K R I V I Č N O M A T E R I J A L N O P R A V O

https://doi.org/10.7251/CEST1726068S UDK. 343.2/.7:004.738.5-053.3/.6

КРИВИЧНОПРАВНА ЗАШТИТА ДЈЕЦЕ У ДИГИТАЛНОМ ОКРУЖЕЊУ

Проф. др Миле Шикман

Правни факултет Универзитета у Бањој Луци, mile.sikman@pf.unibl.org

***Апстракт**: Динамичан развој савремених технологија донио је нове изазове којима су посебно изложени најмлађи корисници, а то су дјеца свакако. Ризици и опасности којима су они изложени мултициплирају се много брже, него што се остварује кривичноправна заштита. Тако су у почетку дјеца углавном била изложена кривичним дјелима сексуалног злостављања и искоришћавања путем интерента, као што је дјечија порнографији и сличним инкриминисаним понашањима. Данас су, поред тога, жртве манипулације и злоупотребе личних података, излагања штетним и опасним садржајима у дигиталном окружју, као и предмет злоупотребе и манипулације путем вјештачке интелигенције. Обим и распростањеност ових понашања је толико широка, да се може поставити питање да ли постојеће инкриминације у Кривичном законику Републике Српске могу пружити дјеци адекватну заштиту у дигиталном окружењу. Управо је наведено предмет овог рада, у којем циљу ћемо прво указати на опасности са којима се суочавају дјеца у дигиталном окружењу, а затим приказати постојеће кривичноправне одредбе чија је сврха управо заштита дјеце.*

***Кључне ријечи**: кривично право, кривично дјело, дјеца, интернет, високотехнолошки криминалитет.*

1. УВОД

Како живимо у ери изразито динамичног развоја савремених технологија, тако можемо сагледати колико оне у многоме утичу на свакодневни живот људи, постепено мијењајући све сфере људске дјелатности и живота (Simović, Šikman, 2023). Тако је дигитално доба[1] створило нову врсту реалности тзв. „дигиталну реалност“, која носи нове изазове како за појединца тако и за друштво (Pylkin, Serkova, Petrov, Pylkina, 2021). Истовремено смо свједоци да дјеца од најранијег узраста користе различите дигиталне уређаје и

[1] Многи ово доба називају Трећом индустријском револуцијом или Дигиталном револуцијом која представља прелазак са аналогне и механичке електронске технологије на дигиталну електронику. Надаље, прави се подјела на Прву и Другу Дигиталну револуцију. Прва дигитална револуција је дигитализовала информациона добра путем персоналних рачунара, док ће Друга дигитална револуција дигитализовати физичка добра путем десктоп 3D штампача. Стога ће се јаз између физичког и дигиталног почети смањивати, што ће додатно утицати на живот људи (види: Rindfleisch, 2020).

"бораве" у дигиталном окружењу (Rideout, Foehr, Roberts, 2010) излажући се при томе реалним ризцима и опасностима[2]. Неке од ових опасности су очигледне и лако уочљиве и од раније препознате, док су друге суптилне и прикривене, а не перципирају се као ризици[3]. Због тога се поставља питање: Како и на који начин прихватити реалност коришћења високих технологија од стране дјеце и истовремено осигурати њихову заштиту и безбједност у дигиталном окружењу? Наиме, ‘’полази се од чињенице да је дигитално окружење од пресудне важности за остварење дјечјих права и да свако дијете има право на приступ дигиталном свијету, као и на то да се у том свијету игра, учи и напредује, а да притом буде заштићено на најбољи могући начин’’[4] (European Network of Ombudspersons for Children, 2019). То значи да сва права која дијете ужива у реалном свијету, треба му бити омогућено да ужива и у дигиталном свијету. У свим активностима које се тичу дјеце у дигиталном окружењу, најбољи интереси дјетета треба да буде главна брига, а то значи да им се треба омогућити остваривање њихових права, у сигруном и безбједном дигиталном окуржењу. Дакле, дјеца имају право да буду заштићена од свих облика насиља, експлоатације и злостављања у дигиталном окружењу. Свака заштитна мјера треба да узме у обзир најбоље интересе и еволуирајуће способности дјетета и не смије непотребно да ограничава остваривање других права. Један од сегмената њихове заштите је и кривичноправна заштита, при чему треба нагласити *ultima ratio* карактер ових норми. То значи да кривичноправне одредбе и не требају бити први избор заштите дјеце у дигиталном окружењу, већ како и јесте крајње средство.

Предмет овог рада операционализован је кроз кривичноправну заштиту дјеце у дигиалном окружењу. Тако обухвата кривичноправне норме садржане у општем и посебном дијелу Кривичног законика Републике Српске[5] (у даљем

---

[2] Поред тога на овај начин се директно остварује утицај и на психофизички развој дјеце, њихову комуникацију и понашање (UNICEF, 2017a).

[3] Посебно забрињавају резултати истраживања из 2019. године којима је утврђено да су: ‘’скоро сви млади адолесценти (95%) имали приступ Интернету: 67% је посједовало мобилни телефон, а 68% је имало налог на друштвеним мрежама. Власништво мобилног телефона није било повезано ни са каквим показатељима благостања (резултати на тестовима из математике и читања, припадност школи, психолошки проблеми, проблеми у понашању или физичко здравље) након контроле демографских фактора. С друге стране, посједовање налога на друштвеним мрежама и учесталост коришћења друштвених медија били су чврсто повезани са проблемима у понашању (објашњавајући ~3% варијација у проблемима понашања)’’ (George, Jensen, Russell, Gassman-Pines, Copeland, Hoyle, Odgers, 2020).

[4] Наведено је заправо перамбула Коначне изјаве о правима дјеце у дигиталном окружењу које је усвојено од стране Европске мреже обудсмана за дјецу 2019. године у Белфасту (European Network of Ombudspersons for Children, 2019).

[5] Кривични законик Републике Српске, Службени гласник Репубике Српске, бр. 64/2017, 104/2018 - одлука УС, 15/2021, 89/2021, 73/2023, "Сл. гласник БиХ", бр. 9/2024 - одлука УС БиХ, "Сл. гласник РС" 105/2024 - одлука УС, 19/2025, "Сл.

тексту КЗ РС) које се тичу заштите дјеце као жртава кривичних дјела у дигиталном окружењу. Иако је првобитна идеја била да се ограничимо на "интернет" као глобалну, децентрализовану мрежу рачунара и других уређаја намијењених за пренос података, одлучили смо се за шири концепт "дигиталног окружења". Наиме, "дигитално окружење" обухвата информационе и комуникационе технологије (ИКТ), укључујући интернет, мобилне и повезане технологије и уређаје, као и дигиталне мреже, базе података, садржаји и услуге[6]. Дакле, дигитално окружење обухвата и интернет, али и све остало што није нужно повезано на мрежу у сваком тренутку: оперативне системе, софтвере који раде "offline", дигиталне уређаје (паметне телефоне, паметне сатове, сензоре), вјештачку интелигенцију, па чак и друштвене норме и законе који регулишу понашање у дигиталном простору. Како су дјеца корисници свих наведених технологија, сматрамо оправданим посматрање проблема истраживања у ширем контексту.

2. ОБЛИЦИ УГРОЖАВАЊА СА КОЈИМА СЕ СУОЧАВАЈУ ДЈЕЦА У ДИГИТАЛНОМ ОКРУЖЕЊУ

Поред корисног и креативног кориштења интернета, посебан проблем представљају опасности којима се дјеца излажу у дигиталном окружењу. Према истраживању Свјетске здравствене организације (WHO) из 2024. године, свако шесто дијете (око 16%) узраста од 11 до 15 година у Европи било је жртва дигиталног насиља. Ово представља пораст у односу на 2018. годину, када је тај проценат био 13% (World Health Organisation, 2024). Ове опасности могу бити истог нивоа и степена као и опасности у реалном свијету.

Општеприхваћена је подјела изазова и ризика у три категорије: ризици садржаја, ризици контакта и ризици понашања (Миладиновић, 2018, стр. 24). Ризици садржаја се односе на изложеност дјетета нежељеном и неприкладном садржају, који могу укључивати сексуалне, порнографске и насилне фотографије, одређене облике оглашавања који промовишу штетне или лажне здравствене савјета, малициозне и комерцијалне садржаје, расистичке, дискриминацијске и материјале који садрже говор мржње, интернет странице које промовишу нездрава и опасна понашања попут самоповређивања, самоубистава или анорексије, као и дезинфомрације и манипулативне садржаје. Непримјереним се сматра сваки садржај који није прилагођен узрасту дјетета и као такав није у његовом интересу.

Сексуална експлоатација дјеце на интернету, према истраживањима Европола укључује читав низ криминалних активности, као што су сексуално злостављање и експлоатацију дјеце путем интернета, производња и

гласник БиХ", бр. 14/2025 - одлука УС БиХ, "Сл. гласник РС", бр. 31/2025 и 85/2025 - одлука УС.

6 Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment (Adopted by the Committee of Ministers on 4 July 2018 at the 1321 meeting of the Ministers' Deputies).

дистрибуција порнографског садржаја, онлине навођење дјеце ради сексуалне експлоатације, "пренос уживо" злостављање дјеце на даљину[7] и др (EUROPOL, 2019, p. 34). Процјењује се да ће глобална индустрија онлајн порнографије порасти за 29.29 милијарди америчких долара од 2024. до 2029. године, са стопом раста од 8.8% (Research and Markets, 2026). Надаље, нове технологије, попут криптовалуте и тамног интернета (engl. Dark web) − подстичу директно приказивање сексуалног злостављања дјеце и других штетних садржаја те представљају изазов за сузбијање ове врсте криминалитета (UNICEF, 2017a).

"Осветничка порнографија" је дистрибуција или пријетња објављивањем, сексуално експлицитних фотографија или видео снимака особа без њиховог пристанка, са намјером стварања страха, јавног понижења и освете жртви. До ових материјала долази се на различите начине, укључујући крађу путем компјутерског хаковања или уобичајене крађе[8] (Beyens, Lievens, 2016, p. 33). Овом понашању слична је "сексуална изнуда" (engl. Sextortion) које се односи на пријетње дијељењем голих или сексуално експлицитних фотографија и видео материјала, како би се жртва приморала да изврши одређене захтјеве, као што су плаћање уцјене, слање још сексуално експлицитних материјала или упуштање у нежељене радње[9]. Наведеним понашањима посебно су угрожена дјеца, која су веома рано изложена овим ризицима, али их не перцепирају као кривична дјела јер код њих постоји увјерење да су особе саме криве ако неко њихову фотографију или видео снимак сексуално-експлицитног садржаја подијели даље, коју су добровољно првобитно послали.

Ризици контакта се односе на учествовање дјетета у ризичној комуникацији са одраслом особом која тражи неприкладан контакт или са појединцима који настоје радикализовати дијете, па код њих стварају увјерења да учествују у нездравим и опасним понашањима. У дигиталном свијету, као и у стварном, постоје појединци, познати као "предатори", који на вјешт начин покушавају да искористе старосну доб и наивност дјеце ради стицања његово повјерење, а све у циљу злоупотребе дјетета[10]. Најчешћи облик овог понашања

---

7 Пренос уживо сексуалног злостављања дјеце или "Live streaming" је радња која се одвија у реалном времену и настаје када је дијете присиљено да се појави пред веб-камером, те да се укључи у сексуално експлицитно понашање или да буде подвргнуто сексуалном злостављању.

8 Нпр. у Сједињеним Америчким Државама, осветничка порнографија представља све већи проблем у савременој медијској култури, гдје је једна од 10 жена млађих од 30 година била изложена овом облику злоупотребе на интернету, односно или су биле објављене фотографије или јој је пријећено да ће то бити урађено (Davis Kempton, 2020).

9 Јавља се у различитим контекстима, укључујући злостављање интимног партнера, дигитално насиље, онлајн упознавање, трговина људским бићима у сврху сексуалне експлоатације, онлајн сексуална експлоатација дјеце, итд. (Ray, Henry, 2025).

10 Према спроведеној прегледној студији предатори који врше намамљивање су углавном мушкарци, старости око 30 година, са мало или без претходних осуда или кривичних дјела која су починили, који могу, али и не морају имати неки

јесте "намањивање" дјетета (engl. Cyber grooming) у којем одрасла особа подстиче дијете да на интернету учествују у интеракцијама сексуалне природе при чему се често излажу нежељеним порнографским садржајима[11]. Такође, намамљивање може послужити као претходница других штетиних понашања, као што је сексуалне изнуде (Миладиновић, 2018, стр. 48).

Ризици понашања подразумијевају понашање дјетета на одређени начин у дигиталном окружењу које може довести до настанка и ризичног понашања или односа. У питању је обично "дигитално вршњачко насиље" (engl. Cyberbulling) које представља агресивни облик понашања, које се спроводи коришћењем неког од електронских уређаја, првенствено рачунарских и мобилних уређаја, у више наврата и током дужег временског периода, све са циљем да се жртва понизи, дискредитује, изопшти из вршњачке заједнице и омаловажи[12] (Cyberbullying Research Center, n.d.). Слање секусално експлицитних фотографија (engl. Sexting) представља понашање на интернету у оквиру којег се шаљу сексуално експлицитне фотографије или поруке сексуалног садржаја другој особи електронским путем[13] (Миладиновић, 2018, 48). Овим понашањем посебно су погођена дјеца (Thorne, Babchishin, Fisico, Healey, 2024; Mori, Park, Temple, Madigan, 2022), јер слање властитих секуално експлицитних фотографија одраслих особа уколико је добровољано, сам по себи није кривично дјело, али може да има несагледиве посљедице и има изразито виктимогени карактер. Ризици понашања укључују и коришћење моблиних телефона и играње видео игрица. Поред свих бенефита кориштења мобилних телефона, постоји и одређени негативни ефекти, а они се прије свега

психолошки поремећај, а уобичајена стратегија коју су користили била је изградња стварне или лажне наклоности, изградња односа повјерења између са жртвом, те постепено тражење сексуално експлицитног садржаја (види: Moosburner, Weber, Kuban, Wachs, Schmidt, Etzler, Rettenberger, 2025).

11 Према подацима Националног удружењу за спречавање окрутности према дјеци (NSPCC) у периоду 2023/2024 забиљежено 7.062 кривична дјела сексуалне комуникације са дјецом путем онлајн мрежа, што је повећање од 89% у односу на период 2017/2018. Најчешће платформе које су починиоци користили биле су: Snapchat (48%), WhatsApp (12%), Facebook и Messenger (10%), Instagram (6%), te Kik (5%). Починиоци су обично користили отворене платформе за успостављање прве комуникације са дјететом (видео игре и апликације за размјену порука повезане са видео играма) прије него што су прешли на горе поменуте апликације (види: NCPSS, 01.11.2024).

12 Према истраживању УНИЦЕФ-а из 2017. године које је спроведено у Србији утврђено је да је међу младима који свакодневно користе интернет, 62% ученика основних школа и 84% ученика средњих школа било је изложено неком ризику (види: UNICEF, 2017b).

13 Истраживање спроведено на подручју Србије у оквиру DeSHAME пројекта, које је обухватило 2.950 ученика прве и треће године средњих школа, показало је да је чак 24% испитаника примило садржај сексуалне природе преко интернета од особе коју познају, док је њих 27.5% примило такав садржај од особе коју не познају (Види: Centar za nestalu i zlostavljanu decu, 2023).

тичу злоупотребе мобилних телефона[14]. Такође, играње видео игара може довести до многих ризика којим се доводи у питање и лична безбједност дјеце, као и безбједност података на рачунару. Савремене видео игре веома често нису прилагођене узрасту дјетета, све већи број видео-игрица у свом садржају укључује различите облике насиља, а у игрицама се често промовише говор мржње, коцкање, употребу алкохола и опојних дрога, блудне радње, као и могућност трошења новца током играња видео игара. Надаље, игрице дају могућност комуникације у реалном времену са другим играчима, која дјеца обично не познају у стварном животу[15].

Поред наведеног посебан проблем представља манипулација подацима и злоупотреба вјештачке интелигенције. Као што се наводи у Мишљењу Европског супервизора за заштиту података (2018): "проблем је стваран и хитан, а вјероватно ће се погоршати како се што већи број људи буде повезивао са Интернетом, уз повећану улогу система вјештачке интелигенције" (European Data Protection Supervisor, 2018). Манипулација подацима подразумијева злоупотребу информационе технологије у сврху прикривеног утицаја на доношење одлука другог човјека, на начин да се искориштава његова слабост (Susser, Roessler, Nissenbaum, 2019). Посебан проблем представља "дигитални идентитет" као укупност идентификационих обиљежја одређеног лица у његовим онлајн налозима и "дигитални отисак" који обухватају активне и пасивне податке који према Лоцардовом принципу[16] функционише и у дигиталној форензици. То је мјешавину личних особина, података и активности на мрежи и не ради се само о томе ко је лице заиста, већ и како друга лица на мрежи виде и опажају тог појединца и његов идентитет (Ghadge, 2024). Дигитални идентитет дјетета често није исти као онај из стварног живота, јер на интернету они могу да буду оно што нису и да сакрију дијелове себе, најчешће оне неке ситне несигурности и мањак самопоуздања из стварног живота.

Вјештачка интелигенција (AI) је способност кибернетичких система да имитира људске активности, као што су расуђивање, учење, планирање и креативност и омогућава им да перципирају (опажају) своје окружење, узму у обзир оно што виде и рјешавају проблеме како би постигли циљ[17]. Као и свака

[14] Наведено може бити учињено на различите начине од стране дјеце, приликом чега они могу постати и жртве комуникације, али и сами учествовати у негативној комуникацији.

[15] Наведено дјецу директно излаже ризику комуникације са непознатим особама (потенцијалним предаторима) путем дописивања у току игре.

[16] Локардов принцип је основна поставка форензике, која каже да "сваки контакт оставља траг" што значи да када учинилац дође у контакт с мјестом злочина, он са собом доноси материјал с тог мјеста и оставља трагове са себе. Установио га је професор Едомонд Локард (Edmond Locard), француски криминолог и пионир модерне форензике.

[17] Један од најпознатијих AI алата, који се и највише користи код нас, нарочито од стране дјеце јесте ChatGPT.

друга напредна технологија, и алати вјештачке интелигенције се злоупотребљавају, доводећи у питање недостатак правне регулативе како би се осигурала одговорна употреба AI (Ai Academy, 2024). Најчешће злоупотребе које се чине уз помоћ алата вјештачке интелигенције су: креирање лажног материјала и коришћење ботова у сврху онлајн превара. То се првенствено односи на производњу реалистичних фотографија и видео материјала користећи напредне AI алгоритме што је познато као "дипфејк" (engl. Deepfake[18]). Лажни материјал обично трансформише постојећи изворни садржај, гдје се једна особа замијени другом, те ствара потпуно оригиналан садржај у којем је неко представљен како ради или говори нешто што није урадио или рекао (Chadha, Kumar, Kashyap, Gupta, 2021). Посебан изазов представља тзв. ‘’дипфејк порнографија" која подразумијева коришћење вјештачке интелигенције (AI) и алатки и алгоритама развијених на бази AI за креирање лажних порнографских видео-садржаја[19]. У овом случају, активности на друштвеним мрежама и објављивање фотографија омогућавају починиоцима да прикупе потребан материјал како би креирали "дипфејк порнографију" (види: Mania, 2024; Karasavva, Noorbhai, 2021. цитирано у: Janković, Putnik, 2025)[20]. Фондација за надзор интернета (IWF) идентификовала је значајну и растућу пријетњу гдје се технологија вјештачке интелигенције користи за производњу материјала о сексуалном злостављању дјеце[21] (Internet Watch Foundation, 2024). Поред тога, све су учесталије преваре засноване на лажном садржају генерсаном вјештачком интелигенцијом (види опширније: Liu, 2024; Salloum, Gaber, Vadera, Shaalan, 2022).

Многа од ових понашања инкриминисана су као кривична дјела, док друга представљају увод у забрањена понашања, а поједина нису ни препозната као штетна понашања.

---

18 „Дубока лаж“ (од engl. Deep - дубока и fake - лаж).

19 Посебно забрињавајући тренд који се заснива на злоупотреби "Al based" технике, којом се постављају фотографије или видео записи преко другог видео записа. Већ је коришћена како би се поставила лица познатих личности на постојеће порнографске видео снимке (EUROPOL, 2019, p. 34).

20 Дјеца су подложнија да буду жртве материјала сексуалног злостављања дјеце креираног уз помоћу алата вјештачке интелигенције. Довољно је да предатор пронађе фотографију дјетета на некој од друштвених мрежа, коју потом преузима уз помоћ алата вјештачке интелигенције, затим генерише и на крају добија потпуно нови садржај, који то дијете приказују наго или у потпуно другом окружењу.

21 Први извјештај Фондације за надзор интернета из октобра 2023. године открио је присуство преко 20.000 фотографија генерисаних вјештачком интелигенцијом на једном од форума на дарк вебу у једном мјесецу, гдје је више од 3.000 фотографија приказивало криминалне активности сексуалног злостављања дјеце. Од тада се овај проблем стално погоршава и константно се биљежи значајан раст оваквог лажног материјала (Internet Watch Foundation, 2024).

3. КРИВИЧНОПРАВНИ ОКВИР ЗАШТИТЕ ДЈЕЦЕ У ДИГИТАЛНОМ ОКРУЖЕЊУ

Један број описаних понашања инкриминисаних као кривична дјела, чији би објекат заштите био "право дјетета на безбједан и сигуран боравак у дигиталном окружењу", условно посматрајући, можемо сврстати у четири категорије: прва, кривична дјела која се своде на пласирање дјечије порнографије путем злоупотребе рачунарске мреже или комуникација другим техничким средствима (Шкулић, 2022, стр. 10), затим кривична дјела којима се путем дигиталних мрежа дјеца уцјењују (тзв. осветничка порнографија) или сексуално узнемиравају, друга, кривична дјела која у свом бићу садрже поједине облике дигиталног насиља усмјереног према дјеци, трећа, кривична дјела којима се повређује права на приватност дјеце и угрожавање личних података дјеце у дигиталном окружењу и четврта, кривична дјела која имају за циљ стицање противправне имовинске користи или друге злоупотребе (нпр. крађа идентитета дјетета, превара). Како смо и нагласили наведена подјела је условног карактера, јер су ова кривична дјела систематизована у различитим групама кривичих дјела, са различитим заштитним објектима, али са заједничком карактеристиком да се њима угоржавају дјеца у дигиталном окружењу. Свакако да наведена кривична дјела не представљају коначну листу кривичних дјела која се могу извршити на штету дјеце путем друштвених мрежа.

У општем дијелу КЗ РС садржане су одредбе које се тичу заштите дјеце, укључујући и заштиту дјеце у дигиталном окружењу. То су одредбе о изузетности краткотрајне казне затвора (чл. 46а) којом је прописано да се наведене одредбе неће се примјењивати на учиниоце, између осталих кривичних дјела из Главе XV (Кривична дјела сексуалног злостављања и искоришћавања дјетета) (ст. 4). Затим, мјером безбједности Забрана вршења позива, дјелатности и дужности (чл. 77) прописано је да се учиниоцу кривичног дјела учињеног на штету полног интегритета дјетета изриче се мјера безбједности забране потпуног вршења позива, дјелатности или дужности, при чијем обављању се остварује непосредан контакт са дјецом (ст. 2). Такође, чл. 92 прописано је да се у оквиру казнене евиденције води посебан регистар лица која су правоснажно осуђена за кривична дјела учињена на штету полног интегритета дјетета (тзв. Регистар педофила). Садржај и обим података, њихово чување, као и услови за давање податка из овог регистра уређује се посебним прописом (ст. 2). На крају, под појмом "дијете као жртва кривичног дјела" сматра се лице које није навршило осамнаест година живота (чл. 123 ст. 1 т. 7 КЗ РС).

Кад је ријеч о посебном дијелу у КЗ РС заштита дјеце у дигталном окружењу може се посматрати кроз више различитих кривичних дјела. Тако је уведена посебна глава XV "Кривична дјела сексуалног злостављања и искоришћавања дјетета"[22] у којој су, поред осталих, инкриминисана кривична

[22] Нова концепција кривичноправне заштите дјеце од сексуалног злостављања и искоришћавања, уведена 2017. године резултат је настојања да се кривичноправна

дјела у вези сексуалног искоришћавања дјетета у дигиталном окружењу[23]. То су четири кривична дјела и то Искоришћавање дјеце за порнографију (чл. 175), Искоришћавање дјеце за порнографске представе (чл. 176), Упознавање дјеце са порнографијом (чл. 177) и Искоришћавање компјутерске мреже или комуникације другим техничким средствима за извршење кривичних дјела сексуалног злостављања или искоришћавања дјетета (чл. 178). У наведена три кривична дјела користи се термин "дјечија порнографија"[24], под којим се подразумијева било какво представљање, било којим средством, дјетета у стварним или симулираним експлицитним сексуалним активностима или било какво представљање сексуалних дијелова тијела (примарних и сексуалних органа дјетета), првенствено у сексуалне сврхе.[25] Иако је широко прихваћено коришћење овог термина сматрамо да би умјесто појма „дјечија порнографија“, требало употребљавати појам "материјал са сексуалним злостављањем дјеце"[26], јер овај термин сугерише да је такав материјал настао сексуалном злоупотребом дјеце, обично путем пријетњи, принуде и изнуде. Поред тога, термин порнографија има широку употребу, а поједини облици порнографије одраслих лица се не сматрају кажњивим, осим ако из њих не произлазе друге злоупотребе, претежно сексуалног карактера.

Кривично дјело Искоришћавање дјеце за порнографију (чл. 175) састоји се у навођењу дијета на учествовању у снимању дјечије порнографије или организовању или омогућавању снимања дјечије порнографије (ст.1). Тежи облик ће постојати уколико се садржај неовлашћено сними, произведе, нуди, чини доступним, дистрибуира, шири, увози, извози, прибавља за себе или за другога, продаје, даје, приказује или посједује дјечију порнографију или му се свјесно приступа путем рачунарске мреже (ст. 2), док ће најтежи облик постојати ако је наведено учињено употребом силе, пријетње, обмане, преваре, злоупотребом положаја или тешких прилика дјетета или односа зависности (ст.

заштита полног интегритета дјеце ускладити са међународним принципима и стандардима (Марковић, 2018, стр. 27).

[23] Сврха прописивања кривичних дјела из ове главе јесте проширивање криминалне зоне, како би се обухватиле и криминализовале све сексуалне радње против дјеце. Препознато је да се сексуално злостављање и искоришћавање дјеце може догодити и на интернету, што доводи до појачавања посљедице. Поред тога, путем интернета, учиниоци могу лакше него икад прије ступити у контакт с дјецом, мамити их на сусрете, дијелити слике злостављања, сакрити свој идентитет и добит, те се међусобно удружити како би избјегли одговорност и учинили нова кривична дјела (Бајичић, 2023).

[24] "Полазећи од етимологије ријечи, појам порнографија (πορνογραφία) представља кованицу која на изворном грчком језику води поријекло од ријечи porne (πορνεία) која означава блудницу или проститутку и ријечи graphein (γράφειν) што значи писати или биљежити" (Pavlović, Petković, Matijašević Obradović, 2014, str. 46).

[25] Наведено према чл. 2 Конвенције Уједињених нација о правима дјетета (Convention on the Rights of the Child, General Assembly resolution 44/25, 20 November 1989).

[26] CSAM је скраћеница од термина "Материјал са сексуалним злостављањем дјеце" (eng. Child Sexual Abuse Material).

3). Казна затвора за основни облик прописана је од шест мјесеци до пет година, за тежи од једне до осам година и за најтежи облик од двије до десет година. Такође, прописано је да ће се предмети кориштени за извршење овог дјела одузетеи, а порнографски материјал који је настао извршењем дјела се уништити (ст. 4). Дијете се неће казнити за производњу и посједовање порнографског материјала који приказује њега лично или њега и друго дијете ако су они сами тај материјал произвели и посједују га уз пристанак сваког од њих и искључиво за њихову личну употребу (ст. 5). Дјечија порнографија је дефинисана као материјал који визуелно или на други начин приказује дијете или реално приказано непостојеће дијете или лице које изгледа као дијете, у правом или симулираном (експлицитном) евидентном сексуалном понашању или који приказује полне органе дјеце у сексуалне сврхе (ст. 6). Наведена дефиниција представља модернизовану дефиницију која препознаје "непостојеће дијете" које може да буде производ алата вјештачке интелигенције. На концу прописано је да материјали који имају умјетнички, медицински или научни значај не сматрају се порнографијом у смислу дефинисаног појма (ст. 7). Управо ово одређење може се сматрати дискутабилним, јер се може тумачити да онда постоје "легитимни" материјали, тј. да одређени снимак не буде порнографски, иако експлицитно приказује сексуални однос или полни орган, јер има умјетнчки, медицински или научни значај27 (упореди: Шкулић, 2022, стр. 11).

Кривично дјело Искоришћавање дјеце за порнографске представе (чл. 176) састоји се у навођењу дијета на учествовање у порнографским представама (ст. 1), док се тежи облик састоји од употребе силе, пријетње, обмане, преваре, злоупотребом положаја или тешких прилика дјетета или односа зависности (ст. 2). Казна затвора прописана за основни облик је од шест мјесеци до пет година, којом ће се казнити и онај ко гледа порнографску представу уживо или путем комуникацијских средстава ако је знао или је требало и могло да зна да у њој учествује дијете (ст. 3). За тежи облик прописана је казна затвора од двије до десет година. Такође, прописано је да ће се предмети кориштени за извршење дјела одузети, а порнографски материјал који је настао извршењем дјела ће се уништити (ст. 4).

Кривично дјело Упознавање дјеце с порнографијом (чл. 177) чини онај ко дјетету млађем од петнаест година прода, поклони, прикаже или јавним излагањем, посредством комјутерске мреже или других видова комуникације или на други начин учини доступним списе, слике, аудио-визуелни материјал или друге предмете порнографске садржине или му прикаже порнографску представу. За ово понашање прописана је казном затвора од шест мјесеци до

[27] "Одређивање који материјали конкретно по свом садржају представљају порнографске материјале, представља questio facti, при чему је некада тешко раздвојити садржаје који су умјетничког карактера и гдје је њихов еротски елемент у функцији умјетничке експресије, слично као што одређени материјали приказују полни чин могу да имају одређене научне, едукативне и друге сличне циљеве" (Шкулић, 2002: 479-480).

три године (ст. 1). Предмети кориштени за извршење овог дјела се одузимају, а порнографски материјал се уништава (ст. 2). Такође, бићем овог кривичног дјела дата је дефиниција порнографије, под којом се сматра материјал који визуелно или на други начин приказује лице у правом или симулираном евидентном сексуалном понашању или који приказује полне органе људи у сексуалне сврхе (ст. 3), а одређено је да се материјали који имају умјетнички, медицински или научни значај не сматрају се порнографијом у смислу овог члана (ст. 4). Управо наведено се може сматрати упитним, са аспекта остваривања сврхе кажњавања. Наиме, узимајући у обзир зрелост дјетета до 15 године живота, поставља се питање колико је оно у стању да разумије умјетнички, медицински или научни значај материјала, ако се у њима приказују сексуални садржаји, односно утврђивање која је "намјера" извршиоца овог кривичног дјела.

Кривично дјело Искоришћавање компјутерске мреже или комуникације другим техничким средствима за извршење кривичних дјела сексуалног злостављања или искоришћавања дјетета (чл. 178) чини онај ко са дјететом старијим од петнаест година, користећи компјутерску мрежу или комуникацију другим техничким средствима, договори састанак ради вршења обљубе или са њом изједначене полне радње, или ради производње порнографског материјала, или ради других облика сексуалног искоришћавања и појави се на договореном мјесту ради састанк. За ово кривично дјело прописана је казна затвора од једне до пет година (ст. 1), а ако је дјело извршено према дјетету млађем од петнаест година, прописана је строжија казна и то казна затвора од двије до осам година.

У оквиру КЗ РС могу се идентификовати и друга кривична дјела која имају елементе сексуалног искоришћавања дјетета у дигиталном окружењу. То би била кривична дјела Полно узнемиравање (чл. 170) и Злоупотреба фотографије и видео записа полно експлицитног садржаја (чл. 170а). Полно узнемиравање (чл. 170) је свако вербално, невербално или физичко нежељено понашање полне природе које је усмјерено на повреду достојанства неког лица у сфери полног живота, а које изазива страх или ствара непријатељско, понижавајуће или увредљиво окружење. Овим понашањем могу бити угрожена и дјеца, а као тежи облик прописано је ако је дјело учињено, између осталог, према лицу које је у односу подређености или зависности према учиниоцу или које је посебно рањиво због узраста (ст. 2). На концу најтежи облик постоји, ако је полно узнемиравање учињено кориштењем компјутерске мреже или неког другог вида комуникације (ст. 3). За основни облик дјела прописана је новчана казна или казна затвора до једне године, док је за тежи облик прописана казна затвора до двије године, а за најтежи облик казна затвора од шест мјесеци до три године. Злоупотреба фотографије и видео-записа полно експлицитног садржаја (чл. 170а), тзв. "осветничка порнографија" састоји се у злоупотријеби однос повјерења и без пристанка другог лица чињења доступним трећем лицу фотографију или снимак полно експлицитног садржаја која је сачињена уз пристанак тог лица за личну употребу и тиме

повређивања приватност тог лица. За ово понашање прописана је казна затвора до двије године, као и уколико је израђена нова или преиначена постојећа фотографија или снимак полно експлицитног садржаја другог лица и тај снимак употријебљен као прави и тиме повријеђена приватност другог лица. Најтежи облик ће постојати ако је кривично дјело учињено путем компјутерског система или компјутерске мреже или на други начин којим је омогућено да фотографија или снимак постану доступни већем броју лица, за шта је прописана казна затвора од једне до три године. Фотографије и снимци или средства којима је извршено кривично дјело из овог члана, одузимају се. Наиме, савремене технологије су омогућиле креирање, слање и стварање сексуално експлицитних текстова, слика или видео-записа, који се обично дешавају између двоје људи у вези (Димовски, 2023, стр. 157). Управо, захваљујући информационо-комуникационим технологијама, дистрибуција осветничке порнографије, може достићи велике размјере и садржаји веома брзо доспијевају до ширег аудиторијума, што појачава последице овог понашања нарочито код дјеце[28].

Поред ових кривичних дјела у КЗ РС могу се идентификовати и друга кривична дјела која могу укључивати различите облике дигиталног или електронског насиља. Тако на примјер кривично дјело Навођење на самоубиство и помагање у самоубиству (чл. 129) прописује тежи облик који се врши према дјетету или према лицу које није могло схватити значај свог дјела или управљати својим поступцима, за који је прописана казна затвора од пет до двадесет година (ст. 4). Дјеца су веома често, нарочито путем дигиталне технологије, изложена понашањима која спадају у домет дигиталног насиља[29]. Тада чак и безазлена шала, уколико је некоме упућена или је неко озбиљно схвати може код лица да изазове контра ефекат, да код њега створи осјећај тјескобе, несигурности, понижења, те да он покуша себи или неким другим лицима да науди.

Кривично дјело Прогањање (чл. 144) чини онај ко упорно и кроз дуже вријеме прати или уходи друго лице или с њим директно или преко трећег лица настоји успоставити или успоставља нежељени контакт или на други начин код тог лица изазива промјене животних навика, тјескобу или страх за властиту сигурност или сигурности њему блиских лица (ст. 1), док тежи облик постоји ако је дјело члана извршено у односу на садашњег или бившег брачног или

[28] Код жртава осветничке порнографије се јавља посттрауматски стресни поремећај (ПТСП), као онај који се јавља код жртава сексуалног узнемиравања и сексуалног насиља (Janković, Putnik, 2025).

[29] Дигитално насиље представља намјеру да се особа понизи, повриједи, да јој се нанесе нека штета путем коришћења дигиталних технологија, односно мобилних телефона и интернета. Дигитално насиље може се испољавати на више начина и постоје његови различити облици, од којих су најраспрострањени уцјењивање, пријетње, узнемиравање, сексуално злостављање путем интернета, вршњачко насиље на интернету, прављење и коришћење лажних профила као и злоупотреба туђих фотографија (Вељковић, Михајловић, Дукић, Деспотовић, 2021).

ванбрачног партнера, лица са којим је извршилац био у интимној вези или према дјетету (ст. 2). За основи облик пропоисана је новчана казна или казна затвора до двије године, док је за тежи облик прописана казна казном затвора од шест мјесеци до три године. Ово кривично дјело може бити извршено и путем уређаја дигиталне технологије, а исто тако жртва може бити дијете. Ово је шири приступ тзв. сајбер прогањања (engl. Cyber stalking) јер се односи прогањање путем свих средстава информационе и комуникационе технологије, а не само путем интернета.

Кривично дјело Угрожавање сигурности (чл. 150) чини онај ко угрози сигурност неког лица озбиљном пријетњом да ће њега или њему блиско лице лишити живота, тешко тјелесно повриједити, лишити слободе или отети, или нанијети зло подметањем пожара, експлозијом или неком другом општеопасном радњом или средством (ст. 1), док ће тежи облик постојати ако је дјело учињено према службеном лицу у вези са вршењем његове функције, или према више лица, или је учињено у саставу групе или организоване криминалне групе (ст. 2). За основни облик прописана је новчана казна или казна затвора до двије године, док је за тежи облик казна затвора од шест мјесеци до три године. Гоњење за основн се предузима по приједлогу (ст. 3). Ово кривично дјело се такође може извршити дигиталним путем. Тако уколико неко упути пријетњу путем друштвене мреже да ће напасти на живот и тијело друге особе извршиће ово кривично дјело. "Пријетња треба да изазове осећај угрожености тј. страха код лица којима се пријети и тек тог момента је остварено биће кривичног дјела" (Пантелић, 2017).

Такође, можемо говорити и о кривична дјела којима се повређује права на приватност дјеце и угрожавањем личних података дјеце у дигиталном окружењу. Тако кривично дјело Неовлаштено објављивање и приказивање туђег списа, портрета и снимка (чл. 156а)[30] састоји се у објављивању или приказивању спиас, портрета, фотографија, видео-записа, филма или фонограма личног карактера, без пристанка лица које је спис саставило или на кога се спис односи, односно без пристанка лица које је приказано на портрету, фотографији, видео-запису или филму или чији је глас снимљен на фонограму или без пристанка другог лица чији се пристанак по закону тражи, а такво објављивање или приказивање је имало или могло да има штетне посљедице по лични живот тог лица. За ово кривично дјело прописана је новчана казна или каза затвора до двије године. Неовлаштено кориштење личних података (чл. 157) чини онај ко супротно условима одређеним у закону без сагласности грађана прибавља, обрађује, саопшти другом или користи њихове личне податке, за шта је прописана новчана казна или казна затвора до једне године. Овим кривичним дјелима могу бити угрожени лични подаци дјеце у дигиталном окружењу.

[30] Ово кривично дјело је уведено 2023. године као дио ширих измјена КЗ РС којим су уведена и дјела против части и угледа, али са примарним циљем заштите приватности појединца у дигиталној сфери.

Кривично дјело Изношење личних и породичних прилика (чл. 208б) састоји се у изношењу или проношењу чега из личног или породичног живота неког лица што може шкодити његовој части или угледу, а што није, нити може представљати чињенице које су од оправданог интереса. За ово кривично дјело прописана је новчана казна од 1.000 КМ до 3.000 КМ. тежи облик овог кривичног дјела ће постојати ако је дјело учињено путем штампе, радија, телевизије, компјутерске мреже или других видова комуникације, на јавном скупу или на други начин, због чега је оно постало доступно већем броју лица, за шта је прописана новчана казна од 2.000 КМ до 5.000 КМ. Кривично дјело Јавно излагање порузи због припадности одређеној раси, вјери или националности (чл. 208в) чини онај ко јавно изложи порузи или презиру лице или групу због припадности одређеној раси, вјери, националности или због етничког поријекла, боје коже или пола, за шта је прописана новчана казна од 2.000 КМ до 6.000 КМ. Кривично дјело Јавно изазивање и подстицање насиља и мржње (чл. 359) састоји се у путем штампе, радија, телевизије, компјутерског система или друштвене мреже, на јавном скупу или јавном мјесту или на други начин јавног позивања, изазивања или подстицања или чињења доступним јавности летка, слика или неке друге материјале којима се позива на насиље или мржњу усмјерену према одређеном лицу или групама због њихове националне, расне, вјерске или етничке припадности, боје коже, пола, сексуално опредјељења, инвалидитета, поријекла, другог личног својства или каквих других особина. За ово кривично дјело прописана је новчана казна или казна затвора до три године. Иако слична, код кривичног дјела Јавно излагање порузи због припадности одређеној раси, вјери или националности није неопходно доказивати да је дошло до директног позива на насиље или ширење нетрпељивости, већ је довољно да је припадник групе јавно изложен руглу или понижењу на основу свог идентитета. Без обзира на наведено, овим кривичим дјелима могу бити изложена дјеца у дигиталном окружењу.

На концу, као посебну категорију навели смо кривична дјела која су усмјерена на стицање противправне имовинске користи и друих злопотреба. На примјер кривична дјела попут крађе и преваре, гдје је правна природа дјела таква да "субјективно биће" доминира, односно гдје неко користи друштвену мрежу као средство да стекне неку непосредну противправну имовинску корист (Пантелић, 2017). Наиме, крађа идентитета представља преузимање „улоге" неког лица на Интернету, у циљу стицања неке материјалне или друге користи (Прља, Рељановић, 2009, стр. 169). То је једно од најчешћих понашања којима су изложена дјеца у дигиталном окружењу. Извршиоци крађе идентитета постижу свој циљ најчешће коришћењем друштвених мрежа како би са туђег рачунара прикупили лозинке, корисничка имена и бројеве кредитних картица које корисник користи на рачунару[31] (Вилић, 2016, стр.

[31] Неки од начина на који је могуће извршити крађу идентитета су: компровитовање дигиталних уређаја (engl. Hacking) фалсификовање веб странце (engl. Phishing), манипулације корисницима на интернету (engl. Pharming), неауторизован приступ некој интернет локацији како би се дошло до других важних података (енгл.

116). Ипак, у КЗ РС крађа идентитата није прописано као посебно кривично дјело, већ се заштита остварује путем других, повезаних кривичних дјела, као што би били нпр. поједини облици преваре. Превара (чл. 230 КЗ РС) као таква се састоји у лажним приказивањем или прикривањем чињеница ради довођења другог лица у заблуду или га одржавања у заблуди и тиме наведе да то лице на штету своје или туђе имовине нешто учини или не учини. Ово кривично дјело се може учинити и путем дигиталних уређаја, а посебно проблематично може бити уколико је извршено нпр. злоупотребом алата вјештачке интелигенције[32].

4. ЗАКЉУЧАК

Уколико доведемо у вези ризике којима су дјеца изложена у дигиталном окружењу и кривичноправне норме којима се пружа заштита од тих угрожавања, онда можемо констатовати да је тренутни правни оквир адекватан. Евидентно је да је законодавац активно пратио посматрану проблематику те је "новим" кривичним закондовством из 2017. године и измјенама из 2023. године уводио одредбе које се тичу заштите дјеце у дигиталном окружењу. Тако су у КЗ РС прописана кривична дјела којима се директно штите дјеца од секусалног злостављања и искорштавања у дигиталном оркужењу, као што су кривична дјела у вези са дјечијом порнографијом. "Новину представља и инкриминисање приступања дјечијој порнографији путем рачунарске мреже, као и кажњавање корисника сексуалних услуга дјеце, ако су знала или могла и требала знати да се ради о дјетету. Поред тога, законодавац је пооштрио казнену политику за ова дјела предвиђајући веће мјере казни код појединих облика кривичних дјела и онемогућавајући ублажавање казне за кривично дјело обљуба са дјететом млађим од петнаест година. Ту је и обавеза изрицања мјере безбједност и забране обављања позива, дјелатности или дужности као и немогућнос брисања осуде за ова кривична дјела из казнене евиденције" (Марковић, 2018, стр. 41). Код других понашања инкриминисани су квалификовани облици кривичних дјела која су учињена на штету дјеце у дигиталном окружењу, као што су кривична дјела сексуалног узнемиравња и тзв. "осветничка порнографија". На концу, код појединих кривичних дјела као што су угрожавање сигурности, прогањање или

Spoofing), превара платним или кредитним картицама у смислу меморисања информација са магнетних трака платних и кредитних картица који се затим рекодирају ради прављења фалсификоване картице, (engl. Skimming), преварама које се шаљу путем електронске поште, најчешће у виду лажних лутрија, (engl. Scam), преусмјеравање слања података, лажни формулари који се попуњавају на интернету, лажна логовања у која се уносе поверљиве шифре за улазак на различите профиле. Ипак, најчешћи облик крађе идентитета и поверљивих информација путем електронске поште – тзв. Фишинг (Вилић, 2016, стр. 117).

[32] "Овде треба имати у виду да у највећем броју случајева особе чији је лик злоупотребљен ради креирања deepfake садржаја то и не сазнају, те ће се у праксиретко поставити питање кривичноправне заштите њихових права, и то права на сопствени визуелни приказ и фотографију in concreto" (Чучиловић, 2024, стр. 332).

превара јасно је да се она могу извршити према дјеци путем савремене информационо-комуникационе технологије.

Свакако да се прописивањем ових кривичних дјела могу остварити ефекти специјалне и генералне превенције, али не треба изгубити из вида се у овим случајевима често ради о повратницима у извршењу кривичног дјела, који ће настојати да искористе високе технологије како би приступили дјеци ради њихове злоупотребе. У том смислу би се требало фокусирати на кривичноправна рјешења која могу да дају боље резултете, као што је нпр. превентивно затварање (по узору на поједине земље) (види опширније: Ђокић, 2020). Исто тако чини се оправданим приједлог увођења нове мјере безбједности "обавезног психијатријског лијчења лица која су осуђена за кривична дјела сексуалног искоришћавања и злостављања дјеце". "На овај начин пружа се оптимизам у погледу постпеналне будућности осуђених лица и проблематике њиховог рецидивизма" (Pavlović, Petković, Matijašević Obradović, 2014, стр. 58). У прилг томе иде и чињеница да је педофилија према МКВ-11 и DSM V класификацијама[33] класификована као поремећај из домена парафилије[34].

На концу појачану пажњу је потребно посветити новим изазовима који се огледају у злоупотреби вјештачке интелигенције и манипулације подацима. Сасвим је сигурно да ће у наредном периоду ово подручје високих технологија додатно бити предмет прилагођавања кривичног законодавства, које ће ићи у правцу "брисања" разлика између стварног снимка и компјутерски генерисаног садржаја. Нека од тих рјешења, како смо навели, већ су уведена, док ће друга тек бити предмет разматрања (ширење дефиниције жртве дјетета, увођење "дипфејка" као новог кривичног дјела, одговорност дигиталних платформи, итд.)

Литература

Ai Academy (2024). *Kako objasniti šta je vještačka inteligencija?* Dostupno putem interneta: https://aiacademy.ba/blogs/wiki/kako-objasniti-sta-je-vestacka-inteligencija pristupljeno: 19.9.2025.

American Psychiatric Association. (2013). Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition. Washington, DC: American Psychiatric Association.

[33] МКВ 11 је скраћеница за Међународну класификацију болести (International Classification of Diseases for Mortality and Morbidity Statistic) гдје педофилија класификована под ознаком 6D32 педофилија (Pedophilic disorder) (World Health Organization, 2025). DSM V је скраћеница за Дијагностички и статистички приручник за менталне поремећаје, пето издање (Diagnostic and Statistical Manual of Mental Illnesses), гдје педофилија класикована у парафилне поремћаје (American Psychiatric Association, 2013).

[34] Ријеч је о трајном и понављајућем сексуалном интересу за дјецу, која су обично предпубертетског узраста или млађа, а који се манифестује кроз снажне сексуалне фантазије, нагоне и понашања усмјерена ка дјеци. Педофили дијете не посматрају као невино биће, већ као објекат који ће довести до задовољења њиховог нагона. Потреба да се гледа дијете без одјеће или да се дијете сексуално злоставља произлази управо из тог сексуалног нагона усмјереног према дјеци. Иако се поремећај манифестује кроз присутност сексуалних фантазија или порива, злостављање настаје када те фантазије прећу у дјело.

Бајичић, В. (2023). *Кривично право – посебни дио*. Бања Лука: Факултет за безбједност и заштиту.

Beyens, J., Lievens, E. (2016). A Legal Perspective on the Non-Consensual Dissemination of Sexual Images: Identifying Strengths and Weaknesses of Legislation in the US, UK and Belgium. *International Journal of Law, Crime and Justice*, 47, 31-43.

Вељковић, Б., Михајловић, М., Дукић, С., Деспотовић, М. (2021). Насиље на друштвеним мрежама. *ПОНС*, 18(2), 84-91, doi: 10.5937/pomc18-36747

Вилић, В. (2016). Повреда права на приватност злоупотребом друштвених мрежа као облик компјутерског криминалитета. *Докторска дисертација*. Ниш: Правни факултет Универзитета у Нишу.

Davis Kempton, S. (2020). Erotic extortion: Understanding the cultural propagation of revenge porn. *Sage open, 10*(2), 1-9. 2158244020931850

Димовски, Д. (2023). Осветничка порнографија: криминолошки и кривичноправни аспект, *Зборник радова Правног факултета у Нишу,* бр. 98, 155-174.

Ђокић, И. (2020). Превентивно затварање учинилаца опасних по друштво– вишеструки поврат и мере безбедности. У: Ђорђе Игњатовић (Уредник) *Казнена реакција у Србији - X део*. (279-299), Београд: Универзитет у Београду – Правни факултет.

EUROPOL. (2019). *Internet Organised Crime Threat Assessment (IOCTA) 2019.* Hague: European Union Agency for Law Enforcement Cooperation. Dostupno putem interneta: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019 pristupljeno 4.4.2022

European Data Protection Supervisor. (2018). *EDPS Opinion on online manipulation and personal data*. Brussels: European Data Protection Supervisor. Dostupno putem interneta: https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf pristupljeno 6.4.2022

European Network of Ombudspersons for Children. (2019). *ENYA Recommendations Children's Rights in the Digital Environment.* Dostupno putem interneta: http://enoc.eu/wp-content/uploads/2019/10/ENYA-recommendations-on-childrens-rights-in-the-digital-environment-FV.pdf pristupljeno 4.4.2022.

George, M., Jensen, M., Russell, M., Gassman-Pines, A., Copeland, W., Hoyle, R., Odgers, C. (2020). Young Adolescents' Digital Technology Use, Perceived Impairments, and Well-Being in a Representative Sample. *The Journal of Pediatric* 219(1), 180-187 doi: https://doi.org/10.1016/j.jpeds.2019.12.002

Ghadge, M. N. (2024). Digital identity in the age of cybersecurity: Challenges and solutions. *London Journal Of Research In Computer Science And Technology*, 24(1), 1-10.

Internet Watch Foundation. (2024). *Artificial Intelligence (AI) and production of Child Sexual Abuse Imagery*. Dostupno na internetu: https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/ pristupljeno: 28.9.2025.

Janković, B. B., Putnik, N. R. (2025). Osvetnička pornografija u pravu i stvarnosti–pojmovna razgraničenja i regulativa. *Strani pravni život*, 69(2), 205-215.

Karasavva, V., Noorbhai, A. (2021). The Real Threat of Deepfake Pornography: A Review of Canadian Policy. *Cyberpsychology, Behavior, and Social Networking*, 24(3), 203–209.

Кривични законик Републике Српске, Службени гласник Репубике Српске, бр. 64/2017, 104/2018 - одлука УС, 15/2021, 89/2021, 73/2023, "Сл. гласник БиХ", бр. 9/2024 - одлука УС БиХ, "Сл. гласник РС" 105/2024 - одлука УС, 19/2025, "Сл. гласник БиХ", бр. 14/2025 - одлука УС БиХ, "Сл. гласник РС", бр. 31/2025 и 85/2025 - одлука УС

Liu, Y. (2024). AI-generated Fake Information and the Crime of Internet Fraud: Current Legal Challenges and Paths to Reform. *Lecture Notes in Education Psychology and Public Media*,73,1-7.

Mania, K. (2024). Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings from a Comparative Legal Study. *Trauma, Violence, & Abuse*, 25(1), 117-129

Марковић, И. (2018). Сексуално злостављање и искоришћавање дјеце (новине у Кривичном законику Републике Српске). *Годишњак Правног факултета Универзитета у Бањој Луци,* 1(40), 27-43.

Миладиновић, А. (2018). *Безбједносни инциденти према дјеци на друштвеним мрежама.* Бања Лука: Министарство унутрашњих послова Републике Српске.

Moosburner, M., Weber, C., Kuban, T., Wachs, S., Schmidt, A. F., Etzler, S., Rettenberger, M. (2025). Understanding cybergrooming: A systematic review of perpetrator characteristics, strategies, and types. *Trauma, Violence, & Abuse*, doi 15248380251316223

Mori, C., Park, J., Temple, J. R., Madigan, S. (2022). Are youth sexting rates still on the rise? A meta-analytic update. *Journal of Adolescent Health*, 70(4), 531-539.

NCPSS (01.11.2024). *Online grooming crimes against children increase by 89% in six years*. Dostupno putem interneta: https://www.nspcc.org.uk/about-us/news-opinion/2024/online-grooming-crimes-increase/ pristupljeno 1.10.2025.

Пантелић, Н. (2017). Кривична дела извршена на друштвеним мрежама: Структура дела и положај извршиоца. *Параграф*. Доступно путем интернета: https://www.paragraf.rs/100pitanja/krivicno_pravo/krivicna-dela-izvrsena-na-drustvenim-mrezama-struktura-dela-i-polozaj-izvrsioca.html, приступљено 10.2.2026.

Pavlović, Z., Petković, N., Matijašević Obradović, J. (2014). Dječja pornografija. *Zbornik radova Pravnog fakulteta u Splitu*, 51(1/2014), 45- 61.

Pavlović, D., Vulić, T. (2014). Izazovi i perspektive novih medija u odnosu na tradicionalne. U: Nedeljković Valić, D., Pralica, D. (Ur.), *Digitalne medijske tehnologije i društveno-obrazovne promene*. (155-164). Novi Sad: Univerzitet u Novom Sadu, Filozofski fakultet.

Прља, Д., Рељановић, М. (2009). Високотехнолошки криминал – упоредна искуства, Страни правни живот бр. 3/09, 161-184.

Pylkin, A., Serkova, V., Petrov, M., Pylkina, M. (2021). Information Hygiene as Prevention of Destructive Impacts of Digital Environment. In: Bylieva, D., Nordmann, A., Shipunova, O., Volkova, V. (eds). *Knowledge in the Information Society*. PCSF CSIS 2020 2020. Lecture Notes in Networks and Systems, vol 184. Cham: Springer. https://doi.org/10.1007/978-3-030-65857-1_4, pristupljeno 15.4.2022

Ray, A., Henry, N. (2025). Sextortion: A scoping review. *Trauma, Violence, & Abuse*, *26*(1), 138-155.

Research and Markets. (2026). *Adult Entertainment Market 2025-2029.* Dostupno putem interneta: https://www.researchandmarkets.com/reports/5914225/adult-entertainment-market?utm_source=GNE&utm_medium=PressRelease&utm_code=tf93vh&utm_campaign=2060925+-+Adult+Entertainment+Market+Report+2025-2029+with+Vendor+Dynamics+of+25+Major+Players&utm_exec=chdomsai, pristupljeno 10.12.2025.

Rideout, V., Foehr, U., Roberts, D. (2010). *Generation M2 Media in the Lives of 8- to 18-Year-Olds.* Henry J. Kaiser Family Foundation. Dostupno putem interneta: https://files.eric.ed.gov/fulltext/ED527859.pdf, pristupljeno 4.1.2022.

Rindfleisch, A. (2020). The Second Digital Revolution. *Mark Lett,* 31, 13–17. https://doi.org/10.1007/s11002-019-09509-4

Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment (Adopted by the Committee of Ministers on 4 July 2018 at the 1321 meeting of the Ministers' Deputies).

Salloum, S., Gaber, T., Vadera, S., & Shaalan, K. (2022). A systematic literature review on phishing email detection using natural language processing techniques. *IEEE Access*, 10, 65703–65727. https://doi.org/10.1109/ACCESS.2022.3183083

Simović, M., Šikman, M. (2023). The Impact Of Digital Environment On Children And Respond To Socially Unacceptable Behavior, *Journal of Criminology and Criminal Law* 61(1), 7-25.

Susser, D., Roessler, B., Nissenbaum, H. (2019). Technology, autonomy, and manipulation. *Internet Policy Review*, 8(2) 1. doi: 10.14763/2019.2.1410.

Thorne, E., Babchishin, K. M., Fisico, R., Healey, L. (2024). Sexting in young adults: A normative sexual behavior. *Archives of Sexual Behavior*, 53(2), 593-609.

UNICEF. (2017a). *Children in a Digital World - The State of The World's Children 2017*. New York: UNICEF. Dostupno putem interneta: https://www.unicef.org/media/48601/file, pristupljeno 10.4.2022.

UNICEF. (2017b). *Nasilje prema deci u Srbiji: Proces istraživanja za politike i prakse (R3P). Determinante, faktori i intervencije. Nacionalni izveštaj*. Dostupno putem interneta: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.unicef.org/serbia/media/2766/file/Nasilje%20prema%20deci%20u%20Srbiji.pdf, pristupljeno 10.12.2025.

Centar za nestalu i zlostavljanu decu. (2023). *DESHAME Istraživanje: Šta učenici doživljavaju na internetu?* Dostupno putem interneta: https://cnzd.rs/deshame-istrazivanje-sta-ucenici-dozivljavaju-na-internetu/ pristupljeno: 1.10.2025.

Convention on the Rights of the Child, General Assembly resolution 44/25, 20 November 1989

Chadha, A., Kumar, V., Kashyap, S., Gupta, M. (2021). Deepfake: an overview. In *Proceedings of second international conference on computing, communications, and cyber-security: IC4S 2020* (557-566). Singapore: Springer Singapore.

Cyberbullying Research Center. (n.d.). *What is Cyberbullying?* Dostupno putem interneta: https://cyberbullying.org/what-is-cyberbullying, pristupljeno 1.10.2025.

Čučilović, I. (2024). Deepfake tehnologija – krivičnopravne implikacije. *Crimen*, 15(3), 325-342. doi: 10.5937/crimen2403325C

Шкулић, М. (2022). Кривичноправна реакција на дечију порнографију/порнографију малолетних лица - пласирану/насталу злоупотребом рачунарске мреже/комуникације другим техничким средствима, *Ревија за криминологију и кривично право*, 60(2), 9-57.

Шкулић, М. (2002). *Малолетници као учиниоци и као жртве кривичних дела*. Београд: досије.

World Health Organisation (2024). *One in six school-aged children experiences cyberbullying, finds new WHO/Europe study.* Dostupno putem interneta: https://www.who.int/europe/news/item/27-03-2024-one-in-six-school-aged-children-experiences-cyberbullying--finds-new-who-europe-study pristupljeno: 1.10.2025.

World Health Organization. (2025). *Internal Classification of Diseases for Mortality and Morbidity Statistics, Eleventh Revision.* Dostupno putem interneta: https://icd.who.int/browse/2025-01/mms/en#517058174, pristupljeno 10.12.2025.

CRIMINAL LAW PROTECTION OF CHILDREN IN THE DIGITAL ENVIRONMENT

Mile Sikman PhD

Full Professor, Faculty of Law, University of Banja Luka, mile.sikman@pf.unibl.org.

Abstract: *The dynamic development of modern technologies has brought new challenges to which the youngest users are particularly exposed, and these are certainly children. The risks and dangers to which they are exposed are multiplying much faster than criminal law protection is being achieved. Thus, initially, children were mainly exposed to criminal acts of sexual abuse and exploitation via the Internet, such as child pornography, then revenge pornography and similar criminal behaviors. Today, they are also victims of manipulation and abuse of personal data, exposure to harmful and dangerous content in the digital environment, and the subject of abuse and manipulation through artificial intelligence. The scope and prevalence of these behaviors is so wide that the question can be raised whether the existing incriminations in the Criminal Code of the Republic of Srpska can provide children with adequate protection in the digital environment. The subject of this paper has just been stated, in which we will first point out the dangers faced by children in the digital environment, and then present the existing criminal law provisions whose purpose is precisely to protect children.*

Keywords: *criminal law, criminal offense, children, internet, cyber crime.*