад изведен преко 560 компјутерских мрежа из више од 50 земаља широм света. Овај инцидент је показао колико озбиљна претња може бити ботнет и како њихова употреба може имати далекосежне и дуготрајне последце.
- *Phishing (фишинг).* Представља савремену и опасну претњу на Интернету која на различите начине може оштетити кориснике мреже. Ова врста напада има за циљ да превари кориснике да открију своје личне и поверљиве информације, као што су корисничка имена, лозинке, бројеви рачуна и кредитних картица. Ове информације се затим користе за чињење кривичних дела, као што су крађа идентитета, финансијска превара и друга кривична дела. Најчешћи начин на који се фишинг напади изводе је путем лажних електронских порука које изгледају из поузданих извора, као што су банке, финансијске институције или поштанске службе. Ове поруке обично захтевају од примаоца да ажурира своје податке или изврши неку другу радњу која може довести до откривања личних података. Фишинг напади нису ограничени само на е-пошту, већ се могу спровести и преко других интернет сервиса као што су месинџери, друштвене мреже и слично. Ова врста напада је посебно опасна јер злоупотреба поверљивих информација може нанети велику штету и појединцима и компанијама.
- *Spam (спем).* Представља појаву која може бити изузетно непријатна и наметљива за сваког корисника интернета. Ове електронске поруке обично садрже разне рекламе, понуде или чак малициозни софтвер, иако корисник није изричито изразио жељу да их прими. Пошиљаоци спам порука често дејствују из земаља где не постоје законски механизми за кажњавање оваквих понашања, што додатно омогућује њихову широку распрострањеност. Адресе

електронске поште се прикупљају на различите начине, укључујући прегледање веб страница, учешће у различитим групама и др.

- *Social engineering (социјални инжењеринг).* Представља добро успостављен, али веома опасан метод напада који се користи у циљу приступа системима и добијања информација. Ова техника манипулише људима тако што искоришћава њихове слабости и друштвене интеракције како би омогућила продор у системе који би иначе били заштићени. Уместо техничког хаковања или хаковања, социјални инжењери раније циљају психолошки и ступају у комуникацију са жртвама како би добили приступ информацијама. Најчешћи начин за извођење оваквих напада је преко телефона, где нападачи користе убедљиве приче и манипулативне технике како би навели жртву да открије информације или изврши одређене радње. Поред тога, друштвени инжењери могу користити друге канале комуникације као што су е-пошта, тренутне поруке и друштвени медији. Циљеви таквих напада могу бити различити, али обично укључују приступ осетљивим информацијама или системима као што су системи одбране, финансијске институције, компаније и владине агенције. Иако се ова врста напада често сматра мање уочљивом у поређењу са техничким хаковањем, њен потенцијал да изазове штету је већи јер користи друштвену интелигенцију и манипулацију људским емоцијама и поверењем.
- *Sniffing (снифинг).* Представља метод праћења мрежног саобраћаја помоћу хардверских или софтверских алата. Ови алати омогућавају приступ информацијама које се преносе преко мреже, у циљу анализе или прикупљања различитих врста података из рачунарских система. Поред легалних апликација, где се њушкари користе за одржавање мреже и решавање проблема, постоје и нелегалне употребе ових алата. Позитивна страна снифинга је њихова способност да помогну у откривању и решавању мрежних проблема, што може бити изузетно важно за ИТ техничаре и мрежне администраторе. Међутим, употреба њушкала може имати негативан утицај на перформансе система. Процес прегледа и анализе великог обима мрежног саобраћаја може довести до успоравања или прекида у раду мреже или рачунарског система.
- *Spoofing (спуфинг).* Представља обману којом се ствара утисак да пренос врши неки овлашћени корисник. То је префињена техника провере аутентичности

једне машине према другој, фалсификовањем пакета из адресе извора којој се верује.

- *Малициозни (злоћудни) програми*. Имају могућност веома брзог и лаког ширења рачунарским системом, нарочито због постојања грешака, неопрезности корисника и сл. То су софтвери који наносе штету одређеном рачунарском систему. Разликујемо следеће злоћудне програме: рачунарски вируси, рачунарски црв (енгл. *worm*), тројански коњ (енгл. *trojan horse*), логичка бомба (енгл. *logic bomb*), временска бомба (енгл. *time bomb*), шпијунски програми (енгл. *spyware*), rootkit, оглашивачки програми (енгл. *adware*) и др.

1.5. Међународни правни акти

Компјутерски (сајбер) криминал је све више заступљен у савременим условима напретка људског друштва, те узрокује настанак бројних кривичних дела из ове области. У ту сврху, потреба за његовим правним дефинисањем и законском регулацијом, све више добија на значају.

Најзначајнији правни документи који се односе на сузбијање и спречавање настанка компјутерског криминалитета настали су под окриљем ОУН, Савета Европе и Европске Уније. Осим тога, постоји још низ других организација и иницијатива које се залажу за борбу против сајбер криминала, као што су: Интерпол, Канцеларија Уједињених нација за борбу против дроге и криминала (UNODC - *United Nations Office on Drugs and Crime*), група држава названих Г-8: Организација америчких држава (OAS - *Organization of American States*); Организација за економску сарадњу Азије и Пацифика (APEC - *Asia Pacific Economic Cooperation*), Организација за економску сарадњу и развој (OECD - *The Organization for Economic Cooperation and Development*), Организација за европску безбедност и сарадњу (OEBS – *Organizacion for Security and Co-operation in Europe*) и др.

У борби против компјутерског криминала, Уједињене нације су предузеле неколико важних корака кроз усвајање различитих резолуција и приручника усмерених на борбу против ове врсте криминала у савременом свету. Свесни значаја који компјутерски криминал може имати на различите аспекте друштва, УН су активно радиле

на стварању механизама и инструмената који би спречили његово ширење и ефикасно сузбили криминалце.

Први значајни кораци у овом правцу почели су 1990. године, када је у оквиру VII Конгреса УН усвојена Резолуција о законодавству у области компјутерског криминала.[22] Ова резолуција представљала је важан први корак ка разумевању и регулисању ове сфере криминала. Надаље, током 1994. године УН су усвојиле Приручник о превенцији и контроли компјутерског криминала[23], који је био значајан допринос креирању упутстава и најбољих пракси за борбу против овог облика криминала. Женевска резолуција о злоупотреби интернета у сврху сексуалне експлоатације[24], усвојена у мају 1998. године, представљала је још један значајан корак у борби против онлајн криминала. Ова резолуција се посебно фокусирала на регулисање трговине људима, проституције и сексуалне експлоатације која се одвија преко интернета.

Усвајањем ових резолуција и приручника, УН су показале своју одлучност да се боре против компјутерског криминала и заштите људска права и онлајн безбедност. Ове акције представљају важан корак ка стварању сигурнијег и праведнијег дигиталног окружења за све.

Глобални развој информационих технологија пратио је и пораст у злоупотреби и криминалним радњама у овом домену. У циљу сузбијања ових негативних појава, Уједињене нације су у периоду од 2000. до 2007. године предузеле важне кораке. У 2000. години, Уједињене нације су усвојиле и потписале Резолуцију која је посветила пажњу борби против злоупотребе информационих технологија[25]. Ова Резолуција наглашава значај мера и алата који су потребни за сузбијање ове негативне праксе.

Међутим, с обзиром на настајање нових облика криминалитета и пораст броја криминалних радњи у вези са рачунарским системима, Уједињене нације су 2007. године

[22] Резолуција Уједињених Нација о законодавству у области компјутерског криминалитета (UN resolution on computer crime legislation), доступно на: http://www.unodc.org/documents/congress//Previous_Congresses/8th_Congress_1990/028_ACONF.14 [14.02.2024]

[23] Приручник УН о спречавању и контроли компјутерског криминала (United Nations Manual on the Prevention and Control of Computer-related Crime) (1994). доступно на: http://www.uncjin.org/Documents/EighthCongress.html [14.02.2024]

[24] Резолуција Уједињених Нација (тзв. Женевска резолуција) о злоупотреби интернета у сврху сексуалне експлоатације (UN Resolution on Missuse of the Internet for the Purpose of Sexual Exploatation), доступно на: http://www.uri.edu/artsci/wms/hughes/ppr.htm [14.02.2024]

[25] Резолуција Уједињених Нација A/res/55/63 о борби против злоупотребе информационих технологија (UN resolution A/res/55/63 on combating the criminal misuse of information technologies), (2000). доступно на: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf [14.02.2024]

донеле Резолуцију 2007/20.[26] Ова Резолуција позива државе да унапреде своје законске оквире у области заштите модерних технологија и безбедности рачунарских система. Циљ ових акција је да се створе ефикасни механизми који ће спречити злоупотребу информационих технологија и омогућити безбедно коришћење и развој ових технологија у свету. Овакве иницијативе су од суштинског значаја за заштиту приватности, безбедности и интереса корисника информационих технологија широм света.

Наставак рада Уједињених нација на сузбијању компјутерског криминала у 2010. години, усвајањем Резолуције 65/230[27], означио је важан корак ка унапређењу глобалне безбедности у дигиталном окружењу. Овом резолуцијом је наглашена потреба формирања групе експерата за анализу компјутерског криминала у различитим земљама, као и степена њихове безбедности.

Сврха овог истраживања је била да се идентификују грешке и пропусти у борби против сајбер криминала, као и да се изнађу могућности за унапређење безбедности националних рачунарских система. Ова иницијатива представља кључну стратегију у борби против све софистицираних облика дигиталних претњи које све више представљају озбиљан изазов за друштво. Сарадњом стручњака из различитих земаља могуће је створити ефикасније механизме за откривање, спречавање и сузбијање компјутерског криминала. Анализа која је резултат овог истраживања омогућава земљама да идентификују своје слабости и унапреде своје националне стратегије за заштиту од сајбер претњи. Имплементација препорука овог истраживања могла би резултирати јачањем међународне сарадње у области безбедности информационих система и допринети изградњи глобалног оквира за борбу против компјутерског криминала. Кроз такве напоре, свет може да постане безбедније дигитално окружење, оснажујући тако друштва да искористе потенцијал дигиталне трансформације уз минималне ризике од сајбер претњи.

Такође, Европска унија је посвећена борби против криминала у области компјутерских система. Од 2005. године на снази је Одлука о нападима на информационе

[26] Резолуција 2007/20 од 26. 07. 2007. године, доступно на: http://www.un.org/.../ecosoc/.../2007 [14.02.2024]
[27] Резолуција Уједињених Нација 65/230 (UN General Assembly resolution 65/230), доступно на: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [14.02.2024]

системе, која регулише приступ информационим системима и безбедност података и прописује санкције за учиниоце кривичних дела у сајбер простору.[28]

Међу правним инструментима које је усвојила Европска унија треба истаћи три директиве. Прва је Директива о правној заштити компјутерских програма, која обезбеђује заштиту интелектуалне својине над компјутерским програмима. Друга је Директива о чувању података добијених или обрађених током пружања јавно доступних електронских комуникационих услуга или јавних комуникационих мрежа. Трећа је Директива 2013/40/ЕУ која се односи на усклађивање законодавства држава чланица о нападима на информационе системе и њиховој кривичноправној заштити.

Ове директиве су кључни алати у борби против онлајн криминала и обезбеђивању прилагођавања правних норми технолошком развоју и променама у сајбер простору. Европска унија настоји да обезбеди безбедност и заштиту података својих грађана, и континуирано је ангажована на јачању свог законодавног оквира како би се суочила са изазовима који произилазе из дигиталног доба.

1.5.1. Домаћа законска регулатива

Укључивши се у потписивање Конвенције о високотехнолошком криминалу и Додатног протокола 2005. године, Република Србија је јасно изразила своју апсолвентност у борби против криминалних дела у виртуелном простору. Ратификацијом ових докумената у 2009. години, Србија је обавезала себе да примени мере које ће омогућити ефикасну заштиту од кибер-преступништва и санкционисање онога који угрожава сигурност и приватност у циљу остварења правне сигурности у дигиталном окружењу.

Одговорност коју је Србија преузела укључује рад на развоју и унапређењу законских оквира који ће адекватно адресирати изазове компјутерског криминалитета. Овим се подразумева стварање детаљних и прецизних закона који ће дефинисати и кривична дела у вези са информационим технологијама и критеријуме за њихово санкционисање. Циљ ових напора је да се обезбеди сигурност и заштита свих грађана на

[28] Оквирна одлука о нападима на информационе системе Комисије европских заједница (Framework Decision on attacks against information systems of the Commission of the European Communities), доступно на: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222&from=EN [14.02.2024]

интернету, како приватних лица тако и институција. Строге законске мере и прецизно дефинисани правни оквири ће послужити за борбу против потенцијалних сајбер преступника и учиниће Србију не само сигурнијом земљом, већ и активним учесником у међународној борби против сајбер криминалитета.

Међу најбитнија правна документа чије одредбе имају утицаја и на области сајбер криминала која су донета у Републици Србији, могу се издвојити следећа: Кривични законик Републике Србије, Законик о кривичном поступку Републике Србије[29], Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала[30], Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима[31], Закон о ауторским и сродним правима[32], Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине[33].

Осим поменутих закона који регулишу област компјутерског криминалитета, треба напоменути и законе донете у Републици Србији који се односе на регулацију електронског пословања, које постаје примаран начин пословања, како физичких, тако и правних лица. Овде спадају следећи законски акти: Закон о електронском потпису[34], Закон о електронској трговини[35], Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању[36] и Закон о оптичким дисковима[37].

У борби против компјутерског криминалитета у Републици Србији, институционални оквир игра кључну улогу. Овај оквир обухвата државне органе који су одговорни за спровођење закона и других правних аката који се односе на сузбијање и заштиту од компјутерског криминалитета. Њихова улога је да допринесу побољшању безбедности и смањењу претњи и инцидената у овом области.

[29] Законик о кривичном поступку, Службени гласник РС, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 – одлука УС и 62/2021 – одлука УС.
[30] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, Службени гласник РС, бр.61/2005 и 104/2009.
[31] Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима, Службени гласник РС, бр. 32/2013.
[32] Закон о ауторским и сродним правима, Службени гласник РС, бр. 104/2009, 99/2011, 119/2012, 29/2016 – одлука УС и 66/2019.
[33] Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине, Службени гласника РС, бр. 46/2006, 104/2009 – др. закони и 129/2021.
[34] Закон о електронском потпису, Службени гласник РС, бр.135/2004.
[35] Закон о електронској трговини, Службени гласник РС, бр. 41/2009, 95/2013 и 52/2019.
[36] Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању, Службени гласник РС, бр. 94/2017 и 52/2021.
[37] Закон о оптичким дисковима, Службени гласник РС, 52/2011.

За ефикасно сузбијање компјутерског криминалитета, неопходно је да државни и надлежни органи буду усавршени и специјализовани у спровођењу одговарајућих мера. Осим организационих јединица, значајан допринос у овом контексту имају и институције као што су Министарство трговине, туризма и комуникација, Републичка агенција за електронске комуникације (РАТЕЛ) и Републичка радиодифузна агенција (РРА). Ове институције играју важну улогу у координацији активности и усмеравању напора ка превенцији и сузбијању компјутерског криминалитета.

Јачање капацитета и специјализација ових институција кључни су за успешну борбу против сајбер криминала у земљи. Само кроз сарадњу и координацију свих релевантних актера, укључујући државне органе и институције, можемо ефикасно одговорити на изазове компјутерског криминалитета и осигурати безбедност истовремено штитећи права и приватност грађана.

2. ОСВЕТНИЧКА ПОРНОГРАФИЈА

2.1. Појам и дефинисање осветничке порнографије као компјутерског криминалитета

Осветничка порнографија, термин који се обично користи да опише злонамерно ширење интимних слика или видео снимака бивших романтичних партнера без њиховог пристанка, привукла је значајну пажњу последњих година. Дефинисан као чин дељења голог или сексуално експлицитног садржаја, често праћеног личним подацима, представља озбиљно кршење приватности и поверења. Препознајући његове штетне ефекте, неколико јурисдикција, укључујући Енглеску и Велс, Сједињене Државе и Аустралију, донело је законе за решавање овог питања, уз додатне позиве на реформе у Европи и на Блиском истоку.[38]

Концепт „осветничке порнографије“ представља изазов већ у самом процесу дефинисања. У јавним расправама, овај термин се често користи као синоним за дистрибуцију сексуалног или интимног материјала без пристанка приказане особе, често уз откривање личних података како би јој се наудило. Објављени садржај може бити креиран са или без сагласности или знања особе која је представљена, а његово дељење је обично намењено за личну употребу, а не за ширу дистрибуцију, са или без злонамерне намере дистрибутера.[39] Дефиниција осветничке порнографије у Оксфордском речнику описује је као откривање или сексуално експлицитне фотографије или видео записе особе које је поставио на мрежи, обично од стране сексуалног партнера без пристанка субјекта, како би их узнемирио или осрамотио. Ова дефиниција указује да освета није увек кључна компонента овог чина и да се осветничка порнографија приказује као интернет феномен, иако су се такви инциденти дешавали и пре него што је Интернет постао широко доступан.

Термин „осветничка порнографија“ се често погрешно схвата, јер сугерише да је фотографисање себе голог или укљученог у сексуални чин (или допуштање неком другом да направи такву слику) порнографски чин. Међутим, стварање експлицитних слика у контексту приватне, интимне везе – све чешћа пракса – није исто што и стварање порнографије. Чин дељења приватне, сексуално експлицитне слике са неким ко није

[38] Bambauer, D. E. (2014). Exposed. *Minnesota Law Review*, 98, стр. 2026.
[39] Citron, D.K. (2014). *Hate Crimes in Cyberspace*. Harvard University Press, стр. 17.

њихова циљна публика може се, међутим, тачно описати као порнографски, јер претвара приватну слику у јавну сексуалну забаву. Због тога многи адвокати жртава користе израз „порнографија без пристанка“.[40] Порнографија без пристанка укључује сексуално експлицитне слике објављене без пристанка и без легитимне сврхе. Овај термин укључује материјале добијене скривеним камерама, споразумно размењене у поверљивим односима, украдене фотографије и снимке сексуалних напада. Порнографија без пристанка често игра улогу у насиљу интимног партнера, при чему насилници користе претњу објављивањем таквог садржаја како би спречили своје партнере да оду или пријавили своје злостављање полицији.

Осветничка порнографија, недобровољна порнографија, порнографија без пристанка или злоупотреба заснована на сликама, укључује различите облике неовлашћеног понашања који често укључују неетичко снимање или дељење интимног садржаја без сагласности особе која је на њој приказана. Ове праксе могу укључивати тајно снимање људи путем камера, дељење интимних фотографија између партнера без пристанка, крађу и објављивање приватних фотографија, или чак снимање сексуалног насиља.[41] Џејкобс (2016) дефинише осветничку порнографију као објављивање и дистрибуцију сексуално експлицитних слика или видео снимака неке особе без њеног пристанка и без икакве основе.[42] Према Халдеру и Јаишанкару (2013), ову врсту порнографије карактерише објављивање лажних или провокативних слика жртве како би се задовољио гнев и фрустрација насилника због прекинуте везе, често користећи материјал добијен током везе или послат њих од стране жртве.[43] Поред тога, Матсуи (2015) истиче да објављивање сексуално експлицитног садржаја бившег партнера путем интернета након раскида често спада у категорију осветничке порнографије.[44] Лонардо и сарадници (2016) такође наглашавају да ширење таквог материјала без пристанка особе на њему може изложити жртву јавној срамоти, понижењу или другим облицима повреде.[45]

[40] Franks, M. A. (2015). *Drafting an Effective „Revenge porn” Law: A guide for legislators*. George Washington University, стр. 2.
[41] Вилић, В. (2019). Порнографија из освете као облик сајбер мизогиније. *Темида*, 22(1), стр. 60-61.
[42] Jacobs, A. (2016) Fighting Back against Revenge Porn: A Legislative Solution. *Northwestern Journal of Law and Social Policy*, 1, стр. 69.
[43] Halder, D., Jaishankar, K. (2013) Revenge Porn by Teens in the United States and India: A Socio-legal Analysis. *International Annals of Criminology*, 1-2, стр. 90.
[44] Matsui, S. (2015) The Criminalization of Revenge Porn in Japan. *Washington International Law Journal*, 2, стр. 289.
[45] Lonardo, T., Martland, T., White, D. (2016) A Legal Examination of Revenge Pornography and Cyber-Harassment. *Journal of Digital Forensics, Security and Law*, 3, стр. 78.

Осветничка порнографија се може дефинисати као процес објављивања и дистрибуције сексуално експлицитног материјала, као што су голотиње или видео снимци, појединцу без њиховог пристанка, са циљем да се жртва изложи јавној срамоти, понижењу или повреди. Овај феномен може бити мотивисан жељом за осветом, застрашивањем или повредом жртве на емоционалном или друштвеном нивоу. Ова врста порнографије често служи као средство за вршење моћи и контроле над појединцем и може имати озбиљне негативне последице по жртву, укључујући трауму, стрес и нарушавање угледа.[46] Ова дефиниција теми осветничке порнографије приступа на аналитички начин, узимајући у обзир психолошке, социолошке и етичке аспекте феномена.

2.2. Карактеристике, преваленције и мотиви осветничке порнографије

Осветничка порнографија је у широј друштвеној перспективи препозната као облик сајбер мизогиније, с обзиром на то да су жене најчешће жртве овог неприкладног понашања, што потврђује и статистика која показује да проценат жена жртава варира између 70% и 90%. Друштвене интеракције између мушкараца и жена често су обликоване друштвеним нормама и вредностима које диктира шира заједница. Концепт сајбер мизогиније укључује различите манифестације родно засноване мржње, узнемиравања и насилног понашања према женама, девојкама и девојкама на интернету и друштвеним мрежама. Овај облик дискриминације јасно указује на однос моћи и маргинализације, који се често манифестује кроз осветничку порнографију, сајбер ухођење, родно заснован говор мржње на интернету, дељење интимних слика без пристанка, као и сексуалну експлоатацију деце.[47]

Недавна научна истраживања указују на значајан родни диспаритет у прављењу порнографије из освете, при чему су мушкарци идентификовани као доминантни преступници. Такође, емпиријски докази наглашавају значајну неравнотежу у представљању полова међу жртвама, при чему је велика већина слика постављених на

[46] Вилић, В. (2019). нав. дело, стр. 63.
[47] Исто, стр. 63-64.

осветничке порно платформе које приказују жене. Статистички гледано, преко 75% појединаца на мети осветничке порнографије су жене.[48]

Свеобухватна студија из 2017. године у Сједињеним Државама открила је да су жене 1,7 пута чешће жртве осветничке порнографије, истичући мушкарце као примарне починиоце. Исто тако, истраживања указују на повећану подложност сексуалних мањина осветничкој порнографији. На пример, подаци из Канцеларије за једнакост владе Уједињеног Краљевства открили су да је четвртина упита била од мушких жртава, при чему је отприлике 40% ових случајева укључивало геј мушкарце. Слично томе, студија коју је спровео Институт података и друштва у САД 2016. године открила је да особе које се идентификују као геј или бисексуалци имају седам пута веће шансе да наиђу на претње или виктимизацију кроз осветничку порнографију у поређењу са својим хетеросексуалним колегама.[49]

Још једно истраживање које су на нивоу Сједињених Америчких Држава представља важан корак у разумевању овог феномена. Тим истраживача, спровео је узорак анализе испитаника прикупљених анкетама. Анкете су биле осмишљене у сарадњи са стручњацима за насиље у породици, сексуалну делинквенцију и услуге подршке жртвама. Анкетна питања која се односе на искуство осветничке порнографије из перспективе починиоца и жртве, уз прикупљање бројних демографских података. Испитаници су били корисници друштвене мреже Фејсбук у периоду од новембра 2016. до марта 2017. године. Путем плаћеног огласа, у којем су пунолетни грађани Сједињених Америчких Држава позвани да учествују у истраживању, 3.044 испитаника пристало је да одговори на питања. При томе се водило рачуна о пропорционалној заступљености људи из свих савезних држава са одговарајућом родном заступљеношћу. Истраживање истиче значајне налазе у вези са виктимизацијом у контексту осветничке порнографије и претњи објављивањем експлицитног материјала. Примарни резултати показују да је 12,8% испитаника истакло да су постали жртве таквих активности или су били мета претњи објављивањем сексуално експлицитних снимака или слика. Од ове групе, 8% је пријавило да су њихови материјали већ објављени, док је 4,8% навело да су доживели претње објављивањем истих. Када се анализирају ови подаци по полу, примећује се да је вероватноћа да жене буду жртве таквих понашања већа за 1,7 пута у односу на мушкарце.

[48] Gauthier, A. (2023). Revenge Porn: A Disturbing Trend in Sexual Violence That Must Be Exposed. *Academic Journal of Criminology X Journal Universitaire de Criminologie*, 2(2), стр. 66.
[49] Исто.

Преузимајући ове проценте, утицај виктимизације или претњи код жена износи 15,8%, док је код мушкараца та вредност 9,3%. Детаљнија анализа ових података показује да су жене изложене већем ризику, према томе, њих 9,2% пријављује виктимизацију у поређењу са 6,6% мушкараца, што индицира 1,5% већи ризик за жене. Уз то, претња објављивањем експлицитног материјала је знатно израженија код жена, где је примећено да су 6,6% жена изложене таквим претњама, у поређењу са само 2,6% мушкараца. У аспекту старосних категорија, највиши ниво виктимизације и претњи је забележен код испитаника у старосној групи од 26 до 33 године, где је пријављен 17,7% учесника. Што се тиче групе између 34 и 41 године, примећен је највећи ниво виктимизације у контексту осветничке порнографије, што износи 12,4%.[50]

Резултати су показали да је 5,2% испитаника изјавило да је у неком тренутку свог живота објавило голишаве фотографије или видео снимке својих бивших партнера. Експлицитне материјале објављивали су мушкарци у већој мери него жене, 7,4% мушкараца наспрам 3,4% жена. Анализа по старосним категоријама показала је да је највећи проценат самопријављивања забележен код испитаника старости од 18 до 25 година, који су чинили 8,2% учешћа. Посебна пажња истраживача је посвећена мотивацији за овакво понашање. Најчешћи разлог за чињење осветничке порнографије, који је изабрало 79% испитаника, била је жеља да се она подели са пријатељима без намере да се повреди бивши партнер. Само 12% испитаника је изјавило да је експлицитан материјал објавило из освете или жеље да науди бившем партнеру. Да би стекли праву слику о феномену осветничке порнографије, истраживачи су детаљно анализирали начине дељења експлицитних материјала. Скоро половина самопријављених извршилаца (71 испитаник) изјавила је да су то урадили путем порука, док је 31,4% испитаника користило друге методе, као што су директно приказивање слика другој особи, ћаскање, већ креиране слике, коришћење клауд сервиса, друштвених мрежа. , имејл или веб локацију. Коначно, истраживачи су се позабавили и последицама овог феномена. Чак и једно дељење експлицитних материјала резултирало је лошијим менталним здрављем и вишим нивоом физиолошких проблема у поређењу са људима који нису били жртве. Претња дељењем експлицитних слика и видео материјала изазива исте последице као и

[50] Димовски, Д. (2023). Осветничка порнографија: криминолошки и кривичноправни аспект. *Зборник радова Правног факултета у Нишу*, LXII(98), стр. 158-159.

сама виктимизација. Ови налази наглашавају озбиљност проблема осветничке порнографије и потребу за даљим истраживањем и превентивним мерама.[51]

Рувалцаба и Еатон (2019) спровели су значајну студију која истражује распрострањеност злостављања заснованог на осветничкој порнографији међу одраслима у Сједињеним Државама. Заступљен је узорак од 3.044 учесника, од којих су 54% биле жене. Прелиминарни резултати показују да је један од 12 одраслих Американаца пријавио да је доживео злостављање кроз осветничку порнографију. Занимљиво је да је истраживање обухватило и самопријављивање, према којем је један од 20 учесника пријавио да је био починилац овог облика злостављања. Анализом података је такође утврђено да младићи и девојке старости од 15 до 29 година имају највећу тенденцију да пријаве претње дељењем својих интимних фотографија и видео записа. Поред тога, истраживачи су истраживали социоекономски статус учесника и открили да су људи из домаћинстава са ниским примањима склонији да буду жртве осветничке порнографије у поређењу са људима са вишим приходима. Као група у највећем ризику од овог облика насиља идентификовани су и припадници небелих раса. Ако се узме у обзир сексуална оријентација жртава, уочено је да су ЛГБТК+ особе изложене већем ризику од хетеросексуалних особа да постану жртве осветничке порнографије. У 17% случајева припадници сексуалних мањина су изјавили да су им претили или су били изложени експлицитним сликама.[52] Ово истраживање значајно доприноси разумевању проблематике осветничке порнографије и наглашава потребу за превентивним и интервентним мерама за заштиту жртава.

У оквиру још једног истраживања учествовали су испитаници који су регрутовани путем оглашавања на друштвеним мрежама, а узорак је обухватио 100 учесника, међу којима је било 16 мушкараца и 84 жене, од којих су сви били пунолетни и стари између 18 и 54 године. Анализирајући прикупљене податке, утврђено је да је 28,6% учесника вероватно започело осветничку порнографију. Изненађујуће је да је већина учесника изразила подршку и уживање у оваквој порнографији (87%), док је 99% изразило одобравање. Ови подаци постављају питање разлике између оних који самостално деле своје интимне снимке и фотографије и оних који подржавају или толеришу такво понашање. Објашњење лежи у чињеници да већи број учесника преузима осветничку порнографију, посебно због њене доступности на интернету. Занимљиво је истаћи

[51] Исто, стр. 158-159.
[52] Исто, стр. 160.

резултате о стереотипима према жртвама осветничке порнографије, који могу бити слични стереотипима о жртвама силовања. Истраживања Пајна, Холанда и Џејмса такође су открила да виши нивои амбивалентног сексизма, макијавелизма, нарцизма и психопатије доприносе већој вероватноћи укључивања у осветничку порнографију. Иако садистичке тенденције нису у корелацији са осветничком порнографијом, ови подаци су у супротности са резултатима других истраживања. У овој студији, истиче се значај макијавелизма и амбивалентног сексизма у одобравању осветничке порнографије, при чему макијавелизам задржава независно предвиђање одобравања таквог понашања. Исто тако, нарцистичке особине имају значајнији утицај на уживање у осветничкој порнографији у поређењу са особинама које су карактеристичне за макијавелизам. Ово истраживање открива да постоји позитивна корелација између амбивалентног сексизма и одобравања осветничке порнографије, као и између нарцизма и уживања у њој.[53]

Феномен осветничке порнографије карактерише вишеструки низ узрочних фактора, од којих сваки представља замршену динамику која доприноси његовом ширењу. У домену интимних партнерских односа, настанак осветничке порнографије може се приписати случајевима насиља у породици, где један партнер користи сексуално експлицитан материјал као механизам за вршење манипулације и доминације над другим.[54] Ова тактика принуде служи као средство за успостављање контроле и одржавање циклуса злостављања у вези.

Такође, финансијски подстицаји играју кључну улогу у покретању ширења порнографског садржаја без пристанка, о чему сведочи његова комерцијализација на специјализованим онлајн платформама.[55] Комодификација таквог материјала наглашава укрштање економске добити и експлоатације, при чему појединци искоришћавају рањивост жртава за новчану добит.

Подмукла природа осветничке порнографије протеже се и до њеног коришћења од стране трговаца људима и макроа као оруђа за увлачење жена и девојака у мрачну стварност проституције. Ширењем компромитујућих слика или видео записа, починиоци

[53] Исто, стр. 161.
[54] Hasinoff, A. (2021). Cessons de parler de revenge porn: ces images sont une forme de violence sexuelle. *Questions de communication*, (40), стр. 338.
[55] Bond, E., Tyrrell, K. (2021). Understanding revenge pornography: A national survey of police officers and staff in England and Wales. *Journal of interpersonal violence*, 36(5-6), 2166-2181.

користе претњу разоткривањем као принудни механизам, приморавајући жртве у ситуације сексуалног ропства и експлоатације.[56]

Дакле, феномен осветничке порнографије настаје из споја међуљудске динамике моћи, економских подстицаја и криминалне експлоатације, наглашавајући замршену међусобну игру друштвених, економских и правних фактора који су у основи његовог одржавања. Напори да се реши ово свеприсутно питање захтевају свеобухватне приступе који обухватају правну реформу, друштвену свест и подршку жртвама, како би се ефикасно борили против безбројних манифестација осветничке порнографије и ублажили њен штетан утицај на појединце и друштво у целини.

2.3. Законско регулисање осветничке порнографије – компаративни приказ

2.3.1. Правна регулисаност осветничке порнографије у УН

Човек сада има не само људски идентитет, већ и дигитални идентитет кроз своје дигиталне интеракције/присуство. Било да су наши дигитални идентитети производ личног избора или акције других, сви смо ми аутономни дигитални подаци. Принципи људских права – људско достојанство и безбедност личности – одјекују кроз резолуције, декларације и уговоре о људским правима, а подједнако се примењују и на Интернет, у његовој континуираној трансформацији.

УН су доследно наглашавале технологију као средство за људска права, уместо нечега што би требало да буде предмет људских права само по себи. Пре пандемије Ковид-19, формализована пажња посвећена дигиталним људским правима била је од суштинског значаја. Током и након пандемије Ковид-19, принципи дигиталних људских права морају бити укључени међу основне принципе људских права. У преамбули Повеље УН је дефинисана сврха Уједињених нација, делимично, да поново потврди веру у основна људска права, у достојанство и вредност људске личности, у једнакост права мушкараца и жена и великих и малих народ и да промовише друштвени напредак и бољи животни стандард у већој слободи.

[56] Gauthier, A. (2023). нав. дело, стр. 67.

УН су прецизирале ове принципе у Универзалној декларацији о људским правима (UDHR). У каснијим уговорима и декларацијама разрађени су основни принципи из UDHR-а о одређеним питањима.

Пошто је обим дигиталних проблема који утичу на људска права готово неограничен и стално се развија, нагласак је на онлајн фотографијама лица у полицијским евиденцијама и осветничкој порнографији, примерима кршења људских права која утичу на људско достојанство и личну безбедност. Из овог фокуса могу се извести и друге забринутости за људска права.

2.3.2. Правна регулисаност осветничке порнографије у Савету Европе

Резолуција Парламентарне скупштине Савета Европе недавно је усвојена на основу извештаја о родним аспектима и аспектима људских права порнографије Франка Хајнриха, известиоца Комитета за равноправност и недискриминацију. Стални комитет Парламентарне скупштине Савета Европе упозорава да порнографија често ствара и одржава стереотипе преносећи слику о женама као подређеним мушкарцима и као објектима, и банализујући насиље над женама. Због тога се залажу за свеобухватно сексуално образовање у школама као главни извор информација о сексуалности за младе људе како би се спречило ширење непоузданих и потенцијално штетних информација путем других извора као што је порнографија. Док се процењује да је више од половине укупног саобраћаја на Интернету повезано са порнографијом и сексом, као и да велики проценат становништва консултује порнографски материјал. Ова тенденција је, како се наводи, порасла током пандемије Ковид-19.[57]

Све је чешћа појава да се порнографски садржаји креирају приватно, од стране појединаца који нису део специјализованих продукцијских кућа, а дистрибуирају се електронски. Стога су предложили неколико препорука за регулисање дистрибуције оваквог садржаја. У резолуцији се наводи да филтери против порнографије треба аутоматски да се активирају на свим новим рачунарима и преносивим уређајима; Интернет провајдери треба да пруже корисницима јасну опцију да се одобре или одустану од приступа таквом материјалу; провера старосних ограничења и

[57] https://www.chvnradio.com/articles/council-of-europe-proposes-measures-to-fight-pornography

порнографских сајтова требало би да буду обавезне да носе упозорења о потенцијалној штети. Сматра се да порнографију треба забранити на радном месту, а од послодаваца захтевати да инсталирају филтере за блокирање.

У одлуци се истиче да треба стриктно проверити сагласност свих приказаних лица, а да провајдери морају бити обавезни да прикупе идентитет и контакте свих који постављају јавни порнографски материјал. Порнографија из освете, или дистрибуција без пристанка, путем е-поште, текста, друштвених медија или било ког другог начина интимних и сексуалних слика како би се осрамотила и понизила приказана лица, је од посебне забринутости и требало би да буде делотворно гоњена. С обзиром да је слобода изражавања стуб демократских друштава и право загарантовано Европском конвенцијом о људским правима, ове препоруке за постављање граница су могуће под условом да су прописане законом и неопходне у интересу, између осталог, превенцију злочина, заштиту морала и заштиту права других, како је наведено у резолуцији Савета Европе.

2.3.3. Правна регулисаност осветничке порнографије у САД

У Сједињеним Државама не постоји јединствени национални закон који регулише случајеве осветничке порнографије. Међутим, постављање компромитујућих интимних видео снимака из освете третира се као кривично дело или прекршај у 34 америчке државе, док се у неким случајевима дефинише и као кривично дело и као прекршај. Поред законских мера које жртва може да предузме у домену кривичног права, постоји могућност кажњавања по законима који штите ауторска права, посебно ако је и особа која је објавила фотографију на интернету жртва. Ова правна заштита представља додатни механизам за сузбијање и санкционисање оваквих прекршаја.[58]

Пре свега, савезна влада Сједињених Америчких Држава је дефинисала осветничку порнографију као чин дељења приватних сексуалних материјала, укључујући фотографије или видео записе, без пристанка особе на њима, са циљем изазивања срамоте или узнемирености. Ова дефиниција је примењена и на нивоу савезних држава, где су законодавци усагласили кривично законодавство у циљу инкриминисања таквих радњи. До краја 2020. велики број држава и Дистрикт Колумбија донели су законе који

[58] Вилић, В. (2019). нав. дело, стр. 69-70.

забрањују осветничку порнографију. Законске одредбе обично захтевају да дистрибутери материјала буду проглашени кривим за слање сексуалног материјала без пристанка особе на њему. То укључује показивање интимних делова тела жртве или сексуалне радње. Такође, многе државе дефинишу осветничку порнографију као постављање или дистрибуцију фотографија или видео снимака који приказују гениталије, анус или женске груди друге особе, са намером да их узнемири или изнервира.[59]

Иако је уочљива разноликост законских норми, закључује се да се само објављивање непријатних слика бившег партнера у купаћем костиму не може сврстати у осветничку порнографију, осим у случајевима када су гениталије видљиве. Ово истраживање и законодавство играју кључну улогу у заштити приватности и сексуалне сигурности грађана у ери дигиталне комуникације.

Међутим, једно од најважнијих питања које се данас поставља у САД јесте како санкционисати починиоце оваквих дела и обезбедити обештећење жртвама. Дефинисање осветничке порнографије као кривичног или грађанског дела представља велики изазов. Ову дилему додатно компликује члан 230. Закона о пристојности у комуникацији (енгл. *Communications Decency Act*, CDA), који штити интерактивне интернет сервисе (као што су оператери осветничких порно сајтова) од грађанске одговорности за садржај који постављају корисници.[60]

Међутим, судски преседани указују на то да оператери ових сајтова губе заштиту коју пружа CDA ако активно доприносе или промовишу незаконит садржај у свом пословању. На пример, 2008. године Савезни жалбени суд је донео одлуку да је сајту укинут имунитет јер је материјално допринео незаконитом понашању. Слично томе, 2012. године, федерални окружни суд је пресудио у случају „*Jones v. Dirty World Entertainment Recordings, L.L.C.*“ да су аутори сајта изгубили имунитет јер су објавили увредљиве садржаје који су представљали деликт. Овакви судски поступци показују да постоји законски оквир кроз који се осветничка порнографија може санкционисати у САД, али указују и на сложеност овог проблема и потребу даљег правног разматрања како би се на прави начин заштитиле жртве и казнили починиоци.[61]

[59] Димовски, Д. (2023). нав. дело, стр. 162.
[60] Calvert. C. (2015). *Revenge Porn and Freedom of Expression: Legislative Pushback to an Online Weapon of Emotional and Reputational Destruction*. 24 Fordham Intell. Prop. Media & Ent. L. J. 673, стр. 677.
[61] Исто.

Касније се поставило питање шта ако се жртва добровољно фотографише или се добровољно фотографише, па јој бивши партнер украде мобилни телефон или компјутер и те фотографије објави на интернету. Наизглед сложена ситуација поставља нас пред дилему која укључује не само питања приватности и безбедности, већ и правна питања везана за ауторска права и одговорност. По закону, особа која је снимила фотографију задржава ауторска права на њу, чак и ако је фотографија добровољно послата или дата другој страни. Међутим, у случају његове неовлашћене дистрибуције или објављивања, тужилац има основ за заштиту својих права.

У овом контексту, Закон о пристојности у комуникацији (CDA) може бити релевантан, али не мора у потпуности заштитити порнографски сајт од грађанске одговорности за федерална кршења ауторских права. Судови су генерално тумачили CDA тако да не пружа имунитет од одговорности за тужбе у којима се наводи кршење традиционалних права интелектуалне својине, као што су тужбе за повреду ауторских права.[62] Међутим, Миленијумски закон о ауторским правима у дигиталном облику (енгл. *Digital Millennium Copyright Act*, DMCA) обезбеђује одређене механизме заштите ауторских права. Према условима DMCA, оператер порно сајта који хостује порнографске видео снимке без сагласности може бити изузет од одговорности за кршење ауторских права ако, након што је обавештен о наводном кршењу, одмах реагује да уклони или онемогући приступ материјалу који је тврди да крши ауторска права или може бити предмет активности кршења ауторских права.[63] Ова правна анализа сугерише да жртва у овим ситуацијама има на располагању правне алате да заштити своја ауторска права и да предузме мере против неовлашћеног коришћења њених фотографија. Истовремено, оператери веб страница су у обавези да одговоре на обавештења о повреди ауторских права како би избегли или ублажили своју одговорност.

Када се ради о кривичном аспекту осветничке порнографије, важно је истаћи да је законодавство широм света почело да реагује на сузбијање овог проблема. Конгрес је 1996. године донео први Међудржавни закон о ухођењу (енгл. *The Federal Cyberstalking Law*), који је имао за циљ да криминализује радње које намерно доводе другу особу у разуман страх од озбиљне повреде или смрти. Важно је напоменути да је овај Закон проширен 2006. године како би укључио понашање ухођења на мрежи, а такође је

[62] Исто, стр. 682.
[63] Исто.

препознао емоционални бол као довољну штету, а не само страх од смрти или озбиљне повреде.

Када је реч о осветничкој порнографији, законодавство се суочава са изазовима као што су несавршеност судских спорова, ауторска права и закони који регулишу сајбер ухођење. Тренутно 26 држава има законе који циљају на осветничку порнографију, али примена ових закона варира од државе до државе. На пример, у неким државама осветничка порнографија се може третирати као кривично дело, док у другим може бити прекршај. Њу Џерси и Калифорнија били су међу првима који су донели законе усмерене на сузбијање осветничке порнографије. Закон о заштити приватности из 2015. године, настоји да порнографију освете класификује као федерални злочин, што додатно указује на озбиљност проблема и потребу за адекватним правним мерама за заштиту жртава овог облика насиља. злоупотреба. Овај закон има за циљ да стави одговорност на веб странице које служе као платформе за дистрибуцију осветничке порнографије, као и на појединце који постављају такав садржај на те платформе. Његова сврха је да подстакне одговорност и затражи од веб локација попут Гугла или Фејсбука да уклоне везе до таквог експлицитног садржаја одмах након што буду обавештени о њиховој природи. Међутим, важно је напоменути да тренутно ове платформе, попут Фејсбука или Гугла, уживају заштиту у складу са CDA, али би претварање порнографије из освете као федералног злочина изузето од ове заштите.[64]

У марту 2022., као део Закона о поновној ауторизацији и Закона о насиљу над женама из 2022. године, Конгрес Сједињених Држава усвојио је историјски савезни закон који има за циљ борбу против осветничке порнографије. Овај закон дозвољава појединцима да поднесу федералну тужбу против особе која је неовлашћено поставила интимне слике или видео записе без пристанка појединца. Поред тога, поменути Закон садржи клаузулу о разумним мерама поверљивости у циљу заштите приватности жртава породичног насиља, сексуалног напада или ухођења. Ове мере обезбеђују да јавне стамбене агенције или власници и управници стамбених јединица не саопштавају локацију станарских стамбених јединица лицима која су извршила наведене облике насиља. До марта 2023. године, 48 америчких држава су донели сопствене законе који стриктно забрањују дистрибуцију или производњу порнографског материјала без

[64] Kamal, M., Newman, W. J. (2016). Revenge pornography: Mental health implications and related legislation. *Journal of the American Academy of Psychiatry & the Law Online*, 44 (3), стр. 365.

сагласности учесника. Важно је напоменути да су Масачусетс и Јужна Каролина биле међу ретким државама које још нису примениле такве законске одредбе.

2.3.4. Правна регулисаност осветничке порнографије у ЕУ

Тренутно, све државе чланице Европске уније, укупно 27, делују у оквиру континенталног правног оквира. Упркос напорима да се хармонизују закони који регулишу области искључивих или заједничких надлежности унутар Европске уније, систем остаје укорењен у принципу аутономије држава чланица у доношењу закона. Сходно томе, значајни диспаритети у приступима идентичним предметима и даље постоје међу земљама чланицама.[65]

Очекивало се да ће Општа уредба о заштити података (енгл. *The General Data Protection Regulation*, GDPR), уведена као решење за спорове у вези са приватношћу и личним подацима, укључујући и питање „порнографије из освете“, обезбедити снажан механизам за спровођење, стављајући контролу чврсто у руке погођених појединаца.[66] Међутим, пет година од његовог доношења, евидентно је да GDPR није ефикасно решио положај жртава „осветничке порнографије“. Уместо тога, терет лежи на корисницима да се крећу кроз сложеност тражења својих приватних слика на мрежи, контактирања појединачних контролора података и убеђивања невољних платформи да уклоне такав садржај – напоран и често бесплодан подухват. Правна помоћ, која обично укључује скупе и дуготрајне радње које омогућавају адвокати, служи као одвраћање за жртве које желе да остваре своја права. Такође, право на брисање, централно начело GDPR-а, показује се као изазов за спровођење због повезаних трошкова, временских ограничења и неизвесних исхода.[67]

Ове изазове отежава екстериторијална природа кршења, која погоршава сложеност надлежности која произилази из различитих тумачења GDPR-а међу државама чланицама, чиме се омета ефикасно спровођење закона. Сходно томе, мимо GDPR-а, појединци који траже обештећење на нивоу ЕУ могу да се обрате Директиви о

[65] Mania, K. (2022). Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study. *Trauma, Violence & Abuse*, 00(0), стр. 3
[66] Goddard, M. (2017). The EU general data protection regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, 59(6), 703–705.
[67] Politou, E., Michota, A., Alepis, E., Pocs, M., & Patsakis, C. (2018). Backups and the right to be forgotten in the GDPR: An uneasy relationship. *Computer Law & Security Review*, 34(6), 1247–1257.

електронској трговини из 2000. године, дизајнираној да разграничи одговорности одређених платформи у вези са отпремљеним садржајем.[68]

У складу са Директивом о аудиовизуелним медијским услугама, платформе за размену видеа дужне су да предузму мере заштите јавности од одређених садржаја, чија дистрибуција представља кривично дело према законодавству Европске уније. Једно од европских решења за проблеме приватности на мрежи може бити Нацрт закона о дигиталним услугама (енгл. *Digital Services Act*, DSA), који намеће обавезе и одговорности посредницима на јединственом тржишту, преко граница, уз обезбеђивање високог нивоа заштите корисника без обзира на место где се налазе. боравак у ЕУ. Као резултат тога, DSA ће усвојити посебан ред у вези са модерацијом садржаја, одабиром реклама или препоруком садржаја путем алгоритама. Њиме ће се ускладити обавезе онлајн платформи и пружалаца информационих услуга у борби против нелегалних садржаја које дистрибуирају корисници, као и у заштити основних права. Такође, члан 24б предложеног закона директно се односи на онлајн платформе које се претежно користе за дистрибуцију порнографског садржаја креираног од стране корисника, намећући им низ организационих и техничких захтева. Европски парламент је одобрио DSA 20. јануара 2022. године. Коначни текст ће бити директно применљив у целој Европској унији.[69]

У недостатку заштитног оквира предвиђеног Општом уредбом о заштити података (GDPR) у вези са феноменима који се разматрају, одговорност се преноси на национална законодавства. Сходно томе, када се спроводи анализа законодавног пејзажа у Европској унији у вези са „порнографијом из освете“ и „дубоком лажном порнографијом“, постаје императив да се на почетку утврди да ли је нека од држава чланица одлучила да криминализује ова дела. Такође, у случајевима када таква криминализација изостаје, потребно је детаљно испитивање законских одредби на које се позивају жртве приликом остваривања права.

У том контексту, посебна пажња је усмерена на законе који се баве „порнографијом из освете“ и ширењем интимних слика без сагласности, који служе као правни темељ за решавање случајева „дубоке порнографије“. Овај нагласак на правним оквирима наглашава значај разумевања механизама путем којих се националне

[68] Mania, K. (2022). нав. дело, стр. 3.
[69] Исто.

јурисдикције боре са овим све присутнијим дигиталним штетама, чиме се олакшава информисани дискурс и формулисање политике и на националном и на наднационалном нивоу.

Енглеска и Велс су међу земљама које су преузеле вођство у криминализовању осветничке порнографије. Пре криминализације порнографије из освете, 14. октобра 2014. године, државни тужилац Уједињеног Краљевства издао је смернице о томе како да се процесуирају случајеви осветничке порнографије. У смерницама се истиче да и постојећи нормативни оквир омогућава кривично гоњење за објављивање експлицитних слика и видео материјала без сагласности. Ипак, законодавац је убрзо покренуо поступак који би криминализовао осветничку порнографију. Законом о кривичном правосуђу и криминалу 2015. године уведено је ново кривично дело које ће гласити: „Објављивање приватне сексуалне фотографије или филма је кривично дело ако је обелодањивање извршено без сагласности лица које се појављује на фотографији или филму и уз намера да се појединцу нанесе невоља“. Током 2021. године забрањена је претња откривањем таквог материјала. Тужилаштво неће морати да доказује постојање слике или филма. За такво понашање биће предвиђена тренутна максимална казна од две године затвора или новчана казна, или обоје. Непосредно након Енглеске и Велса, Француска је донела Закон о дигиталној републици 2016. године. Омогућава санкционисање оних који су проглашени кривим за осветничку порнографију. Према законском тексту, починиоцима прети казна од две године затвора или новчана казна од 60.000 евра.[70]

2.3.5. Правна регулисаност осветничке порнографије у земљама бивше СФРЈ

Већина земаља бивше СФРЈ немају законе који посебно регулишу неовлашћену обраду и дистрибуцију слика и видео записа (порнографија из освете или злоупотреба слика на основу секса) уграђене у своје кривичне законе, осим Хрватске и Словеније (обе чланице ЕУ). Свака земља, међутим, криминализује скуп кривичних дела која се могу применити на случајеве осветничке порнографије. Ова кривична дела генерално спадају у две категорије: 1) Заштита тела и сексуалног интегритета (нпр. сексуално узнемиравање, узнемиравање, ухођење) и 2) Заштита од кршења приватности путем технолошких средстава (нпр. неовлашћено снимање/снимање, објављивање личних

[70] Димовски, Д. (2023). нав. дело, стр. 162-163.

података).[71] Иако су ове примене кривичних дела ограничене, оне могу да обезбеде, из нормативне перспективе, заштиту од осветничке порнографије. Међутим, много је теже проценити да ли ова апликација нуди значајну заштиту у пракси.

У Словенији и Хрватској, Кривични законик препознаје порнографију из освете као посебно кривично дело. Хрватски Кривични закон такође се посебно бави дубоким лажима и другим облицима сексуалног злостављања заснованог на имиџу и прописује веће казне за ширу дистрибуцију садржаја без пристанка. У неким земљама (Северна Македонија, Косово), промене политике су у току како би се обезбедила компатибилност националних кривичних закона са Истанбулском конвенцијом. Ово пружа важну прилику да се прошире дискусије са законодавним тијелима о кривичном гоњењу порнографије из освете, како би се осигурало да она буде значајније укључена у израду будућих закона. Иако није увек неопходно укључити директне одредбе, као у случају Словеније или Хрватске, ипак је важно осигурати да се осветничка порнографија широко идентификује и укључи, као и да се постојећи проблематични законски захтеви измене (као што је поменуто у случајевима Црна Гора и Србија). Пре него што се предложи (или примени) било каква законска измена, од највеће је важности да се изврши детаљан преглед и истраживање судске праксе како би се боље разумеле претходне судске одлуке и тренутна правна логика која се користи у судском процесуирању случајева дигиталног рода. засновано насиље. Ово истраживање сугерише да су постојећи Кривични закони и судска пракса, када се у потпуности имплементирају, довољни да обезбеде заштиту, и да иницијативе заступања треба да се усредсреде на стратешке парнице, подизање свести и изградњу капацитета за правосуђе и полицију.[72]

У Србији и Црној Гори кривична дела сексуалног узнемиравања и неовлашћеног снимања се гоне на основу приватних кривичних пријава, што значи да људи не добијају помоћ од полиције/тужилаштва и, што је још важније, пријаве морају бити поднете у року од три месеца од објављивања садржаја.. У свакој од земаља, осим у Србији, ови предмети су у надлежности Канцеларије главног тужиоца, са специјалним полицијским јединицама за борбу против сајбер криминала. Нејасно је да ли ове јединице такође

[71] See Digital Rights Network, Revenge porn – comparative analysis in South East Europe, доступно на: https://cms.seedigitalrights.network/wp-content/uploads/2022/05/Comparative-analysis_short-version_non-consensual-processing.pdf [15.02.2024]

[72] See Digital Rights Network, Revenge porn – comparative analysis in South East Europe, доступно на: https://cms.seedigitalrights.network/wp-content/uploads/2022/05/Comparative-analysis_short-version_non-consensual-processing.pdf [15.02.2024]

истражују случајеве осветничке порнографије или, што је још важније, пружају помоћ током извршних поступака (нпр. захтеви за уклањање садржаја). У неким земљама, као што су Србија и Албанија, постоје специјалне полицијске јединице за борбу против насиља у породици које имају одређени ниво стручности у раду са случајевима родно заснованог насиља.[73]

Такође, невладине организације (НВО) у Северној Македонији користе платформе за заговарање родне равноправности како би оспориле не само законске оквире већ и друштвене наративе који окружују осветничку порнографију, бавећи се питањима као што су окривљавање жртава и стигматизација сексуалности. Њихов вишестрани приступ, који обухвата јавне демонстрације, бесплатну правну помоћ и психолошку подршку преживјелима, означава заједнички напор да се изврши системска промјена и пружи хитна помоћ погођенима. Недавни правни поступци у Северној Македонији, који су резултирали осудама за производњу и ширење дечје порнографије, наглашавају посвећеност правосуђа борби против онлајн експлоатације. Слично томе, текуће ревизије законодавства на Косову, са обновљеним фокусом на решавање насиља над женама у дигиталним просторима, обећавају да ће повећати капацитет земље за борбу против насиља заснованог на роду.[74]

У Србији, национална стратегија за спречавање и борбу против родно заснованог насиља над женама и насиља у породици (2021-2025) признаје осветничку порнографију као посебан облик родно заснованог насиља који захтева повећану пажњу и напоре за подизање свести.[75] Користећи акумулирану стручност и деценијама искуства у развоју свеобухватних система подршке за преживеле, ови колективни напори имају потенцијал да утичу на суштинске промене, подстакну већу друштвену свест и пруже непосредну помоћ онима који су погођени насиљем заснованим на роду.

2.3.5.1. Хрватска

У јулу 2021. усвојене су измене у Кривичном закону Хрватске, којима је у члан 144а уведено кривично дело „злоупотреба сексуално експлицитног материјала“. Први

[73] Исто.
[74] Исто.
[75] Стратегија за спречавање и борбу против родно заснованог насиља над женама и насиља у породици (2021-2025), Службени гласник РС, бр. 47/2021.

део члана 144а гласи: „Ко злоупотреби поверење и без сагласности лица које је приказано, омогући трећем лицу приступ сексуално експлицитном материјалу снимљеном уз сагласност лица које је приказано за личну употребу, на овај начин нарушава приватност лица које је приказано на снимцима, казниће се затвором до једне године“.[76]

Неколико фактора игра улогу у овој дефиницији. Прво, починилац мора да злоупотреби поверење жртве. Дакле, кривично дело може починити само неко ко је имао или још увек има блиску везу са жртвом (на пример, бивши партнер). Тиме се аутоматски елиминише кривично гоњење починилаца који су жртви непознати. Дакле, ако би потпуни странац направио сексуалну слику особе и поделио је, не би се суочио са кривичним гоњењем. Иако је разумљиво да постоје случајеви у којима људи добровољно снимају и шаљу приватне сексуалне слике себе својим партнерима/другим особама којима верују, а затим ти људи нарушавају то поверење и деле садржај, постоје многе друге врсте злоупотребе засноване на сликама које нажалост не потпадају под ову дефиницију. Поред тога, неопходно је нагласити да тренутна дефиниција налаже да заједнички снимци морају бити набављени уз изричит пристанак појединца и за личну употребу. Ова одредба даље ограничава већ ограничену дефиницију. Важно је напоменути да чак и интимни партнер појединца, да не помињемо друге, може тајно снимити слике или видео записе без пристанка и након тога их ширити без овлашћења. Према овој рестриктивној дефиницији, такве радње се не би сматрале кривичним дјелима јер садржај није првобитно прибављен уз сагласност нити намењен за личну употребу.[77]

Ови примери наглашавају како је хрватско законодавство, стриктно придржавајући се наведених критеријума, усвојило уски приступ, криминализујући тако само делић случајева сексуалног злостављања заснованог на имицу и остављајући бројне потенцијалне жртве без правне заштите. Сходно томе, сваки облик стварања и/или ширења приватних сексуалних слика без пристанка, треба да се категорише као кривично дело, без обзира на мотиве починиоца или њихов однос са жртвом. Такав ревидирани оквир би се ефикасније позабавио сложеностима и нијансама својственим случајевима

[76] Казнени закон Републике Хрватске, Народне новине бр. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/18, 84/21, чл. 144а.
[77] Živković, I., Čubrilo, V., Dujić, K. 'Revenge Porn': An Exploration into Redefinition in the Interest of Changing Legislation, доступно на: https://portal.ejtn.eu/PageFiles/20512/Team%20Croatia_Revenge%20Porn%20An%20Exploration%20into%20Redefinition%20in%20the%20Interest%20of%20Changing%20Legislation.pdf [15.02.2024]

сексуалног злостављања заснованог на имицу, чиме би се потенцијалним жртвама пружила већа правна заштита.

2.3.5.2. Словенија

Правни концепт „озбиљног нарушавања нечије приватности“ је такође садржан у словеначком Кривичном законику из 2017. Конкретно, у параграфу VI члана 143, бави се ширењем порнографије из освете. Овом одредбом прописано је да се казна од три месеца до три године затвора подлежу појединцима који јавно обелодањују снимке или поруке са сексуалним садржајем другог лица без њиховог пристанка, чиме значајно утичу на њихову приватност. Тумачење законског услова „озбиљно утиче на његову приватност“ зависи од последица починиоца. Починилац мора да поседује или директну намеру или барем пристанак (*dolus eventualis*) за озбиљно нарушавање приватности жртве. Овај услов не представља објективан критеријум за кривичну или строгу одговорност. Процена да ли су права на приватност појединца суштински повређена слична је процени која се спроводи у случајевима клевете.[78]

Неопходно је напоменути да повреда приватности мора испунити објективне критеријуме, иако није предуслов да жртва субјективно доживљава себе као озбиљно погођену. Међутим, субјективно искуство жртве може утицати на њену одлуку да покрене судски поступак против починиоца. Посебно, околности као што су ментални капацитет, емоционална отпорност или ексхибиционистичке тенденције (у медицинском смислу) могу утицати на субјективно искуство жртве. Утврђивање да ли снимак или порука објективно резултира тешким оштећењем захтева процену различитих фактора укључујући временски контекст, околне околности, друштвене норме и појединце који су укључени.

2.3.5.3. Босна и Херцеговина

[78] Šepec, M. (2019). Revenge Pornography or Non-Consensual Dissemination of Sexually Explicit Material as a Sexual Offence or as a Privacy Violation Offence. *International Journal of Cyber*, 13(2), стр. 431.

У Босни и Херцеговини релевантни кривични закони ентитета Република Српска и Федерације Босне и Херцеговине не праве разлику између неовлашћеног снимања и дистрибуције фотографија и видео записа, што имплицира да жртва може покренути судски поступак само ако је снимак направљен. без њеног изричитог пристанка и дистрибуирана у таквом облику. Ако појединац сам снима и добровољно подели снимак, по кривичном закону није под заштитом закона. Ако се стриктно придржавамо термина „њене просторије“, то би значило да ванбрачни партнер може позвати жртву у свој дом, снимити је и користити тај снимак како жели, јер се то не сматра снимањем у „њеној“ сфери. Чак и ако је неко незаконито снимљен у својим просторијама, а слике или видео снимци буду објављени на интернету, барем у Федерацији, „мало се обраћа пажња“ ако нема конкретних доказа да је наводни починилац покушавао да изнуди новац од жртва.[79]

Таква ситуација у БиХ се манифестује кроз ниску стопу процесуирања од 2016. до 2020. године, гдје је од 104 особе обухваћене истрагом процесуирано само 26, од којих је 18 осуђено условно, а шест новчано. Иако закон предвиђа затворске казне до три године, ниједан случај није резултирао изрицањем максималне казне.[80]

2.3.5.4. Црна Гора

Тема осветничке порнографије у Црној Гори представља изазов у домену родно заснованог насиља, чија се законска регулатива тренутно усавршава. Осветничку порнографију карактерише неовлашћено дељење или доступност сексуално експлицитног материјала са другим људима, често без њиховог пристанка. Уобичајено је да су жртве жене, док су мушкарци често починиоци таквих радњи.

Друштвене мреже, затворене групе и мобилне апликације служе као главни канали дистрибуције оваквог садржаја. Министарство правде Црне Горе је предложило измјене и допуне закона у циљу ефикаснијег сузбијања ове појаве. Предлози су прослеђени Европској комисији на мишљење, након чега ће бити представљени Скупштини на усвајање.

[79] https://detektor.ba/2021/10/18/necija-kcerka-strasan-nekaznjen-danak-osvetnicke-pornografije-na-balkanu/
[80] Исто.

До сада су се случајеви осветничке порнографије решавали кроз шест чланова Кривичног законика, углавном кроз приватне тужбе. Међутим, предложене измене омогућиле би кривично гоњење по службеној дужности. Недостатак прецизних података о распрострањености овог облика насиља чини кључним даље истраживање и праћење. Нажалост, из надлежних институција није било одговора на упит о броју пријављених случајева осветничке порнографије. Организације попут Приме се активно залажу за законодавне промене како би се осигурала заштита жртава и одговарајуће санкције за починиоце. Сматрају да је неопходно да институције одреде високе казне како би се послала јасна порука да се овакво насиље неће толерисати.

У Црној Гори, као и у другим земљама, овај облик насиља често пролази некажњено, а постојећи закони често нису довољни да се на адекватан начин сузбије ова појава. Дакле, предложене измене Кривичног законика, којима су прописане казне затвора до две године за неовлашћено дељење сексуално експлицитног материјала, као и до три године за дистрибуцију истих путем интернета, представљају искорак у борба против осветничке порнографије.

Даље, за случајеве у којима су жртве малолетне, предложене су још ригорозније казне, што указује на важност заштите најугроженијих чланова друштва. Овакве законске иницијативе представљају основу за борбу против осветничке порнографије и стварање амбијента у коме се починиоци оваквих дела сматрају одговорним за своја дела.

2.3.5.5. Северна Македонија

Северна Македонија се, као и многе земље, суочава са изазовима регулисања порнографске индустрије, посебно у контексту феномена осветничке порнографије. Осветничка порнографија, позната и као "порнографија освете" или "порнографија без пристанка", представља озбиљан друштвени и правни проблем чије последице могу бити дугорочне и штетне за жртве. И поред све већег препознавања овог проблема на глобалном нивоу, Северна Македонија још увек нема адекватне законске механизме за регулисање ове врсте злоупотреба.

Садашње стање правног оквира у Северној Македонији не пружа довољну заштиту жртвама осветничке порнографије. Иако постоје одређени закони који се односе

на заштиту приватности, дигитални криминал и сексуално узнемиравање, недостаје посебна регулатива која би се на адекватан начин позабавила проблемом осветничке порнографије. Одсуство јасних дефиниција, санкција и процедура за борбу против ове врсте злостављања ствара правни вакум који жртве оставља незаштићеним.

Неопходно је утврдити посебне законе који ће јасно дефинисати овај облик злостављања, прописати одговарајуће санкције за починиоце и обезбедити адекватну заштиту жртвама. Такође, неопходно је улагати у обуку релевантних правосудних актера како би се обезбедила ефикасна примена закона. Само свеобухватним правним приступом може се на адекватан начин суочити са овим сложеним друштвеним проблемом и заштитити интегритет грађана Северне Македоније.

2.3.6. Нормативни оквир у праву Републике Србије

Република Србија, у свом кривичном законодавству, не регулише феномен „осветничке порнографије“. Међутим, анализом одговарајућих законских одредби, могуће је идентификовати кривична дела која се односе на специфичне облике порнографског садржаја и неправилног објављивања приватних информација. Пре свега, Кривични закон Србије садржи одредбе које су применљиве на случајеве неовлашћеног фотографисања (члан 144), неовлашћеног објављивања и приказивања туђег материјала, укључујући и снимке (члан 145). Додатно, постоје законске норме које се односе на сексуално узнемиравање (члан 182а), као и на приказивање, прибављање и поседовање порнографског материјала, као и искоришћавање малолетних лица за порнографију (члан 185).

Као што се може видети, ове одредбе Кривичног закона обухватају аспекте који су релевантни у контексту осветничке порнографије. Елементи који чине основу ових кривичних дела укључују неовлашћено преузимање, објављивање или приказивање материјала без дозволе, као и сексуално узнемиравање и експлоатацију малолетних особа у порнографији.

Кривично дело неовлашћеног фотографисања представља облик угрожавања приватности и личног живота грађана. Први степен овог кривичног дела укључује неовлашћено сачињавање фотографског, филмског, видео или другог снимка неког лица, при чему се нарушава њихова приватност и лични живот. Циљ овог дела може бити

предаја или показивање трећем лицу или на други начин омогућавање да се снимак упозна. Прописана казна за овај облик кривичног дела укључује новчану казну или казну затвора до једне године. Други степен овог кривичног дела је тежи облик, који се карактерише тиме да га учини службено лице у вршењу својих дужности. У овом случају, извршилац ће бити кажњен затвором до три године. Овај степен кривичног дела укључује злоупотребу положаја и поверења у служби у циљу кршења приватности и личног живота грађана.[81]

На основу анализе овог кривичног дела, можемо закључити да је предмет заштите интимност особе. Радња извршења је алтернативно одређена. Ако бисмо овај злочин посматрали кроз призму осветничке порнографије, видели бисмо да постоји делимична неслагања са објављивањем експлицитних слика или снимака без претходне дозволе другог лица са мотивом освете. Наиме, у случају осветничке порнографије, каква је криминализована у другим земљама, суштина је објављивање или дистрибуција експлицитне фотографије са мотивом освете. У случају кривичног дела неовлашћено фотографисање радња се одређује алтернативно, при чему се неке од радњи поклапају са осветничком порнографијом – приказивањем или на други начин омогућавањем гледања видео снимка. Полазећи од чињенице да се осветничка порнографија најчешће ради путем интернета, односно друштвених мрежа (видети истраживање из главе под насловом Карактеристике осветничке порнографије), поставља се питање да ли интернет и друштвене мреже могу бити један од начина почињења овог кривичног дела. Мишљења смо да могу бити, чиме би се појединцима пружила свеобухватнија заштита од објављивања експлицитних слика. Исто тако, у кривичном делу осветничке порнографије није потребно да снимак озбиљно задире у лични живот особе на снимку. Исто тако, спорно је и одсуство осветничког мотива. Иако би ово могло бити замењено применом члана 54. КЗ. Наиме, прописано је да се при одређивању казне посебно води рачуна о мотивима из којих је кривично дело извршено. Тако би се као отежавајућа околност приликом изрицања казне могла навести освета.[82]

Неовлашћено објављивање и излагање туђих досијеа, портрета и снимака, као кривично дело, је радња којом се без дозволе објављује или приказује материјал приватне природе, као што је листа, портрет, фотографија, филм или фонограм који је у вези са неким. или више особа. Ово дело се састоји од дела задирања у приватни живот других

[81] Кривични законик, чл. 144.
[82] Димовски, Д. (2023). нав. дело, стр. 166.

без њиховог пристанка, што се сматра кршењем њиховог права на приватност. Примарни критеријум за оцењивање је нарушавање приватности, као и потреба за изричитим дозволама за објављивање или приказивање. За кршење ових правила предвиђене су казне у виду новчане или казне затвора до две године, што наглашава озбиљност овог дела и његов значај у заштити приватности и личних права грађана.[83]

Анализом овог кривичног дела долазимо до закључка да је радња извршења сложена и да постоје две алтернативне радње – објављивање или приказивање. Неопходно је осетљиво задирање у лични живот пасивног субјекта (жртве). Упоређујући ово кривично дело са осветничком порнографијом, може се закључити да се углавном ради о подударности у погледу неовлашћеног објављивања експлицитних слика без сагласности, са мотивом освете. Као иу претходно анализираном делу, поставља се питање да ли интернет и друштвене мреже могу бити средство извршења. Одговор је да. Што се тиче мотива извршења овог кривичног дела, можемо применити члан 54. Кривичног законика како би се извршилац осветничке порнографије строже казнио.[84]

Кривично дело полног узнемиравања, дефинисано у члану 182а Кривичног законика. Појам овог дела обухвата акт полног узнемиравања над другим лицем, за који је предвиђена казна у облику новчане санкције или затвора у трајању до шест месеци. Уколико је узнемиравање учињено према малолетном лицу, закон предвиђа тежу казну, у виду затвора у трајању од три месеца до три године. У спецификацији дела, у ставу три истог члана, законодавац дефинише појам полног узнемиравања. Овде се под полним узнемиравањем подразумева свако вербално, невербално или физичко понашање које има за циљ или представља повреду достојанства лица у сфери полног живота, а које изазива страх или ствара непријатељско, понижавајуће или увредљиво окружење.[85] Важно је напоменути да се поступак гоњења за овим кривичним делом предузима по предлогу, што покаже на значај представљања доказа и изношења случаја пред надлежним органима правосуда.[86]

Последње кривично дело које захтева анализу јесте кривично дело приказивања, прибављања и поседовања порнографског материјала и искоришћавање малолетних лица за порнографију, као што је предвиђено одредбама члана 185 Кривичног законика

[83] Кривични законик, чл. 145.
[84] Димовски, Д. (2023). нав. дело, стр. 167.
[85] Кривични законик, чл. 182а.
[86] Димовски, Д. (2023). нав. дело, стр. 167.

Републике Србије. Ово кривично дело обухвата више облика. Први облик кривичног дела описаног у ставу 4 састоји се од прибављања за себе или за друге, поседовања, продаје, приказивања, јавног излагања или електронског, односно другог начина чињења доступним слика, аудио-визуелних или других предмета порнографске природе, који су произведени искоришћавањем малолетних лица. За овај облик кривичног дела предвиђена је казна затвора у трајању од три месеца до три године. Други облик кривичног дела, како је наведено у ставу 5, односи се на кажњавање особа које свесно приступају сликама, аудио-визуелним или другим предметима порнографске природе, који су створени искоришћавањем малолетних лица, путем коришћења информационих технологија. За овакво понашање предвиђена је новчана казна или казна затвора која може трајати до шест месеци. Законодавац у ставу 6 детаљно дефинише шта се сматра предметима порнографске природе који су произведени искоришћавањем малолетних лица, познатије као дечија порнографија. Овим предметима сматрају се сви материјали који визуелно приказују малолетно лице у актуалном или симулираном сексуално експлицитном понашању, као и сваки приказ полних органа детета у сексуалне сврхе.[87] Напослетку, члан 185 предвиђа и меру безбедности у облику одузимања предмета, што је ближе уређено у члану 87 Кривичног законика.[88]

Посматрајући наведене облике кривичних дела у контексту осветничке порнографије, можемо приметити да се кроз овај законски оквир пружа правна заштита малолетницима (односно лицима млађим од 18 година, како је дефинисано чланом 112. КЗ) против приказивања, јавног приказивања или електронског преноса слика, аудио-визуелних или других облика порнографског садржаја. Важно је нагласити да је код овог дела кривичног права мотив недетерминистички елемент, што значи да не мора доћи до потпуне конфронтације са осветничком порнографијом. Када анализирамо други наведени облик кривичног дела, уочавамо да нема случајности са осветничком порнографијом, али је њено уврштавање у кривичноправни оквир значајно због спречавања даље виктимизације малолетника чији експлицитни садржај, аудио-визуелни или др. облици порнографског материјала, доступни јавности, што може довести до ситуације да други људи буду изложени таквом садржају.[89]

[87] Кривични законик, чл. 185.
[88] Димовски, Д. (2023). нав. дело, стр. 168.
[89] Исто.

2.4. Осветничка порнографија у Кривичном законику Републике Србије – кривично дело или не?

У различитим земљама широм света, законодавство усмерено на сузбијање осветничке порнографије је у великој мери присутно и кривично дело је строго кажњиво. Међутим, у Србији, иако постоје гласови и иницијативе које сугеришу потребу за усвајањем сличних закона, Кривични законик не препознаје осветничку порнографију као засебно кривично дело. Ово представља знатан изазов, посебно с обзиром на тенденцију растућег броја случајева осветничке порнографије у контексту развоја интернет технологије.

У последње време, уз напредак технологије и доступности интернета, постаје сувише лако за појединце да објављују приватне снимке или слике других особа без њиховог пристанка. Ово је посебно проблематично у случајевима осветничке порнографије, где се интимни снимци објављују са намером да се нанесе штета или да се посрами жртва. Управо због оваквих случајева, многе земље су увеле законе који строго кажњавају овакве поступке и препознају их као кривична дела.

У Србији, иако постоји одређено законодавство које би могло да се примени на случајеве осветничке порнографије, као што је закон који санкционише неовлашћено објављивање снимака, проблем се јавља у примени закона. Често, ова кривична дела се гоне по приватној тужби, што чини доказивање случаја изузетно тежим. Постоји и стигматизација жртава, као и чињеница да се није прописана довољно оштра санкција за починиоце, што доприноси томе да веома мали број људи се одлучује на правне поступке. Ово често води до поновне виктимизације жртава и услојава да се случајеви не пријављују.

Дакле, неопходно је да се у српском кривичном законодавству направе измене које би специфично препознале осветничку порнографију као кривично дело и предвиделе строже санкције за починиоце. Ово би укључивало и гонење кривичних дела по службеној дужности. Најважније је да закони буду тако формулисани да одражавају суштину проблема и обезбеде адекватну заштиту за жртве осветничке порнографије, без обзира на мотиве извршиоца.

Тема осветничке порнографије и непостојање адекватног правног одговора на њу представља сложен друштвени и правни изазов који захтева пажљиву анализу и

деловање. У данашњем контексту, све већа доступност технологије омогућава људима да нарушавају приватност и достојанство других особа кроз ширење осветничке порнографије, често без узимања у обзир моралних и друштвених норми.

Анализирајући ситуацију у Србији, примећује се изостанак реакције државних институција на овај проблем, што изазива озбиљну забринутост. Док друге европске земље предузимају кораке у борби против ове појаве, Србија заостаје у пружању адекватног одговора. Одсуство брзих и ефикасних правних механизама за заштиту жртава осветничке порнографије додатно компликује ситуацију.

Иако се разматрају измене Кривичног законика, то само по себи није довољно. Неопходно је развити свеобухватнији правни оквир који ће на адекватан начин заштитити жртве, узимајући у обзир специфичности овог облика високотехнолошког криминала. Примери као што је Хрватска, где жртва мора да покрене кривично гоњење починиоца, указују на недостатак ефикасних механизама заштите.

Да би се превазишли изазови у борби против осветничке порнографије, неопходно је не само донети строже законе, већ и обезбедити њихову ефикасну примену. Ово захтева ангажовање свих релевантних актера, укључујући државне институције, невладине организације и активну подршку заједнице. Важно је пружити подршку жртвама, омогућити им приступ правди и осигурати да се њихова права у потпуности поштују. Само кроз такав интегрисани приступ можемо напредовати у заштити људских права и промовисању правде у друштву.

3. АНАЛИЗА ДОБИЈЕНИХ РЕЗУЛТАТА О ПРИЈАВАМА УПУЂЕНИМ ПОСЕБНОМ ЈАВНОМ ТУЖИЛАШТВУ ЗА ВИСОКОТЕХНОЛОШКИ КРИМИНАЛ

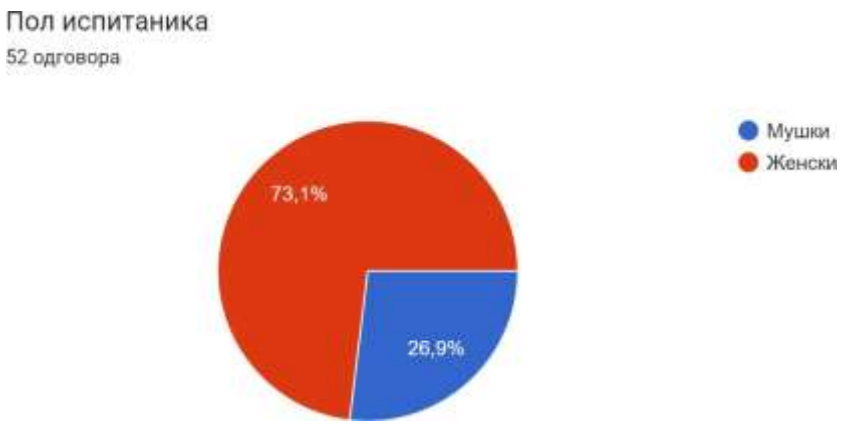
3.1. Опис истраживања

Осветничка порнографија је последњих година предмет интересовања и истраживања како стручњака, тако и лаика. Упркос бројним досадашњим истраживањима специфичност и тежина ових кривичних дела дају му епитет непресушног извора. Узорак и метод истраживања: Овом анкетом - истраживањем обухваћена је статистика узраста, пола, степена образовања као и тип насеља у којем живи испитаник, њихов љубавни статус, основа за постајањем жртве остветничке порнографије узимајући у обзир сва релевантна питања која су постављена како би добили процентуални увид приказан кроз графиконе сходно добијеним резлтатима.

Критеријуми којима сам се водила приликом одабира су били случајни испитаници, мушкарци и жене, различите старосне доби како образовања, тако и статуса.Узорак су чинили 50 испитаника који су учествовали у онлине анкенти. Циљ истраживања је да се утврди да ли су и ако јесу на који начин били жртве било каквог вида дигиталног партнерског насиља, уколико јесу – какве је то последице оставило на њих, да ли су упознати правном регулативом и начином на који могу заштити своја права.

3.2. Интерпретација и дискусија резултата

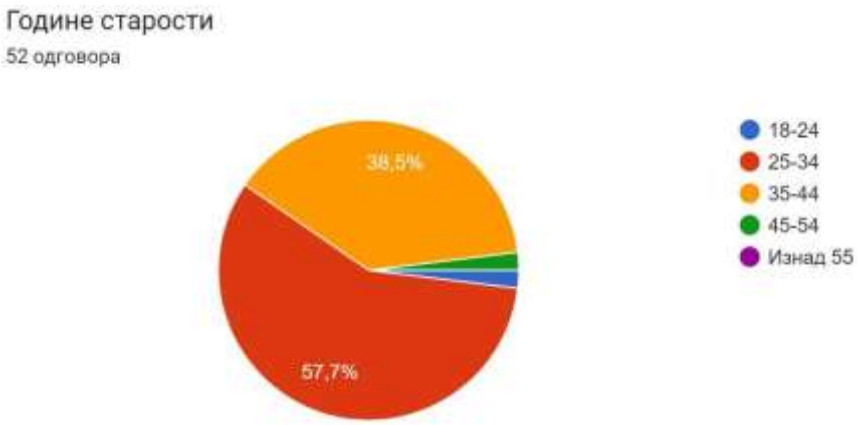
Прво питање у оквиру упитника односило се на пол испитаника. Резултати су приказани на графикону 1.



Графикон 1. Пол испитаника

Подаци на графику изнад указују на пол испитаника. Наиме, у испитивању је учествовало 26,9% мушкараца и 73,1% жена.

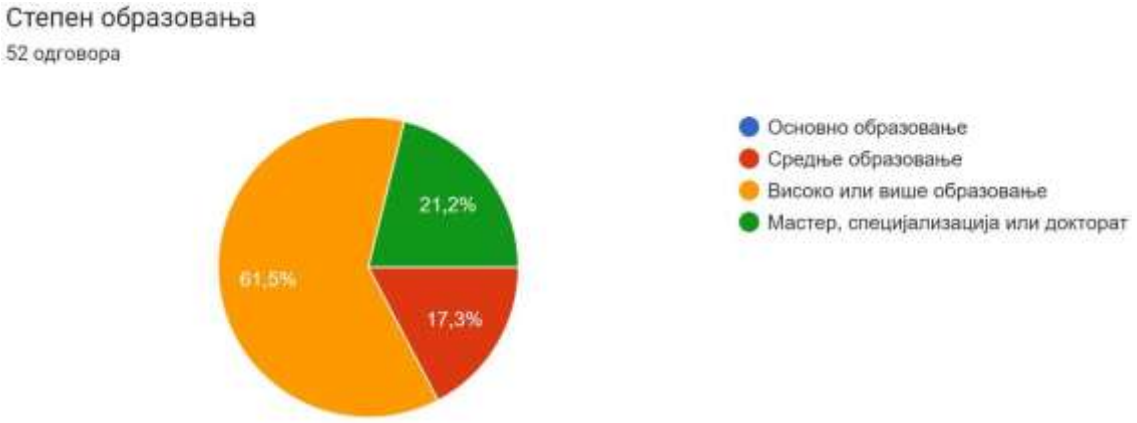
Надаље, на графикону 2 налазе се подаци о старости испитаника.



Графикон 2. Године старости испитаника

Подаци на графику 2 приказују године старости испитаника. Највећи проценат испитаника је старости од 25-34 година (57,7%), затим следе испитаници старости од 35-44 година (38,5%), старости од 18-24 година (1,9%), и старости од 45-54 година (1,9%). Није било испитаника старости изнад 55 година.

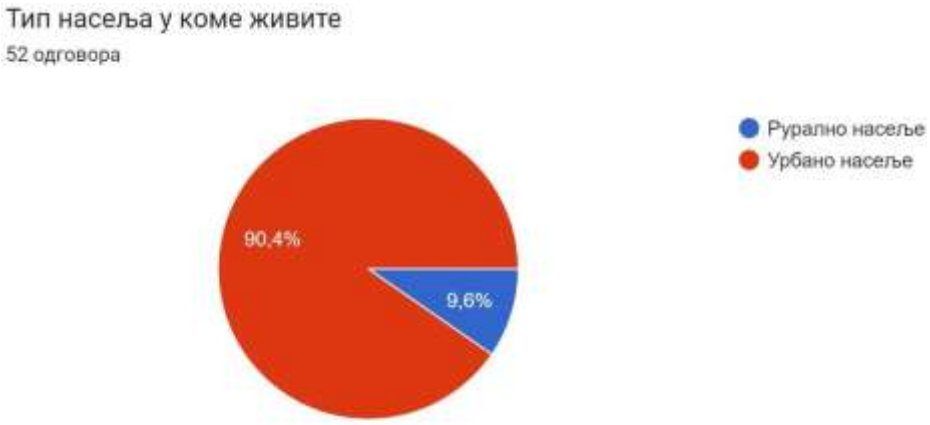
На графикону 3 приказани су резултати о степену образовања испитаника који су учествовали у анкетном истраживању.



Графикон 3. Степен образовања

Око 61,5% изјаснило да има високо или више образовање, затим 21,2% испитаника који имају завршену магистратуру, специјализацију или докторат, док је 17,3% испитаника са завршеним средњим образовањем. Није било испитаника са завршеним само основним образовањем.

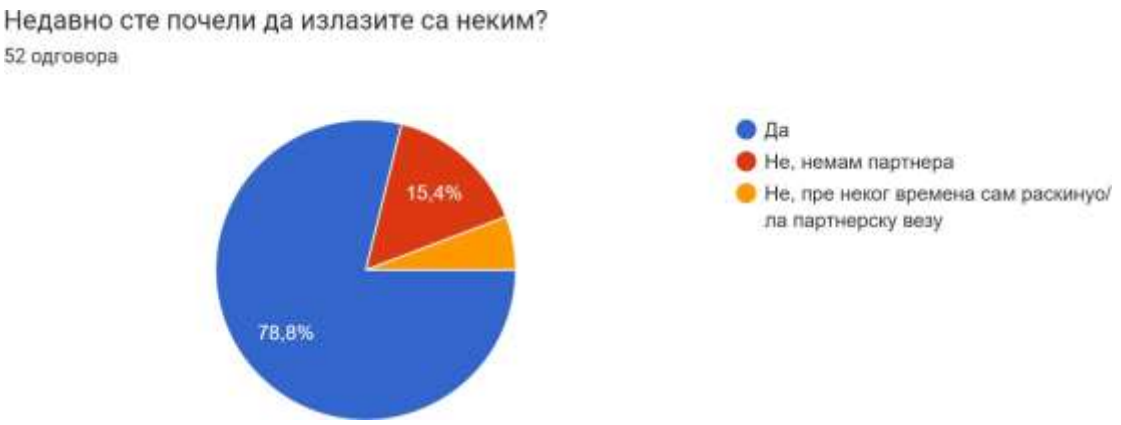
Надаље, на графикону 4 приказани су резултати о типу насеља у коме живи испитаника.



Графикон 4. Тип насеља у коме живи испитаник

Највећи број испитаника који су учествовали у анкети живи у урбаном насељу (90,4%), док је свега 9,6% оних који живе у руралним срединама.

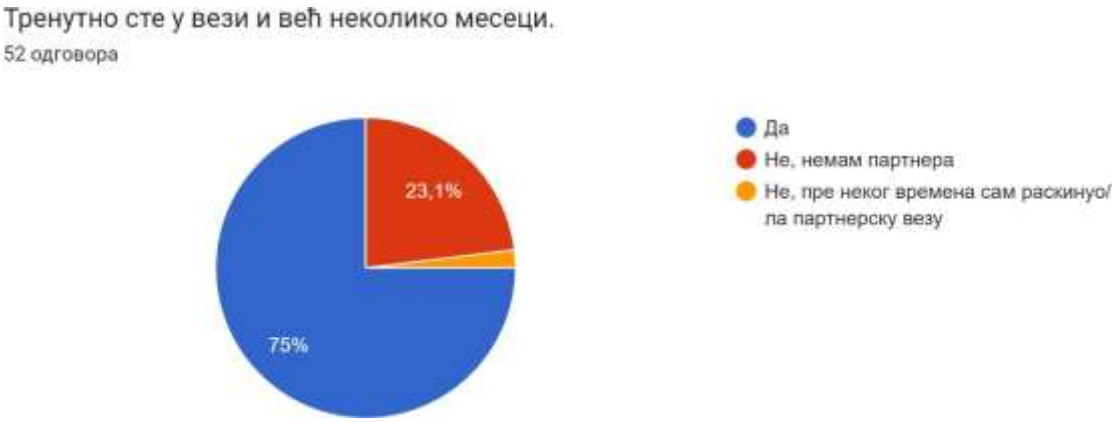
Наредно питање у анкети гласило је: *Недавно сте почели да излазите са неким?*



Графикон 5. Недавно сте почели да излазите са неким?

Највећи број испитаника наводи да је од скоро почело да излази са неким (78,8%), следе они који немају партнера (15,4%) и на крају они који су пре извесног времена прекинули партнерску везу (5,8%).

Следеће питање гласило је: *Тренутно сте у вези већ неколико месеци?*

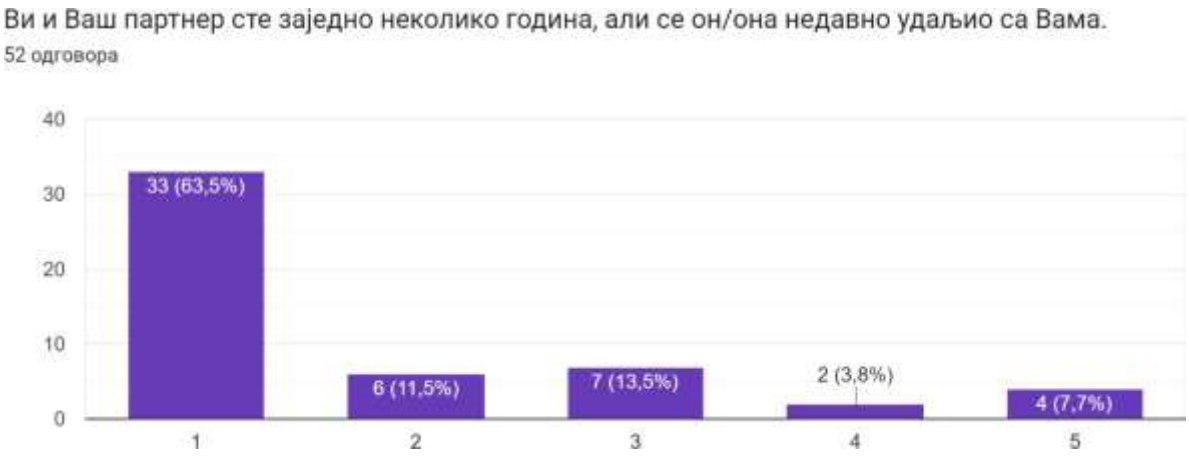


Графикон 6. Тренутно сте у вези већ неколико месеци?

Највећи број испитаника наводи да је у вези већ неколико месеци (75%), док 23,1% наводи да нема партерску везу. На крају су испитаници који су пре неког времена прекинули партнерску везу (1,9%).

Надаље, анкета је обухватала одређене тврдње, на које је испитаници требало да дају одговоре према следећем критеријуму: 1- У потпуности се не слажем, 2- Не слажем се, 3- Нити се слажем нити се не слажем, 4- Слажем се, 5- У потпуности се слажем.

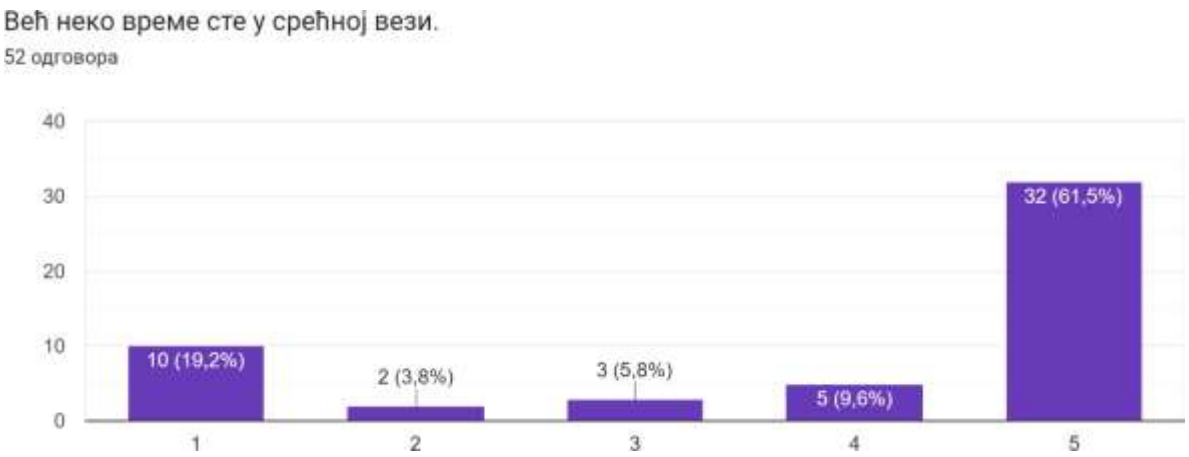
Прва тврдња гласила је: *Ви и Ваш партнер сте заједно неколико година, али се он/она недавно удаљио са Вама*.



Графикон 7. Ви и Ваш партнер сте заједно неколико година, али се он/она недавно удаљио са Вама.

Према одговорима испитаника, највећи је проценат оних који је у потпуности не слажу са овом тврдњом (63,5%), док је најмањи проценат оних који се нити слажу нити не слажу (3,8%).

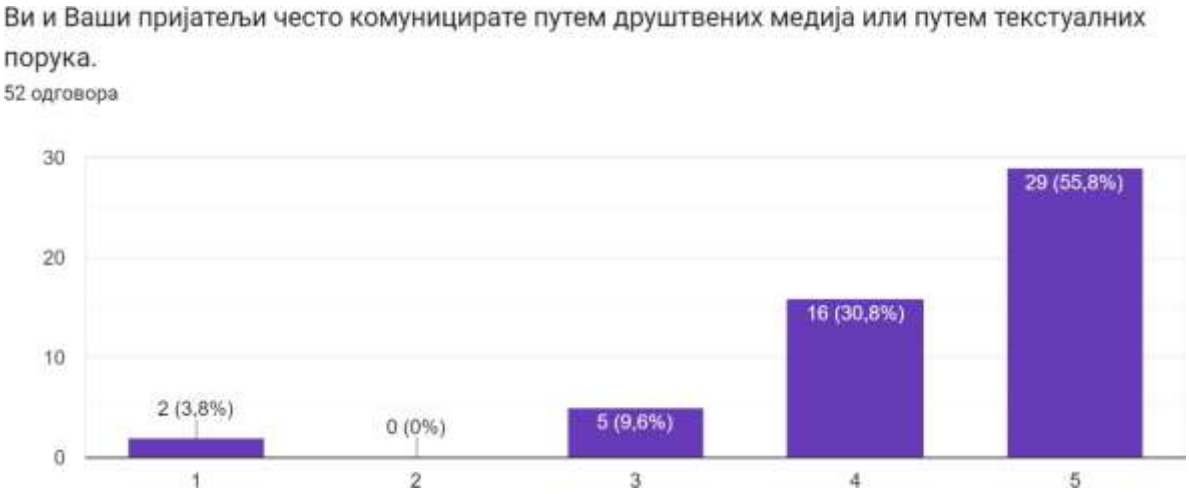
Наредна тврдња гласила је: *Већ неко време сте у срећној вези*.



Графикон 8. Већ неко време сте у срећној вези.

Највећи проценат испитаника се у потпуности слаже са овом тврдњом (61,5%), док је најмањи проценат оних који се не слажу (3,8%).

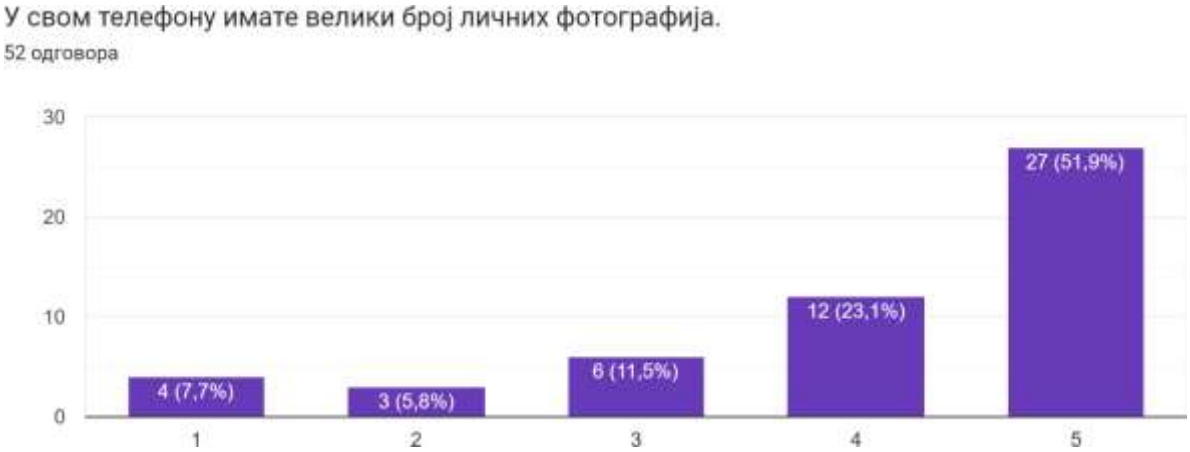
На графикону 9 налазе се одговори испитаника на тврдњу: *Ви и Ваши пријатељи често комуницирате путем друштвених медија или путем текстуалних порука*.



Графикон 9. Ви и Ваши пријатељи често комуницирате путем друштвених медија или путем текстуалних порука.

Према одговорима испитаника, највећи је проценат оних који је у потпуности слажу са овом тврдњом (55,8%), а исто тако је висок проценат и оних који се слажу (30,8%), док није било испитаника који се не слажу (0%).

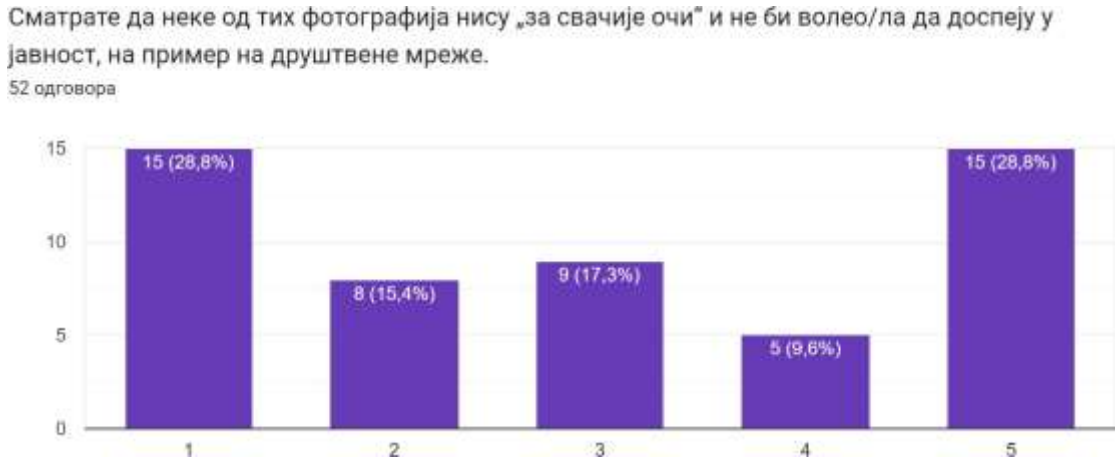
Наредна тврдња у анкети гласила је: *У свом телефону имате велики број личних фотографија.*



Графикон 10. У свом телефону имате велики број личних фотографија

Највећи број испитаника се у потпуности слаже са тиме да у свом телефону има велики број личних фотографија (51,9%), док је 23,1% оних који се само слажу. Најмањи је проценат оних који се не слажу (5,8%).

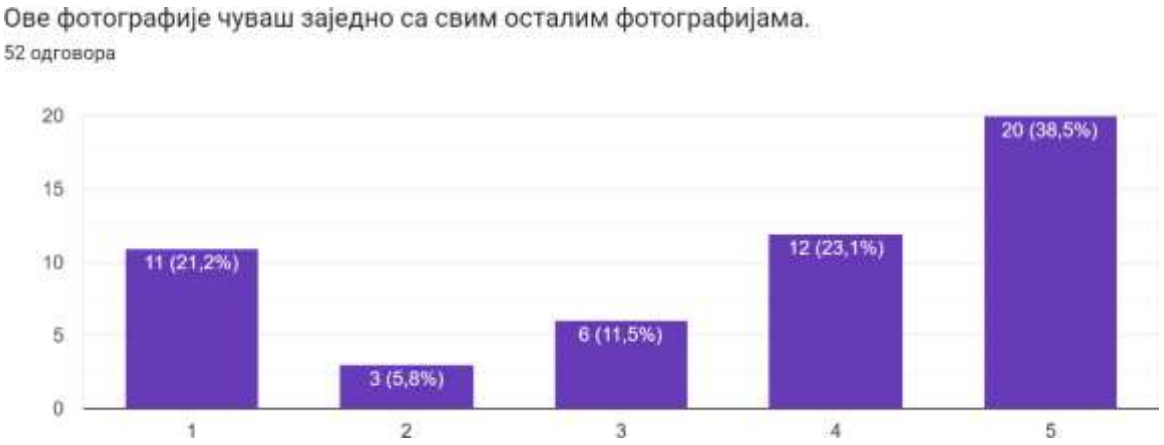
Следећа тврдња у анкети формулисана је као: *Сматрате да неке од тих фотографија нису „за свачије очи“ и не би волео/ла да доспеју у јавност, на пример на друштвене мреже.*



Графикон 11. Сматрате да неке од тих фотографија нису „за свачије очи“ и не би волео/ла да доспеју у јавност, на пример на друштвене мреже

Одговори на ово питање су различито дистрибуирани. Наиме, највећи број испитаника изјаснило се да се у потпуности не слаже (28,8%) и у потпуности слаже (28,8%) са наведеном тврдњом. Затим, 17,3% је оних који су били неодлучни, док је 15,4% оних који се не слажу и 9,6% оних који се слажу.

Наредна тврдња надовезала се на претходну и гласила је: *Ове фотографије чуваш заједно са свим осталим фотографијама.*

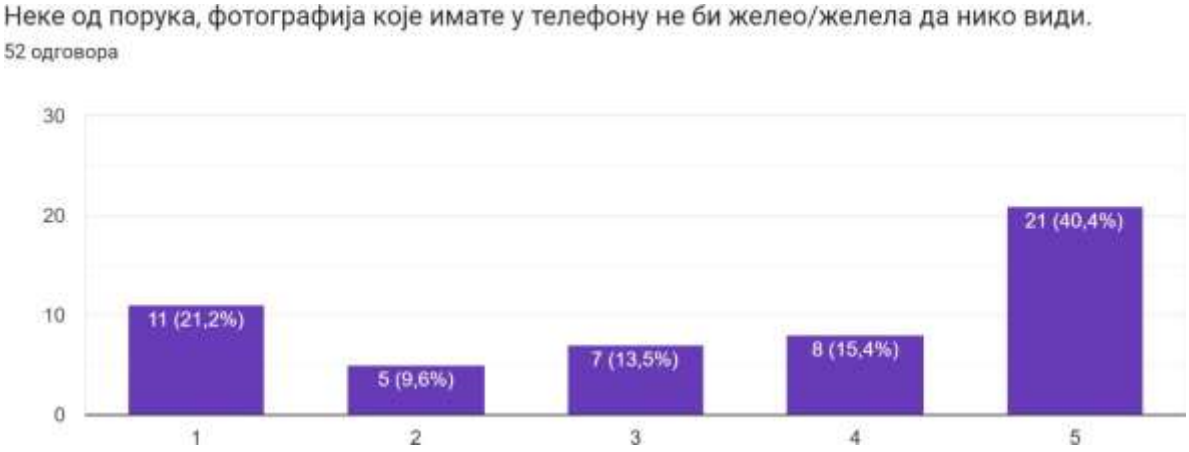


Графикон 12. Ове фотографије чуваш заједно са свим осталим фотографијама

Према одговорима испитаника, највећи је проценат оних који је у потпуности слажу са овом тврдњом (38,5%), а исто тако је висок проценат и оних који се слажу (23,1%) и оних који се у потпуности не слажу (21,2%), док је било 5,8% испитаника који се не слажу.

Наредна тврдња у анкети гласила је: *Неке од порука, фотографија које имате у телефону не би желео/желела да нико види*.

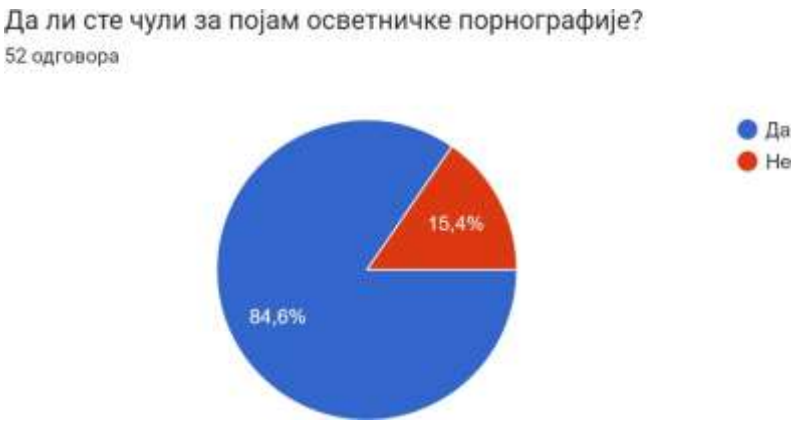
Највећи број испитаника се у потпуности слаже са тврдњом да неке од порука, фотографија које имају у телефону не би желео/желела да нико види (40,4%), док је најмањи проценат оних који се не слажу са овом тврдњом (9,6%).



Графикон 13. Неке од порука, фотографија које имате у телефону не би желео/желела да нико види

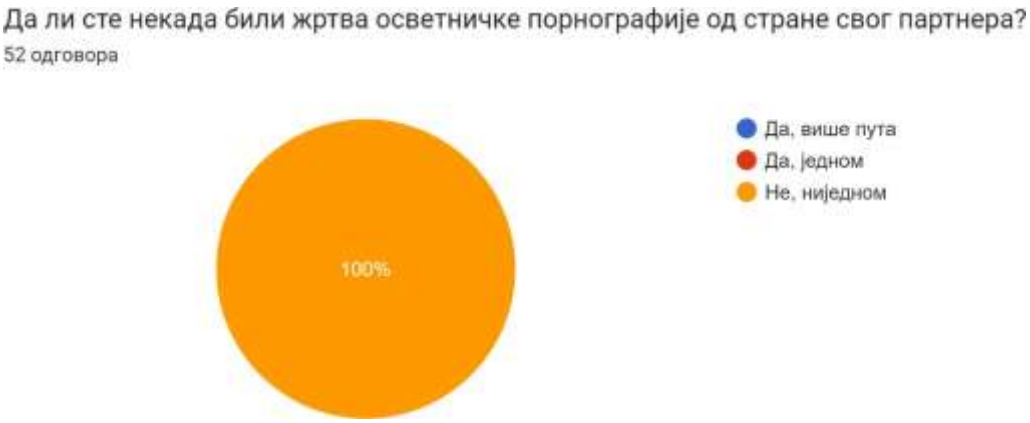
Проценат од 84,6% испитаника навело је да је чуло за појам осветничке порнографије, док 15,4% испитаника није упознато са овим појмом.

Наредна питања односила су се на појам осветничке порнографије. Питање је гласило: *Да ли сте чули за појам осветничке порнографије?*



Графикон 14. Да ли сте чули за појам осветничке порнографије?

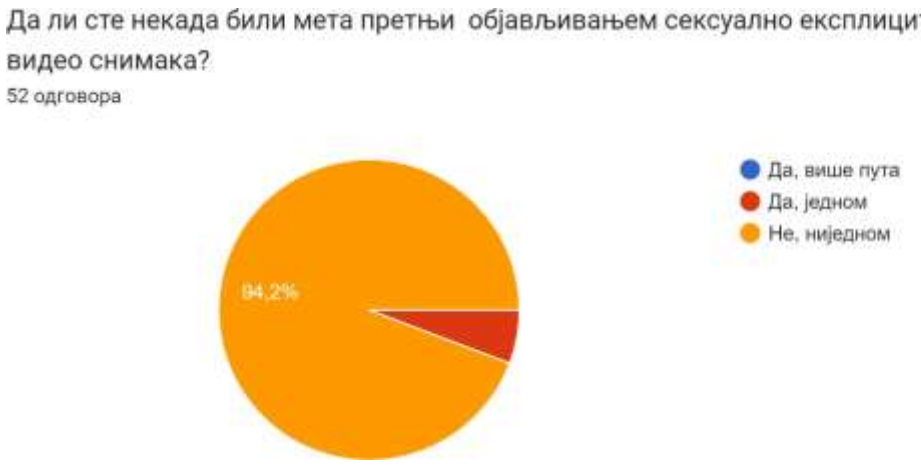
Следеће питање гласило је: Да ли сте некада били жртва осветничке порнографије од стране свог партнера?



Графикон 15. Да ли сте некада били жртва осветничке порнографије од стране свог партнера?

Сви испитаници навели су да нису никада били жртва осветничке порнографије од странр свог партнера.

Наредно питање у анкети гласило је: Да ли сте некада били мета претњи објављивањем сексуално експлицитних фотографија/ видео снимака?



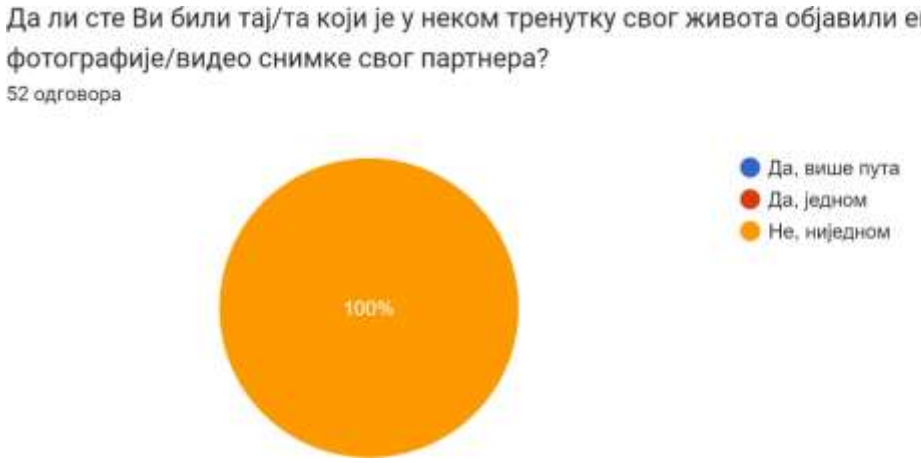
Графикон 16. Да ли сте некада били мета претњи објављивањем сексуално експлицитних фотографија/ видео снимака?

Највећи број испитаника, тачније њих 94,2% наводи да никада није било мета претњи објављивањем сексуално експлицитних фотографија/ видео снимака, док је 5,8% који су навели да су то били једном.

Следеће питање гласило је: Да ли сте као жртва/мета осветничке порнографије имали неке од следећих последица?

Графикон 17. Да ли сте као жртва/мета осветничке порнографије имали неке од следећих последица?

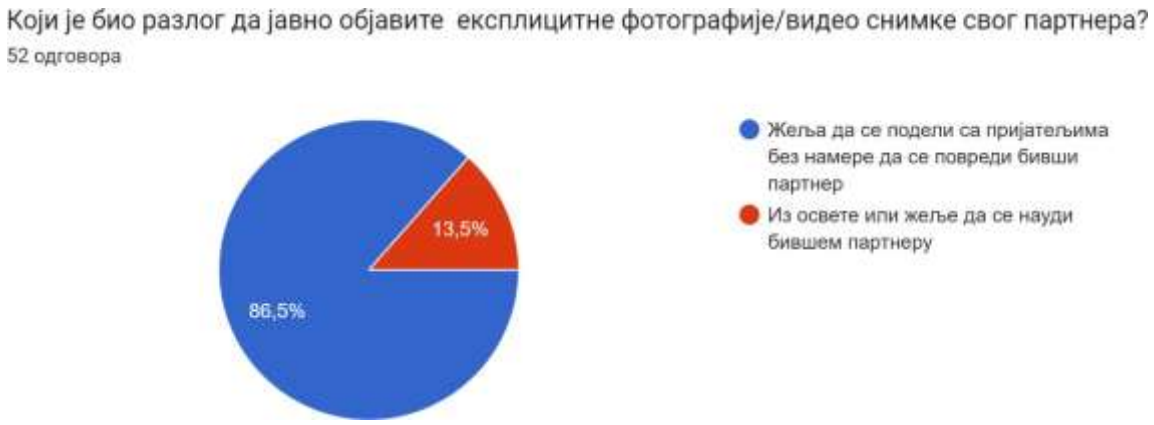
Надаље, питање у анкети гласило је: Да ли сте Ви били тај/та који је у неком тренутку свог живота објавили експлицитне фотографије/видео снимке свог партнера?



Графикон 18. Да ли сте Ви били тај/та који је у неком тренутку свог живота објавили експлицитне фотографије/видео снимке свог партнера?

Сви испитаници навели су да ниједном нису били тај/та који је у неком тренутку свог живота објавили експлицитне фотографије/видео снимке свог партнера.

Наредно питање формулисано је као: Који је био или би био разлог да јавно објавите експлицитне фотографије/видео снимке свог партнера?

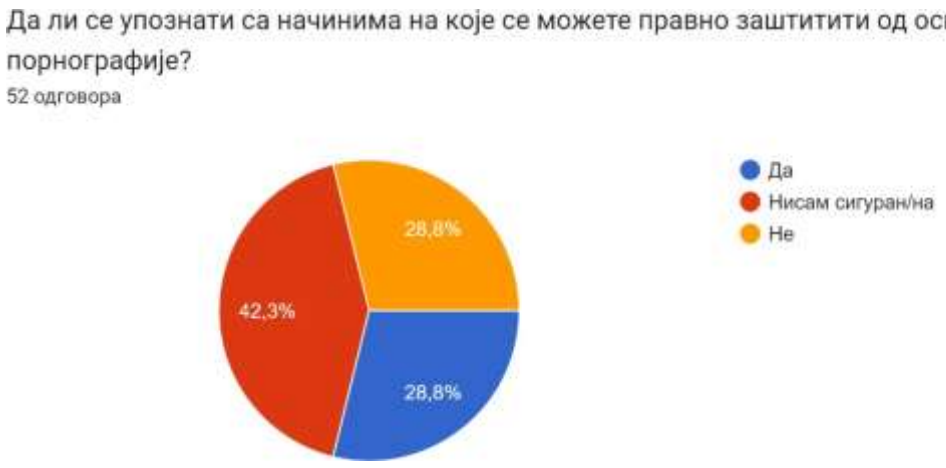


Графикон 19. Који је био или би био разлог да јавно објавите експлицитне фотографије/видео снимке свог партнера?

С обзиром на то да су испитаници првобитно навели да ниси објављивали фотографије и видео снимке свог партнера, на ово питање одговарали су тако да пруже иноформације о томе који би био разлог таквог њиховог чина. Око 86,5% испитаника

навело је да би то учинили из жеље да поделе са својим пријатељима, без намере да повреде партнера, док је 13,5% оних који наводе да би то било из освете или жеље да се науди бившем партнеру.

Следеће питање гласило је: Да ли се упознати са начинима на које се можете правно заштитити од осветничке порнографије?

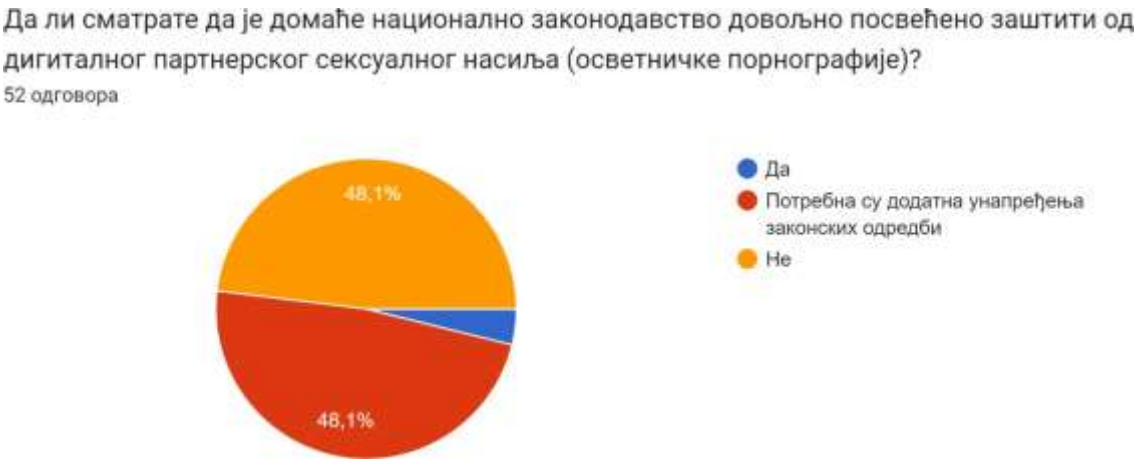


Графикон 20. Да ли се упознати са начинима на које се можете правно заштитити од осветничке порнографије?

Највећи број испитаника наводи да није сигурно у правне начине на које се може заштитити од осветничке порнографије (42,3%), док је 28,8% оних који наводи да познају правне начине за заштиту. Исти проценат од 28,8% наводи да нису упознати са овом правном заштитом.

Последње питање у анкети гласило је: Да ли сматрате да је домаће национално законодавство довољно посвећено заштити од дигиталног партнерског сексуалног насиља (осветничке порнографије)?

Највећи је проценат испитаника који сматрају да домаће национално законодавство није довољно посвећено заштити од дигиталног партнерског сексуалног насиља (осветничке порнографије) (48,1%) или да су потребна додатна унапређења истог (48,1%). На крају, 3,8% испитаника навело је да је домаће законодавство у овој области задовољавајуће.



Графикон 21. Да ли сматрате да је домаће национално законодавство довољно посвећено заштити од дигиталног партнерског сексуалног насиља (осветничке порнографије)?

ЗАКЉУЧАК

У савременом контексту, развој технологија претставља двосмислен феномен, који, иако доноси значајне предности у свакодневном животу, истовремено отвара врата за разне форме злоупотребе. Међу новим изазовима које ове технологије донеле је и појава deepfake технике и revenge porn, облици насиља који се често примењују према женама. Осветничка порнографија има широке негативне последице, а уклањање спорних садржаја с интернета и друштвених мрежа представља изазов, управо због комплексности дигиталног окружења.

Осветничка порнографија представља забрињавајући феномен у друштву са широким друштвеним и психолошким последицама за жртве. Овај облик порнографије обухвата непрописно објављивање интимних или експлицитних материјала особе без њеног сагласја, са честим намерама да се наштети, понизи или оштети репутација жртве. Пре свега, осветничка порнографија представља оштру инвазију у право на приватност, док истовремено подстиче и сајбер малтретирање, а често и насилство према женама, што додатно угрожава њихову безбедност на мрежи.

Многе државе широм света реаговале су на овај проблем увођењем закона који стављају ван снаге осветничку порнографију и прописују казне за њене починиоце. Иако се закони разликују по својој специфичности и строгој примени од државе до државе, суштина је у заштити права и интереса жртава, као и у сузбијању ове негативне и штетне праксе. Унапређење свесности о осветничкој порнографији и ефикасно примењивање одговарајућих закона представљају важан корак у борби против овог друштвеног проблема.

Ефикасна борба против осветничке порнографије захтева не само превентивне мере, већ и систематско образовање. Кључно је првенствено едуковати женску популацију о ризицима слања експлицитног материјала другима, као и сагледати улогу мушке популације која је често починилац оваквих дела. То укључује и препознавање неприхватљивости таквог понашања и увођење санкција за прекршиоце. Посебно је важно обратити пажњу на ученике основних и средњих школа, који су активни корисници интернета и друштвених мрежа. Образовање у овом контексту треба да подстакне јавност да заузме критички приступ својим онлајн активностима и да развије свест о последицама дељења приватног садржаја.

Даље анализе су се фокусирале на ефикасност правног система у суочавању са овим изазовима. Утврђено је да постоје одређене препреке у процесу идентификације, гоњења и кажњавања починилаца, укључујући недостатак специјализованог кадра и техничке опреме, као и сложеност прикупљања доказа у дигиталном окружењу. На основу налаза, предложене су одређене препоруке за унапређење ефикасности правног система у борби против сајбер криминала, укључујући унапређење сарадње између релевантних институција, јачање обуке особља, као и унапређење законодавства ради боље заштите рачунарских система и података. Ова рад пружа корисне увиде креаторима политике, правним стручњацима и другим релевантним актерима у борби против сајбер криминала.

У светлу потребе за адекватном казном осветничке порнографије у Републици Србији, неопходно је разматрати могућности измена у кривичним законима или увођења нових кривичних дела. Међутим, приликом таквих промена, неопходно је узети у обзир постојећи нормативни оквир и његову (не)способност да пружи адекватну кривичноправну заштиту. Иако постоје одређена кривична дела која могу бити примењена у контексту осветничке порнографије, утицај тумачења одредби може бити ограничен, што може резултирати недовољно ефикасном заштитом.

У овом контексту, потребно је разматрати могућност инкриминације осветничке порнографије као посебног кривичног дела у кривичном законодавству. Такво ново кривично дело би омогућило законодавцу да прецизније дефинише понашање које се тиче објављивања експлицитних слика без дозволе у циљу освете. Истовремено, такво законодавство би послужило као јасан сигнал да се друштво не толерише ова врста непријатног и кривичног понашања.

Међутим, постоји питање зашто постојећа решења у Кривичном законику не пружају потпуну заштиту од осветничке порнографије. Овде лежи проблем у способности постојећег законодавства да одговори на нове и разноврсне облике кривичног понашања у друштву, што може остати незадовољено применом само постојећих законских одредби. Стога, неопходно је да законодавац прати трендове у другим државама и примени их у националном контексту, што укључује инкриминацију осветничке порнографије као посебног кривичног дела. Ово је неопходан корак ка повећању степена заштите особа од потенцијалних непријатности и злоупотреба у виртуелном простору.

ЛИТЕРАТУРА

1. Алексић, Ж., Шкулић М. (2007). *Криминалистика*. Београд: Службени гласник.
2. Bambauer, D. E. (2014). *Exposed*. Minnesota Law Review, 98, 2025-2102.
3. Бошковић, М. (2020). *Криминологија*. Нови Сад: Правни факултет за привреду и правосуђе.
4. Bond, E., Tyrrell, K. (2021). Understanding revenge pornography: A national survey of police officers and staff in England and Wales. *Journal of interpersonal violence*, 36(5-6), 2166-2181.
5. Вилић, В. (2016). *Повреда права на приватност злоупотребе друштвених мрежа као облик компјутерског криминалитета.* Докторска дисертација, Ниш.
6. Вилић, В. (2019). Порнографија из освете као облик сајбер мизогиније. *Темида*, 22(1), 59-77.
7. Вулетић, Д. (2017). Сајбер безбедност. У: *Интегрална безбедност Републике Србије*, Београд: Факултет за пословне студије и право, Факултет за стратешки и оперативни менаџмент, Универзитет „Унион-Никола Тесла“.
8. Goddard, M. (2017). The EU general data protection regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, 59(6), 703–705.
9. Gauthier, A. (2023). Revenge Porn: A Disturbing Trend in Sexual Violence That Must Be Exposed. *Academic Journal of Criminology X Journal Universitaire de Criminologie*, 2(2), 65-70.
10. Димовски, Д. (2023). Осветничка порнографија: криминолошки и кривичноправни аспект. *Зборник радова Правног факултета у Нишу*, LXII(98), 155-174.
11. Živković, I., Čubrilo, V., Dujić, K. 'Revenge Porn': An Exploration into Redefinition in the Interest of Changing Legislation, доступно на: https://portal.ejtn.eu/PageFiles/20512/Team%20Croatia_Revenge%20Porn%20An%20Exploration%20into%20Redefinition%20in%20the%20Interest%20of%20Changing%20Legislation.pdf [15.02.2024]
12. Игњатовић, Ђ. (1991). Појмовно одређење компјутерског криминалитета. *Анали Правног факултета*, 39(1-3), Београд: Правни факултет.

13. Jacobs, A. (2016) Fighting Back against Revenge Porn: A Legislative Solution. *Northwestern Journal of Law and Social Policy*, 1, 68-90.
14. Kamal, M., Newman, W. J. (2016). Revenge pornography: Mental health implications and related legislation. *Journal of the American Academy of Psychiatry & the Law Online*, 44 (3), 359-367.
15. Lonardo, T., Martland, T., White, D. (2016) A Legal Examination of Revenge Pornography and Cyber-Harassment. *Journal of Digital Forensics, Security and Law*, 3, 78-106.
16. Matsui, S. (2015) The Criminalization of Revenge Porn in Japan. *Washington International Law Journal*, 2, 289-317.
17. Mania, K. (2022). Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study. *Trauma, Violence & Abuse*, 00(0), 1-13.
18. Петровић, С. (2004). *Компјутерски криминал*. Београд: Војно-издавачки завод.
19. Politou, E., Michota, A., Alepis, E., Pocs, M., & Patsakis, C. (2018). Backups and the right to be forgotten in the GDPR: An uneasy relationship. *Computer Law & Security Review*, 34(6), 1247–1257.
20. Subotin, M., Obradović, J. M. (2019). Criminological and criminal aspects of computer crime. *Pravo i digitalne tehnologije*, 37(3), 1-12.
21. Franks, M. A. (2015). *Drafting an Effective „Revenge porn" Law: A guide for legislators*. George Washington University.
22. Halder, D., Jaishankar, K. (2013) Revenge Porn by Teens in the United States and India: A Socio-legal Analysis. *International Annals of Criminology*, 1-2, 85-111.
23. Hasinoff, A. (2021). Cessons de parler de revenge porn: ces images sont une forme de violence sexuelle. *Questions de communication*, (40), 337-354.
24. Citron, D.K. (2014). *Hate Crimes in Cyberspace*. Harvard University Press.
25. Calvert. C. (2015). *Revenge Porn and Freedom of Expression: Legislative Pushback to an Online Weapon of Emotional and Reputational Destruction*. 24 Fordham Intell. Prop. Media & Ent. L. J. 673.
26. Šepec, M. (2019). Revenge Pornography or Non-Consensual Dissemination of Sexually Explicit Material as a Sexual Offence or as a Privacy Violation Offence. *International Journal of Cyber*, 13(2), 418–438.

- Правни извори

27. Законик о кривичном поступку, Службени гласник РС, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 – одлука УС и 62/2021 – одлука УС.
28. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, Службени гласник РС, бр.61/2005 и 104/2009.
29. Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима, Службени гласник РС, бр. 32/2013.
30. Закон о ауторским и сродним правима, Службени гласник РС, бр. 104/2009, 99/2011, 119/2012, 29/2016 – одлука УС и 66/2019.
31. Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине, Службени гласника РС, бр. 46/2006, 104/2009 – др. закони и 129/2021.
32. Закон о електронском потпису, Службени гласник РС, бр.135/2004.
33. Закон о електронској трговини, Службени гласник РС, бр. 41/2009, 95/2013 и 52/2019.
34. Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању, Службени гласник РС, бр. 94/2017 и 52/2021.
35. Закон о оптичким дисковима, Службени гласник РС, 52/2011.
36. Кривични законик Републике Србије, Службени 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.
37. Казнени закон Републике Хрватске, Народне новине бр. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/18, 84/21.
38. Оквирна одлука о нападима на информационе системе Комисије европских заједница (Framework Decision on attacks against information systems of the Commission of the European Communities), доступно на: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222&from=EN [14.02.2024]
39. Приручник УН о спречавању и контроли компјутерског криминала (United Nations Manual on the Prevention and Control of Computer-related Crime) (1994). доступно на: http://www.uncjin.org/Documents/EighthCongress.html [14.02.2024]

40. Резолуција Уједињених Нација о законодавству у области компјутерског криминалитета (UN resolution on computer crime legislation), доступно на: http://www.unodc.org/documents/congress//Previous_Congresses/8th_Congress_1990/028_ACONF.14 [14.02.2024]
41. Резолуција Уједињених Нација (тзв. Женевска резолуција) о злоупотреби интернета у сврху сексуалне експлоатације (UN Resolution on Missuse of the Internet for the Purpose of Sexual Exploatation), доступно на: http://www.uri.edu/artsci/wms/hughes/ppr.htm [14.02.2024]
42. Резолуција Уједињених Нација A/res/55/63 о борби против злоупотребе информационих технологија (UN resolution A/res/55/63 on combating the criminal misuse of information technologies), (2000). доступно на: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf [14.02.2024]
43. Резолуција 2007/20 од 26. 07. 2007. године, доступно на: http://www.un.org/.../ecosoc/.../2007 [14.02.2024]
44. Резолуција Уједињених Нација 65/230 (UN General Assembly resolution 65/230), доступно на: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [14.02.2024]
45. Стратегија за спречавање и борбу против родно заснованог насиља над женама и насиља у породици (2021-2025), Службени гласник РС, бр. 47/2021.

- Интернет извори

46. https://www.chvnradio.com/articles/council-of-europe-proposes-measures-to-fight-pornography

САЖЕТАК

ДИГИТАЛНО ПАРТЕРСКО СЕКСУАЛНО НАСИЉЕ (ОСВЕТНИЧКА ПОРНОГРАФИЈА) КАО ОБЛИК КРИМИНАЛИТЕТА

Развој технологија представља двосмислен феномен, који, иако доноси значајне предности истовремено отвара и врата за разне форме злоупотребе. Међу новим изазовима које је ова технологија донела је и дигитално партнерско насиље(осветничка порнографија).

Мастер рад „Дигитално партнерско сексуално насиље (осветничка порнографија)“ конципиран је тако да у првом делу говори о појмовима и облицима компјутерског криминалитета разматрајући посебно појам распрострањеност и врсте компјутерског криминалитета, затим појам и врсте напада и нападача у сајбер простору, затим међународну и домаћу регулативу.

Други део рада посвећен је осветничкој порнографији са посебним освртом на карактеристике, преваленције и мотиве осветничке порнографије. Затим је уследио и компаративни приказ законског регулисања освеничке порнографије са посебним освртом на правну регулисаност у УН, Савету Европе, САД, ЕУ, као и земљама бивше СФРЈ. Након тога посебно се образлаже нормативни оквир у праву Републике Србије са посебним аспектом на кривични закон Републике Србије.

На самом крају налази се истраживање које сам спровела посредством анкете која нам даје одговоре да ли су испитаници били жртве осветничке порнографије, да ли су они некада објављивали туђе експлицитне фотографије, да ли су упознати са заштитом од дигиталног партнерског насиља и да ли сматрају да је домаће законодавство доволјно посвећено заштити од дигиталног партнерског сексуалног насиља.

Кључне речи: дигитално сексуално партнерско насиље, компјутерски криминалитет, осветничка порнографија.

SUMMARY

DIGITAL PARTNER SEXUAL VIOLENCE (REVENGE PORNOGRAPHY) AS A FORM OF CRIMINALITY

The development of technologies represents an ambiguous phenomenon, which, although it brings significant advantages, also opens the door for various forms of abuse. Among the new challenges that this technology has brought is digital partner violence (revenge pornography).

The master's thesis "Digital partner sexual violence (revenge pornography)" was designed in such a way that in the first part it talks about the concepts and forms of computer crime, considering the concept of prevalence and types of computer crime, then the concept and types of attacks and attackers in cyberspace, then international and domestic regulation.

The second part of the paper is devoted to revenge pornography with special reference to the characteristics, prevalence, and motives of revenge pornography. This was followed by a comparative presentation of the legal regulation of confessional pornography with a special focus on legal regulation in the UN, the Council of Europe, the USA, the EU, as well as the countries of the former SFRY. After that, the normative framework in the law of the Republic of Serbia is specifically explained, with a special aspect of the criminal law of the Republic of Serbia.

At the very end, there is research that I conducted through a survey that gives us answers as to whether the respondents were victims of revenge pornography, whether they once published other people's explicit photos, whether they are familiar with protection against digital partner violence and whether they think that it is domestic legislation sufficiently dedicated to protection against digital partner sexual violence.

Keywords: digital sexual partner violence, computer crime, revenge pornography.

БИОГРАФИЈА АУТОРА

Данијела Вукићевић рођена је 10.05.1989. године у Нишу. Основну школу „Мирослав Антић“ и „Гимназију Стеван Сремац“ завршила је у Нишу. Основне студије на Правном факултету у Нишу уписала је школске 2008/2009. године и на истом дипломирала 2015. године са просечном оценом 8.55. Након дипломирања, приправнички стаж у трајању од две године обављала је у Адвокатској канцеларији „Иљац“. 27.04.2018. положила је правосудни испит а 19.06.2018. почела да се бави адвокатуром којом се бави и данас. Мастер академске студије на Правном факултету у Нишу уписала је 2022/23. године и то смер – право и информационе технологије, и испите положила са просечном оценом 10.00. Говори немачки и енглески језик, а служи се и руским језиком.