Примљено: 20. јун 2023.
Прихваћено: 25. јул 2023.

342.738:004.738.5-053.2
COBISS.SR-ID 112252681
DOI 10.5937/ssb202301029N

ЗАШТИТА ПОДАТАКА О ДЕЦИ НА ИНТЕРНЕТУ

Ана Нешић, демонстратор*
Универзитет у Београду, Факултет безбедности

* ana.didanovic@fb.bg.ac.rs

ЗАШТИТА ПОДАТАКА О ДЕЦИ НА ИНТЕРНЕТУ

Сажетак: *Дигитализација података олакшала је свакодневну комуникацију и размену података, убрзала пословање, али и отворила пут различитим злоупотребама података у сајбер простору. Злонамерни субјекти могу лако, употребом нових технологија, доћи у посед различитих података о интернет корисницима. Подаци се углавном прикупљају без знања корисника, међутим, неретко се користи и непажња и недовољна информисаност корисника о потенцијалним опасностима на интернету. Деца, које велики део свог времена проводе на интернету, најчешће нису свесна тих опасности, па често остављају информације и садржаје на интернету који лако могу бити злоупотребљени од стране заинтересованих субјеката. Додатна опасност по децу на интернету је могућност сексуалне експлоатације. Поред тога, све више је вршњачког насиља на интернету, које ствара код деце посебне психолошке и социјалне проблеме. Како деца немају довољно животног искуства, неопходно је предузети мере и активности којима ће њихови подаци на интернету бити заштићени. Најважнију улогу имају родитељи и образовно-васпитне установе у којима деца бораве, али је и од великој значаја законско регулисање заштите података о деци на интернету.*

Кључне речи: *деца, интернет, подаци о личности, родитељска контрола, образовно-васпитне установе, законска регулатива*

Увод

У савременом друштву скоро да је назамисливо функционисање без интернет технологија. Међу најзначајније промене које нам је интернет донео убрајају се остваривање лакше и брже коминикације, знатно олакшано пословање, свакодневна забава. Но, поред добрих страна, постоје и извесни ризици када је употреба интернета у питању. Услед недовољно развијене дигиталне писмености и свести о могућности виктимизације на интернету, људи често постају жртве

појединих облика сајбер криминала. С проблемом ове врсте се често сусрећу и најмлађи чланови друштва, који значајан део свог времена проводе на интернету (Балтезаревић, 2022).

Технолошки напредак и глобализација довели су до нових изазова када је реч о заштити података о личности. Данас се на интернету налази мноштво података који у сваком тренутку могу бити изложени различитим облицима злоупотреба (Брзуловић Станисављевић, 2019). Ширење информација у оквиру сајбер простора тешко се може ограничити, јер сајбер простор не познаје географске нити политичке границе. Безбедносне претње које данас постоје у сајбер простору нису лако уочиве и не могу се једноставно категоризовати. С тога, сваки члан „електронске друштвене заједнице" може бити потенцијални нападач (Путник, 2022). У оквиру сајбер простора корисници откривају велики број личних података, чиме се свесно одричу дела своје приватности, али и омогућавају злонамерним субјектима да на разне начине манипулишу тим подацима. На пример, постављање фотографија може омогућити идентификацију корисника употребом програмских алата за препознавање лица, али и откривање места на којем се корисник на тој фотографији налази (Вилић, 2016, стр. 83).

Узимајући у обзир наведено, јасно је да остваривање сајбер безбедности није лак задатак. Апсолутни ниво безбедности у сајбер простору није могуће достићи, нити је остварив потпуно елиминисање свих ризика које виртуелни свет са собом носи. Сајбер безбедност би, према томе, требало да подразумева остваривање контроле над ризицима, као и непрестано трагање за компромисом између вредности онога што се штити, нивоа потребне заштите и цене такве заштите (Кешетовић и Путник, 2013). Ова мисао би требало да буде основ за размишљање и поступање када је реч о заштити података о деци на интернету. Како није могуће одстранити све ризике са којима се деца могу сусрети у сајбер простору, а истовремено им се не може ускратити приступ интернету услед непрестане дигитализације, контрола њихових активности се намеће као најадекватније решење.

Подаци о личности

Право на заштиту података о личности представља људско право гарантовано Уставом Републике Србије чије је остваривање детаљније уређено законом (Устав РС, 2006). Према члану 4, ставу 1, Закона

о заштити података о личности, податак о личности је сваки податак који се односи на физичко лице чији је идентитет одређен или одредив, непосредно или посредно, посебно на основу ознаке идентитета, као што су име и идентификациони број, то је сваки податак о локацији, идентификатору у електронским комуникационим мрежама, а који поседује једно или више обележја његовог физичког, физиолошког, генетског, менталног, економског, културног и друштвеног идентитета (Закон о заштити података о личности, 2018). Појам података о личности је новим законом широко формулисан и односи се на све објективне и субјективне информације о једној особи. Информације могу бити опште или се односити на одређене, посебне категорије података о личности. Такође, информације могу бити у различитим формама (папирној, бинарној, дигиталној итд.). Заштита података о личности се односи искључиво на физичка лица, односно физичка лица су носиоци права на заштиту података (Diligenski i dr., 2018, str. 23–25).

Дигитализација података о личности

Сајбер простор представља глобалну дигиталну мрежу које је постала саставни део нашег свакодневног живота. Током последњих година дошло је брзог развоја који је омогућио да се у оквиру сајбер простора остварује комуникација и размена података, а временом је сајбер простор постао и доминантни глобални медиј за комуникацију (McEvoi Manjikian, 2010).

Када данас говоримо о подацима о личности, не мислимо више само на име и презиме, јединствени матични број грађана и сл., већ и на многе друге податке до којих се може доћи употребом интернета, попут *IP* адресе, налога електронске поште, разних шифри корисника, налога на друштвеним мрежама. Сви ови подаци спадају у податке о личности а због широко распрострањене употребе интернета су доступнији него што је то раније био сличај (Брзуловић Станисављевић, 2019, стр. 53).

Дигитализација података о личности спроведена је у многим областима, а развој нових технологија утицао је на потребу за усклађивањем рада бројних субјеката у складу са датим променама. Примери дигиталне трансформације могу се видети код многих организација, са једне стране код приватних компанија, које на тај начин чувају своју конкурентност, док се, са друге стране, и у оквиру државних институција могу видети напори на плану дигитализациије.

Како би се прилагодиле променама и очувале своју конкурентност, организације морају да спроведу дигиталну реконструкцију која се огледа у променама пословног и оперативног модела, ширењу људских знања и вештина у тој области (Bobera and Stojanović, 2020). Поред тога, јавља се и потреба за дигитализацијом документације, односно трансформацијом докумената са папирне у дигиталну форму. Предности дигитализације података су вишеструке и садржане су у уштеди простора, смањењу броја људи који се ангажују на пословима заштите и обраде документације, бржем и лакшем приступу подацима, могућности коришћења документа од стране више корисника истовремено, знатно бољој заштити података (CERAT, 2023).

У складу са технолошким променама, дигитализација се у нашој земљи спроводи и у другим сферама, попут здравства где је донет Програм дигитализације у здравственом систему Републике Србије за период 2022–2026. године, са Акционим планом за спровођење за период 2022–2023 (Министарство здравља РС, 2022) или области финансијских институција. Од изузетне је важности да банке искористе развој интернет услуга како би побољшале своје пословање али и како би осигурале безбедност података којима располажу (Зеленовић и Дукић Мијатовић, 2019).

Облици угрожавања безбедности података о деци на интернету

Савремено друштво постало је зависно од информационо-комуникационих технологија, што је довело до нових безбедносних ризика и претњи (Putnik and Bošković, 2013, str. 115). Угроженост личних података само је једна од постојећих опасности на интернету. Неке од претњи које се могу сусрести на интернету су пресретање података, илегални приступ подацима, *spyware* и *malware*, ботнет мреже, корупција података, саботажа, *DoS* (engl. *denial-of-service*), крађе идентитета (International Federation of Library Associations and Institutions, 2021).

Интернет је, између осталог, омогућио вршење бројних кривичних дела. Посебно рањиву категорију корисника представља млађа популација. Млади често нису свесни опасности са којима се могу сусрести у сајбер простору, па у великом броју случајева остављају информације и садржаје на интернету које лако могу бити злоупотребљени од стране злонамерних корисника (Путник и др., 2013, стр. 75). Сер-

виси углавном поседују заштиту за малолетнике, која за циљ има онемогућавање потенцијалних злоупотреба на интернету, до којих може доћи због постојања отвореног приступа личним подацима корисника (Rambam, 2009).

Употреба нових технологија ради прикупља личних података на интернету

Нове технологије омогућиле су развој бројних метода које за циљ имају прикупљање огромне количине података о активностима интернет корисника (Nikolić, 2021). Иако постоје ситуације у којима људи добровољно остављају своје личне податке на интернету, на пример, попуњавањем образаца на интернету, учесталији су случајеви где се подаци прикупљају без знања корисника, кроз анализу *IP* заглавља, *HTTP* захтеве или употребом *Java Script* и *Flash* програма који се уграђују у интернет странице (Bujlow et al., 2017).

„КОЛАЧИЋИ"

Један од најчешће коришћених метода за прикупаљање података на интернету су „колачићи" (engl. *cookies*). „Колачићи" представљају датотеке које садрже низове текстуалних знакова који кодирају битне информације о кориснику приликом приступа одређеној интернет страници. Подаци који се кодирају су углавом имена и презимена корисника, бројеви кредитних картица, њихове адресе и сл. (Park and Sandhu, 2000, p. 36). Сврха „колачића" је прикупљање података који ће се употребити приликом остваривања наредних комуникација, без потребе поновног тражења истих података (Nikolić, 2021). Поред разних улога које „колачићи" имају, једна од примарних је препознавање корисника приликом претраживања садржаја на интернету (Ševo, 2021, str. 4–5).

"WEB BEACON"

Још једна од метода која се може применити за потребе прикупљања података о корисницима на интернету је web beacon или „интернет багови". Web beacon је сликовна датотека која се користи за праћење активности корисника кроз једну или низ интернет страница. Web beacon се може користити у комбинацији са колачићима, о којим је већ било речи, како би се корисницима омогућило лакше ко-

ришћење интернет странице (Croft and McNally, 2023). Интернет багови су често саставни делови интернет страница.. Сваки web beacon је повезан са HTLM кодом за преузимање датотетке, која када је једном преузета, шаље нападачу информације о кориснику, нпр. IP адресу са које је уређај отворио слику (Zabawa, 2020).

"SPYWARE" ПРОГРАМИ

Spyware програми су злонамерни програми који циљано прикупљају податке о кориснику, које затим шаљу на унапред одређено одредиште, а све то без знања корисника. *Spyware* програми представљају велика претњу приватности корисника, подацима на његовом рачунару, и могу проузроковати значајну материјалну штету. Главно обележје ових програма је да су то злонамерни програми који надгледају и прикупљају податке о кориснику, које потом могу употребити у различите сврхе. Такође, то су злонамерни програми који шаљу корисничке податке трећој особи без знања или пристанка корисника (CARNet CERT–a i LS&S, 2009, str. 4). Информације о којима *spyware* програми обавештавају трећу заинтересовану страну су подаци о активности корисника на интернету, односно информације о интернет страницама које корисник посећује и податке које прикупља или дели са другима (Ševo, 2021).

Првобитно су *spyware* програми били коришћени у маркетиншке сврхе, и били су познатији под називом *adware* програми. Међутим, временом се показало да *spyware* програми могу имати и другачији потенцијал, пошто велики број људи свакодневно користи интернет, а та околност је утицала на развој нових врста злонамерних *spyware* програма. Већина корисника под *spyware* програмима подразумева злонамерне програме који се користе за нежељено оглашавање, крађу података и друге активности (CARNet CERT–a i LS&S, 2009, str. 6).

Сајбер криминал као облик угрожавања података на интернету

Савремено доба је донело напредак информатичке индустрије и технологије, али је истовремено утицало на појаву многих облика сајбер криминала. Развоју сајбер криминала највише доприноси интернет који је нападачима пружио велики број могућности за нападе на податке који се налазе на интернету, а развој технологије олакшао је и

убрзао незаконите поступке којима се долази до жељених информација (Vukoje, 2022, str. 29).

У Стратегији за борбу против високотехнолошког криминала (у даљем тексту: Стратегија), коју је Република Србија усвојила за период 2019–2023 године, се наводи да је *сајбер криминал* облик криминалног понашања код кога се коришћење рачунарске технологије и информационих система испољава као начин извршења кривичног дела, при чему се рачунар или рачунарска мрежа употребљавају као средство или циљ извршења. Рачунари и рачунарска технологија се могу злоупотребљавати на разне начине, а криминал који се реализује помоћу рачунара може имати облик било ког од традиционалних облика криминала, попут крађа, утаја, проневера, док се подаци који се неовлашћено прибављају злоупотребом информационих система могу на разне начине користити за стицање противправне користи (Стратегија за борбу против високотехнолошког криминала, 2018).

Сврха сајбер напада је углавном приступ информацијама, измена података или ускраћивање информација. Нападачи улазе у криминалну зону како би дошли до информација до којих законитим путем не би могли доћи, и како би сазнали одређене поверљиве или тајне податке (Vukoje, 2022).

СЕКСУАЛНА ЕКСПЛОАТАЦИЈА ДЕЦЕ НА ИНТЕРНЕТУ

Сексуално злостављање деце преко интернета подразумева било који сексуално оријентисани контакт путем интернета, а неки од честих појавих облика су производња, прикупљање и дистрибуција дечије порнографије, нежељено излагање деце порнографији, сексуални туризам (O'Leary and D'Ovidio, 2007, p. 2). Контакт са децом се обично остварује путем различитих форума, ћаскањима, порукама, апликацијама, игрицама (Вилић, 2016, стр. 163).

У оквиру Стратегије за борбу против високотехнолошког криминала истакнута је важност супротстављању овој интернет претњи путем обезбеђивања истраживачких средстава и активном применом мера за борбу против „онлајн" сексуалне експлоатације деце. Употребом система за евидентирање и анализу би требало да се региструју различите врсте „онлајн" сексуалних кривичних дела, која су пријављена од стране деце или су повезана са децом као жртвама. Стратегија, такође, наводи да је од изузетног значаја подизање свести и рад на изради мера превенција, са посебним нагласком на потребу

боље едукације деце и родитеља (Стратегија за борбу против високотехнолошког криминала, 2018).

Вршњачко насиље на интернету

Појава и све већа заступљеност друштвених мрежа и стално коришћење интернета, утицала је на појаву „виртуелног" насиља међу вршњацима (Вилић, 2016). За разлику од насиља које се одвија међу младима у физичком свету, насиље на интернету се одвија у дигиталном свету. У оквиру дигиталног света не постоје физичке границе, напади се могу извршити из било којег дела свега, а последице напада се могу испољити и након дужег временског периода (Поповић-Ћитић, 2009). Још једна од карактеристика насиља путем интернет је да насилници могу лако сачувати своју анонимност, што није случај када је реч о насиљу „лицем у лице". Употребом надимака, измишљањем адреса или профила на друштвеним мрежама, али и коришћењем непознатог броја мобилних уређаја, на једноставан начин се прикрива идентитет нападача (Kodžoman et al., 2013).

Вршњачко виртуелно насиље представља сваку комуникацију појединца или групе путем интернета, блогова, e-*maila*, *web* страница, *chatova*, видеа или мобилних уређаја, која је усмерена на понижавање, задиркивање или директне претње другом детету. Такође, укључује слање претећих и злонамерних порука и израду интернет-страница које за циљ имају омаловажавање других (Bilić et al., 2012). Овај обилк насиља се најчешће спроводи кроз слање порука, постављање фотографија на интернет, упућивањем увреда и неистинитих гласина путем интернет, који се на интернету шире великом брзином (Batori et al., 2020).

Начини превенције угрожавања података о деци на интернету

Значај родитељске контроле у заштити података о деци

Како је интернет потенцијално небезбедан простор, родитељи, као најважнији чиниоци васпитања, би требало да буду упућени у ризике коришћења интернета од стране деце, како би правовремено усмери-

ли и регулисали њихово понашање на интернету (Зуковић и Слијепчевић, 2015, стр. 243). Истраживање које је спроведено 2015. године на тему перцепције родитеља о активностима деце на интернету обухватило је и питање о мишљењу родитеља о опасностима коришћења интернета и социјалних мрежа. Иако готово петина (21%) испитаних родитеља није дало одговор на ово питање, 5% испитаника је истакло да не зна са којим све опасностима се деца могу сусрести на интернету. Оно што је значајно је да је већина испитаника (око 75%) навела различите врсте опасности које вребају децу на интернету. Највећи број испитаних родитеља сматра да су те опасности доступност непримерених садржаја на интернету, могућност да деца остваре контакт са непознатим особама, али и друге потенцијалне опасности, попут педофила, утицаја насилних игрица и секти, опасности од крађе идентитета (Зуковић и Слијепчевић, 2015, стр. 248). Истраживање је показало да не постоји довољно развијена свест код родитеља по питању вршњачког насиља на интернету (Зуковић и Слијепчевић, 2015, стр. 251).

У оквиру истраживања спроведеног 2020. године о повезаности рестриктивних стратегија родитељског надзора и учесталости дигиталног насиља код адолесцената, испитани су учесталост изложености и вршења вербалног насиља на интернету, скривања идентитета и обмањивања на интернету, као и облици контроле родитеља када су у питању активности деце на интернету. Резултати истраживања указују да је три четвртине испитаних родитеља користи рестриктивне стратегије контроле активности деце на интернету, при чему се наводи да родитељи често (у 37% случајева) поседују шифру рачунара детета (Matović i Zunić-Pavlović, 2020, str. 39,44).

Када је у питању заштита деце на интернету, родитељима на располагању стоје различити облици заштите. Разговор родитеља са децом представља значајан начин праћења и контроле активности деце на интернету. Но, постоје одређене ствари које деца не желе да поделе са родитељима, па је поред разговора о интернету и социјалним мрежама, родитељи морају применити и друге методе како би контролисали активности деце на интернету. Један од начина је „претраживање историје" (Зуковић и Слијепчевић, 2015, стр. 251). Ипак, најефикасније механизми заштите деце и њихових података на интернету јесу заштите које се постављају на уређајима која деца користе.

Годинама уназад постоје и активно се користе паметни телефони и паметни сатови. Употребом тих уређаја дете може да позива само бројеве са одобрене листе, док долазни позиви могу бити од само унапред одређених и одабраних контаката. С тих телефона и паметних сатова се не може конектовати на интернет. Један од првих уређаја тог типа био *је Samsung Galaxy Tab 3 Kids* таблет, који је био намењен коришћењу „прихватљивог" интернета. Улога родитеља је да конфигуришу које ће апликације дете моћи да покрене и да унапред одреде колико времена дете може да проведе са таблетом. Поред тога, родитељи имају могућност да надгледају и ограниче приступ деце интернету, као и да забране приступа одређеним веб локацијама. Заштита се може остварити и на нивоу провајдера, кроз опцију „родитељски надзор", којом се блокирају нежељене веб локације (Бјелајац и Филиповић, 2020, стр. 266).

Улога образовно-васпитних установа у заштити података о деци

Интерес је образовно-васпитних установа да повећају безбедност деце у погледу задирања у податке о њиховим свакодневним активностима у виртуелном свету (Димитријевић и др., 2018). С тога, задатак образовно-васпитних установа је да утичу на свест наставника, ученика и родитеља о безбедности деце на интернету. Неопходно је едуковати ученике о хардверској и софтверској заштити уређаја, јер самом заштитом уређаја, заштитиће и своје податке на интернету (Vukoje, 2022).

Увођење мониторинга активности ученика на друштвеним мрежама у Сједињеним Америчким Државама може послужити као пример укључивања школе у заштиту података о деци на интернету. Употребом софтвера *Social Sentinel* прикупљају се, процењују и анализирају јавно доступни подаци са друштвених мрежа, који затим служе за идентификовање претњи према деци. Када дође до објава које садрже насиље, школа прослеђује податке о томе полицији (Димитријевић и др., 2018, стр. 134–135).

Међутим, поред активности образовно-васпитних установа усмерених на заштиту деце и њихових података на интернету, ове установе могу и угрозити податке о деци. Наиме, предшколске установе у којима деца бораве располажу фотографијама деце и њиховим личним подацима. Питање које се често поставља је да ли су оне и на

који начин овлашћене да презентују фотографије и податке о деци на својим интернет-страницама или друштвеним мрежама, без изричитог пристанка родитеља. Честа примена принципа што није забрањено, дозвољено је, доводи нас до ситуације у којој деца предшколског узраста нису адекватно заштићена у сајбер простору. Анализом посећених страница преко 70 предшколских установа, приватних вртића и играоница, као и њихових *Facebook* страница, дошло се до закључка да од 134 посећене странице, чак 115, односно 85% установа, презентује фотографије деце (Prtljaga, 2020, str. 115-116). Поједине установе, али и родитељи који дају пристанак за постављање ових садржина, или не дају пристанак али не реагују поводом таквих објава, немају свест о могућим опасностима и последицама до којих може доћи постављањем фотографија и других података о деци на интернету (Prtljaga, 2020, str. 116).

Правно регулисање заштите података о деци

МЕЂУНАРОДНОПРАВНА ЗАШТИТА ПОДАТАКА О ДЕЦИ

Међународноправна заштита деце огледа се у усвајању конвенција и доношењу протокола у области заштите деце од насиља, злостављања и занемаривања. У области заштите деце најзначајна је Конвенција о правима детета (у даљем тексту: Конвенција) из 1989. године којом се уводи нови приступ у заштити права детета кроз посебно истицање концепта заштите људског достојанства, физичког и психолошког интегритета деце. У Конвенцији се наводи да дете има слободу изражавања која укључује право да тражи, прима и даје информације и идеје свих врста, усмено или писмено, преко штампе или неког другог медија по његовом избору. Државе потписнице гарантују детету приступ информацијама које за циљ имају развој његове друштвене, духовне и моралне добробити, физичког и менталног здравља, те су у обавези да дају и развијају смернице које за циљ имају заштиту деце од информација и материјала који могу штетно деловати на њих (Конвенција о правима детета, 1989). Државе потписнице су, између осталог, у обавези да децу заштите од свих облика сексуалног искоришћавања и сексуалног злостављања, и да предузму све неопходне активности како би се спречило искоришћавање деце за порнографске представе (Човић, 2014, стр. 380).

На међународном нивоу се истичу и активности Савета Европе у заштити права деце. Усвајањем Конвенције о сајбер криминалу и Конвенције о заштити деце од сексуалног искоришћавања и сексуалног злостављања детаљније се регулише област заштите деце од насиља, а конвенције представљају значајни инструмент у превенцији насиља над децом и превенцији дечије порнографије (Човић, 2014).

НАЦИОНАЛНИ ПРОПИСИ О ЗАШТИТИ ПОДАТАКА О ДЕЦИ

На темељу Конвенције се заснива обавеза свих држава потписница у успостављању националних стандарда у области заштите права деце, који обухватају обавезу доношења законодавних и других прописа у вези заштите деце од насиља (Симовић-Хибер и Милошевић, 2012, 21). Уставом Републике Србије зајемчена је заштита личних података и одређено да се прикупљање, држање, обрада и коришћење података о личности прецизније уређује законом (Устав РС, 2006).

Кривичноправна заштита података о личности се у нашем законодавству остварује прописивањем одређених кривичних дела. Од инкриминација значајних за заштиту података о личности могу се издвојити следећа кривична дела из Кривичног законика Републике Србије: неовлашћено прислушкивање и снимање (чл. 143 КЗ РС), неовлашћено фотографисање (чл. 144 КЗ РС), неовлашћено објављивање и приказивање туђег списа, портрета и снимка (чл. 145 КЗ РС), неовлашћено прикупљање личних података (чл. 145 КЗ РС), приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију (чл. 185 КЗ РС), искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу (чл. 185б КЗ РС) (Кривични законик РС, 2019).

На националном нивоу предузете су одређене мере, попут доношење Нацрта националне стратегије за превенцију и заштиту деце од трговине и искоришћавања у порнографији и проституцији (2012-2016) са Акционим планом за превенцију и заштиту деце од искоришћавања у порнографији злоупотребом информационих и комуникационих технологија за период од 2012- 2014 године (Човић, 2014, стр. 384–385).

У складу са обавезама преузетим потписивањем конвенција Савета Европе, Република Србија је 2013. године усвојила Закон о посебним мерама за спречавање вршења кривичних дела против полне

слободе према малолетним лицима (у јавности познатији као „Маријин закон"), како би се регулисала заштита деце од сексуалног искоришћавања и сексуалног злостављања. Једна од новина предвиђена овим законом је да педофили, односно особе које су правноснажно осуђене за неко од кривичних дела против полне слободе према малолетним лицима, буду регистровани, односно уписани у посебну евиденцију (Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима, 2013).

Правилник о протоколу поступања у установи у одговору на насиље, злостављање и занемаривање (у даљем тексту: Правилник) представља једну од обавеза Србије насталом ратификовањем Конвенције о правима детета. Правилник дефинише дигитално насиље и злостављање као злоупотребу информационих технологија која може имати за последицу повреду друге личности и угрожавање достојанства, које се остварује слањем порука електронском поштом, СМС-ом, ММS-ом, путем веб-сајта, четовањем, укључивањем у форуме, социјалне мреже и сл. У Правилнику се врши разврставање насиља, злостављања и занемаривања на три нивоа. На првом нивоу се облици насиља и злостављања злоупотребом информационих технологија и других комуникационих програма наводи позивање, слање узнемиравајућих порука СМС-ом, ММS-ом; на другом нивоу су то оглашавање, снимање и слање видео записа, злоупотреба блогова, форума и четовања, снимање камером појединаца против њихове воље, снимање камером насилних сцена, дистрибуирање снимака и слика; док трећи ниво подразумева снимање насилних сцена, дистрибуирање снимака и слика и дечију порнографију (Правилник о протоколу поступања у установи у одговору на насиље, злостављање и занемаривање, 2020).

Закључак

Дигитализација података значајно је олакшала свакодневну размену података и активности различитих субјеката, али је, истовремено, отворила пут различитим облицима злоупотреба података у сајбер простору. Корисници дигиталних технологија, услед недостатка технолошких вештина и дигиталне писмености, могу лако постати жртве различитих облика сајбер напада. Најмлађи чланови друштва, који велики део свог времена проводе у виртуелном свету (често без

надзора родитеља), а не поседују довољно технолошких вештина, посебно су угрожени активностима злонамерних интернет корисника (Балтезаревић, 2022, стр. 131). Злонамерни субјекти могу лако, употребном неких од метода за прикупљање података на интернету, попут „колачића", "web beacon-a" или "spyware" програма доћи у посед личних података корисника, које затим могу искористити на најразличитије начине.

Савремено доба довело је и до развој различитих облика сајбер криминала, који значајно угрожавају безбедност података на интернету. Најмлађи интернет корисници се суочавају и са ризиком сексуалне експлоатације, односно сексуалног злостављања преко интернета. Најчешћи појавни облици сексуалне експлоатације деце путем интернета су производња, прикупљање и дистрибуција дечије порнографије, нежељено излагање деце порнографији, сексуални туризам (O'Leary and D'Ovidio, 2007). Истовремено, деци прети опасност и од вршњачког насиља на интернету које може, такође, имати најразличитије облике испољавања, као што су прогањање, слање увредљивих и вулгарних порука на друштвеним мрежама, застрашивање преко интернета и сл. (Mishna et al., 2009).

Како би се деца и подаци о њима адекватно заштитили у сајбер простору, неопходно је да поједини субјекти и институције буду свесни потенцијалних опасности са којима се деца могу сусрести у виртуелном свету, како би их могли правовремено заштити. Родитељи имају најодговорнију улогу у том смислу, од праћења активности деце на интернету, разговору са њима, па све до коришћења различитих механизама заштите на уређајима које деца користе. Образовно-васпитне установе имају задатак да заштите податке које поседују о деци, али и да спроводе мониторинг њихових активности на интернету. Да би родитељи и образовно-васпитне установе могли да остваре своје улоге у заштити података о деци на интернету, морају бити адекватно информисани и едуковани о начинима заштите података на интернету.

Правно регулисање заштита података о деци је битан механизам заштите података о деци на интернету. Национални прописи, који своје упориште имају у међународноправним документима из области заштите права детета, имају значајну улогу у регулисању ове области. У погледу законске регулативе значајна је кривичноправна заштита података која се остварује прописивање одређених кривичних дела у Кривичном законику Републике Србије. Поред тога, значајан

је и Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима, који регулише област заштите деце од сексуалног искоришћавања и сексуалног злостављања, као и Правилник о поступању установа у одговору на насиље, злостављање и занемаривање.

ЛИТЕРАТУРА

Batori, M., Ćurlin, M., i Babić, D. (2020). Nasilje putem interneta među adolescentima. *Zdravstveni glasnik*, 6 (1), str. 104–114.

Bilić, V., Buljan Flander, G., i Hrpka, H. (2012). *Nasilje nad djecom i među djecom*. Jastrebarsko: Naklada slap.

Bobera, D., and Stojanović, S. (2020). Digital Transformation of Organizations. In *Proceedings of the 25th International Scientific Conference Strategic Management and Decision Support Systems in Strategic Management*. https://doi.org/10.46541/978-86-7233-386-2_27.

Bujlow, T., Carela, V., Solé-Pareta, J., and Barlet-Ros, P. (2017). A Survey on Web Tracking: Mechanisms, Implications, and Defenses. *Proceedings of the IEEE*, 105 (8), pp. 1476–1510.

CARNet CERT–a i LS&S. (2009). *Spyware programi CCERT-PUBDOC-2009-10-280*. Pristupljeno 13.06.2023. ca: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-10-280.pdf.

CERAT (2023). *Digitalizacija dokumentacije*. Приступљено 27.03.2023. са https://www.cerat.rs/usluge/digitalizacija-dokumentacije/.

Croft, P., and McNally, C. (2023). *What Is a Web Beacon and Why Should You Care?* All About Cookies. Приступљено 06.04.2023. са https://allaboutcookies.org/what-is-a-web-beacon.

Hodak Kodžoman, I., Velki, T., i Cakić, L. (2013). Izloženost djece starije školske dobi elektroničkom nasilju. *Život i škola*, 30 (59), str. 110–128.

International Federation of Library Associations and Institutions. (2021). *Internet Governance in 2021: takeaways and insights for libraries*. Приступљено са 29.03.2023.https://www.ifla.org/news/internet-governance-in-2021-takeaways-and-insights-for-libraries/.

Kesetovic, Z., i Putnik, N. (2013). *Cyber security.* In K. B. Penuel, M. Statler, and R. Hagen (Eds.) (2013). *Encyclopedia of Crisis Management* (pp. 217–219). SAGE Publications.

Matović, M. i Zunić-Pavlović, V. (2020). Povezanost restriktivnih strategija roditeljskog nadzora i digitalnog nasilja u adolescenciji. *CM Komunikacija i mediji*, 15 (47), str. 35–56.

McEvoy Manjikian, M. (2010). From Global Village to Virtual Battlespace: the Colonizing of the Internet and the Extension of Realpolitik. *International Studies Quarterly*, 54 (2), pp. 381–401.

Mishna, F., McLuckie, A., and Saini, M. (2019*).* Real-world dangers in an online reality: a qualitative study examining online relationships and cyber abuse. *Social Work Research*, 33 (2), pp. 107–118.

Nikolić, J. (2021). *Stavovi, znanje i zabrinutost studenata o zaštiti osobnih podataka na internetu*. Diplomski rad. Zagreb: Sveučilište u Zagrebu – Fakultet hrvatskih studija, odsjek za komunikologiju.

O'Leary, J.R., and D'Ovidio, R. (2007). Online sexual exploitation of children. *The International Association of Computer Investigative Specialists*. Приступљено 09.04.2023. са https://studylib.net/doc/8823386/online-sexual-exploitation-of-children.

Park, J. S., and Sandhu, R. (2000). Secure cookies on the Web. *IEEE internet computing*, 4 (4), pp. 36-44.

Prtljaga, P. (2015). Zaštita integriteta dece predškolskog uzrasta na internetu. U *Obrazovanje za menadžment – 13. međunarodna naučno-stručna konferencija doba znanja* (str. 112-116). Univerzitet „Union – Nikola Tesla" – Fakultet za menadžment.

Putnik, N., and Bošković, M. (2013*).* Contemporary security challenges – hactivism as a new form of social conflict. *Kultura polisa*, 10 (21), pp. 115–132.

Rambam, S. (2009). *Privacy is Dead – Get over it*. Documentary 24. Приступљено 02.04.2023. са https://www.documentary24.com/privacy-is-dead-get-over-it--317/.

Ševo, I. (2021). *Kolačići, privatnost i kibernetička sigurnost.* Završni rad. Zadar: Sveučilište u Zadru, Stručni preddiplomski studij Informacijske tehnologije.

Vukoje, G. (2022*). Sigurnost djece na internetu – zaštita osobnih podataka.* Pula: Sveučilište Jurja Dobrile u Puli, Fakultet Informatike u Puli.

Zabawa, T. (2020.) *The Internet and Web Tracking. Technical Library* (Grand Valley State University Libraries).

Балтазаревић, Р. (2022). Дигитална писменост као средство превенције сајбер криминала. *Баштина*, 57, стр. 131–139.

Бјелајац, Ж., и Филиповић, А. (2020). Поремећај зависности од интернета (иад) као парадигма недостатка безбедносне културе**.** *Култура полиса*, XVII (43), стр. 239–258.

Брзуловић Станисављевић, Т. (2019). Ново доба заштите података о личности. *Библиотекар: часопис за теорију и праксу библиотекарства*, 61 (2), стр. 51–66.

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

Димитријевић, И., Путник, Н., и Кучековић, З. (2018). Мониторинг друштвених мрежа као облик надзора у образовно-васпитним установама. У: М. Липовац, С. Станаревић, и З. Кешетовић (Ур.) (2018). *Безбедност у образовно-васпитним установама и видео надзор* (стр. 127-143). Београд: Универзитет у Београду – Факултет безбедности.

Закон о заштити података о личности. (2018). Сл. гласник РС, бр. 87/2018.

Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима. (2013). Службени гласник РС, бр. 32/2013.

Зеленовић В., и Дукић Мијатовић, М. (2019). *Дигитална трансформација банкарства као стратешки императив*. XXIV Интернационални научни

симпозијум Стратегијски менаџмент и системи подршке одлучивању у стратегијском менаџменту, Суботица, 17. мај 2019. године.

Зуковић, С., и Слијепчевић, С. (2015). Родитељска контрола понашања деце на интернету и социјалним мрежама. *Настава и васпитање*, 64 (2), стр. 239–254.

Ковненција о правима детета. (1989). Приступљено 15.06.2023. са: http://www.atina.org.rs/sites/default/files/Konvencija%20o%20pravima%20deteta.pdf.

Кривични законик Републике Србије. (2005). Сл. гласник РС, бр. 85/05, 88/05, 107/05, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19.

Министарство здравља Републике Србије. (2022). *Програм дигитализације у здравственом систему*. Приступљено 30.03.2023. са: https://www.zdravlje.gov.rs/tekst/364590/program-digitalizacije-u-zdravstvenom-sistemu.php.

Поповић-Ћитић, Б. (2009). Вршњачко насиље у сајбер простору. *ТЕМИДА – часопис о виктимизацији, људским правима и роду*, (3), стр. 43–62.

Правилник о протоколу поступања у установи у одговору на насиље, злостављање и занемаривање. (2019). Сл. гласник РС, бр. 46/2019 и 104/2020.

Путник, Н. (2022). *Сајбер рат и сајбер мир*. Београд: Универзитет у Београду – Иновациони центар Факултета безбедности.

Путник, Н., Милошевић, М., и Цветковић, В. (2013). Проблем заштите образовно-васпитних установа од високотехнолошког криминала и електронског насиља. *Социолошки преглед*, XLVII (1), стр. 75–92.

Симовић-Хибер, И., и Милошевић, М. (2012). Анализа законског оквира за заштиту деце од насиља, злостављања и занемаривања у васпитно-образовним установама. У Б. Кордић, А. Ковачевић, Б. Бановић (Ур.) (2012). *Реаговање на безбедносне ризике у образовно-васпитним установама* (стр. 15–35). Београд: Универзитет у Београду – Факултет безбедности.

Стратегију за борбу против високотехнолошког криминала за период 2019–2023. године. (2018). Сл. гласник РС, бр. 71 од 25. септембра 2018.

Уредба (ЕУ) 2016/679 европског парламента и савета од 27. априла 2016. о заштити физичких лица у односу на обраду података о личности, и о слободном кретању таквих података и о стављању Директиве 95/46/ЕЗ ван снаге (Општа уредба о заштити података, 2016). Приступљено 12.06.2023. са: https://www.paragraf.rs/propisi/uredba-evropskog-parlamenta-i-saveta-od-27-aprila-2016-o-zastiti-fizickih-lica.html.

Устав Републике Србије. (2006). Сл. гласник РС, бр. 98/2006 и 115/2021.

Човић, А. (2014). Начини злоупотребе деце путем интернета. У: Д. Тодоровић, Д. Петровић, и Д. Прља (Ур.) (2006). *Интернет и друштво* (стр. 379–393). Српско социолошко друштво, Универзитет у Нишу – Филозофски факултет, Институт за упоредно право.

DATA PROTECTION ABOUT CHILDREN ON THE INTERNET

Ana Nešić, Student-Assistant
University of Belgrade, Faculty of Security Studies

Summary

Digitization of data has facilitated everyday communication and data exchange, accelerated business, but has also enabled different forms of data abuse in cyberspace. Malicious subjects can easily, by using new technologies, come into possession of various data about Internet users. The data they mainly access is ussualy collected without the knowledge of the users. Perpertrators often use insufficient information of the users about potential dangers on the Internet. Children spend a large part of their time on the Internet, but they usually are not aware of dangers they can come across while using the Internet, so they often leave there information and content that can easily be misused. An additional danger for children on the Internet is the possibility of sexual exploitation. In addition, there is more and more peer violence on the Internet, which creates special psychological and social problems for children. Since children do not have enough life experience, it is necessary to take measures and activities to protect their data on the Internet. The parents have most important role, then an educational institutions where children stay, but the legal regulation of the protection of data about children on the Internet is also of great importance.

Keywords: *children, internet, personal data, parental control, educational institutions, legal regulations*