BLOKIRANJE SPLETNIH STRANI KOT UKREP BOJA PROTI RAZŠIRJANJU POSNETKOV SPOLNE ZLORABE OTROK

Peter Košnik
Danijela Frangež

Namen prispevka:
Namen prispevka je prikazati blokado dostopa do spletnih strani, ki jo uvrščamo med ukrepe boja proti vse večji razširjenosti posnetkov spolne zlorab otrok.
Metodologija:
Prispevek je pregledni in teoretični. Temelji predvsem na dostopni tuji in domači literaturi o obravnavani problematiki.
Ugotovitve:
Izvedba blokade spletnih strani, ki gostijo slikovne in video datoteke, ki prikazujejo spolno zlorabo otrok, je še vedno v veliki meri odvisna od volje ponudnika internetnih storitev. Predviden ukrep bi bilo mogoče izvajati predvsem v sodelovanju s ponudniki internetnih storitev, nevladnih organizacij, ki se v sklopu mednarodne organizacije INHOPE ukvarjajo s preprečevanjem razširjanja tovrstnega materiala ter organov pregona. Sodelovanje bi moralo potekati usklajeno, s tesnim medsebojnim sodelovanjem in zaupanjem. Ob izostanku kateregakoli izmed teh članov oz. ob njegovi nepripravljenosti za sodelovanje, izvedba takega ukrepa ne bi bila možna, ali pa bi bila celo nezakonita. V prispevku so po opredelitvi posnetkov spolne zlorabe otrok predstavljene možnosti ter nekatere pomanjkljivosti izvedbe navedenega ukrepa. Predstavljen je tudi primer »cenzure« oz. blokade interneta v Sloveniji, in sicer v povezavi z blokado dostopa do tujih spletnih stavnic.

Izvirnost/pomembnost prispevka:
Prispevek, ki predstavlja pomembnost predlaganega ukrepa blokade dostopa do spletnih strani, ki gostijo posnetke spolne zlorabe otrok, je pomemben predvsem za internetne ponudnike, ki so eden izmed najpomembnejših členov pri preprečevanju in zatiranju tovrstne kriminalitete.

Ključne besede: spolna zloraba otrok, posnetki spolne zlorabe otrok, blokada interneta, blokada spletne strani

1 UVOD

Sodobna računalniška in informacijska tehnologija človeštvu prinašata dobre in slabe stvari. Začeli so se pojavljati prvi pozivi k obravnavanju interneta oz. dostopnosti do njega kot temeljne človekove pravice, ki jo zagovorniki enačijo s pravico do izobraževanja. Neoviran dostop do interneta zaradi možnosti kulturnega izražanja, dostopa do znanja, demokratičnega udejstvovanja ter stika med generacijami zagovarjajo tudi predstavniki Evropska parlamenta (Callanan, Gercke, De Marco in Dries-Ziekenheiner, 2009). Wolfgarten (2006) opozarja, da hiter napredek informacijske tehnologije, lahka dostopnost široko pasovnih internetnih povezav ter dinamičnost interneta in njegove vsebine predstavljajo velike tehnološke izzive. Svetovni splet uporabnikom ponuja anonimnost, zamenjavo identitete in jim daje občutek varnosti pred izsleditvijo in sankcioniranjem, kar predstavlja idealno okolje za razmah kibernetične kriminalitete. In če so storilci še nekaj let nazaj skrbno izbirali oblačila in krinko, da jih ljudje med izvrševanjem tatvine ali ropa ne bi prepoznali, v sedanjem času udobno sedejo za mizo, prižgejo računalnik, z uporabo programske opreme skrijejo svojo identiteto, vdrejo v računalniško omrežje banke ter pričnejo s prenakazovanjem denarja.

Informacijska tehnologija je tako rekoč prisotna na vseh področjih kriminalitete. Omogoča izvrševanje premoženjske kriminalitete, gospodarske kriminalitete in kriminalitete s področja pravnega prometa. Z uporabo informacijske tehnologije je mogoče izvršiti celo kazniva dejanja zoper človečnost. Evolucija kriminalitete je tako opazna tudi v informacijskem svetu. Med drugim tudi med kaznivimi dejanji, ki so v povezavi s spolnimi zlorabami otrok ter s proizvodnjo, razširjanjem in posestjo vseh vrst pornografskega gradiva, ki prikazuje spolno zlorabo otrok. Razširjanje tovrstnega gradiva predstavlja sodobni družbi in preiskovalcem tovrstne kriminalitete velik problem. Še večja težava so prizori spolne zlorabe otrok, ki krožijo po medmrežju in s katerimi se zlorabljene osebe redno srečujejo in podoživljajo travmatične izkušnje. 4. 11. 2011 sta Evropski parlament in Svet Evrope sprejela direktivo "o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji, ki razveljavlja Okvirni sklep 2004/68/PNZ", s katero so se določila minimalna pravila glede opredelitve kaznivih dejanj in njihovih sankcij na področju spolne zlorabe in izkoriščanja otrok, posnetkov spolne zlorabe otrok in izkoriščanja otrok za spolne namene ter uvedle določbe za okrepitev preprečevanja tovrstnih kaznivih dejanj in zaščite žrtev teh dejanj (Evropska Unija, 2011).

Prispevek tako po opredelitvi posnetkov spolne zlorabe otrok predstavlja direktivo o boju proti spolni zlorabi in spolnemu izkoriščanju otrok in predstavi nekatere ukrepe omejevanja tovrstnega materiala na internetu.

2 OPREDELITEV POSNETKOV SPOLNE ZLORABE OTROK

Posnetki spolne zlorabe otrok[1] so oblika spolne zlorabe otrok[2] (Akdeniz, 2008), kjer so vizualno prikazani mladoletniki pri seksualnih aktivnostih (Waters IV in Harrell, n. d.). Finkelhor in Ormrod (2004) posnetke spolne zlorabe otrok opredeljujeta s tistimi deviantnostmi, ki primarno vključujejo posedovanje, ali distribucijo pornografskih posnetkov, ki upodabljajo mladoletnike. Saytarly (2005) med posnetke spolne zlorabe otrok uvršča seksualne aktivnosti med otrokom/otroci in odraslim/odraslimi ter med otrokom/otroci in otrokom/otroci, medtem ko jih odrasli opazuje(jo), ali se jim pridruži(jo). Interpol (Fournier de Saint Maur, 1999) k posnetkom spolne zlorabe otrok uvršča tiskane posnetke in/ali avdio in video posnetke, ki prikazujejo seksualne aktivnosti ali intimne predele otrok. Podobno navaja tudi Deisinger (2002), ki navaja, da je pornografsko gradivo lahko tiskano (revije, knjige ali slike), avdiovizualno v obliki filmov, videa, klipov ali računalniške komunikacije prek spletnih strani (npr. klepetalnice). Lanning (v Taylor in Quayle, 2003) je izpostavil pomembno razliko med posnetki spolne zlorabe otrok, ki je seksualno eksplicitna proizvodnja otrokove podobe, in otroško erotiko, ki je material, povezan z otroki, ki ima seksualni namen za posameznika.[3] Ta razlika je pomembna predvsem z vidika preiskovanja, saj je v preiskavo treba zajeti vse posnetke in ne samo tiste, na katerih so razgaljeni otroci. Lanning (v Taylor in Quayle, 2003) posnetke spolne zlorabe otrok deli v tri kategorije: (1) indikativni/nakazovalni (to so posnetki, ki prikazujejo oblečene otroke, in nakazujejo na seksualno zanimanje za otroke), (2) nedostojni (to so posnetki, ki prikazujejo gole otroke, in nakazujejo na seksualno zanimanje za otroke), in (3) obsceni (to so posnetki, ki prikazujejo otroke v eksplicitnih seksualnih aktivnostih). Bolj podrobno posnetke spolne zlorabe otrok razčlenjujejo Taylor, Holland in Quayle (2001), ki navajajo deset kategorij posnetkov, in sicer (1) nakazovanje, (2) nudizem, (3) erotiko, (4) poziranje, (5) erotično poziranje, (6) eksplicitno erotično poziranje, (7) eksplicitno spolno

[1] V strokovnih krogih se namesto izraza »otroška pornografija«, ki je z vidika pomena posameznih besed neprimeren, uporablja izraz »posnetki spolne zlorabe otrok«.
[2] 1. člen Konvencije o otrokovih pravicah (1989) določa, da je »otrok vsako človeško bitje, mlajše od osemnajst let«.
[3] Taylor in Quayle (2003) navajata, da so lahko odrasli, ki imajo seksualno zanimanje za otroke, zelo zahtevni pri iskanju fotografij. Včasih zahtevajo točno določene fizične karakteristike otrok ali pa točno določene pozicije na fotografijah. Na podoben način je lahko organizirana tudi njihova zbirka. Slednja je lahko namenjena lastni uporabi, lahko pa je uporabljena pri pridobivanju otroka v zlorabljajoč odnos (Parsons, 2000).

aktivnost, (8) napad, (9) krut napad, in (10) sadizem/bestialnost. V zadnjem obdobju se vse pogosteje pojavlja tudi tako imenovan psevdo – pornografski material,[4] ki se bo z razvojem 3-D tehnike še povečal.[5] Pri tem bo tako še pomembneje postaviti jasne opredelitve tovrstne problematike ter v iskanju skupnih rešitev slediti tudi direktivam EU. Ena izmed slednjih vsebuje ukrepe, s katerimi bi preprečili dostop do spletnih strani, ki vsebujejo posnetke spolne zlorabe otrok, ali jih širijo med spletnimi uporabniki na njihovem ozemlju (Evropska Unija, 2011).

3 DIREKTIVA O BOJU PROTI SPOLNI ZLORABI IN SPOLNEMU IZKORIŠČANJU OTROK TER OTROŠKI PORNOGRAFIJI

Direktiva Evropskega parlamenta in Sveta o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji in nadomestitvi Okvirnega sklepa Sveta 2004/68/PNZ (Evropska Unija, 2011) nalaga državam članicam EU sprejetje zakonodaje, v katero naj se vnesejo ukrepi, s katerimi bi bila lahko možna takojšna odstranitev spletnih strani na strežnikih na njihovem ozemlju, ki vsebujejo, ali širijo posnetke spolne zlorabe otrok. Države članice naj bi si prizadevale za odstranitev takšnih strani tudi na strežnikih izven njihovega ozemlja. Kot je zapisano v uvodu omenjene direktive EU, so posnetki spolne zlorabe otrok vrsta vsebine, ki ne pomeni izražanja mnenja.[6] Kot eno izmed oblik boja proti kriminaliteti, povezani s posnetki spolne zlorabe otrok, omenja oteževanje nalaganja tovrstnih vsebin na javno dostopni splet. Na

[4] To so prirejene fotografije, na katerih se z določenimi orodji in digitalno tehnologijo ustvari podoba, ki ni fotografija realne osebe oziroma realnega dogodka. Na primer na golo telo ženske »namestijo« glavo otroka, telo pa s posebno obdelavo spremenijo tako, da zgleda »otroško«. Podoba otroka, ki jo ustvarijo, je lahko nekako povezana s tistim, ki »ustvarja«. Lahko je to nečakinja/nečak ali otrok prijatelja, o katerem posameznik fantazira. Lahko pa so tudi otroci znanih oseb. Nekatere psevdo – fotografije imajo manj razvidne motive; npr. na telo fanta »namestijo« glavo deklice, ali pa deklici »prilepijo« nabrekel penis. Včasih pa je pri simulacijah otrok upodobljen skupaj z odraslim; npr. otrok, ki na realni fotografiji drži v rokah igračo, je s simulacijo dodan na fotografijo moškega in v rokah namesto igrače (navidezno) drži njegov penis (Taylor in Quayle, 2003).

[5] Psevdo – material prikazuje podobe in dejanja, ki se v resnici sploh niso zgodila, ali se sploh ne bi mogla zgoditi, ker oseba na fotografijah sploh ne obstaja, vendar vseeno vzbuja polemike o tem, kako te posnetke obravnavati z vidika kazenske zakonodaje. McCabe in Gregory (1998) dodajata, da tisti, ki zlorabljajo otroke, pogosto uporabljajo posnetke spolne zlorabe otrok, da privabijo otroke v poziranje za fotografiranje ali snemanje filmov, in je zato dejstvo ali otrok ali situacija legalno obstajata s tega vidika v teh situacijah nepomembno. V ZDA in na Irskem zakon tako določa, da je kaznivo vsakršno vizualno prikazovanje, kjer je zaradi seksualnih namenov upodobljen otrok (Taylor in Quayle, 2003). Podobno bi lahko sklepali tudi iz 3. odstavka 176. člena Kazenskega zakonika RS (2008), ki navaja, da se kaznuje vsak, ki »proizvede, razširi, proda, uvozi, izvozi ali drugače ponudi pornografsko ali drugačno seksualno gradivo, ki vključuje mladoletne osebe ali njihove realistične podobe, ali kdor poseduje tako gradivo, ali razkriva identiteto mladoletne osebe v takem gradivu«.

[6] Svoboda govora je ena temeljnih človekovih pravic (39. člen, Ustava RS, 1991), vendar posnetki spolne zlorabe otrok niso zajeti med tiste vrste izražanja, ki bile zavarovane z ustavo.

ta način direktiva EU predvideva zmanjšanje obtoka gradiva, ki prikazuje spolno zlorabo otrok ter odstranitev teh vsebin pri samem viru. Vendar pa odstranjevanje tovrstnih vsebin pri viru ni vedno mogoče. Gradivo se lahko nahaja na strežnikih izven Unije, ali pa država, v kateri so strežniki, ni pripravljena sodelovati, oziroma je postopek za odstranitev gradiva v državi posebej dolg. V izogib takšnim težavam je bila predlagana vzpostavitev mehanizmov, s katerimi bi z ozemlja Unije preprečili dostop do spletnih strani, za katere je ugotovljeno, da vsebujejo, ali razširjajo posnetke spolne zlorabe otrok. Po določilih direktive EU naj bi bila spletna stran, ki prikazuje spolno zlorabo otrok, blokirana po tem, ko take spletne strani ne bi bilo mogoče umakniti. Gre za sodelovanje z državami izven EU, kjer proces ugotavljanja vsebine spletnih strani ter izvajanje kakršnegakoli ukrepa zoper tovrstno stran, traja več tednov ali mesecev. Nove težave na tem področju pa predstavlja še t. i. računalništvo v oblaku, ki omogoča shranjevanje, obdelavo in izmenjevanje takšnega gradiva prek strežnikov, ki so več tisoč kilometrov oddaljeni od njihovih uporabnikov.

Callanan et al. (2009) ugotavljajo, da blokiranje interneta, ali pa njegovo filtriranje, ni nov fenomen. Taka dejavnost je prisotna že več let. Sam izraz zajema širok izbor ukrepov, strojne opreme, programske opreme in storitev, tako da bi bilo napačno misliti, da so vse vrste blokiranja interneta enako učinkovite. Obstajajo namreč različni načini blokiranja interneta. Glavni cilj blokiranja interneta je, da se internetna vsebina ne prikaže na osebnem računalniku, oz. na zaslonu tega računalnika. Eden izmed prvih takšnih splošno znanih filtrov je povezan z e-poštnim poslovanjem. Gre za samodejno filtriranje nezaželene elektronske pošte[7] (angl. spam ali junk mail) (Carreras in Marquez, 2001). Callanan et al. (2009) pa opozorijo na najpogostejša, ki sta osebno filtriranje ter blokiranje omrežja. Osebno filtriranje vsebine interneta povzema skupek ukrepov, s katerimi uporabnik računalnika sam prepreči prikazovanje določenih spletnih strani, določene vsebine spletnih strani ali pa npr. določene e-pošte, na lastnem računalniku, medtem ko blokiranje omrežja izvajajo njegovi administratorji, ter z izvedbo ukrepa preprečijo več uporabnikom računalnikov, ki so povezani v tako omrežje istočasno blokado e-pošte, spletnih strani ali zgolj vsebine spletnih strani. Znani so tudi hibridi oz. kombinacije obeh sistemov. Za potrebe tega prispevka se bomo osredotočili na blokiranje omrežja oz. izvedbo ukrepa, s katerim bi istočasno blokirali dostop do določenih spletnih strani, zaradi česar bomo v nadaljnjem besedilu uporabili termin blokada spletnih strani.

[7] Osebno filtriranje neželene e-pošte Wang (2004) združi v štiri različne skupine: (1) filtriranje po številu naslovnikov, (2) filtriranje po ključni(-h) besedi(-ah), (3) filtriranje po naslovu pošiljatelja in (4) filtriranje po veljavnosti poštnega predala (to pomeni, da je naslovnik originalnega sporočila pri ponudniku e-poštnih storitev že zabeležen kot pošiljatelj neželene e-pošte).

4 BLOKADA SPLETNE STRANI

Blokiranje spletnih strani naj bi izvajali ponudniki internetnih storitev (v manjšem obsegu pa tudi administratorji lokalnih omrežij; npr. v podjetjih, hotelih, gostinskih lokalih). Odločiti se morajo, kakšno vrsto aktivnosti ali vsebine bodo blokirali in komu bodo omejili dostop. V veliki večini primerov taka omejitev velja za vse uporabnike mreže. Glavni vprašanji, s katerimi se soočajo administratorji, ko se odločajo za vzpostavitev blokade, sta (1) »Kako tehnično določiti, kaj bo blokirano?« in (2) »Kdo je tisti, ki bo odločil, kaj bo blokirano?«. Pri tem je poleg poznavanja načina izvedbe ukrepa blokade spletnih strani pomembno tudi poznavanje načinov razširjanja posnetkov spolne zlorabe otrok.

4.1 Načini razširjanja posnetkov spolne zlorabe otrok preko interneta

Callanan et al. (2009) ugotavljajo, da je možno slikovne in video datoteke, ki ponazarjajo spolno zlorabo in izkoriščanje otrok razširjati preko interneta na več možnih načinov, predvsem v zadnjem obdobju, ko opažamo porast spletnih socialnih omrežij. Razširjanje je tako mogoče preko spletnih strani, e-pošte oz. nezaželene e-pošta (angl. spam), novičarskih skupin, omrežij P2P (angl. peer to peer), ki delujejo po principu medsebojne izmenjave datotek, in neposrednih sporočanj (MSN, mIRC, Skype, Google ali Yahoo klepet ipd.). Vsi ti načini razširjanja omogočajo enostavno, hitro in (navidezno) anonimno razširjanje gradiva, pri čemer državne meje niso pomembne, kar še dodatno olajša distribucijo tovrstnega gradiva. Ukrepi omejevanja morajo tako poleg že znanih načinov razširjanja upoštevati tudi tehnološki napredek in iskati možnosti, kako učinkovito omejiti razširjanje tovrstnega materiala ali vsaj njegovo prikazovanje. Eden izmed zadnjih ukrepov omejevanja prikazovanja posnetkov spolne zlorabe otrok je blokiranje spletnih strani, ki ga predvideva direktiva o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji (Evropska Unija, 2011).

4.2 Blokada spletni strani s posnetki spolne zlorabe otrok

Blokade spletnih strani, ki vsebujejo slikovne ali video datoteke s posnetki spolne zlorabe otrok, se že uspešno izvajajo v nekaterih evropskih državah (Norveški, Združenem kraljestvu, Danski, Švedski, Finski, Malti in Italiji), kot partner nacionalnim ponudnikom internetnega dostopa pa

deluje tudi Interpol (Interpol, 2011). Interpol je v oktobru 2010 postavil listo najhujših spletnih strani (angl. ″Worst of″ - list), na kateri so navedene domene spletnih strani, ki glede na objavljene kriterije, prikazujejo prizore najhujših zlorab otrok. Lista se dopolnjuje s pomočjo policij, članic Interpola, in predstavlja eno izmed orodij boja proti tovrstni kriminaliteti. Lista je dostopna tudi ponudnikom internetnih storitev, ki se za sodelovanje z organi pregona odločijo prostovoljno. Njihovo sodelovanje je izrednega pomena, vendar kljub temu vsi ne sodelujejo pri izvajanju tega ukrepa. Tisti, ki se odločijo za sodelovanje, dobijo prej omenjeno listo ter v ta namen izdelano ″STOP stran″, ki uporabnika seznani, da se je njegov brskalnik hotel povezati z domeno spletne strani, ki razširja gradivo, ki prikazuje spolno zlorabo otrok, dostop do strani pa je onemogočil njegov internetni ponudnik. Kot je opisano v Interpolovi predstavitvi (Interpol, 2011), je orodje namenjeno izključno preprečevanju dostopa in je tako po tej plati preventivne narave. Preiskovalci s pomočjo tega orodja namreč ne morejo pridobiti informacij, kdo izmed uporabnikov se je na tovrstno stran želel povezati.

Spletna stran oz. njena domena se na listo uvrstita s prijavo občana. Prijava se lahko posreduje po elektronskem obrazcu. Po prejemu prijave si vsebino ogledata najmanj dve različni organizaciji oz. policijski enoti, ki delujeta pod okriljem CIRCAMP.[8] Organizaciji oz. policijski enoti ugotavljata, ali se na prijavljeni spletni strani nahaja sporno gradivo. Za blokiranje spletne strani mora gradivo izpolnjevati naslednje kriterije (Interpol, 2011): (1) gradivo je resnično in ni plod dela z računalniškimi grafičnimi programi ali animacijami, (2) žrtve na slikah ali video posnetkih so stare, ali pa izgledajo stare manj kot 13 let, (3) gradivo prikazuje samo spolno zlorabo, ali pa je osredotočeno na intimne predele žrtve, in (4) domena deluje najmanj zadnje tri mesece[9].

Organizacija INHOPE sodeluje in povezuje mrežo »vročih linij« v več desetih državah, ki sprejemajo prijave o posnetkih spolne zlorabe otrok na internetu. V Sloveniji se s sprejemom prijave o posnetkih spolne zlorabe otrok na določeni spletni strani ukvarja organizacija Spletno oko. »Usposobljeni pregledovalci prijavne točke Spletno oko prijavo pregledajo in jo, če ocenijo, da gre za domnevno nezakonito vsebino, posredujejo organom pregona. V primeru, da je prijavljena stran na slovenskem strežniku, le-to nadalje obravnava Policija, hkrati pa prijavna točka po navodilih Policije o obstoju nezakonite vsebine na strežniku obvesti tudi ponudnika

[8] CIRCAMP pomeni Cospol Internet Related Child Abusive Material Project. To je združenje nekaterih evropskih policij, ki pod projektom s tem imenom izvajajo različne aktivnosti v boju proti proizvodnji in razširjanju posnetkov spolne zlorabe otrok.

[9] Kriterij je postavljen po vsej verjetnosti zaradi velike spremenljivosti interneta ter selitev vsebin iz ene domene na drugo.

gostiteljstva. V primeru da gre za prijavo strani na tujem strežniku, pa se le-ta preko slovenske Policije posreduje tudi Interpolu in, če obstaja, tudi prijavni točki pod okriljem Inhopa v državi, kjer gostuje strežnik z domnevno nezakonito vsebino. Pregledovalci prejete prijave obravnavajo v najkrajšem možnem času oz. najkasneje v dveh dneh od prejetja prijave« (Spletno oko, n. d.). Prav iz tega je jasno razvidna potreba po sodelovanju med nevladnimi organizacijami, policijo ter ponudniki internetnih storitev.

V Sloveniji je bila pred leti že izvedena cenzura interneta. Cenzura interneta s strani državnih organov ter posledična blokada dostopa do spletne strani v tujini je bila izvedena v zvezi s prirejanjem iger na srečo, točneje športnih stav pri stavnicah, ki delujejo na internetu. V tem primeru so ponudniki interneta za blokado dostopa do spletnih strani uporabili tehniko ugrabljanja DNS naslova. Gre za podoben ukrep, kot ga predvideva tudi omenjena direktiva za boj proti posnetkom spolne zlorabe otrok, zato ga v nadaljevanju tudi predstavljamo.

4.2.1 Poskus cenzure interneta v Sloveniji

Kovačič (2010) opisuje, kako je Urad RS za nadzor nad prirejanjem iger na srečo po tem, ko je Državni zbor sprejel novelo Zakona o igrah na srečo, ki uvaja cenzuro spletnih strani, v začetku leta 2010 ponudnikom dostopa do interneta pričel izdajati prve odločbe o blokadi dveh spletnih mest, ki ponujata igre na srečo brez koncesije Republike Slovenije. Ponudniki dostopa do interneta so morali v 15 dneh po prejemu odločbe omejiti dostop do dveh domen, kar naj bi storili tako, da so na svojih imenskih strežnikih te domene ugrabili in vračali napačno preusmeritev na ciljni strežnik (gre za tim tehniko ugrabljanja DNS zahtevkov (ang. DNS hijacking)). Kovačiču (2010) se zdi zanimivo, da je Urad RS za nadzor nad prirejanjem iger na srečo zahteval samo omejitev dostopa do domene v obliki www.domena.com, ne pa tudi do domena.com ali www2.domena.com, kot alternativni različici spletnega naslova.[10]

Slovenija oz. njeni izvršilni organi in slovenski ponudniki internetnih storitev tako že imajo izkušnje z blokado dostopa do spletnih strani. Te so sicer bile opravljene zaradi zaščite finančnih interesov, ki izvirajo iz priredbe iger na srečo, natančneje športnih stav. Nedvomno pa bi lahko enako prakso prenesli tudi na področje blokade spletnih strani ki prikazujejo posnetke spolne zlorabe otrok. V nadaljevanju prispevka so predstavljene možnosti, ki jih imajo ponudniki internetnih storitev pri blokiranju dostopa do spletnega mesta.

[10] Lastnik blokiranega spletnega mesta bi npr. lahko v DNS nastavitve strežnika vpisal alternativne različice spletnega naslova ter tako omogočil dostop do iste vsebine.

4.2.2 Način izvedbe ukrepa blokade spletnih strani

Callanan et al. (2009) med ukrepe blokade razširjanja posnetkov spolne zlorabe otrok štejejo blokado e-pošte,[11] blokado novičarskih skupin (s strani administratorja skupine, če bi se na taki strani pojavilo tako gradivo), blokado rezultatov v iskalnikih, [12] blokado P2P omrežij in blokado spletnih strani. Božič (2010) pojasnjuje, da lahko omejimo dostop do nekega strežnika oz. spletnega mesta na štiri načine: (1) z blokado prometa glede na ciljni IP naslov, (2) s spreminjanjem tabel za usmerjanje prometa, (3) s preusmerjanjem s pomočjo lažnih DNS odgovorov ter (4) s tehnologijo DPI.

Blokada prometa glede na ciljni IP naslov je najbolj enostavna metoda, saj komunikacija na internetu poteka na podlagi IP naslovov, za katerimi stoji strežnik in na njem spletna stran. Tako bi lahko ponudnik internetne storitve na usmerjevalniku prometa (ang. router) ali požarnem zidu (ang. firewall) strežnika preprosto filtriral promet z vnosom pravila, da se promet, namenjen na določen IP naslov oz. spletno stran na tem naslovu, preprosto zavrže. Ker pa se lahko na istem strežniku oz. IP naslovu poleg spletne strani, ki vsebuje gradivo s spolnimi zlorabami otrok, nahaja tudi več različnih spletnih strani s povsem drugo, legalno, vsebino, bi na ta način ponudnik internetnih storitev onemogočil dostop tudi do drugih spletnih strani ter avtorjem oz. lastnikom spletne strani z legalno vsebino naredil škodo. Takemu ukrepu se lahko oseba, ki bi vseeno želela dostopati do spletne strani, ki prikazuje spolno zlorabo ali izkoriščanje otrok, preprosto izogne z uporabo posredniškega strežnika (proxy strežnika) ali z namestitvijo programa, ki uporabnika poveže v omrežje Tor.[13]

Kot drugi tovrstni ukrep Božič (2010) navaja spremembo tabel za usmerjanje prometa. Usmerjevalniki prometa (ang. router) namreč vedo, kam komunikacijske pakete prometa pošiljati, da bodo le-ti prišli na pravi naslov. Če se v nastavitvah usmerjevalnikov vpiše novo pravilo oz. preimenuje tabla za usmerjanje prometa na drug spletni naslov, usmerjevalnik nato sledi novemu pravilu ter uporabnika preusmeri na drug internetni naslov. V tem primeru bi se namreč uporabnik, ki bi želel obiskati sporno spletno stran, povezal z drugo, nesporno, spletno

[11] Že prej opisani filtri za preprečevanje prejemanja e-pošte.
[12] Iskalnik, kot je npr. Google, ne bi izpisal strani, povezanih z iskanimi pojmi, ki bi vsebovali posnetke spolne zlorabe otrok.
[13] TOR (kratica, angl. The onion router) je programska oprema, ki komunikacijo med prejemnikom in sprejemnikom zakodira v večplastni ovoj in ga prek različnih TOR uporabnikov na internetu pošlje k naslovniku. Pri tem vsak od vmesnih uporabnikov odvije en ovoj.

stranjo. Slaba stran tega ukrepa je, da bi lahko taka preusmeritev iz usmerjevalnika ponudnika spletnih storitev ušla tudi na druge usmerjevalnike oz. omrežja.

Tretja možnost je v podtikanju lažnih DNS (ang. domain name system*)* odgovorov. Spletno mesto se lahko s pomočjo DNS sistema blokira tako, da v DNS strežnik dodamo črno listo imen. Ko tako spremenjen DNS strežnik na črni listi najde stran, za katero uporabnik zahteva, da se poveže, namesto pravega odgovora vrne IP naslov vnaprej določenega spletnega mesta, kjer se uporabniku prikaže sporočilo, da do spletnega mesta ne sme. Kot je to opisano v prej opisanem Interpolovem ukrepu.[14] Temu se lastnik sporne spletne strani ne more izogniti na lahek način, uporabnik, ki se pa želi povezati s sporno spletno stranjo, pa se blokadi izogne z nastavitvijo Googlovega DNS strežnika, ter na ta način zaobide blokado oz. preusmeritev. Wolfgarten (2006) pojasnjuje, da je enega prvih takih ukrepov izvedla deželna vlada nemške pokrajine Severnega Porenja in Westfalije, ki je prisilila kar 78 ponudnikov internetnih storitev, da blokirajo dostop do dveh spletnih naslovov, ki sta delovala na ameriškem strežniku in propagirala idejo nacizma.

Kot četrto možnost pa Božič (2010) navaja možnost DPI (angl. deep packet inspection), filtriranje prometa, ki temelji na vpogledu vsebine, samodejnem pregledovanju celotnega prometa in iskanju vzorcev v njem. DPI se uporablja kot dodatek pri nekaterih požarnih zidovih, je pa tudi idealno orodje za nadzor nad prometom zaposlenih. Ker ukrep temelji na pregledu vsebine komunikacijskih paketov, ki jih prestreže postavljeni filter, Božič (2010) ta poseg smatra kot poseg v zasebnost komunikacije. Ta ukrep je glede na trenutno veljavno zakonodajo in glede na velikost posega v eno temeljnih človekovih pravic, pravice do zasebnosti, neizvedljiv.

Klemenčič (2003: 101) opozarja, da razvoj tehnologije v informacijski družbi in globalno računalniško omrežje prinašata »počasno, a gotovo oženje življenjskega prostora ene izmed temeljnih človekovih pravic, tj. pravice do zasebnosti«. Iz tega torej izhaja, da je resničnost popolnoma drugačna in da je »varnost« v spletu le navidezna. Uporaba interneta tako sproža najrazličnejša vprašanja tako z vidika človekovih pravic (Klemenčič, Tičar in Makarovič, 2007) kot tudi vprašanj, kaj je tehnološko mogoče narediti. In kot kaže analiza učinkovitosti blokiranja spletnih strani se pojavi več težav, ki se nanašajo na uspešnost same blokade. Tako vsak poskus blokade še dodatno zaplete že tako zapleteno in prepleteno internetno omrežje, hkrati pa se

[14] Gre za prej opisano STOP stran, izdelano s strani INTERPOLA, na katero je preusmerjen uporabnik interneta ob njegovem poskusu dostopa do spletne strani iz liste spletnih strani, na katerih so datoteke s posnetki spolne zlorabe otrok.

blokade že z malo tehničnega znanja ali pa programske opreme lahko zaobidejo (Callanan et al., 2009).

5 ZAKLJUČEK

Posnetki spolne zlorabe otrok so obravnavani kot grob poseg v spolno nedotakljivost otrok, posest takega gradiva pa v večini sodobnih držav pomeni storitev kaznivega dejanja. Posest in razširjenje takšnega gradiva po mnenju Evropskega parlamenta ne predstavlja gradiva, ki bi bilo zaščiteno s človekovo pravico do svobodnega izražanja. Zaradi tega je eden izmed ciljev zaščite otrok tudi omejevanje razširjanja posnetkov spolne zlorabe otrok. Kljub temu se obseg posnetkov spolne zlorabe otrok povečuje, kar so s sprejeto direktivo o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji jasno pokazali tudi organi Evropske skupnosti. Med ukrepi, ki jih direktiva predlaga, je tudi blokada dostopa do spletnih strani. Pri čemer je za implementacijo tega ukrepa ključnega pomena sodelovanje nevladnih organizacij (ki s pomočjo javnosti najdejo in ocenijo sporno spletno stran), policije in ponudnikov internetnih storitev.

Ob predpostavki, da se navedena direktiva sprejme in da bodo ponudniki internetnih storitev pripravljeni za sodelovanje, bo ukrep uporabnikom interneta onemogočal, oziroma vsaj na določen način oviral dostop do spletnih strani s tovrstnim gradivom. Implementacija predlaganega ukrepa je preprosta in pomeni zelo učinkovit odgovor mednarodne skupnosti na porast spletnih strani s tovrstno vsebino. Je pa tovrstno onemogočanje dostopa zgolj preventivni ukrep, ki ga izvede zainteresiran ponudnik dostopa do internetnih strani. Pri tem pa je potrebno upoštevati, da lahko takšne ukrepe uporabniki interneta s povprečnim računalniškim znanjem in programsko opremo tudi zaobidejo.
Blokiranje dostopa do spletnih strani, ki vsebujejo posnetke spolne zlorabe otrok je torej preprost, predvsem pa poceni ukrep oz. metoda boja proti spolni zlorabi otrok, ki ga lahko v sodelovanju izvedejo nevladne organizacije, ponudniki internetnih storitev ter policija.

6 LITERATURA

Akdeniz, Y. (2008). *Internet Child Pornography and the Law: National and International Responses.* Hampshire: Ashgate Publishing Limited.

Božič, G. (2010). *Problemi blokiranja spletnih mest.* Pridobljeno 21. 11. 2011 na *http://hr-cjpc.si/pravokator/index.php/2010/01/06/problemi-blokiranja-spletnih-mest/*

Callanan, C., Gercke, M., De Marco, E. in Dries-Ziekenheiner, H. (2009). *Internet blocking – balancing cybercrime responses in democratic societies (Executive Summary).* Pridobljeno 22. 11. 2011 na http://www.aconite.com/sites/default/files/Internet_Blocking_and_Democracy_Exec_Summary.pdf

Carreras, X. in Marquez, L. (2001). *Boosting Trees for Anti-Spam Email Filtering.* Pridobljeno 11. 12. 2011 na http://arxiv.org/PS_cache/cs/pdf/0109/0109015v1.pdf

Deisinger, M. (2002). *Kazenski zakonik s komentarjem.* Ljubljana: GV založba.

Europska Unija. (2011). *Direktiva Evropskega parlamenta in Sveta o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji in nadomestitvi Okvirnega sklepa Sveta 2004/68/PNZ.* Pridobljeno 21. 11. 2011 na http:// register.consilium.europa.eu/pdf/sl/11/pe00/pe00051.sl11.pdf

Finkelhor, D., Ormrod, R. (2004). *Child Pornography, Patterns From NIBRS. U.S. Department of Justice, Office of Justice Programs, Office of Juvenile Justice and Delinquency Prevention (december).* Pridobljeno 18. 12. 2011 na https://www.ncjrs.gov/pdffiles1/ojjdp/204911.pdf

Fournier de Saint Maur, A. (1999). *Sexual Abuse of Children on the Internet, A New Challenge for Interpol.* Pridobljeno 13. 12. 2011 na http://unesdoc.unesco.org/images/0011/001147/114734eo.pdf

Interpol. (2011). *Access blocking.* Pridobljeno 21. 11. 2011 na http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking

Kazenski zakonik RS. (2008). *Uradni list RS,* (55).

Klemenčič, G. (2003). Internet in pravica do zasebnosti. V B. Makarovič, D. Možina, Š. Mežnar, D. Bizjak, M. Bogataj in G. Klemenčič (ur.), *Internet in pravo* (str. 101-141). Ljubljana: Univerza v Ljubljani, Pravna fakulteta.

Klemenčič, G., Tičar, K., Makarovič, B. (2007). Internet in človekove pravice. V M. Bogataj Jančič, G. Klemenčič, B. Makarovič, K. Tičar in J. Toplišek (ur.), *Pravni vodnik po internetu* (str. 316-395). Ljubljana: GV založba.

Konvencija o otrokovih pravicah. (1989). Pridobljeno 03. 12. 2011 na http://www.varuh-rs.si/index.php?id=105

Kovačič, M. (2010). *Izdane prve odločbe o blokadi interneta v Sloveniji.* Pridobljeno 21. 11. 2011 na http://hr-cjpc.si/pravokator/index.php/2010/03/20/izdane-prve-odlocbe-o-blokadi-interneta-v-sloveniji

McCabe, K. A. in Gregory, S. S. (1998). Recognizing the illegal activities of computer users. *Social Science Computer Review, 16* (4), 419-422.

Parsons, M. (2000). Protecting Children on the Electronic Frontier, A Law Enforcement Challenge. *FBI Law Enforcement Bulletin*, (oktober), 22-26.

Saytarly, T. (2005). *Fighting Child Porn Online*. Pridobljeno 03. 12. 2011 na http://www.crime-research.org/articles/Saytarly01/

Spletno oko. (n. d.). *Kako deluje.* Pridobljeno 21. 11. 2011 na https://www.spletno-oko.si/c/706/Kako_deluje/?preid=704

Taylor, M. in Quayle, E. (2003). *Child Pornography, An Internet Crime*. New York: Brunner – Routledge.

Taylor, M., Holland, G. in Quayle, E. (2001). Typology of Peadophile Picture Collections. *The Police Journal*, *74* (2), 97-107.

Ustava RS. (1991). *Uradni list RS*, (33).

Wang, C. (2004). *Sender and Receiver Addresses as Cues for Anti-Spam Filtering*. Pridobljeno 26. 12. 2011 na http://www.jrpit.acs.org.au/jrpit/JRPITVolumes/JRPIT36/JRPIT36.1.3.pdf

Waters IV, M. G. in Harrell, J. (n. d.). *Child Pornography on the Internet.* Pridobljeno 31. 10. 2011 na http://gsulaw.gsu.edu/lawand/papers/sp97/law&int.htm

Wolfgarten, S. (2006). *Investigating large-scale Internet content filtering.* Pridobljeno 21. 11. 2011 na http://www.security-science.com/pdf/investigating-large-scale-internet-content-filtering.pdf

O avtorjih:

Peter Košnik, kriminalist SKP PU Ljubljana

Danijela Frangež, asistentka za kriminalistiko, Fakulteta za varnostne vede UM