UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Maja Ružič

Varnost otroških socialnih omrežij in klepetalnic pred zlorabami

Magistrsko delo

Ljubljana, 2013

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Maja Ružič

Mentor: izr. prof. dr. Jaroslav Berce

Varnost otroških socialnih omrežij in klepetalnic pred zlorabami

Magistrsko delo

Ljubljana, 2013

ZAHVALA

Hvala vsem vam, *mojim najbližjim*, ki mi na moji študijski poti stojite ob strani, me vzpodbujate in pri vseh mojih odločitvah podpirate.
Brez vas ne bi zmogla vsega, kar sem!

Hvala tudi mojemu mentorju, izr. prof. dr. Jaroslavu Bercetu, ki mi je svetoval pri pisanju te naloge in mi kljub gužvi omogočil, da sem jo zaključila. Najboljši ste!

Varnost otroških socialnih omrežij in klepetalnic pred zlorabami

Vedno več otrok in mladostnikov ima na spletnih družabnih omrežjih ustvarjen profil ter uporablja neposredno spletno komuniciranje, uporaba spletnih storitev pa med njimi še vedno narašča. V raziskavi me je zanimalo, kako ponudniki spletnih klepetalnic in družabnih omrežij za otroke in mladostnike rešujejo vprašanje varnosti pred zlorabami. Zanimalo me je, kako zagotavljajo varnost svojih uporabnikov in katere mehanizme pri tem uporabljajo. V ta namen sem opravila kvalitativno raziskavo desetih spletnih klepetalnic ali družabnih omrežij, namenjenih zgolj otrokom ali mladostnikom, starim manj kot 18 let. Uporabila sem tehniko skrivnega nakupovalca. Ugotovila sem, da je na vseh obravnavanih straneh zagotovljeno varovanje osebnih podatkov. Pri devetih od desetih spletnih strani je neželeno vedenje med klepetanjem jasno opredeljeno, otrokom in mladostnikom so na voljo informacije o varni uporabi spletnih storitev in možnost podajanja mnenj in poročil ponudniku strani. Vzpodbuja se tudi premišljeno ravnanje z osebnimi podatki. Informacije za otroke in mladostnike so v veliki večini predstavljene preprosto in razumljivo. Najbolj pogosta oblika vzdrževanja reda med neposrednim komuniciranjem je uporaba človeških moderatorjev, ki pa so se izkazali za učinkovite le v polovici primerov. Tehnološki načini so redkejši, med njimi se pojavlja zlasti uporaba raznih filtrov in določene programske opreme, ki se kažejo kot učinkoviti. Pri ponudnikih storitev za otroke in mladostnike je potrebno povečati ukrepe, ki niso odvisni od ravnanja ciljnega občinstva. V tem trenutku je namreč več poudarka na informiranju uporabnikov.

KLJUČNE BESEDE: otroci, klepetalnice, varnost, zlorabe, družbeno omrežje

Child social networks and chat rooms safety from abuses

More and more children and adolescents own a profile on social networks and use instant messaging yet the use of internet services is still rising. By this research I tried to find out how owners of chatrooms and online social networks for children and adolescents cope with the safety dilemma from abuses. I was interested in how they keep their users safe and which mechanisms they use. Therefore I performed a qualitative research of ten online chatrooms or social networks aiming the children and adolescents under 18 years. I used the method of mystery shopping technique. I found out that every site protects private data. On nine out of ten internet sites unwanted behavior is clearly determined, children and adolescents have information on safe use of the online services and the possibility to sent opinions and reports to page owners. Cautious dealing with private data is encouraged. Information for children and adolescents is presented in a simple and clear way. The most used form of site moderation is human moderation, which turned out to be useful on only half the sites. Technical moderation is rare, among which the use of diverse filters and special program software most frequently appears to be useful. The owners of services for children and adolescents need to enhance measures that do not depend on the actions of the target audiences, there is namely more accent on user information at the moment.

KEY WORDS: children, chatroom, safety, abuse, social network

KAZALO

KAZALO TABEL

1 UVOD

Magistrska naloga spada v 1. področje družboslovne informatike, to je področje interakcije med informacijsko komunikacijsko tehnologijo (IKT) in družbo, natančneje med interakcijo na osebni ravni (človek – računalnik) (Vehovar in Petrič 2006).

Otroci danes odraščajo z računalnikom in jim uporaba tega medija ni tuja, saj 69 % slovenskih otrok, starih od 10 do 15 let, uporablja internet vsak dan (SURS 2012). Računalnik se nahaja skoraj v vsakem gospodinjstvu, na internet pa se lahko dostopa tudi s telefonom in drugimi napravami. Uporaba računalnika je za otroke naravna kot dihanje (Buckingham 2006, 47). Kar 95 % gospodinjstev z otroki je imelo konec leta 2012 dostop do interneta, leta 2010 je bilo to število za 3 % nižje (SURS 2012). Otroci so s tem izpostavljeni internetnim trendom, ki s seboj prinašajo tudi negativne plati, kot so neprimerne vsebine, »mobing«, spolno nadlegovanje in drugo. Kot pravi Tapscott (v Moinian 2006, 50), je internet za otroke ustvaril svobodno okolje, kjer imajo otroci kontrolo nad svojim računalnikom in socialnim komuniciranjem. Internet pa se kot pripomoček vse bolj uporablja tudi v izobraževalnih ustanovah, kar ga za nepridiprave naredi še bolj zanimivega (O'Donnell in Milner 2007, 35).

Ta naloga obravnava ozek pas spletnih zlorab, in sicer možnosti pedofila, da s pomočjo spletnih klepetalnic in socialnih omrežij vzpostavi stik z otroki. V medicini je pedofilija definirana kot psihološka motnja, pri kateri odrasli začuti spolno nagnjenost do spolno nezrelih otrok. Je vrsta parafilije, pri kateri oseba teži k spolnemu vedenju z otroki ali pa o tem sanjari, kar povzroča stisko in težave v medosebnih odnosih. V pravnem smislu se termin »pedofil« uporablja za osebe, ki so obtožene spolnega napada na otroke. Med otroke pri tem uvrščamo najstnike in predpubertetnike (Hughes 2007, 667). Termin otrok je pri tem težko definirati (Buckingham 2006, Taylor in Quayle 2003). Sodobni pedofili na otroke ne prežijo na igriščih, ampak jih najdejo na spletnih portalih, ki jim omogočijo, da izkoristijo otrokovo naivnost, radovednost in zaupljivost. Na tak način lahko z otroki sčasoma zgradijo trden prijateljski odnos, ki ga nato izkoristijo, da se z njimi srečajo tudi v živo (Barak 2005, 80–81; Yar 2006, 129). Vedno večji problem so zlasti tako imenovani spletni osvajalci, saj internet nudi veliko možnosti za takšno komunikacijo (Mcalinden 2006; Pratt 2009; Webb, Craissait in Keen 2007; Young 2008).

Odrasli, predvsem starši, se teh nevarnosti vse bolj zavedajo (Yar 2006, 4). Začele so nastajati strani, namenjene zgolj otroškemu občinstvu (Livingstone in drugi 2011). Med njimi se, poleg takih, ki ponujajo video igre, potrošni material in druge interesne dejavnosti, najdejo tudi klepetalnice, forumi in druga socialna omrežja, namenjena zgolj otrokom. Internetna anonimnost pa uporabnikom kljub temu omogoča zavajanje, zaradi česar lahko zlasti otroci in mladostniki zaidejo v težave. Za uspešen boj proti prežečim nevarnostim na internetu je zato potreben nadzor vlade, industrije in staršev, pri čemer je najbolj pomembna ustrezna definicija nevarnih vsebin (Oswell 1999, 43). Za varnost na internetu pa je poleg nadzora pomembno tudi informiranje uporabnikov in izkoriščanje naprednih tehnologij (Hunter 2000; Tynes 2007, 575). V Sloveniji se s tem problemom obširno ukvarja tudi nekaj spletnih mest, na primer: Safe.si, Spletno-oko.si in nasvetzanet.si. Obstajajo tudi projekti, ki se ukvarjajo z razvojem programske opreme, ki bi ščitila otroke pred pedofili, na primer projekt ISIS Univerze Lancester, ki v pogovoru otrok z določenimi algoritmi zazna govor odrasle osebe.

Cilj magistrske naloge je raziskati načine zagotavljanja varnosti otrok pri uporabi spletnih klepetalnic in socialnih omrežij ter ugotoviti, kakšne novosti so na tem področju. V ta namen sem analizirala slovenske in tuje klepetalnice ter socialna omrežja, ki so namenjena zgolj otrokom in najstnikom. Poskušala sem ugotoviti, kako in koliko se proti temu problemu borijo snovalci spletnih strani ter koliko so pri tem uspešni. Zanimali so me obstoječi načini varovanja otrok in najstnikov pred morebitnimi nadlegovalci na spletnih straneh, prav tako pa tudi načini, ki morda še niso v uporabi.

V prvih treh poglavjih magistrske naloge so predstavljene teoretične osnove: definiran je termin otroštva, opisan odnos med otrokom in internetom ter opredeljen pojem spletnega nadlegovanja otrok. Sledi poglavje o varnosti otrok na internetu, kjer sem opisala ravnanje otrok v primeru nevarnosti, s kakšnimi težavami se pri vzpostavljanju varnosti na omrežju srečujejo ponudniki spletnih storitev, kako se hranijo osebni podatki uporabnikov in kakšna je varnost spletnih klepetalnic in socialnih omrežij. V nadaljevanju so predstavljene uporabljene raziskovalne metode. V osrednjem delu magistrske naloge pa je predstavljena raziskava internetnih spletnih klepetalnic in socialnih omrežij, namenjenim otrokom. Na podlagi dobljenih rezultatov sem na koncu magistrske naloge problematizirala varnost otrok in najstnikov na spletnih socialnih omrežjih in klepetalnicah ter podala predloge, kako bi lahko izboljšali njihovo varnost na takšnih straneh.

2 KAJ JE OTROŠTVO

»Pomen otroštva je nenehen predmet konstantnega boja in pogajanj, tako v javnem diskurzu medijev, akademskih teorijah in družbenih zakonih kot v medsebojnih odnosih, med prijatelji in v družini« (Buckingham 2006, 6). Mediji brišejo meje med otroštvom in odraslostjo, istočasno pa te meje tudi krepijo. Pojma odraslost in otroštvo je v zadnjih desetletjih vedno težje definirati. Otroka se definira s pomočjo njegovega nasprotja, torej kot nekoga, ki ni odrasel. Vedno težje je določati meje med tema dvema nasprotjema, kljub temu je to vedno znova potrebno početi. Otroško občinstvo se tako le s težavo določi, njegovo poznavanje pa je postalo ključnega pomena (Buckingham in drugi 1999, Taylor in Quayle 2003). Poleg tega je otroštvo tudi kulturni termin, ni pa nujno, da se koncept otroštva zahodnih kultur ujema s konceptom ostalih kultur. Še posebej to velja za področje otroškega dela in spolnosti (Taylor in Quayle 2003, 3).

Po 16. stoletju je za otroke začelo veljati, da potrebujejo pomoč in zaščito. S šolskim sistemom se je to razmišljanje okrepilo. Ker so se dečki lahko prej izobraževali, so status otroka dobili prej kot deklice. Otroci iz nižjih slojev, ki se niso izobraževali, pa so bili še naprej obravnavani kot majhni odrasli. V prvi polovici 20. stoletja so bili otroci označeni kot nedolžni, bili so izolirani in zaščiteni pred kruto realnostjo sveta. Oblačili so jih drugače kot odrasle in z njimi uporabljali drugačen jezik. Nekatere besede in teme niso smele zaiti v otroška ušesa. Glede na starost otroka se je točno vedelo, kaj bi naj ta vedel in česa še ne. To se je zrcalilo tudi v šolskem sistemu (Meyrowitz 1986, 259).

Vloga in razumevanje otroštva sta se v zadnjih tridesetih letih povsem spremenila. Otroci so danes ponovno podobni odraslim. Govorijo, obnašajo in oblačijo se kot odrasli. Poleg tega se dogaja tudi obratno. Odrasli se v zadnjih dvajsetih letih približujejo podobi otroka, saj se oblačijo, govorijo in delno vedejo kot oni. Ti dve nasprotji sta si s tem postali podobni (Meyrowitz 1986, 227). Meyrowitz prav tako ugotavlja (1986, 227), da se v neki kulturi razlike v statusu kažejo v načinu oblačenja in pojavnosti. Oblačenje otrok nakazuje njihov status v družbi. Včasih otroci niso smeli nositi enakih oblačil kot odrasli in je bil s tem viden njihov podrejen status (Meyrowitz 1986, 227).

Otroštvo je družbeni in zgodovinski konstrukt, sestavljen iz kulture, reprezentacije in elektronskih medijev. Otroštva ne določa biologija, zato to ni neka univerzalna in naravna kategorija. Prav tako nima fiksnega pomena. Otroštvo se spreminja glede na kulturo, zgodovino in družbo, v kateri se pojavlja, zato se je na otroke skozi zgodovino

gledalo različno. Danes bi naj otroci bili odrasli in zreli, istočasno pa se jim kratijo pravice, ki jim jih odraslost prinaša. Prav tako imajo otroci o sebi različna mnenja. (Buckingham 2006, 6–8).

Kljub različnim definicijam pa ima družba še zmeraj skupino oseb, ki ji pravimo »otroci«. Združujejo jih specifične lastnosti, ki so se skozi zgodovino spreminjale. Ena izmed takšnih lastnosti je starost (Buckingham 2006, 6). Te lastnosti so določene in lahko tudi uzakonjene. Kadar so pravilne ali zaželjene, se jih vzpodbuja. Spodbuja se vedenje, ki posameznika uvrsti v njemu primerno kulturno ali družbeno skupino (Buckingham 2006, 7). Otroštvo ima lahko tudi funkcijo varnostnega ukrepa. Odrasli želijo določene lastnosti izkoreniniti že v otroštvu. Te lastnosti velikokrat vidijo pri sebi. Koncept otroštva je tako namenjen odraslim, da obvladujejo svojo prihodnost. Otroci so torej po eni strani grožnja, saj bi naj bili vedno bolj nasilni, antisocialni in kriminalni. po drugi strani pa so zaradi zlorab in kratenja njihovih pravic sami ogroženi. Otroke se lahko prikaže kot nedolžne in ranljive, nagnjene h kršitvam ali pa izobražene in kreativne (Buckingham 2006, 6–8).

Danes vse kaže na združevanje otroštva in odraslosti, saj je vedenje, oblačenje in način govora med otroki in odraslimi velikokrat podoben. Otroci nosijo oblačila, ki so bila nekoč na voljo zgolj odraslim, na primer kompleksne obleke in suknje. Odrasli pa velikokrat posežejo po kratkih majicah z različnimi otroškimi motivi. Homogenizacija teh dveh pojmov se pojavlja zlasti v zabavni industriji, pa tudi v pravnem sistemu. Pravice otrok so vedno bolj postavljene nad pravice staršev. Otrokom se v vedno večih primerih sodi kod odraslim osebam, saj so njihovi prekrški podobni kriminalnim dejanjem odraslih oseb. Jezikovne lastnosti govora odraslih, ki nakazujejo nadrejenost odraslih, izginjajo. Veliko otrok tako svoje starše kliče po imenu. Za otroke prepovedanih ali neprimernih tem je vedno manj. Otroci pa za njih zvedo že zelo zgodaj, mnogi še pred začetkom šolanja. Podobne spremembe se dogajajo tudi pri odraslih. Kariera, izobrazba in razvoj niso več vezane na otroka, ampak so odvisne od odraslega posameznika, ki se zanje odloči na podlagi svojih želja. Odrasli najprej pomislijo na sebe in niso več pripravljeni žrtvovati zanje pomembnih stvari za možnost imeti otroka. Kljub temu nekateri odrasli še vedno sprejemajo tradicionalen način življenja in koncept otroštva ter odraslosti (Meyrowitz 1986, 227–231).

3 OTROCI IN INTERNET

Po Buckinghamu sta pri obravnavi odnosa med mediji in otroki značilna dva pogleda. Prvi pogled je družinski in obravnava otroka kot ranljivega in nedolžnega. Drugi pa razume otroke kot posameznike, ki so vešči uporabljanja medijev z nekim po naravi pridobljenim znanjem. Vse, kar je vmes, je v akademskih razpravah in raziskavah prezrto. Pomen medijskih tekstov je ustvarilo občinstvo (Buckingham 2006, 106–109). Danes si je nemogoče predstavljati, da mladi ne bi uporabljali interneta. Zdi se, da so neločljivo povezani z njim. Že od mladih let so vešči uporabe novih tehnologij, še zlasti interneta (Boonaert in Vettenburg 2011, 54). Otroci so aktivno občinstvo. So prej kompetentni in sofisticirani kot pa pasivne žrtve medijske manipulacije. Popolnoma naivno je trditi, da lahko kdaj gledamo svet z otrokove perspektive in da nas iskanje pravih vprašanj pripelje tja. Težko je priti do psihološke analize le s pomočjo lingvističnih analiz, čeprav je to socialno dejanje. Kar otrok pravi, ne pomeni nujno tega, kar mi mislimo, da pomeni (Buckingham 2006, 115–117).

3.1 RABA INTERNETA MED OTROKI V SLOVENIJI IN EVROPSKI UNIJI

Internet je medij, ki omogoča povezavo vseh obstoječih omrežij, komunikacijo med njimi in jih združuje v eno omrežje (Yar 2006, 7). Od komercializacije interneta v 90-ih letih se njegova uporaba naglo širi (Yar 2006, 8). Po podatkih Statističnega urada Republike Slovenije za prvo četrtletje leta 2012 ima dostop do interneta 95 % gospodinjstev z otroki. Kar 93 % otrok, starih od 10 do 15 let, redno uporablja internet. Redna uporaba pomeni, da so anketiranci navedli, da so internet uporabljali v zadnji treh mesecih vsaj enkrat. Mladostniki, stari od 16 do 24 let, vodijo le za 1 %. Vsak dan ali skoraj vsak dan pa internet uporablja 69 % otrok in 90 % mladostnikov. Sporočila v spletne klepetalnice pošilja 13 % otrok in 18 % mladostnikov, ki so redni uporabniki interneta. V spletnih družabnih omrežjih sodeluje 84 % otrok in 88 % mladostnikov, kar je za 10 % več, kot je bilo v istem obdobju leta 2010 (SURS 2012). Uporaba interneta močno narašča tudi pri zelo mladih otrokih, starih 8 ali manj let. Tako mladi otroci še niso sposobni na varen način uporabljati internet in so iz tega razloga nevarnostim še bolj izpostavljeni (Holloway in drugi 2013, 12).

V kvalitativni raziskavi o varnosti otrok na internetu, ki jo je po naročilu Direktorata za informacijsko družbo in medije Evropske komisije leta 2007 izvedel OPTEM, je za otroke uporaba interneta samoumevna. V raziskavo je bilo vključenih 27 držav Evropske unije z Islandijo in Norveško. Raziskovalci so uporabili fokusne skupine, v katere so bili vključeni otroci, stari od 9 do 10 in od 12 do 14 let, ki so internet uporabljali redno vsaj enkrat na mesec. Leta 2008 je za isti direktorat raziskavo za varnejšo uporabo interneta v EU opravila tudi organizacija Gallup iz Madžarske, ki je prav tako v raziskavo vključila 27 držav članic EU. V tej raziskavi so se o varnosti otrok na internetu pogovarjali s starši otrok, starih od 6 do 17 let. Dve leti kasneje je podobno raziskavo izvedla tudi Sonia Livingstone s svojo ekipo, ki je v raziskavo vključila otroke, stare od 9 do 16 let, ter njihove starše iz 25 evropskih držav.

Večina intervjuvanih otrok ima širokopasovni dostop do interneta, največkrat doma. Starejši otroci uporabljajo internet večinoma dnevno in več časa kot mlajši, ki ga uporabljajo nekajkrat na teden. Čez vikend se uporaba interneta poveča, če pa imajo otroci veliko hobijev, se zmanjša. Do dva otroka v vsaki skupini starejših otrok sebe opisujeta kot močno »odvisna« od interneta, saj ga uporabljata tudi po več ur dnevno (Directorate general information society and media 2007, 5–17). Podobne rezultate je tri leta kasneje dobila tudi ekipa Sonie Livingstone. Vedno več otrok ima računalnike v svojih sobah ali nekje drugje, kjer starši niso direktno prisotni. V Evropi starost otrok pri prvi uporabi interneta pada, zato je pomembno, da se kampanje za ozaveščanje otrok in same spletne strani, namenjene otrokom, temu prilagodijo (Livingstone in drugi 2011, 24).

Otroci začetka uporabe interneta ne dojemajo kot učenje, ampak kot nekaj, kar je prišlo spotoma. Pojavljata se dva načina učenja uporabe interneta. Otroci so se osnovne uporabe naučili od staršev, prijateljev in drugih sorodnikov, ki so jim to načrtno pokazali, ali pa so na tem področju samouki, ki so zgolj opazovali bližnje uporabnike interneta in to sami poizkusili. Otroci so večinoma bolj vešči uporabe interneta kot njihovi starši, ki jim morajo otroci, po besedah nekaterih izmed njih, kdaj kaj razložiti. Fantje se uporabe interneta učijo največkrat z igranjem iger, dekleta pa s spletnim pogovarjanjem. Učenje uporabe interneta med poukom v šoli otroci dojemajo kot dolgočasno in ga v pogovorih omenjajo kasneje. Večinoma predavane vsebine že znajo (Directorate general information society and media 2007, 13–15). Zlasti mlajši otroci, stari od 11 do 12 let, nimajo toliko znanj o delovanju funkcij spletnih strani. Približno 45 % jih zna blokirati sporočila neželene osebe in poiskati informacije o varni uporabi

interneta. Zgolj 35 % izmed njih zna spremeniti varnostne nastavitve na spletnem socialnem omrežju. Največ znanj si pripisujejo otroci s Finske, Slovenije, Nizozemske in Estonije (Livingstone in drugi 2011, 27).

3.1.1 NADZOR OTROK PRI UPORABI INTERNETA

V omenjenih raziskavah Direktorata za informacijsko družbo in medije ter v raziskavi Sonie Livingstone so se raziskovalci pogovarjali s starši in otroci tudi o nadzoru nad otroki pri uporabi interneta. Ugotovili so, da se otroke ob uporabi interneta nadzira in da so posvarjeni o morebitnih nevarnostih. Otroci staršem pokažejo, katere strani obiskujejo in se disciplinirajo sami, kar velja zlasti za dekleta. Kljub temu ima velika večina otrok občutek, da lahko internet uporabljajo relativno svobodno. Mlajši otroci v večji meri uporabljajo internet pod nadzorom staršev, na primer v isti sobi, kjer lahko starši vidijo vsebino. Starejši otroci imajo manj omejitev, sploh če imajo računalnik v svoji sobi. Starši uporabo računalnika najprej omejijo časovno. Mlajšim otrokom dovolijo do 30 minut, starejšim pa eno do dve uri uporabe računalnika dnevno. Otroci smejo uporabljati internet po opravljeni domači nalogi in ne med drugimi družinskimi aktivnostmi, kot so skupni obroki in druženje. Prav tako naj otroci ne bi uporabljali interneta v času spanja in bi naj zaključili do 21. ali 22. ure, še posebej to velja za mlajše otroke (Directorate general information society and media 2007, 18–19).

Z otroki se o njihovih aktivnostih na internetu najraje pogovori 70 % vprašanih staršev. Pogovor z otrokom je s tem najbolj pogost način nadzora otroka pri uporabi interneta. V otrokovi bližini, ko je ta na internetu, želi ostati 58 % vprašanih staršev. Starejši kot so otroci, manjši je starševki nadzor pri njihovi uporabi interneta. Sonia Livingstone je s svojo ekipo ugotovila, da ena četrtina odgovorov otrok in staršev o starševskem nadzoru ni bila koherentna. V nekaterih primerih so morda starši želeli biti bolj strogi, kot so v resnici, ali pa so otroci svoje starše prikazati kot bolj skrbne. Več kot polovica staršev otroku razloži, zakaj so nekatere strani slabe ali dobre, kako se naj obnaša do drugih uporabnikov, se z njim pogovarja o negativnih izkušnjah in pomaga, če je to potrebno (Livingstone in drugi 2011, 103–107). Večina staršev otroku prepove spletno nakupovanje, srečanje z neznanci s spleta in predolgo dnevno uporabo interneta (Directorate general information society and media 2008, 6).

Otroci dobro vedo, katerih vsebin ne smejo obiskovati, ni pa nujno da se tega držijo, kar velja zlasti za starejše dečke. Starši so otrokom najpogosteje prepovedali obiskovanje pornografskih vsebin, nasilnih video iger, plačljivih vsebin in strani, ki so lahko okužene z virusi. Najbolj resni prepovedi v vseh fokusnih skupinah sta bili izdajanje osebnih informacij in osebno srečanje s poznanstvi z interneta (Directorate general information society and media 2008, 6; Livingstone in drugi 2011, 108). Slednje starejši otroci vseeno počnejo, vendar, kot sami pravijo, le v spremstvu drugih otrok. Nekaj otrok, predvsem mlajših, poroča o varnostnih programih, ki so jih namestili starši. Tri leta kasneje se ta odgovor pojavlja zgolj še pri četrtini vprašanih otrok (Livingstone in drugi 2011, 113). Programi otroke opozorijo, ko so prekoračili dovoljen čas uporabe in/ali izključijo internet. Starši nekaterih otrok preverjajo tudi obiskane vsebine, profil spletnih socialnih omrežij in druge stike. Takšno preverjanje s starostjo otrok upada (Livingstone in drugi 2011, 110).

V glavnem nadzor, ki ga izvajajo starši, otroke ne moti, čeprav nekatere starejše otroke, zlasti dekleta, katerih mame berejo njihova sporočila in druge spletne pogovore, vdiranje v njihovo zasebnost moti. Starši prepoved interneta pogosto uporabijo kot kazen za slabe ocene in grdo obnašanje ali pa kot nagrado za dobre ocene. To so raziskovalci še posebej opazili na Nizozemskem, Finskem, v Estoniji, Španiji, na Poljskem, Malti in v Sloveniji (Directorate general information society and media 2007, 19–20). Otroci omejitve staršev dojemajo kot nekaj, kar je namenjeno zgolj za njihovo zaščito in jih v glavnem podpirajo. Zanje je najbolj smiseln razlog za omejitev časa na internetu zdravje. Velikokrat so omenjali negativne posledice za oči, koncentracijo in nevarnost sevanja. Po mnenju otrok jim starši omejujejo čas uporabe interneta predvsem zaradi fizične zaščite pred zlorabami in njihove psihološke stabilnosti, saj bi naj pogosta uporaba povzročila odvisnost, morebitne grozljive vsebine pa nočne more za mlajše otroke (Directorate general information society and media 2007, 20–21).

Kar 70 % vprašanih otrok podpira nadzor, ki ga izvajajo starši, 44 % jih meni tudi, da ta nadzor ne omejuje njihovega početja na internetu. Navodil staršev ne upošteva 29 % vprašanih otrok, 8 % otrok pa navodil pogosto ne upošteva. Deleža otrok, ki si želijo več ali manj nadzora staršev, sta enaka, dosegata približno 15 %. Posredovanju staršev pri uporabi interneta otrok sledi posredovanje učiteljev in šele nato posredovanje prijateljev. Enako pomembni pri ozaveščanju kot prijatelji so ostali sorodniki otrok. Le 20 % otrok dobi informacije o varni uporabi interneta iz drugih medijev in zgolj 12 % otrok z interneta. Kar ena tretjina otrok še nikoli ni dobila takšnih informacij. Starši

svoje znanje o varnosti na internetu črpajo od družinskih članov in prijateljev, sledijo televizija, radio in tisk, šola, ponudniki internetnih storitev in ostale spletne strani (Livingstone in drugi 2011, 114–129). Velika večina staršev, kar 88 %, meni, da bi k varnejšemu ravnanju otrok na spletu pripomoglo več takšnih vsebin v šoli. Skoraj četrtina staršev pa bi rada takšna izobraževanja obiskovala tudi sama (Directorate general information society and media 2007, 7).

3.1.2 KAJ OTROCI POČNEJO NA INTERNETU

Otroci kot dve glavni funkciji uporabe interneta navajajo: igranje spletnih iger in iskanje informacij o stvareh, ki otroke zanimajo, to pa so v glavnem vsebine za zabavo. Fantje večinoma igrajo spletne igre, dekleta pa internet najraje uporabljajo za spletno pogovarjanje (Livingstone 2011, 34; Cassell in Cramer 2008, 66). Otroci omenjajo tudi iskanje informacij za šolske obveznosti, kar pa jim ni toliko zanimivo, saj to ni prostočasna aktivnost. Starejši dečki presenetljivo manj omenjajo to funkcijo kot mlajši otroci in starejše deklice. Viden je porast gledanja videoposnetkov na internetu. Za starejše otroke je pomembna funkcija interneta tudi pridobivanje filmov in drugih datotek, zlasti to velja za dečke (Livingstone 2011, 34). Predšolski otroci najraje gledajo videoposnetke in igrajo spletne igre (Holloway in drugi 2013, 12).

Neposredno spletno komuniciranje narašča s starostjo, največ pa ga uporabljajo deklice. Internet ustvarja prostor, ki je skrit odraslim očem. Uporaba spletnih klepetalnic je med mlajšimi otroki dokaj nizka, prevladuje pa pri starejših otrocih, še posebej pri deklicah (Directorate general information society and media 2007, 22–25). Uporaba spletnih klepetalnic se je od leta 2007 zmanjšala. Mlajši otroci so s ponudbo spletnih vsebin najmanj zadovoljni. Le 34 % jih trdi, da je na internetu veliko zanimivih stvari za otroke njihovih let. Viden je pojav spletnega portala Facebook, ki uporabo spletnih socialnih omrežij postavlja pred uporabo neposrednega spletnega komuniciranja (Livingstone 2011, 34–36).

Otroci preko spleta načeloma komunicirajo z osebami, ki jih poznajo. Starejši kot so, več komunicirajo z nepoznanimi ljudmi. To počne 13 % otrok, starih od 9 do 10 let, in 26 % otrok, starih od 15 do 26 let, kar pomeni, da mlajši otroci to počnejo redkeje. Med spoloma ni razlik. Od starosti je prav tako odvisno, ali se otroci dobijo z neznanci ali ne. Z neznanimi ljudmi se je dobilo le 2 % otrok, starih od 9 do 10 let, 4 % otrok, starih od

11 do 12 let, 9 % otrok, starih od 13 do 14 let, in 16 % otrok, starih od 15 do 16 let. Več kot polovica otrok, ki so neznano osebo spoznali v živo, pravi, da je na tak način spoznalo le eno do dve osebi v zadnjem letu. Enak odstotek teh otrok pravi, da so neznanca poznali prijatelji in je bil v skupni družbi že prej. Upoštevajoč populacijo vseh otrok, vključenih v raziskavo, se je 3 % otrok srečalo z osebo, ki ni bila niti malo povezana z njihovim življenjem pred tem (Livingstone 2011, 85–91).

3.2 OTROŠKE KLEPETALNICE IN SOCIALNA OMREŽJA

»Ko računalniško omrežje povezuje osebe ali organizacije, se smatra kot socialno omrežje. Tako kot je računalniško omrežje skupek strojev, povezanih s kabli, je socialno omrežje skupina oseb (ali organizacij ali drugih družbenih enot), povezanih z družbenimi odnosi, kot so prijateljstvo, sodelovanje ali izmenjava informacij« (Garton in drugi 1999, 75). Odnosi so določeni z vsebino, smerjo in močjo. Vsebina se nanaša na kontekst, ki ga osebi obravnavata in so lahko usmerjeni ali neusmerjeni. Usmerjeni odnosi izvirajo iz ene osebe in so namenjeni drugi osebi. Neusmerjeni odnosi pa so namenjeni vzdrževanju odnosa in nimajo smeri, lahko so tudi neenakomerni, na primer ko ena oseba čuti več prijateljstva kot druga. Moč odnosa se lahko določa glede na vsebino, pogostost vzpostavitve odnosa in druge lastnosti. En ali več odnosov določa vez med dvema osebama. Tudi vezi se določajo glede na vsebino, smer in moč, vendar se večinoma delijo na močne in šibke. Močne vezi vsebujejo bolj intimne in prijateljske odnose, šibke pa ne (Garton in drugi 1999, 78–80).

Spletna socialna omrežja so podobna mnogim drugim socialnim medijem, vendar imajo nekaj ključnih elementov, zaradi katerih so edinstvena. Uporabnik lahko v omrežju ustvari javni ali zasebni profil, določi, kateri uporabniki lahko dostopajo do njegovega profila in ta seznam stikov ureja (Boyd 2011, 43). Spletna socialna omrežja lahko nudijo možnost neposrednega sporočanja. To je oblika sporočanja, ki omogoča hitro in hkratno prenašanje informacij med dvema ali več uporabniki (Safe-si). Neposredno sporočanje lahko najdemo tudi v spletnih igrah, spletnih klepetalnicah ali na katerikoli drugi spletni strani. Strani lahko omogočajo skupinsko ali zasebno komuniciranje, slednje poteka med dvema osebama (Childnet international 2009). Otrokom in mladostnikom družabna omrežja in klepetalnice omogočajo ustvarjanje lastne vsebine, ki jo lahko pokažejo drugim, nov način samoizražanja, učinkovit način komuniciranja z drugimi in eksperimentiranje s svojo osebnostjo. Nudijo jim prostor, ki ga ne nadzirajo

odrasli, in možnost razkazovanja svojih tehnoloških sposobnosti (Home Office 2008, 11).

Spletna socialna omrežja so ena izmed najhitreje rastočih elementov interneta in predstavljajo veliko priložnosti ter tveganj za otroke, saj združujejo klepet, pošiljanje sporočil in druge funkcije. Javnost po eni strani odobrava razvijajoče se možnosti izobraževanja, druženja in drugih kreativnih zadev v povezavi s spletnimi socialnimi omrežji, po drugi strani pa so politični akterji zaskrbljeni glede uporabe teh omrežij. Skrbi jih dojemanje prijateljstva, upravljanje z intimnostjo in zasebnostjo, zavedanje stalnosti naloženih podatkov, preverjanje starosti pri registracijah in možnosti zavajanja, vdiranja v zasebnost, zlorabe ter druge tvegane komunikacije. Zaenkrat »migracije« tveganj iz starejših oblik spletnega sporočanja na novejša spletna socialna omrežja še niso dokazane (Livingstone 2011, 36).

Vedno več otrok, to je 59 %, ima na spletnih omrežjih lasten profil (Livingstone 2011, 36–38). Svoj profil ima ustvarjen 25 % otrok, ki so stari med 9 in 10 let, in kar 82 % otrok, starih med 15 in 16 let. V Sloveniji ima spletni profil 66 % 10 do 15 let starih otrok in 77 % 16 do 20 letnih (Vehovar in drugi 2011, 10). Posedovanje profila s starostjo narašča. Povprečno ima polovica otrok, ki imajo ustvarjen profil, od 11 do 50 kontaktov, 20 % jih ima manj kot 10 kontaktov, drugih 20 % pa med 100 in 300 kontaktov. Le 9 % jih ima več ko 300 kontaktov (Livingstone 2011, 36–38). Pri predšolskih otrocih so zelo priljubljeni virtualni svetovi, ki so mešanica socialnega omrežja in spletnih iger. Uporablja jih od 37 do 64 % otrok, starih od 6 do 9 let. (Holloway in drugi 2013, 12).

Kljub temu, da je število kontaktov lahko faktor tveganja za otroka, pa otroci novih kontaktov ne sprejemajo povsem lahkomiselno in prav tako ne delijo osebnih informacij z vsemi. Zaseben spletni profil ima 43 % otrok, 28 % jih ima delno zasebnega, 26 % pa ima javen profil, ki ga lahko vidijo vsi. Nevarnost javnega profila je odvisna od tipa informacij, ki jih otroci objavljajo. Večina jih ne objavlja naslova in telefonske številke, vendar je med otroki vseeno pogosto, da objavijo kakšno osebno informacijo, kot je na primer osebna fotografija, priimek, šola in drugo (Livingstone 2011, 38–40). Zanimivo je, da je 24 % fantov in 42 % punc, starih od 10 do 15 let, na socialnem omrežju objavilo fotografijo sebe ali nekoga drugega v provokativni pozi. Prav tako je 21 % punc in 23 % fantov iz te starostne skupine objavilo sliko s pomanjkljivo oblečeno osebo. Vse ostale starostne skupine so to počele v manjši meri (Vehovar in drugi 2011, 22).

Ker imajo nekatera omrežja starostno omejitev svojih članov, 17 % otrok prikrije pravo starost, da se lahko vpišejo. Spletna socialna omrežja se razlikujejo glede na privzete nastavitve in varnostna opozorila. Na tem področju je potrebno najti neko ravnotežje za varnost otrok. Otroci se večinoma pogovarjajo s prijatelji, ki jih poznajo osebno, vendar odstotek kontaktov, ki so jih prvič spoznali na internetu, s starostjo narašča. Z ljudmi, ki so jih prvič spoznali na internetu, komunicira 33 % od 15 do 16 let starih otrok (Livingstone 2011, 38–40). Otroci pri uporabi socialnih omrežij v 63 % ne doživljajo omejitev. Ostalim otrokom starši največkrat določijo pravila v povezavi z izdajanjem osebnih informacij, objavljanjem fotografij in srečevanjem neznancev v živo. Največji delež otrok vedno upošteva navodila staršev, prav tako je 70 % otrok prijateljev s svojimi starši, če ti imajo svoj profil na socialnem omrežju (Vehovar in drugi 2011, 28–30).

3.2.1 RAZISKOVANJE SPLETNIH SOCIALNIH OMREŽIJ IN KLEPETALNIC

Kako se dejansko lotimo raziskovanja interneta? Kot ugotavlja Jones (1999, 12), je internet nek tekoč medij, ki nikoli ni enak in stalen, čeprav od njega ostanejo tekstovne sledi, ki mu navidezno dajejo obliko. Dognati človeško dimenzijo interneta je prav tako težko kot raziskovati človeške interakcije. Z e-pošto in spletnimi teksti ujeta komunikacija nam daje lažen občutek oprijemljivosti interneta. Ti navidezni podatki kaj hitro dajo vtis, da predstavljajo nek del realnosti, postavljen na splet (Jones 1999, 12).
Tradicionalna definicija skupnosti se je nanašala na fizičen prostor, kamor so se raziskovalci odpravili, tam ostali in opazovali. V kolikšni meri se lahko tradicionalne tehnike etnografskih študij prenesejo v prostor spletnih skupnosti, je še zmeraj nejasno. Če je internet poosebljen množični medij, bi morda raziskovalci morali zaznati svojo lastno izkušnjo z internetom in se osredotočiti na posameznike znotraj skupnosti (Jones 1999, 17–19).
Raziskovanje interneta predstavlja izziv, saj so teksti in lastnosti interneta, kljub podobnostim s tradicionalnimi elementi raziskovanja, še vedno specifični. So intertekstualni, obsežni, multimedijski, mednarodni, nestalni in vprašljivega porekla (Mitra in Cohen 1999, 199). Raziskovalci prenašajo znane in testirane metode v kontekst spleta ali pa razvijajo nove metode, prilagojene posebej za splet (Lobe in drugi 2007, 25). Najbolj uporabljene metode za raziskovanje spleta so: spletne ankete, spletni

intervjuji, spletne fokusne skupine, virtualna etnografija in razne vrste avtomatiziranega zbiranja podatkov o obiskanosti spletnih strani in migracijah uporabnikov, kot so podatki registracij uporabnikov spletnih strani, piškotki in drugi (Lobe in drugi 2007, 29).

Raziskave spletnih socialnih omrežij se nanašajo na vzorce odnosov med ljudmi, organizacijami in drugimi akterji. Večina raziskav spletnega komuniciranja se nanaša na tehnične lastnosti različnih spletnih komunikacij in na to, kaj se z njimi lahko povzroči ali stori. Prav tako študije spletnega komuniciranja, ki se nanašajo zgolj na skupinsko dinamiko, odvračajo pozornost od pomembne naloge spletnega komuniciranja, to je podpiranje interakcije in prepredanje odnosov v spletnih socialnih omrežjih (Garton in drugi 1999, 76–77). Skupek odnosov in vezi razkrije socialno omrežje. Z opisovanjem odnosov in vezi lahko analitiki opišejo socialna omrežja. Podatki o socialnih omrežjih se običajno zbirajo z vprašalniki, intervjuji, dnevniki, opazovanji in računalniškim nadzorom (ang. Computer monitoring) (Garton in drugi 1999, 90).

4 ZAPELJEVANJE OTROK NA INTERNETU

Raziskovanje spolnih napadov na internetu je v začetni fazi in slabo razvito (Taylor in Quayle 2003; Barak 2005; Yar 2006; Briggs in drugi 2010). Internet je okolje, ki omogoča tako zdrave kot patološke vedenjske vzorce (Suler v Barak 2005, 77). Prav tako je lahko uporabljen v zle ali dobre namene (Taylor in Quayle 2003, 14). Specifične lastnosti interneta ne le podprejo in okrepijo spolno nadlegovanje, ampak ga tudi omogočijo, saj nudijo okolje, kjer nadlegovalci dobijo potrditev in se obnašajo kot jim narekujejo njihove potrebe. Nadlegovalec izkoristi anonimnost, nevidnost in enostavno ter hitro možnost pobega iz situacije (Barak 2005, 82–83). V enaki meri pa se lahko možne žrtve pred spolnimi nadlegovalci s temi lastnostmi zavarujejo, morda celo bolj kot v fizičnem svetu (Barak 2005, 82). Briggs in drugi pa anonimnosti dodajajo še možnost učinkovitejšega raziskovanja spolnega kriminala, saj lahko drugo identiteto prevzamejo tudi policisti in ostali raziskovalci (Briggs in drugi 2010, 73).

Spolno nadlegovanje na internetu je eden izmed glavnih razlogov, ki kvari funkcionalnost in pozitivnost interneta, saj odganja uporabnike, tistim, ki pa vztrajajo, povzroča bolečino in jih čustveni prizadene (Morahan-Martin v Barak 2005, 77). Spolno nadlegovanje otrok na internetu spada v kategorijo kiberkriminala, torej

nelegalnih kriminalnih dejanj, ki za uresničitev potrebujejo internet (Yar 2006, 9). Sodi v skupino kiberkriminala, kjer ima računalnik z internetom vlogo orodja. Tak kriminal je obstajal že pred razvojem računalnikov in interneta, za razliko od nekaterih drugih oblik kiberkriminala, ki so nastale skupaj z razvojem računalniške tehnologije (Furnel v Yar 2006, 10). Kljub temu, da je spolno nadlegovanje otrok obstajalo že pred razvojem interneta, pa internet nudi platformo, kjer so nastale nove skupine spolnih prestopnikov, ki prej v takšni obliki in meri niso obstajale (Sheldon in Hewitt v Briggs in drugi 2010, 73). Wall (v Yar 2006, 10) kiberkriminal deli na štiri skupine:

- spletni vdor, kjer zlikovci vdrejo v računalnik uporabnika in/ali povzročijo škodo;
- spletne prevare in kraje, kjer so oškodovanci okradeni ali žrtve prevare;
- spletna pornografija, kjer se krši zakon zaradi nespodobnosti in nedostojnosti;
- spletno nasilje, načrtovanje ali izvajanje fizičnega nasilja in s tem kršitev zakona zaščite oseb.

Zapeljevanje otrok bi lahko uvrstili v spletno nasilje takrat, kadar nepridipravi komunicirajo z otroki, da bi jih zlorabili tudi fizično. Kadar pa se to stopnjuje v pornografske dejavnosti ali pa pedofili nimajo namena fizično škodovati otroku, se to uvršča v spletno pornografijo (Yar 2006, 10).

4.1 PEDOFILIJA

Danes velja prepričanje, da je pedofilija mentalna motnja. Kot tako jo je na koncu prejšnjega stoletja definiral že Kraft-Ebing. Nekateri znanstveniki menijo, da pedofili niso zmožni oceniti kvalitete svojih dejanj in se podrediti legalnim zahtevkom dejanj. Osebe, ki širijo pedofilijo, niso nujno same pedofili, ampak jih žene profit. Njihov interes je podoben preprodajalcu drog, ki sam ni nujno odvisnik (Fontana-Rosa in Cesar 2001, 119). Pedofilijo lahko enačimo s perverzijo, ki jo Stubrin (v Fontana-Rosa in Cesar 2001, 121) določa kot spolno vedenje, kjer ni neoporečne obojestranske privolitve.

V medicini je pedofilija definirana kot psihološka motnja, pri kateri odrasli začuti spolno nagnjenost do spolno nezrelih otrok (Taylor in Quayle 2003; Hughes 2007). Je spolni akt med odraslo osebo in predpubertetnim otrokom (Hughes 2007, 667). Hughes nadalje ugotavlja, da so žrtve večinoma deklice. Tipičen pedofil je star okrog 26

let, z nižjo izobrazbo in travmatičnimi izkušnjami v otroštvu (Hughes 2007, 677). Prav tako naj bi bil samski, nikoli poročen in naj bi živel sam ali s starši (Fontana-Rosa in Cesar 2001, 122). Spletni spolni nadlegovalci otrok bi naj bili stari povprečno 35 let, izobraženi, zaposleni in brez prekrškov (Briggs in drugi 2010, 75). Spolni nadlegovalci, ki preko spleta komunicirajo z otroki, bi naj v večini imeli hebefilijo ali pa ehebefilijo. Hebefilija se nanaša na spolno nagnjenost k mlajšim otrokom v puberteti, ehebefilija pa k spolni nagnjenosti do otrok v kasnejšem obdobju pubertete (Wolak in drugi v Briggs in drugi 2010, 75).

Ameriško psihiatrično združenje APA je določilo naslednje kriterije, ki določajo osebo s pedofilijo:

- Oseba ima vsaj šest mesecev spolna nagnjenja, sanjarjenja ali vedenja, ki vključujejo spolno aktivnost z otrokom, starim manj kot 13 let.
- Oseba se je na te potrebe odzvala ali pa so te potrebe povzročile stres in težave v medosebnih odnosih.
- Oseba je stara vsaj 16 let in pet let starejša od omenjenih otrok iz prve točke (Hughes 2006, 667–677).

V pravnem sistemu se termin »pedofil« uporablja za osebe, ki so obtožene spolnega napada na otroke; med otroke so zajeti najstniki in predpubertetniki. Takšno poimenovanje naj bi bilo neprimerno, ker združi več tipov različnih prestopnikov. Tako se nanaša na kateregakoli odraslega, ki ga spolno privlačijo otroci ali pa je otroka tudi zlorabil (Hughes 2007). Večina pedofilov je moških, vendar se pedofilija pojavlja tudi pri ženskah (Pratt 2009). Zaradi stereotipa o moških pedofilih, je težko določiti delež žensk. Ženske zlorabe otrok niso nikoli bile v ospredju raziskav, poleg tega je ženska pedofilija težje definirana kot moška, saj imajo ženske več sprejemljivega fizičnega dostopa do otrok, s tem je meja do zlorabe tanjša. Ženske lahko svoje vzburjenje tudi lažje skrijejo kot moški (Taylor in Quayle 2003, 67–68).

Osebe s pedofilijo se delijo na izključne in izbirne. Slednje privlačijo tudi odrasle osebe. Izključne pedofile privlačijo le otroci. Ne kažejo zanimanja za osebe svojih let, v določenih primerih jih lahko vzburijo le fantazije ali bližina otrok. Večina pedofilov je izbirnega tipa. Za diagnozo osebe kot pedofila ni potrebno dejanje zlorabe otroka. Dovolj so sanjarjenja in potreba po spolnih odnosih z otrokom (Huges 2007). Pedofilija pa ni le spolna usmerjenost, ampak je način življenja, ki ga podpira subkultura. Ta ločuje med pedofili in nadlegovalci otrok. Pedofilija se v tem primeru nanaša na spolno

zanimanje in ljubezen do otrok, nadlegovalci pa otroke fizično spolno zlorabijo (Taylor in Quayle 2003, 12).

Osebe, ki čutijo slo po otrocih, delimo v štiri skupine:

- trgovci, ki trgujejo z otroško pornografijo;
- osvajalci, ki se lotevajo neprimerne spolne komunikacije z otroki;
- potniki, ki otroke fizično poiščejo;
- lahko pa pedofili uporabljajo internet zgolj za druženje med seboj (Durkin v Alexy, Burges in Barker 2005, 810).

Zlasti tako imenovani spletni osvajalci so vedno večji problem, saj internet nudi veliko možnosti za to početje (Mcalinden 2006, Pratt 2009). Podpora okolja, ki je pedofilom na voljo na internetu, jih opogumlja k zlorabi otrok. Internet s tem močno vpliva na omrežje pedofilov, saj jim omogoča povezavo in dostop do oseb z istim mišljenjem, kar je še bolj razvilo področje pedofilskega vedenja (Durkin in Bryant v Taylor in Quayle 2003, 13).

4.2 OBLIKE SPLETNE SPOLNE ZLORABE

Durkin (v Taylor in Quayle 2003, 106) navaja štiri oblike zlorabe interneta, ki jih lahko uporabijo odrasli, ki kažejo spolno zanimanje za otroka: posredovanje otroške pornografije, iskanje otrok z namenom zlorabe, neprimerno spolno komuniciranje z otroki in komuniciranje z drugimi pedofili. Na internetu anonimnost omogoča, da oseba prevzame več osebnosti, s katerimi se lahko približa otrokom. Odrasli, ki se pretvarjajo, da so otroci, to lahko počnejo daljše obdobje. Izmišljena osebnost postane del njih, ima svoje hobije in dodelano življenjsko zgodbo. Dogajalo se je tudi, da so se pedofili, ki so se izdajali za otroke, pogovarjali z otroki, ki so v resnici prav tako bili odrasli. Imeli so romantične in poglobljene odnose, si pošiljali darila in svoje vsakdanje življenje podrejali spletnemu (Taylor in Quayle 2003, 107–109).

Eden izmed pedofilov, ki sta jih v svoji raziskavi intervjuvala Taylor in Qayle, je kot namišljen otrok na spletu sam doživel spletne zlorabe, v katerih je z veseljem sodeloval. Odrasle, ki so ga zapeljevali, je razdelil na plenilce, ki so se na vsak način želeli dobiti z njim v živo, samozadovoljevalce, ki so bili zadovoljni s pogovorom o spolnosti, in družabnike, ki so se zanimali za njegov namišljen jaz kot neke vrste prijatelji. Ko se je nekaj mesecev izdajal za otroka in večkrat odkril, da se intimno pogovarja z odraslimi,

se je na spletu predstavil s svojo pravo osebnostjo. Tako je spoznal enako misleče in začel s prenašanjem otroške pornografije. Prvi korak pedofila, ki se želi na internetu približati otrokom, bi tako lahko bil prav izdajanje za otroka. Ko je na spletu našel sebi enake osebe in slišal njihove izkušnje, je želel svoje ideje tudi uresničiti. Prelevil se je v plenilca (Taylor in Quayle 2003, 107–115).

Poznamo tri tipe spolnega nadlegovanja: spolno nasilje, vezano na spol, neželena spolna pozornost in spolno prisiljevanje. Na internetu se pojavljajo vse tri oblike, najmanj je prisotno spolno prisiljevanje. To je verjetno vezano na dejstvo, da se tudi v resničnem svetu pojavlja najbolj poredko (Barak 2005, 79). Najbolj pogosto je spolno nadlegovanje, vezano na spol. Lahko je aktivno ali pasivno. Aktivno spolno nadlegovanje je namenjeno točno določeni osebi, največkrat se izvaja prav v klepetalnicah in forumih, kjer nadlegovalci podajajo na spolnost vezane izjave in fraze. Pasivno spolno nadlegovanje pa je namenjeno vsem zainteresiranim uporabnikom, na primer vzdevek »potreben«, in ni vezano na točno določeno osebo. Poznano je tudi grafično spolno nadlegovanje, ki je prav tako lahko aktivno ali pasivno, le da so namesto besed prisotne slike (Barak 2005, 79–80).

Da se razvije neželena spolna pozornost, je potrebna direktna komunikacija med nadlegovalcem in žrtvijo. Tukaj so sporočila največkrat vezana na poizvedovanje o spolnih organih osebe ali njenih spolnih navadah. Nadlegovalci v tem primeru želijo žrtvi povzročiti nelagodje, njihov namen v prvi vrsti ni želja po spolnem kontaktu (Barak 2005, 80). Spolno prisiljevanje se od drugih dveh spolnih nadlegovanj razlikuje po prisili, ki jo izvaja nadlegovalec na žrtev. Nepridiprav tako z različnimi načini, ki jih omogoča internet, poskuša prisiliti žrtev v spolno sodelovanje. Takšni poskusi lahko pri žrtvi povzročijo paniko in tudi strah pred uporabo interneta (Barak 2005, 80). Raziskovalna ekipa Sonie Livingstone je prišla do rezultatov, da je 15 % otrok, starih 11 do 16 let, v zadnji 12 mesecih na internetu prejelo ali videlo sporočilo s spolno vsebino. Odstotek otrok narašča s starostjo – s 7 % mlajših otrok, starih od 11 do 12 let, na 22 % otrok, starih 15 do 16 let. Glede na spol ni bilo vidnih razlik. Mlajšim otrokom tega vprašanja niso postavili. Otroci ta sporočila največkrat vidijo ali prejmejo s pojavnimi okni, preko neposrednega spletnega komuniciranja ali spletnih socialnih omrežij. Starši podcenjujejo izpostavljenost svojih otrok sporočilom s spolno vsebino, kar ponovno nakazuje na dejstvo, da otroci staršem teh izkušenj v večini ne povedo (Livingstone 2011, 73–78).

O'Connell navaja več stopenj zapeljevanja otrok, začenši z razvijanjem prijateljstva, torej spoznavanje otroka. Sledi nadgrajevanje odnosa, da postane ta oseba otrokov najboljši prijatelj, kar se nadaljuje v zadnjo fazo, kjer pride do intimnosti, zaupanja in skrivanja. Komaj ko je vez med pedofilom in otrokom tako globoka, zlikovec predlaga spolni kontakt ali srečanje živo (O'Connell v Yar 2006, 132). Kot opaža Malesky (v Briggs in drugi 2010, 75), se internetni zapeljevalci osredotočijo na stiske otrok in mladoletnikov, da bi si s tem pridobili njihovo zaupanje. V klepetalnicah iščejo otroke z razburljivimi vzdevki in iščejo takšne otroke, ki že v pogovoru z drugimi uporabljajo spolne izraze, nato jih zapeljujejo in na koncu prepričujejo v zmenek v živo (Malesky v Briggs in drugi 2010, 75). Ponujajo jim možnost delanja v manekenstvu, poceni vstopnice na koncerte, zmenke z raznimi zvezdniki ali materialna darila (Home Office 2008, 18). Takšna srečanja se v 98 % končajo s spolnim odnosom ali drugimi vrstami spolnega kontakta (Wolak v Briggs in drugi 2010, 75).

4.3 PROFIL SPLETNEGA NADLEGOVALCA

Briggs, Simon in Simonsen so izvedli analizo 51 obsojenih internetnih spolnih nadlegovalcev otrok. En del nadlegovalcev je na vsak način želel z otrokom imeti fizičen kontakt, drugi del pa je z otrokom delil spolne fantazije in izmenjavo zasebnih spolnih slik, torej je spolno komuniciranje na spletu predstavljalo cilj in ne pot do cilja kot pri prvi skupini (Briggs in drugi 2010, 85). Prestopniki, ki so želeli fizičen kontakt z otroki, so bili mlajši, nikoli poročeni, večinoma nezaposleni in z nižjo izobrazbo kot druga skupina prestopnikov (Briggs in drugi 2010, 86). Nadlegovalci so z otroki komunicirali preko portalov Yahoo, AOL, MSN ali Myspace. 70 % jih je otrokom pošiljalo svoje gole slike, 40 % jih je ob pogovoru masturbiralo, približno 30 % pa je otroke učilo veščine samozadovoljevanja. Takšen odnos z otrokom je v povprečju trajal 20 dni. Prestopniki so približno po treh dneh z otrokom poskušali vzpostaviti fizičen kontakt. Če so se takrat pogovarjali s policistom pod krinko, je v tem času prišlo do aretacije (Briggs in drugi 2010, 82–85).

Osebe, ki na spletu iščejo pornografski material in se naslajajo nad spolnimi slikami otrok, menijo, da s tem delajo dobro, saj preprečijo, da bi otrok trpel v živo, saj so to po njihovem mnenju le slike (Taylor in Quayle 2003, 184). Po drugi strani pa internet omogoča, da pedofili še bolj razvijejo željo po nadlegovanju otrok, kar hitreje vodi v fizično nadlegovanje otroka (Alexy, Burges in Barker 2005, 810). Definirati splošen tip

pedofila je težko, saj je pojem zelo kompleksen in odvisen od mnogih lastnosti osebe (Alexy, Burges in Barker 2005, 811). Spolni prestopniki, ki na spletu komunicirajo z otroki, pa večinoma niso pedofili, saj se običajno pogovarjajo z najstniki, starimi od 13 do 17 let, in ne iščejo kontakta z mlajšimi otroki. Zanje je pomembna vizualna zrelost mladostnika (Briggs in drugi 2010, 74).

Stopnja tveganja, da bi se otrok v živo dobil s starejšo osebo, ki jo je spoznal na internetu, in bil zlorabljen, je kljub temu izredno nizka. Prav tako uporaba spletnih socialnih omrežij, kot sta Facebook in MySpace, ne povišuje tega tveganja. Stopnja tveganja je dvisna od načina uporabe teh omrežij in nevarnih pogovorov z neznanimi osebami o spolnosti, kar povečuje tveganje. Več kot polovica otrok prepozna starejše osebe s spolnimi željami in jih ignorira brez občutka stresa (Nigam in Collier 2010, 11–12). Prav tako večino kriminala nad otroki zagrešijo družinski člani, prijatelji in znanci otrok, ne pa tipična podoba odraslega tujca, ki otroka osvaja preko interneta. Le 8 % kriminala nad dekleti, starimi do 17 let, izvajajo tujci. Ko mladostniki odraščajo, se delež nadlegovalcev, ki so družinski člani, manjša, veča pa se delež znancev. Ena petina kriminalcev so sorodniki, tretjina pa so znanci, ki so večinoma mladostniki. Podoba spletnega zalezovalca tako ne sme zasenčiti kriminalcev, ki so jim otroci izpostavljeni doma ali v ožjem krogu poznanstev (Cassell in Cramer 2008, 58).

5 VARNOST OTROK NA INTERNETU

Ob vsakem pojavu nove tehnologije so starši zaskrbljeni nad možnimi učinki na otroke, še zlasti na mlada dekleta. Še posebej, če tehnologija omogoča neke vrste mobilnost otroka izven nadzora staršev. Sprva je pozornost namenjena kriminalcem, ki se lahko poslužujejo novih tehnologij, nato pa tudi vedenju otrok na spletu, zlasti deklet. Enake reakcije so se pojavile ob izumu telegrafa, telefona in sedaj interneta. Pri tem problema ne predstavlja sama tehnologija, ampak potencialno seksualno vedenje mladostnikov, zlasti deklet, izguba nadzora staršev in moč, ki jo otrok ali dekle pridobi z uporabo interneta (Cassell in Cramer 2008, 70).

Definicija spletne varnosti mladih se je v zadnji desetih letih razširila in postala bolj kompleksna, kar velja tudi za njene uporabnike in tehnologijo. Tako ni nobene univerzalne rešitve za dilemo varnosti otrok na internetu. Potrebni so elementi varnosti, ki ustrezajo starosti in okoliščinam spletnega brskanja posameznega otroka. To so: izobraževanja o varni uporabi, nadzorovalne tehnologije za starše in ponudnike storitev, družinska, šolska ter ustavna pravila in navodila o uporabi interneta. Vsi akterji, vpleteni v produkcijo interneta, imajo vlogo pri ustvarjanju varnega okolja za otroke. Vedno večjo vlogo imajo sovrstniki otrok, ki pomembno pripomorejo k otrokovemu zavedanju in ravnanjem v primeru spletne nevarnosti (Nigam in Collier 2010, 5–18).

Izvajanje nadzora in ukrepov v primeru kršitev zakona je zaradi globalnosti interneta težavno. Žrtev je lahko v eni državi, kršitelj pa v drugi. Oblasti v takšnih primerih težje odreagirajo, saj so fizično oddaljene od kršitelja. Problem so tudi različne zakonske odredbe v posameznih državah in definicije otroštva ter samih kršitev (Hick in Halpin 2001, 7; Jenkins 2011, 6; Yar 2006, 16–17). Zato se mnoge organizacije trudijo ustvariti nek enoten zakon, ki bi se prenesel na vse države. Slednje je težje izvedljivo, se pa mednarodne oblasti v primeru tiralic aktivno povezujejo (Yar 2006, 114). Poleg zakonskih uredb je potrebno izboljšati izobraževanje potencialnih žrtev in kršiteljev ter spremeniti organizacijsko kulturo družbe (Barak 2005, 85).

Internet se je v zadnjih destih letih krepko spremenil, z njim pa tudi naše znanje o tveganjih na internetu in možnostih varovanja mlajših uporabnikov. Še vedno pa velja, da morata ozaveščanje in tehnologija za varno uporabo delovati skupaj (Nigam in Collier 2010, 18–19). Internet prinaša nova tveganja za svoje uporabnike in varnostne izzive, nadzor pa je vseeno povezan z dilemami in nevarnostmi. Največji problem je ravnotežje med nadzorom in zasebnostjo uporabnikov. Po eni strani naj bi izgubili

nadzor nad zbiranjem podatkov in samimi podatki, po drugi strani pa naj bi bil nadzor zaradi velikih tveganj nujen (Yar 2006, 140). Trud za zaščito družbe pred kiberkriminalom dolgoročno prinaša posledice za prihodnost svobode na spletu (Yar 2006, 141).

V letu 2008 je raziskovalne skupine, javnost in politične akterje na tem področju začel skrbeti nov fenomen spletnih socialnih omrežij in v njih skritih nepridipravov. Presenetljivo so ugotovili, da otroke bolj nadlegujejo sovrstniki kot pa neznani odrasli (Nigam in Collier 2010, 4). Na spletu je največ tveganj za otroke, ki so tveganjem izpostavljeni tudi v živo. Zato je potrebno programe proti nasilju na spletu prilagoditi predvsem tem skupinam (Nigam in Collier 2010, 18–19).

5.1 KAJ OTROCI STORIJO V PRIMERU NEVARNOSTI

Otroci se na starše ali starejše sestre, brate obrnejo zgolj takrat, ko nastane kak problem. Pogovor s starejšimi o težavah v povezavi z internetom, tudi če gre za kakšne zlorabe in nadlegovanje, je izhod v sili. Otroke je strah, da bi starši videli vsiljeno vsebino in jih obtožili, da so jo otroci sami poiskali ali pa da bi jim prepovedali brskati po internetu (Directorate general information society and media 2007, 32–34). Podobne rezultate so dobili tudi raziskovalci Sonie Livingstone. Kadar so otroci prejeli sporočila s spolno vsebino, je 27 % otrok poskušalo problem rešiti brez pomoči, 22 % jih ni storilo ničesar in upalo, da bo problem minil. Večina otrok, 40 %, je problematično osebo blokirala ali pa izbrisala neljubo sporočilo. Nekaj, 24 %, jih je spremenilo nastavitve filtra, 18 % pa jih je zaradi tega za nekaj časa nehalo uporabljati internet, problem prijavilo z gumbom za pomoč na spletni strani ali pa so kontaktirali odgovornega za spletno stran (Livingstone 2011, 82–83).

Velika večina otrok, to je kar 60 %, ki so naleteli na takšna sporočila, je o tem z nekom govorila. Prijatelju je poročalo 38 % otrok, 30 % pa staršem, manj otrok je o tem govorilo z drugimi osebami (Livingstone 2011, 82–83). Na Danskem, Cipru in v Sloveniji je več kot 45 % staršev poročalo, da so jih otroci prosili za pomoč pri uporabi računalnika in interneta, kar je največ med državami EU (Directorate general information society and media 2007, 31). Otroci se obrnejo na starše večinoma za pomoč pri drugih težavah z računalnikom ali internetom, le 4 % staršev je imelo izkušnjo, da je otrok prosil za pomoč zaradi spolnega nadlegovanja ali ustrahovanja na

spletu. Le na Nizozemskem in v Angliji je bil delež takšnih staršev okrog 25 %. (Directorate general information society and media 2007, 6).

Kadar so se otroci dobili v živo z osebo, ki je prej niso poznali, in so naleteli na težave, je 30 % otrok ostalo pasivnih in čakalo, da bo problem minil sam. Problem je poskušalo rešiti na drugačen način 18 % otrok. Za 10 % več otrok je po neprijetni izkušnji srečanja v živo za nekaj časa nehalo uporabljati internet, 37 % otrok je izbrisalo vse pogovore s to osebo, skoraj enak odstotek otrok pa je kontakt blokiralo. Le 10 % otrok je težavo prijavilo na spletno stran. Več kot polovica otrok za pripetljaj ali problem ni povedala nikomur, 35 % pa se jih je o tem pogovorilo s prijatelji (Livingstone 2011, 94–95).

Otroci poznajo razne spletne potegavščine, ki so namenjene za zbiranje osebnih podatkov ali vsiljevanje plačila. Prav tako so omenjali fizične nevarnosti interneta. Jasno so bile izražene skrbi nehotenega kontakta s starejšimi osebami, ki bi jih rade zlorabile in jim škodovale. Starejše deklice so omenjale ugrabitve in posilstva, mlajši dečki pa, na primer, umore in poškodbe. Otroci so pogosto eksplicitno omenili »pedofila« kot tisto osebo, ki jim želi škoditi. Izkazalo se je, da otroci dobro poznajo načine, kako se zaščititi pred možnimi zlorabami. Izpostavili so, da je potrebno biti pazljiv, ko se pogovarjaš po internetu, ne izdajati osebnih podatkov in se ne dobivati z neznanci z interneta. Čeprav otroci ta načela poznajo, jih nekateri kršijo. Nekateri so se že dobili z neznanci, ampak v družbi ostalih otrok, ali pa so neznancu izdali, na primer, naslov e-pošte. Na splošno otroci trdijo, da lahko hitro razkrinkajo odraslo osebo, ki se izdaja za mlajšo, saj uporablja drugačno besedišče, izraze in postavlja nenavadna vprašanja. Otroci prav tako poročajo o psihološkem pritisku ali grožnjah, ki so jim bili izpostavljeni na internetu. Mlajši otroci se o tem velikokrat pogovorijo s starši, ki zadevo rešujejo naprej. Otroci so na splošno dobro poučeni o tveganjih uporabe interneta. O tem jih v večji meri poučijo starši, šola ali pa mediji (Directorate general information society and media 2007, 32–37).

V delu raziskave Direktorata za informacijsko družbo in medije so raziskovalci otrokom predstavili anekdoto otroka, ki si dopisuje z drugim otrokom in mu pove svoje osebne podatke, potem pa odkrije, da je ta oseba starejša in da bi mu mogoče lahko škodovala. Otroci so nato povedali svoje misli ob tej zgodbi. Tukaj so otroci veliko bolj odkrito povedali svoje izkušnje kot v prejšnjih delih raziskave, kjer so govorili zgolj o tem, »kako bi naj bilo«. V skoraj vseh skupinah, ne glede na državo, so otroci pripovedovali anekdote, ki so se zgodile njim ali njihovim najbližjim; te so pričale o resničnih,

potencialno nevarnih kontaktih. Očitno je torej, da otroci prevzamejo bolj tvegano vedenje na spletu, kot sami mislijo in povedo, sploh to velja za otroke starejših skupin. Glede na to, da o tem neradi govorijo s starši in odraslimi nasploh, je tega vedenja verjetno več, kot si predstavljamo. Mlajši otroci se tako hitreje in radi obrnejo na starše ali pa na starejše brate ali sestre, medtem ko starejši otroci raje rešujejo probleme sami ali pa s prijatelji. Starši so zanje izhod v sili (Directorate general information society and media 2007, 46–48).

Izmed vseh otrok, ki uporabljajo internet, se jih je 9 % že dobilo v živo z nepoznano osebo z interneta. Srečanje je motilo 11 % teh otrok in jim bilo tudi neprijetno. Čeprav je odstotek mlajših otrok, ki so se kdaj dobili v živo z nepoznano osebo, najmanjši, so ravno ti otroci tisti, ki jih je srečanje največkrat motilo in je bilo zanje neprijetno. Polovica vseh otrok, ki jih je srečanje motilo, je izjavila, da so bili zelo ali še kar vznemirjeni zaradi srečanja. Izmed otrok, ki jih je srečanje motilo, se je 22 % dobilo s starejšim najstnikom/co, 8 % pa z odraslo osebo, to je osebo, staro nad 20 let. Večina otrok je na neljubo srečanje s seboj pripeljala prijatelja/ico. Večina, to je 70 % otrok, je nekomu povedala, kam gre, od tega je 42 % otrok to povedalo prijatelju/ici iste starosti. Ena tretjina pa ni povedala nikomur. Otroke, stare 11 let in več, so vprašali, kaj se je na srečanjih neprijetnega zgodilo. Na to je 22 % otrok poročalo, da jih je oseba zmerjala, 11 % otrok je imelo neko seksualno izkušnjo, 3 % so doživeli fizične poškodbe. Nekateri so rekli, da ne vedo, drugi, da raje ne bi povedali, tretji pa so rekli, da se je zgodilo nekaj drugega hudega (Livingstone 2011, 89–94).

5.2 TEŽAVE PONUDNIKOV SPLETNIH STORITEV PRI ZAGOTAVLJANJU VARNOSTI SPLETNIH STRANI

Ponudniki spletnih storitev so si med seboj različni po stilu, znanju in moči. Nekateri so velike multinacionalne korporacije, kot sta na primer Facebook in MySpace, spet drugi so majhne lokalne organizacije, ki bodo takšne tudi ostale. Poleg teh dveh skupin so še nove neuveljavljene skupine ponudnikov in take s še nepoznanimi produkti. Večja kot je organizacija, boljše lahko poskrbi za varnost na spletni strani in ukrepe ob morebitnih slabih izkušnjah uporabnikov. Za varnost in odzivnost so lahko zadolženi oddelki za delo z uporabniki, varnost ali morda programerska ekipa. Nekatere organizacije pa na tem področju ne storijo ničesar (Aftab 2010, 96).

Za veliko večino ponudnikov je s finančnega vidika težko postaviti ustrezen varnostni sistem za uporabnike, saj morajo izdatki biti čim nižji, če želi ponudnik storitev ponujati brezplačno. Le z brezplačno ponudbo lahko ostanejo konkurenčni ostalim ponudnikom in če si velika večina ponudnikov želi podati čim boljšo rešitev za varnost in odzivnost na probleme uporabnikov, si večji del teh ponudnikov tega ne more privoščiti, kot ugotavlja Aftab (2010, 97). Pred produkcijo portala, sistema in ponudbe je potrebno misliti na varnost, zasebnost in tveganja, kar stori premalo ponudnikov. Večji del ponudnikov se dnevno bori s prilagajanjem tehnologije in ponudbe rasti uporabnikov in pozabijo ali pa ne zmorejo posodobiti in dopolniti varnostnega sistema. Imajo namen vse popraviti in se vrniti k opaženim problemom, kar pa jim zaradi denarja, pomanjkanja časa ali pozabljivosti večinoma ne uspe. Zgodi se tudi, da ne poznajo vseh razsežnosti uporabljene tehnologije in nimajo vseh potrebnih znanj za zagotovitev vseh potrebnih varnostnih ukrepov (Aftab 2010, 97).

Proizvajalci se srečujejo tudi s težavo nadgradnje že dokončanega sistema. Pri razvoju sistema in ponudbe ne pustijo možnosti za spremembe in dopolnjevanje in spreminjanje določenih elementov projekta je zato problematično. Ponudniki ne predvidijo hitrega spreminjanja povpraševanja, tehnologije in zakonskih določil in stroškov, povezanih s tem. Prav tako so o zlorabah otrok na internetu premalo izobraženi. Nevarnih vsebin ne ločijo od sprejemljivih in preveč vsebin tolerirajo (Aftab 2010, 97).

Ponudniki ne vedo, kako naj odreagirajo v primeru zlorabe, saj ni jasnih navodil, prav tako ni jasnih posledic, ki bi doletele tiste ponudnike, ki to prezrejo. Ponudniki uporabnikom zagotavljajo zasebnost in varnost odvzetih podatkov, ki pa bi jo ob morebitni zlorabi in ukrepanju morali kršiti, saj bi podatke morali posredovati preiskovalnim organom ali drugim ustanovam. Ponudniki v večini želijo izpolniti vse zahtevane in zaželene kriterije. Ti problemi jih zanimajo, saj so pogosto starši in podjetniki, vendar je to zanje večinoma pretežko ali nemogoče. Tematiko bi jim bilo potrebno obrazložiti in jim omogočiti, da lahko izpolnijo zahteve brez zmede. Vsi zakoni, ki naslavljajo varnost otrok na internetu, bodo brez tega manj učinkoviti, kot bi lahko bili (Aftab 2010, 97–98).

5.3 HRANJENJE PODATKOV

Varstvo komunikacijske zasebnosti je bolj pravno varovano kot varstvo informacijske zasebnosti (Kovačič 2006, 175). Tehnološke spremembe omogočajo večji nadzor nad uporabo interneta, ki je zagotavljanje nadzorovanja in zasebnosti otežil. Z njimi se lahko spremlja in omeji dejavnost uporabnikov. Posamezniku se odvzame svobodna volja, dodeli pa se mu geslo, ki mu dostop omogoči ali zavrne. Računalnik kot tehnologija omogoča nadzorovanje, ga poglablja in krepi. Omogoča zbiranje in hranjenje podatkov. Globalizacija, konvergenca med tehnologijami in multimedialnost so elementi, ki še posebej ogrožajo zasebnost. Internet predstavlja stično točko med temi tremi elementi in se lahko dojema tudi kot grožnja zasebnosti (Kovačič 2006, 28–29). Podatke lahko zbirajo spletne strani same s piškotki, uradne vladne organizacije ali pa razni filtri, na primer filtriranje pošte (Yar 2006, 143–146).

Odgovorne osebe lahko izsledijo iskano osebo, ki je preko interneta zagrešila zločin le, če imajo možnost to osebo identificirati. V ta namen se išče internet protokol naslov (v nadaljevanju IP) osebe, ki ji ga je dodelil ponudnik internetnega dostopa (v nadaljevanju PID), datum in čas obiska strani. Podatke pa bi naj shranjevali tudi ponudniki spletnih storitev (v nadaljevanju PSS), sem spadajo tudi ponudniki spletnih socialnih omrežij in klepetalnic. Podatki, ki jih posredujejo PID in PSS, lahko imenujemo »izvirni podatki«. Ti odgovornim osebam omogočajo sledenje viru kriminalne spletne komunikacije. Brez teh podatkov začetek raziskave kriminalnega dejanja ni možen. Pomemben je tudi čas hranjenja podatkov, ki je od podjetja do podjetja različen. Nekatera podjetja shranjujejo podatke do nekaj tednov, spet druga več mesecev ali let. Velikokrat so kriminalna dejanja odkrita veliko pozneje, kot so se dejansko zgodila, zato so podatki v večini primerov že izbrisani (Nigam in Collier 2010, 100–105).

Da bi podatki bili koristni oblastem, bi morali PID in PSS ponudniki hraniti podatke dovolj dolgo časa in bolj konsistentno. Pomemben element varnosti so tudi »proxy serverji«, to so računalniki, ki prejemajo, modificirajo in prenašajo spletno komunikacijo tako, da prikrijejo izvoren IP in ga nadomestijo z drugim. Ti »proxy serverji« bi morali spremljati in shranjevati IP uporabnika, ki je vstopil na internet in IP, ki ga je ta uporabnik ob vstopu prejel. Tako bi lahko oblastem podali identiteto uporabnika ob morebitnih kršitvah (Nigam in Collier 2010, 105–106).

Hranjenje in beleženje osebnih podatkov, v tem primeru sledenje uporabnikom, je vedno kontroverzno. Zastavlja se vprašanje, ali je tak ukrep sorazmeren ali pa

neupravičeno posega v pravice posameznika (Kovačič 2006, 204). Dostop do teh podatkov bi naj tako imele le uradne osebe, zadolžene za raziskovanje kriminalnih dejanj. Podatki bi morali biti zaščiteni pred vdorom neavtoriziranih oseb, zlorabami in preprodajo (Kovačič 2006, 173; Nigam in Collier 2010, 106). Predstavniki ponudnikov storitev so glede takšnega zbiranja in hranjenja podatkov skeptični. Navajajo, da bi pred takšnim zbiranjem podatkov bilo treba preveriti efektivnost takšnega zbiranja. Prav tako bi bilo potrebno bolj natančno določiti primere, v katerih so uradne osebe do teh podatkov upravičene. Glede na majhno število primerov, v katerih so takšni podatki potrebni, bi lahko bile ogromne količine teh podatkov nepotreben vir zlorab (Kovačič 2006, 173; Nigam in Collier 2010, 108–112). »Podatki kažejo, da se zakoniti nadzor interneta v Sloveniji uporablja minimalno in da preiskovalci praviloma ne naletijo na primere, ko ponudnik dostopa do interneta sodne odredbe ni mogel izpolniti« (Kovačič 2006, 204). Hranjenje podatkov tako zahteva ravnotežje med potrebami uradnih oseb po podatkih uporabnikov, zasebnostjo in varnostjo uporabnikov ter stroški in možnostmi ponudnikov spletnih storitev, povezanimi s hranjenjem in arhiviranjem teh podatkov (Nigam in Collier 2010, 116).

Nekatera gibanja so mnenja, da internet omogoča osvoboditev posameznika od države in je zaradi svoje narave odporen proti nadzoru. Demokratični potencial bi naj bilo tako možno uničiti zgolj s prepovedjo uporabe. Tehnologije nadzora so kljub temu zelo razširjene in družbeno sprejemljive. Brez njih vključitev v spletni svet skoraj ni več možna. Množični nadzor podatkov s tem postaja rutina. Identifikacija tveganja, priložnosti in ciljnih skupin postaja ključna. Posledica je razvrščanje posameznikov v kategorije. Kategoriziranje, predvidevanje in preventiva so vedno bolj pomemben element pri razvoju nadzorovalnih sistemov. Tveganje ali priložnost, ki ga skupina ljudi predstavlja za organizacijo, je bolj pomembno kot krivda ali nedolžnost posameznika (Kovačič 2006, 209–214).

5.4 VARNOST SPLETNIH KLEPETALNIC IN SOCIALNIH OMREŽIJ

Starši in drugi odrasli so se začeli vedno bolj zavedati nevarnosti spletnih družabnih omrežij in klepetalnic, zato so začele nastajati strani, namenjene samo otroškemu občinstvu. Med njimi so se, poleg takih, ki so ponujale video igre, potrošni material in druge interesne dejavnike, našle tudi klepetalnice in forumi. Forumi so zlasti popularni, ker si mladostniki lahko izmenjujejo mnenja in izkušnje, v klepetalnicah pa spoznavajo

nove ljudi (Yar 2004, 4). Internet je ustvaril svobodno okolje za otroke, kjer imajo otroci kontrolo nad svojimi računalnikom in socialnim komuniciranjem. Pri tem je zelo pomemben element anonimnost, ki omogoča brezskrbno izražanje in vedenje, zaradi česar se uporabniki lahko sprostijo. Žal pa je prav ta dejavnik razlog, da prihaja do nasilnih vsebin in groženj, za katere nihče ne prevzema odgovornosti. Anonimnost uporabnikom omogoča zavajanje, zaradi česar lahko zlasti otroci in mladostniki zaidejo v težave (Moinian 2006, 55–66).

Otroške klepetalnice in forumi naj bi bili otrokom prijazni in varni. Za varnost skrbijo različni mehanizmi. Obstajajo tudi programi, ki jih starši lahko instalirajo na računalnik in s tem otroku preprečijo dostop do določenih strani in funkcij, beležijo pa se tudi podatki o uporabi interneta in spletnih strani (pr. Starr007, Parents friend…). Vendar so še premalo razviti, saj lahko preprečijo vstop tudi na kakšne uporabne strani ali pa ne prepoznajo kakšne neprimerne strani, zato je nadzor staršev še vedno potreben. Za uspešen boj proti prežečim nevarnostim na internetu je tako potreben nadzor vlade, industrije in staršev, kjer je najbolj pomembna ustrezna definicija nevarnih vsebin (Oswell, 1999).

»Dobre« spletne strani za otroke naj bi imele nasvete o varnosti med klepetanjem in varnostna orodja ter mehanizme, ki omogočajo prijavo neprimernega vedenja ali nevarnosti. Med varnostna orodja spada ponudnikovo vzdrževanje reda v klepetalnici ali omrežju, gumb za blokiranje ali ignoriranje uporabnika, ki otroku želi škoditi, in možnost prijave neprimernih vsebin pogovora nadzorniku ali ponudniku strani. Navodila za varno uporabo strani morajo biti jasno vidna in napisana na razumljiv način. Ponudniki spletnih strani naj bi objavili tudi povezave do spletnih strani, ki varno uporabo interneta razlagajo bolj natančno (Childnet international 2009, 3). Primer v Sloveniji sta npr. Safe-si ali Spletno oko.

Najbolj pogost način varovanja takšnih otroških spletnih strani je uporaba nadzora oziroma moderiranja (angl. Moderation), ki predstavlja pomemben del varnosti spletne strani. To je proces, pri katerem oseba ali tehnološki filter pregleduje vsebino vnesenih pogovorov. Z moderiranjem se lahko odstrani neželene, žaljive ali neprimerne vsebine pogovorov. Tehnološko moderiranje je računalniški program, ki iz pogovorov samostojno izloča besede ali fraze, ki so bile določene. Običajno so to osebni podatki, telefonske številke ali naslov spletne pošte. Človeško moderiranje opravljajo nadzorniki oziroma moderatorji. Ti lahko po lastni presoji odstranijo vsebino, opozorijo uporabnika in ga po potrebi izključijo iz klepetalnice ali strani. Različni načini izvajanja moderacije

nudijo različne stopnje varnosti. Eden izmed načinov je pre-moderacija, kjer se vsa vsebina preveri pred objavo, lahko pa se izvaja tudi post-moderacija, kjer se vsebina objavi takoj, neustrezna vsebina pa odstrani naknadno. Pri vzorčni post-moderaciji se pregleda le vzorec pogovorov, pri reaktivni pa je moderator uporabnikom na voljo ves čas. Zaenkrat tehnološka moderacija še ni tako učinkovita kot človeška (Childnet international 2009, 4).

5.4.1 PRIPOROČILA PONUDNIKOM SPLETNIH STORITEV ZA OTROKE

Za ponudnike spletnih storitev za otroke je priporočljivo, da sodelujejo s starši, izobraževalnimi ustanovami, vlado in vladnimi organizacijami, policijo, civilno družbo ter uporabniki svojih storitev (European Commission 2009, 5). Evropska komisija je leta 2009 izdala uradni dokument s sedmimi priporočili, namenjenimi ponudnikom spletnih storitev za otroke:

1. Osveščanje uporabnikov, učiteljev in staršev o varnosti in primerni uporabi storitev na internetu na jasen in starosti primeren način.

Ponudniki spletnih storitev naj bi svojim mladim uporabnikom nudili jasen in njim namenjen izobraževalni material, ki bi jim omogočil varno uporabo spletne strani. Takšna vsebina mora biti razumljiva, objavljena na mestih, kjer uporabniku pride prav ali pa jo ta lahko hitro in enostavno najde. Nezaželeno vedenje in njegove posledice morajo biti jasno navedene, po možnosti ne pod pogoji uporabe. Ponudnik pa mora na strani nagovoriti tudi starše in izobraževalne vsebine ali povezave nuditi tudi zanje (European Commission 2009, 6).

2. Storitve naj bodo primerne za ciljno starost uporabnikov.

Ponudniki morajo pri gradnji strani in ponujenih storitvah upoštevati kakšne nevarnosti lahko sledijo za mlade z uporabo teh storitev in možnost izpostavljenosti neprimernim vsebinam ali kontaktom čim bolj zmanjšati. V ta namen si lahko ponudniki storitev pomagajo z naslednjimi priporočili, po katerih morajo:

- jasno opredeliti, katere vsebine niso primerne za določeno starostno skupino, in kdaj je primerno določiti minimalno starost uporabnika;
- iznajti mehanizme za odkrivanje in odstranitev premladih uporabnikov;

- iznajti mehanizme, ki premladim uporabnikom onemogočijo ponovni poskus prijave na stran z navedbo drugačne starosti, npr. z uporabo piškotkov;
- s tehničnimi in pravnimi mehanizmi obrazložiti in promovirati nujnost določitve minimalne starosti;
- podpirati in oglaševati nujnost nadzora staršev nad uporabo storitve;
- nuditi mehanizme, ki uporabnikom, staršem in ostalim omogočijo označitev, oceno ali omejitev vsebine, kjer je to potrebno;
- objavljanje nekaterih vsebin le v določenem delu dneva (European Commission 2009, 2–3).

3. S pomočjo spletnih orodij in tehnologije uporabniku dati moč.

Mladostniki in otroci morajo imeti možnost nadziranja in upravljanja s storitvami, ki so jim namenjene. Merila, ki lahko zmanjšajo neprimeren kontakt med otroki ali mladostniki in odraslimi:

- zagotoviti, da profilov mlajših otrok ali mladostnikov ni mogoče najti v iskalnikih;
- v osnovnih nastavitvah za mlajše uporabnike nastaviti najvišjo mero zasebnosti;
- možnost nastavitve profila na zasebno obliko naj zajema največjo možno mero zasebnosti;
- uporabnikom dati možnosti izbire, kdo lahko vidi njihov profil, in omogočiti blokiranje ali zavrnitev prošenj za prijateljstvo;
- uporabnikom nuditi možnost izbire o objavljanju komentarjev prijateljev na njihovem zidu in možnost izbrisati neželene komentarje;
- uporabnikom omogočiti urejanje objav drugih uporabnikov na njihovem zidu, preden se te objavijo;
- nuditi enostavna orodja, ki omogočajo prijavo neprimernih vsebin in kontaktov;
- izobraževanje staršev o spletnih orodjih za večjo varnost otrok (European Commission 2009, 7–8).

4. Nuditi enostavne mehanizme za prijavo neprimerne vsebine, ki ni v skladu s pogoji uporabe strani.

Takšna orodja morajo biti enostavna za uporabo, napisana na razumljiv način in redno obravnavana. Uporabniki morajo imeti na voljo navodila za uporabo teh orodij in informacije o načinu obravnave teh prijav (European Commission 2009, 8).

5. Ponudnik se mora na morebitne prijave kršitev odzvati.

Ponudnik mora za morebitne prijave uporabnikov imeti zagotovljene učinkovite mehanizme za pregled prijav in izvedbo ukrepov. Prav tako naj bi za takšne primere imeli ustaljene postopke sodelovanja z oblastmi in klicnimi centri, kar je odvisno od pravne ureditve v posamezni državi. Priporočljivo je na stran vključiti povezave do strani uradnih represivnih organov in nujne telefonske številke v primeru nevarnosti, kot je npr. 112 (European Commission 2009, 8).

6. Uporabnikom omogočiti varnost osebnih podatkov in jih vzpodbujati k premišljenem ravnanju z njimi.

Uporabnikom je potrebno nuditi možnost varovanja njihovih osebnih podatkov z varnimi nastavitvami profilov in jih o tem tudi informirati. Uporabnik mora vedno imeti možnost enostavnega urejanja varnosti in zasebnosti svojega profila. Prav tako ga je potrebno obvestiti, kako se bo njegove osebne podatke uporabilo (European Commission 2009, 9).

7. Ponudnik mora nadzorovati spletno stran in onemogočiti neprimerno vsebino ali vedenje.

Ponudniki morajo spletne strani redno pregledovati in morebitna tveganja za uporabnike izločiti. Za nadzor spletne strani imajo več možnosti:

- človeški ali tehnološki nadzor oz. moderacijo,
- tehnična orodja za označitev in detekcijo neprimernih vsebin, npr. razne filtre,
- sistem za javljanje nevarnosti,
- poročila uporabnikov.

Pri človeški moderaciji je potrebno izbrati primerno in zanesljivo osebo, saj ima ta neposreden dostop do otrok in njihovih podatkov (European Commission 2009, 9).

6 METODOLOGIJA

Teoretični del magistrske naloge je sestavljen iz sekundarnih podatkov, v nadaljevanju pa sem zbrala tudi primarne podatke za vpogled v varnost spletnih strani za otroke. Uporabila sem kvalitativno raziskavo varnosti na različnih spletnih klepetalnicah in omrežjih, namenjenih zgolj otrokom ali najstnikom. Raziskava je potekala v avgustu 2013 in je zajemala namenski neverjetnostni vzorec desetih spletnih strani. Izbrala sem jih z vpisom besednih zvez v iskalnik Google, ki je med najbolj uporabljanimi spletnimi brskalniki na svetu (Ebizmba 2013). Najprej sem v iskalnik vpisala besedne zveze v slovenskem, nato v angleškem in na koncu še v nemškem jeziku. Besedne zveze so se navezovale na temo spletnih klepetalnic in pogovorov. Uporabljene besedne zveze so bile: *klepetalnica, otroška klepetalnica, kids chat* in *kinder chat*. Izbrala sem klepetalnice, namenjene zgolj otrokom in mladostnikom, ki so bile med prvimi desetimi zadetki v brskalniku. Za takšen vzorec sem se odločila, ker sem sklepala, da sem s tem dobila med otroki najbolj uporabljene strani, nanje pa med prvimi naletijo tudi možni nepridipravi.

Najprej sem na vsaki strani preiskala ukrepe za varnost otrok. Seznam sem sestavila na podlagi priporočil Evropske komisije in dobrodelne organizacije Childnet International. Zabeležila pa sem tudi morebitne druge ukrepe strani.

Pri vsaki spletni stran sem preverila naslednje trditve:

- klepetalnica deluje le določen del dneva;
- na voljo so informacije o varni uporabi spletne storitve za učitelje in starše;
- ponudnik storitve vzpodbuja starše in učitelje k večji kontroli otrok in mladostnikov pri uporabi storitve;
- na voljo so informacije o varni uporabi spletne storitve;
- informacije o varni uporabi so napisane na jasen in otrokom razumljiv način;
- informacije o varni uporabi spletne storitve so objavljene na mestu, kjer uporabnikom najbolj koristijo, ali pa je povezava do njih jasno vidna;
- objavljena je povezava do spletnih strani, ki so namenjene osveščanju mladih o varni uporabi interneta, ali drugih povezavanih organizacij, ki nudijo pomoč otrokom v stiski;

- na strani je povezava do represivnih organov (npr. policija) ali njihova telefonska številka;
- ponudnik vzpodbuja uporabnike k premišljenemu ravnanju z osebnimi podatki;
- stran omogoča varovanje osebnih podatkov;
- nezaželeno vedenje na strani je jasno opredeljeno;
- jasno so opredeljene posledice neželenega vedenja;
- ponudnik omogoča uporabo storitev le uporabnikom določene starosti;
- spletna stran ima mehanizme za odkrivanje in odstranjevanje uporabnikov, ki zaradi starosti ne morejo uporabljati storitev, ki so namenjene otrokom;
- uporabnikom neprimerne starosti je ponovna prijava onemogočena;
- na strani je obrazloženo, zakaj je starostna omejitev prisotna;
- stran ponuja enostavna orodja za prijavo neprimernih vsebin in kontaktov;
- stran ponuja navodila za uporabo orodij za prijavo neprimernih vsebin in kontaktov;
- ponudnik nadzira spletno stran z uporabo človeške moderacije;
- ponudnik nadzira spletno stran z uporabo orodij za označitev neprimernih vsebin;
- ponudnik nadzira spletno stran z uporabo tehnološke moderacije;
- stran omogoča označitev neprimerne vsebine;
- stran uporabnikom omogoča podati mnenje ali poročilo o delovanju in varnosti strani.

Nato sem navedene trditve spletnih strani kot uporabnica tudi preverila. Pri tem sem uporabila tehniko skrivnega nakupovalca, kjer raziskovalec preizkusi izdelek ali storitev brez vednosti ponudnika storitve (MSPA North America). Zaradi etičnih razlogov, omenjenih v naslednjem poglavju, sem na straneh, kjer je bil možen zasebni pogovor, ustvarila dva profila (uporabniška imena), ki sem ju uporabljala hkrati, vsakega na svojem računalniku. Tako sem lahko pošiljala zasebna sporočila med tema dvema profiloma in videla, kako so otroci zavarovani med zasebnim pogovorom z drugo osebo. S tem v svojo analizo nisem vpletala otrok. Zaradi možnega shranjevanja pogovorov na strežnike ponudnikov in v izogib nesporazumom sem v pogovor med mojima dvema profiloma vnesla sporočilo »*Chat test for study purposes on safety for children in chat rooms. Student, Department for Social Informatics, Faculty for Social Scienses Ljubljana. Interaction between Test profiles Lili1 and Lulu1*. Nato sem vnašala besede *address, street, sex, msn, young* in *fuck*. Enako sem naredila v nemškem jeziku. Kadar nisem vedela, ali je v klepetalnici prisoten moderator, sem uporabnike v javnem

delu klepetalnice o tem povprašala. Drugačnih načinov preverjanja prisotnosti moderatorja zaradi etičnih razlogov nisem uporabljala. Na koncu sem varnostne elemente različnih spletnih strani in njihovo preizkušeno učinkovitost med seboj primerjala.

6.1 ETIČNOST UPORABLJENE METODOLOGIJE

Vsak raziskovalec se mora najprej odločiti, ali bo sledil teleološki ali deontološki etični paradigmi. Za teleologe je dejanje etično, če so njegove posledice pozitivne za čim več ljudi. Deontologi pa na prvo mesto postavljajo pravice posameznika, saj za skupno dobro hitro pride do zlorab posameznih vpletenih (Kimmel v Malnar 2010, 7). Pri vprašanju etičnosti sem se oprla tudi na Kodeks profesionalne etike Slovenskega sociološkega društva, ki poudarja upravičenost raziskovanih oseb do zasebnosti in dostojne obravnave. Ker me v raziskavi niso zanimali otroci ali druge osebe, sta bila zaupnost in anonimnost zagotovljena. Prav tako internetno okolje kot tako ni vplivalo na rezultate, saj sem opazovala internetni pojav in ne osebe, ki so v njega vpletene.

Kodeks v nadaljevanju določa, da »v teku raziskovanja oseb ne smemo izpostavljati večjemu tveganju ali jim osebno škodovati. V primeru, da tveganje lahko predvidimo, moramo prizadeto osebo s temi možnostmi izčrpno seznaniti, še preden si zagotovimo njen pristanek za sodelovanje« (Slovensko sociološko društvo, 1. člen). Haggerty (v Malnar 2010, 12) opaža, da se raziskave brez privolitve vedno bolj omejuje, s čimer nastaja velika spoznavna škoda. Po drugi strani pa Hinejeva trdi, da privolitev posameznikov lahko prinese nova spoznanja in poglede na raziskovano tematiko (Hine 2004, 2)

Pomembno se je torej vprašati, kako zastaviti raziskavo tako, da bodo tveganja in negativni učinki čim manjši. Pri raziskavah z otroki bo vedno prisotno nekaj neugodja. Težko je določiti mejo med sprejemljivimi tveganji in dobrobitom za otroke. Prav tako je treba otrokom na njim razumljiv način obrazložiti, pri čem sodelujejo in da je sodelovanje prostovoljno (Helseth in Slettebo 2004, 305). Jezik sporočanja mora biti prilagojen otrokovi stopnji razumevanja (Lobe in drugi 2007, 21). Še posebej je potrebno biti pazljiv pri pisnih sporočilih, kjer so otroci obveščeni v pisni obliki in je težje preveriti, če so otroci sporočilo razumeli. Na splošno spletno raziskovanje zastavlja etična vprašanja z enakimi temelji, kot jih poznamo pri tradicionalnem načinu

raziskovanja izven spleta, zato jih ne moremo uvrščati v posebno kategorijo in jih ločevati od ostalih (Thomas v Lobe in drugi 2007, 33).

6.2 OMEJITVE RAZISKAVE

Raziskave ne gre posploševati na celotno ponudbo klepetalnic in socialnih omrežij za otroke, saj je vzorec za to premajhen. Prav tako bi bilo potrebno predhodno opraviti raziskavo o tem, na kakšen način otroci in mladostniki na spletu iščejo klepetalnice. Torej kakšne besedne zveze za to uporabljajo in ali so kakšne klepetalnice še posebej priljubljene. Težko sem preverjala tudi delo moderatorjev, saj je to z etičnega vidika do otrok v klepetalnici sporno. Potrebno bi bilo namreč podajati neprimerne komentarje in izjave, ki bi lahko negativno vplivali na otroke.

7 REZULTATI RAZISKAVE

Spletne strani so opisane po vrsti, kot so se pojavljale v spletnem brskalniku. Pri opisu posamezne strani sem najprej navedla splošen opis in namen strani, nato pa še posebnosti in dodatna pojasnila glede varnostnih ukrepov. Ostali ukrepi za varnost strani po priporočilih Evropske komisije so navedeni na koncu v Tabeli 7.1. V naslednjem poglavju sem rezultate raziskave tudi analizirala in med seboj primerjala.

1. Modri Jan

URL: http://klepetalnica.modri-jan.si/

Je edina slovenska spletna stran s klepetalnico, namenjeno otrokom, ki sem jo našla med zadetki. Je v lasti Holdinga Slovenskih elektrarn. Poleg klepetalnice ima za uporabnike veliko informacij o ekološkem ravnanju z viri energije, ki jih predstavi na otrokom zelo prijazen način, otroške spletne igre, pobarvanke, nagradne igre in druge dejavnosti za otroke. Na podstrani za starše in učitelje je vabilo šolam in vrtcem za sodelovanje pri ekoloških projektih in brezplačna istoimenska ekološko osveščena revija za otroke. Vse njene številke so na voljo za brezplačen ogled, revijo pa se lahko preko strani brezplačno tudi naroči.

Navodila za varno uporabo so vidna in dostopna le v desnem zgornjem kotu z belo barvo in malim tiskom. V sami klepetalnici ni nobenih navodil ali možnosti ukrepanja za uporabnike ob neprimerni vsebini. Klepetalnica deluje od ponedeljka do petka od 14. do 17. ure. Je pod nadzorom moderatorja, ki ga ob mojem obisku nisem zaznala. Za vstop v klepetalnico se lahko ustvari profil ali pa se zgolj navede vzdevek. Če uporabnik nima profila, se ob vsakem obisku klepetalnice samodejno prijavi z vzdevkom in likom, ki si ga je prvič izbral. Na strani zbirajo piškotke ob prijavi. Na spletni strani ni navedeno, kateri starostni skupini otrok je stran namenjena. Prav tako ni takšne omejitve za klepetalnico. Klepet se pojavlja v obliki oblačkov. Zasebnega pogovora ni. Informacije o varovanju podatkov so napisane samo na dnu strani, z majhnim tiskom. Povezava na Safe-si. je pozicionirana neopazno na dnu strani.

2. Kids chat

URL: http://www.kidschat.net/

Stran ima zgolj funkcijo spletne klepetalnice. Osnovna stran grafično ni tako prijazna, kot je Modri Jan. Namenjena je starejšim otrokom in najstnikom. Sama klepetalnica je oblikovana v drugačnem stilu kot osnovna stran, del programske opreme je 123 flash chat, ki se ga lahko doda na katerokoli stran.

Uporabnik lahko izbere sličico, ki se nahaja ob vzdevku, in sporočila tudi nariše z grafičnim oblikovalcem. Starost uporabnikov je omejena na 13 do 19 let. Prijavi se lahko kdorkoli, samo z vnosom gesla. Uporabniku ni potrebno podati nobenih informacij, niti starosti. Lahko pa informacije doda kasneje, ko je že v klepetalnici. Čeprav so na strani prepovedani neprimerni vzdevki in kletvice, se ti redno pojavljajo v klepetalnici. Moderatorjev v času, ko sem bila jaz prijavljena na stran, ni bilo, prav tako ni bilo nobenih sankcij za neprimerno vedenje uporabnikov. Uporabnik lahko blokira določene uporabnike, ki se s tem uvrstijo na seznam blokiranih uporabnikov. Ta seznam lahko uporabnik med nastavitvami ureja. Med nastavitvami klepetalnice se lahko onemogoči tudi prejemanje zasebnih sporočil. Ob kliku na ime drugega uporabnika sem lahko videla njegovo ime, starost in lokacijo, če je uporabnik te podatke vnesel v profil.

3. Kids chat – chat for kids and youth

URL: http://www.chat-avenue.com/kidchat.html

Tudi ta stran ima le funkcijo spletne klepetalnice. Starostna skupina, ki ji mora uporabnik pripadati, na uvodni strani ni navedena, Za vstop v klepetalnico je potrebno vnesti datum rojstva. V kolikor starost ni ustrezna, se uporabnikov vpis zavrne in pojavi se obvestilo, da je za vstop potrebno biti star med 13 in 16 let. Uporabnik, ki je vnesel napačno starost, se ne more več vpisati. Po izbrisu piškotkov pa je ponoven vpis vseeno mogoč. Uporabnik po vnosu datuma rojstva izbere vzdevek in se prijavi v klepetalnico. Tudi ta stran uporablja programsko opremo 123 Flash chat, zato so v tej klepetalnici pogoji uporabe enaki kot na strani Kids chat. Moderatorji bi naj bili prisotni, ampak nikjer ni navedeno kdaj. Preostali čas je klepetalnica nezavarovana.

4. Kidz World

URL: http://www.kidzworld.com/chat

Je spletno socialno omrežje, ki omogoča uporabnikom kreiranje profila, pisanje blogov, poezije, igranje spletnih iger in druge aktivnosti. Imajo zavarovano klepetalnico in forum. Stran je prijetnega izgleda in otrokom prijazno zasnovana. Namenjena je otrokom, starim med 9 in 17 let.

Klepetalnica deluje vsak dan, med 11. in 17. uro, zavarovana je z moderatorjem. Ponudnik navaja, da je stran zavarovana s sistemom za prepoznavanjem vedenja, kar pa ni natančno razloženo. Čeprav stran zelo izčrpno navaja varno uporabo storitev za otroke in starše, so povezave do informacij slabo pozicionirane, saj so vidne samo na dnu strani. Za uporabo klepetalnice se je potrebno registrirati. Z registracijo lahko uporabnik dostopa tudi do ostalih vsebin na strani. Potrebno je podati ime, prvo črko priimka, spol, starost, naslov spletne pošte in kraj bivanja. V kolikor se prijavlja oseba, mlajša od 12 let, ponudnik zahteva le starost, spol, lokacijo in elektronsko pošto starša ali skrbnika. Starš ali skrbnik prejme potrditveno sporočilo, na katerega mora odgovoriti. V kolikor se to ne zgodi v 21 dneh, se prošnja izbriše. Ob vstopu v klepetalnico se uporabniku pokaže navodilo, kako blokirati uporabnika. Zasebna sporočila niso možna. Ob mojem obisku strani moderatorjev ni bilo.

5. Kidscom

URL: http://www.kidscom.com/

Je stran, ki nudi poleg klepetalnice tudi spletne igre in izobraževanje za otroke. Delno je zasnovana kot virtualni svet. Izgled strani motijo velika reklamna sporočila. Del vsebin je plačljiv, poleg tega se uporabnikom za njihovo aktivnost podeljujejo točke, ki omogočajo nekatere dodatne storitve. Na voljo je tudi spletni denar, ki ga lahko kupijo starši. Ta omogoča uporabniku, da kupi pohištvo, oblačila in hrano za svoj spletni lik.

Na osnovni strani so informacije o varnosti, namenjene staršem in učiteljem.

Stran omogoča zasebno sporočanje samo med člani s plačljivim profilom, ki imajo za to dovoljenje staršev. Uporabnik mora registracijski list natisniti, starši ga nato podpišejo in pošljejo ponudniku. Za osnovno registracijo je potrebno podati ime, vzdevek, ki se ga izbere iz danih predlogov na strani, spol, starost in kraj bivanja. Stran omogoča registracijo tudi starejšim uporabnikom.

V klepetalnici filter onemogoča objavljanje prepovedanih besed, na primer: naslov, msn, kletvice in razni izrazi, povezani s spolnostjo. Navodila za uporabo klepetalnice in varnostni nasveti za otroke so objavljeni na prvi strani klepetalnice, ki je oblikovana kot virutalni prostor, v katerem se posamezni liki v obliki oseb med seboj srečujejo. V kolikor se uporabnik ne vede v skladu s pravili, se ga izključi za en dan ali dlje. Uporabnik ima na voljo gumb, kjer lahko prijavi uporabnika. Izpiše se obrazec, kjer se vnese ime uporabnika in razlog prijave. Prijave pregledajo moderatorji. Uporabnik lahko v klepetalnici na podobnem obrazcu predlaga tudi besede, ki naj se jih doda na seznam prepovedanih besed. Tudi te predloge pregledajo moderatorji. Uporabnike, ki v klepetalnici dlje časa niso aktivni, se samodejno izpiše iz klepetalnice. Čeprav bi naj bili moderatorji prisotni, jih nisem zaznala.

6. Kinderchat

URL: http://www.kinderchat.ch/

Sam izgled strani otrokom ni prijazen in je nekoliko staromoden. Stran je namenjena uporabnikom do 18. leta. Stran, poleg klepetalnice, ponuja tudi spletne igre, forum, kviz, blog, zmenkarije in druge rubrike.

Klepetalnica je na voljo od 8. do 24. ure. Informacije o varnosti na spletu in uporabi klepetalnice za otroke in starše so sicer izčrpne, a navedene čisto na dnu strani. Med drugim so na istem mestu navedene tudi povezave do drugih strani in klicnih centrov, ki nudijo pomoč. Za obisk klepetalnice se je potrebno registrirati z vzdevkom, geslom, naslovom spletne pošte in starostjo. Registracija poteka brez pošiljanja potrditvene povezave na spletni poštni naslov uporabnika. Z istim naslovom spletne pošte sem lahko ustvarila več profilov. V klepetalnico lahko vstopa tudi uporabnik, ki je starejši od 18 let, saj ni mehanizmov, ki bi to preprečili. Ker sem v klepetalnici bila sama, sem preizkusila vpisati neprimerne besede. Objavile so se vse besede, na strani ni bilo nobenega moderatorja. Tudi možnosti za prijavo neprimernih besed ni bilo.

7. Seitenstarke

URL: http://seitenstark.de/

Je v prvi vrsti iniciativa, ki združuje preko 50 različnih spletnih strani, namenjenih otrokom. Njihov cilj je varna spletna izkušnja otrok. Otrokom nudijo različne spletne aktivnosti, od spletnih iger do informativnh vsebin. Na strani pa, pod okriljem maskote po imenu Pepe, deluje tudi spletna klepetalnica. Izgled strani je otrokom prijazen in prijeten. Struktura strani je zelo pregledna in jasna.

Klepetalnica je odprta od ponedeljka do petka med 14. in 19. ter v soboto med 14. in 16.30. uro Namenjena je otrokom, starim med 8 in 16. let. Navodila so na strani opisana zelo jasno, so dobro pozicionirana in otrokom primerna, kljub temu pa posledic neupoštevanja pravil ni navedenih. V klepetalnici so moderatorji, ki so na strani tudi predstavljeni. Za obisk klepetalnice se je potrebno registrirati, za kar sta potrebna le vzdevek in geslo. Nato je za vstop v klepetalnico potrebno počakati, da moderator potrdi primernost vzdevka. Če uporabnik dlje časa ni aktiven v klepetalnici, se ga samodejno izključi. Moderatorji so vedno prisotni in odgovarjajo na vprašanja. Klepet je »pre-moderiran«, kar pomeni, da je vsa vsebina pred objavo pregledana.

8. Kinderchat

URL: http://www.kids-chat.eu/

Na strani delujejo: klepetalnica, forum, spletne igre in funkcija pridobivanja spletnih kovancev za kupovanje spletnih dobrin virtualnim likom. Na prvi pogled je to neresna stran, ki pa ima zelo dobro opredeljen in natančno razložen varnostni sistem.

Klepet je na voljo od 8. do 23. ure. Registrirajo se lahko le uporabniki, ki imajo dovoljenje staršev. Ob registraciji se staršem pošlje sporočilo po spletni pošti. Otrok mora biti star med 6 in 17 let. Preden se lahko uporabnik prijavi v klepetalnico, se njegovi podatki registracije preverijo. To ne traja več kot en dan. Nato dobijo starši po spletni pošti povezavo za aktivacijo profila otroka in varnostno šifro. Ob vstopu v klepetalnico ima novi uporabnik zeleno obarvan vzdevek in za vzdevkom črko N, da se ga lažje spozna. Po šestih urah primerne uporabe klepetalnice dobi možnost pošiljanja zasebnih sporočil in drugih funkcij. Če želi uporabnik ustvariti novo sobo v klepetalnici, mora to sporočiti ekipi klepetalnice, ki preveri primernost imena sobe.

Klepetalnica ima besedni filter, v katerem je več kot 50 besed. V kolikor poskuša uporabnik ta filter zaobiti, se ga izključi. Na strani je tudi filter, ki prepozna povezave do raznih prepovedanih strani. Če uporabnik poskuša objaviti takšno povezavo, je samodejno izključen. Na strani se uporabnikom med klepetom vsakih 20 minut pojavljajo nasveti za varno uporabo strani. V vsaki sobi se za uporabnike nahaja gumb s funkcijo klica na pomoč. Ob aktivaciji gumba se otroku prikaže obrazložitev, kaj ta gumb povzroči, ob ponovnem kliku pa se njegovo sporočilo posreduje vsem prisotnim moderatorjem v klepetu. Moderatorji imajo ob vzdevku veliko črko T. To so lahko administratorji, nekateri uporabniki in določene druge odrasle osebe. Prav tako je v glavni sobi prisoten klepetalni robot, ki samodejno odgovarja na določena vprašanja uporabnikov in reagira na določene prekrške uporabnikov. Uporabniki lahko tudi izpolnijo določene formularje, ki se pošljejo ekipi klepetalnice. Ekipa nato te formularje pregleda in ustrezno ukrepa. Shranjujejo se vsi pogovori med uporabniki, ki jih lahko vidijo le ponudnik storitve in administratorji. V kolikor je javljena pritožba utemeljena, dobi pošiljatelj nagradne kovance, krivec pa ustrezno kazen.

Moderatorji in celotna ekipa ukrepajo na različne načine:

- brca: uporabnika se izloči iz klepetalnice;
- uporabnika se premesti v drugo sobo, kjer se nekdo iz ekipe z njim pogovori;
- blokada IP-naslova: uporabnik za določen čas ne more vstopiti v klepetalnico;
- uporabnika se vrže k pravilom klepetalnice;
- popolna blokada uporabnika.

9. Wuschelchat

URL: http://www.wuschelchat.de/

Ta stran nudi samo klepetalnico. Na prvi strani pozornost vzbudi neprimerna reklama, ki oglašuje mlada tajska dekleta. Za prijavo v klepetalnico se je treba registrirati. V ta namen se najprej vnese naslov spletne pošte. Nato uporabnik na tja prejme povezavo do nadaljnje registracije, pri kateri je potrebno vnesti ime, vzdevek in geslo. Preden uporabnik vstopi v klepetalnico, se mora strinjati s pogoji uporabe in navodili za varno uporabo klepetalnice, ki so na tem mestu navedeni. V klepetalnici je prisoten

administrator. Možen je zasebni klepet, pri tem ni omejitve glede uporabe različnih neprimernih besed. Je pa pregledno nameščena možnost ignoriranja uporabnika.

10. Kindersache

URL: http://www.kindersache.de/

Je stran Združenja za pomoč otrokom Nemčije, ki otrokom nudi informacije o njihovih pravicah. Na voljo so: klepetalnica, spletne igre in možnost objavljanja lastnih vsebin. Stran je članica inciative Seitenstark.

Klepetalnica je na voljo od 15. do 17. ure. V klepetalnici so moderatorji, pa tudi uporabniki, ki opravljajo to funkcijo. V klepetalnico je možno vstopiti tudi brez registracije, le z vpisom vzdevka. Moderator je aktivno prisoten. Objave niso »pre-moderirane«. Na vrhu klepetalnice je dobro vidna povezava, ki uporabnika vodi na stran, kjer je razloženo, kako ravnati v določenih situacijah. Zaseben klepet ni možen.

Tabela 7. 1: Ukrepi za varnost otrok po priporočilih evropske komisije na analiziranih spletnih straneh

Ukrepi / Šifra spletne strani	1	2	3	4	5	6	7	8	9	10
Klepetalnica deluje le določen del dneva.	✓			✓		✓	✓	✓		✓
Na voljo so informacije o varni uporabi spletne storitve za učitelje in starše.	✓			✓	✓	✓	✓			
Ponudnik storitve vzpodbuja starše in učitelje k večji kontroli otrok in mladostnikov pri uporabi storitve.	✓			✓	✓		✓			
Na voljo so informacije o varni uporabi spletne storitve za otroke.	✓	✓		✓	✓	✓	✓	✓	✓	✓
Informacije o varni uporabi so napisane na jasen in otrokom razumljiv način.	✓	✓		✓	✓	✓	✓	✓		✓
Informacije o varni uporabi spletne storitve so objavljene na mestu, kjer uporabnikom najbolj koristijo, ali pa je povezava do njih jasno vidna.		✓		✓	✓		✓	✓	✓	✓
Objavljena je povezava do spletnih strani, ki so namenjene osveščanju mladih o varni uporabi interneta, ali drugih organizacij, ki nudijo pomoč otrokom v stiski.	✓				✓	✓	✓			
Na strani je spletna povezava do represivnih organov (npr. policija) ali njihova telefonska številka.										

Ponudnik vzpodbuja uporabnike k premišljenemu ravnanju z osebnimi podatki.	✓	✓		✓	✓	✓	✓	✓	✓	✓
Stran omogoča varovanje osebnih podatkov.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Nezaželeno vedenje na strani je jasno opredeljeno.	✓	✓		✓	✓	✓	✓	✓	✓	✓
Jasno so opredeljene posledice neželenega vedenja.	✓	✓		✓	✓			✓	✓	✓
Ponudnik omogoča uporabo storitev le uporabnikom določene starosti.		✓	✓			✓	✓	✓		
Spletna stran ima mehanizme za odkrivanje in odstranjevanje uporabnikov, ki zaradi starosti ne morejo uporabljati storitev, ki so namenjene otrokom.			✓					✓		
Uporabnikom neprimerne starosti je ponovna prijava onemogočena.			✓					✓		
Na strani je obrazloženo, zakaj je starostna omejitev prisotna.										
Stran ponuja enostavna orodja za prijavo neprimernih vsebin in kontaktov.					✓			✓		✓
Stran ponuja navodila za uporabo orodij za prijavo neprimernih vsebin in kontaktov.					✓			✓		
Ponudnik nadzira spletno stran z uporabo človeške moderacije.	✓	✓		✓	✓		✓	✓	✓	✓
Ponudnik nadzira spletno stran z uporabo tehnološke moderacije.					✓			✓		
Stran omogoča označitev neprimerne vsebine.					✓			✓		
Stran uporabnikom omogoča podati mnenje ali poročilo o delovanju in varnosti strani.	✓	✓		✓	✓	✓	✓	✓	✓	✓

Seznam šifer spletnih strani uporabljenih v Tabeli 7.1:

1 – Modri Jan

2 – Kids chat

3 – Kids chat-chat for kids online

4 – Kidz World

5 – Kidscom

6 – Kinderchat

7 – Seitenstark

8 – Kinderchat

9 – Wuschelchat

10 – Kindersache

8 ANALIZA REZULTATOV

V analizo so bile vključene: ena slovenska, ena švicarska, štiri ameriške in štiri nemške strani. Nobena analizirana spletna klepetalnica ali socialno omrežje, namenjeno zgolj otrokom ali mladostnikom, ne izpolnjuje vseh priporočenih ukrepov. V povprečju imajo strani razvitih 11 od skupno 22 priporočenih varnostnih ukrepov. Od tega imajo tri strani 10 ali manj ukrepov. Dve spletni strani imata 16 in 17 ukrepov, kar je največ izmed vseh strani, ena spletna stran pa ima zgolj štiri ukrepe. Več kot polovica klepetalnic ne deluje ves dan. Običajno so na voljo med 11. in 19. uro, vse dni v tednu. Dve klepetalnici sta na voljo od ponedeljka do petka, ena poleg tega še v soboto. Tri klepetalnice so na voljo ves čas, dve pa od 8. do 23. ali 24. ure.

Način registracije se med stranmi zelo razlikuje. Pri polovici primerov je registracija zelo preprosta, saj se na tri klepetalnice lahko prijavimo samo z vzdevkom, pri eni je potrebno dodati tudi starost, pri drugi pa geslo. V enem primeru se najprej vnese naslov spletne pošte, nanj se prejme povezavo, na kateri se nato vnese vzdevek, ime in geslo. Pri treh primerih je potrebno ob registraciji napisati svoje ime, spol, starost, naslov spletne pošte, kraj bivanja, vzdevek in geslo. Pri enem izmed teh treh primerov se za otroke, stare manj kot 12 let, navede poštni naslov starša ali skrbnika, ki mora registracijo potrditi. Za registracijo je potrebno dovoljenje staršev ali skrbnikov še v dveh primerih. V enem primeru starši potrdijo registracijo otroka s šifro, prejeto po spletni pošti, v drugem primeru pa je dovoljenje potrebno le za zasebno klepetanje, javni del pa je dostopen tudi brez njega, zgolj z navedbo imena, vzdevka, spola, starosti in kraja bivanja.

Na vseh analiziranih spletnih straneh je zagotovljeno varovanje osebnih podatkov. Običajno se izjava o tem nahaja na dnu strani. Poleg tega devet od desetih raziskanih spletnih strani nudi informacije o varni uporabi spletne storitve za otroke, uporabnike vzpodbuja k varni in premišljeni uporabi osebnih podatkov, jasno opredeljuje neželeno vedenje pri storitvah in uporabnikom omogoča podajanje mnenja ali poročanje o varnosti na strani in morebitnih drugih pripombah. Pri osmih od desetih strani so informacije za otroke napisane na jasen in razumljiv način, pa tudi objavljene so na mestih, kjer uporabniku koristijo. Pri sedmih straneh se na teh mestih nahaja povezava, ki uporabnika usmeri na drugo podstran. Le štiri strani imajo objavljeno povezavo do drugih spletnih strani ali organizacij, ki se ukvarjajo z osveščanjem mladih o varni

uporabi interneta, ali drugimi povezavami do organizacij, ki nudijo pomoč otrokom v stiski.

Sankcije, ki sledijo ob neupoštevanju pravil, določenih na strani, so pojasnjene na sedmih straneh. Večinoma se moderatorji s takšnimi uporabniki pogovorijo in jih posvarijo. Ob neupoštevanju svarila, se uporabnika za določen čas izključi iz klepetalnice, v kolikor se vedenje ponavlja, se ga trajno izključi in onemogoči njegov ponovni vpis. To bi se naj zgodilo na vseh omenjenih sedmih straneh, dejansko pa se je samo na dveh. Večina strani, to je osem od desetih strani, pri klepetu uporablja nadzor v obliki človeške moderacije. To sem kot učinkovito zaznala zgolj pri štirih straneh, pri ostalih o moderatorju ni bilo sledu. Na dveh straneh so mi uporabniki povedali, da so moderatorji prisotni le občasno. Res pa je, da prisotnosti moderatorjev zaradi etičnih razlogov nisem mogla neposredno izzvati.

Le polovica strani nudi tudi informacije o varni uporabi strani in varnosti otrok na internetu, ki so namenjene za starše ali učitelje. Zgolj štiri strani vzpodbujajo starše in učitelje k večji kontroli in osveščanju mladostnikov ali otrok. Čeprav so vse analizirane strani namenjene le otrokom ali mladostnikom, starim pod 18 let, ima starostno omejitev pri registraciji le polovica strani. Zares funkcionalna je ta omejitev le pri dveh straneh, kjer se uporabnik z vneseno napačno starostjo ne more prijaviti, niti še enkrat poskusiti s prijavo, razen če izbriše spletne piškotke. Nobena od teh petih strani ne navaja, zakaj ima omejitev starosti. Prav tako nobena analizirana stran nima objavljene povezave do represivnih organov, npr. policije, ali pa objavljene vsaj njihove telefonske številke.

Le tri strani nudijo orodja za prijavo neprimernih vsebin ali kontaktov, njihovo delovanje in uporaba sta obrazloženi pri dveh. Samo dve strani nudita poleg človeške tudi tehnološko moderacijo in možnost označitve neprimernih vsebin. Tehnološka moderacija je prisotna v obliki besednih filtrov, ki onemogočijo objavo vnaprej določenih besed; analitičnih programov, ki imajo podobno funkcijo kot moderatorji in prepoznavajo negativno vedenje; ali filtrov spletnih povezav, ki prepoznavajo objavo neželenih spletnih povezav. Tehnološka podpora se pri eni izmed strani kaže tudi kot nudenje že sestavljenih stavkov, med katerimi lahko uporabnik izbira. Ta stran je neprimerno izbiro vzdevka preprečila z vnaprej določenimi vzdevki in njihovimi kombinacijami, katerih izbira je nadalje odvisna od uporabnika.

Kar sedem analiziranih strani otrokom in mladostnikom poleg klepetanja nudi tudi druge storitve, kot so kvizi, forumi, možnost pisanja bloga, spletne igre in druge

storitve. Še posebej izstopajo 3 strani, ki imajo tudi izobraževalno funkcijo. Med njimi tudi slovenska stran Modri Jan, ki je usmerjena precej ekološko. Večina strani ima otrokom in mladostnikom prijazen izgled. Negativno izstopa le ena stran, na kateri je bila v času mojega raziskovanja reklama s samskimi tajskimi dekleti. V večini primerov izgled in funkcionalnost strani kvarijo reklame.

9 SKLEP

Cilj magistrske naloge je bil raziskati načine zagotavljanja varnosti otrok pri uporabi spletnih klepetalnic in socialnih omrežij. Ugotovila sem, da ta problematika ni aktualna zgolj za starše in ostale odrasle (Yar 2006, 4), ampak se z njo vse bolj ukvarjajo tudi ponudniki spletnih storitev, saj so vse analizirane spletne strani imele vsaj nekaj varnostnih ukrepov. Tudi Evropska komisija ter druge mednarodne in vladne organizacije se vedno bolj posvečajo tej tematiki. Večina organizacij, tako vladnih kot tudi dobrodelnih, se ravna po priporočilih Evropske komisije, ki v splošnem določajo sedem ukrepov za varnost spletnih storitev, namenjenim otrokom:

- *osveščanje uporabnikov, učiteljev in staršev o varnosti in primerni uporabi storitev na internetu na jasen in starosti primeren način,*
- *storitve naj bodo primerne za ciljno starost uporabnikov,*
- *s pomočjo spletnih orodij in tehnologije uporabniku dati moč,*
- *nuditi enostavne mehanizme za prijavo neprimerne vsebine, ki ni v skladu s pogoji uporabe strani,*
- *ponudnik se mora na morebitne prijave kršitev odzvati,*
- *ponudnik mora uporabnikom omogočiti varnost osebnih podatkov in jih vzpodbujati k premišljenem ravnanju z njimi,*
- *ponudnik mora nadzorovati spletno stran in onemogočiti neprimerno vsebino ali vedenje* (European Commission 2009, 5–9).

Ta priporočila so po mojih ugotovitvah pri ponudnikih storitev le delno prisotna in tudi če jih ponudnik na svoji strani navaja, ni nujno, da se dejansko izvajajo. Najbolj opazna je razlika med nadzorom, ki bi se naj na strani izvajal, in med dejanskim nadzorom strani. Na sedmih od desetih strani so bile sankcije, ki sledijo neprimernemu vedenju, navedene, po mojih ugotovitvah pa sta te sankcije dejansko izvajali le dve strani. Velika

večina ponudnikov naj bi za varovanje uporabnikov uporabljala človeške moderatorje, po mojih ugotovitvah pa jih je od osmih spletnih strani uporabljala le polovica. Moderatorji so bili zelo aktivni zlasti na dveh straneh. Na eni izmed slednjih je bila vsa vsebina klepetalnice »pre-moderirana«, kar je pomenilo bolj počasno interakcijo med uporabniki, ki pa je zato bila varnejša.

Informiranje o varni uporabi interneta, zasebnosti podatkov, nadzoru uporabe storitev in faktorjih tveganja je na straneh zelo prisotna, sploh za otroke in mladostnike, za starše, skrbnike in učitelje pa nekoliko manj. Na straneh, kjer so bile poleg človeških moderatorjev prisotne tudi tehnološke oblike moderiranja, sta bila nadzor in primernost vsebine boljša, saj tehnološka moderacija deluje vedno. Na splošno bi naj veljalo, da je človeška moderacija zanesljivejša (Childnet international 2009, 4), vendar morajo moderatorji v tem primeru biti zares prisotni. Prednost tehnološke moderacije se je v mojem primeru pokazala kot bolj zanesljivo nadziranje objavljene vsebine. V glavnem so se za to uporabljali različni filtri, v enem primeru pa tudi programski sistem v obliki klepetalnega robota, ki je odgovarjal na vprašanja, izločal in opozarjal na neprimerno vedenje. Pri analizi spletnih klepetalnic sem ugotovila, da je pri ponudnikih spletnih storitev popularno zlasti vzpodbujanje samoiniciative uporabnikov storitev in ne toliko regulacija in nadzor storitev na samih spletnih straneh. Tudi pri pregledu literature sem največkrat naletela na informiranost uporabnikov o varni uporabi.

Glede na omejena sredstva manjših ponudnikov storitev (Aftab 2010, 97), ki onemogočajo, da so moderatorji na voljo ves dan vse dni v tednu, pa čeprav morda delajo kot prostovoljci, je omejitev delovanja spletnih klepetalnic smiselna. Strani, ki sta imeli najbolj aktivna moderatorja, sta imeli tudi omejen delovni čas klepetalnice na nekaj ur dnevno. Pomemben del varnosti strani je lahko tudi postopek registracije, čeprav ni nujno, da enostaven način registracije pomeni nevarnost za otroke. Pri analizi spletnih strani se je izkazalo, da način registracije ni bil pomemben, če so bili ostali mehanizmi učinkoviti. Na strani s prisotnimi moderatorji se je bilo potrebno prijaviti samo s kombinacijo vzdevka, gesla ali naslova spletne pošte, pa je bil klepet vseeno prijeten za vse prisotne. Tudi starostna omejitev ni bila pomembna, saj so moderatorji dobro opravljali svoje delo.

Glede na trend naraščanja uporabe interneta s strani mlajših uporabnikov in vedno večjega števila otrok z lastnim profilom na družabnih omrežjih (Livingstone 2011, 36–38) je razvoj tehnologij za nadziranje vsebin in uporabnikov pri neposrednem komuniciranju preko spleta nujen. Pomembna je tudi ustrezna izbira človeških

moderatorjev in njihovo izobraževanje (European Commission 2009, 9). Pomanjkanje omenjenega bi morda lahko bil vzrok, da pri polovici spletnih klepetalnic moderatorjev nisem zaznala. Ponudniki spletnih storitev bi na svojih straneh v večji meri morali navajati povezave do drugih organizacij, društev ali skupin, ki se ukvarjajo z varno uporabo spleta za otroke. S tem bi pripomogli k večji prepoznavnosti in pojavnosti drugih organizacij, hkrati pa povečali tudi zaščito svojih uporabnikov. Uporabnikom bi morali nuditi več možnosti prijave neprimernega vedenja ali vsebine in jih o tem izobraziti. Povezave do represivnih organov, na primer policije, in objava pomembnih telefonskih številk so za učinkovit odziv uporabnikov ob zlorabah nujne.

Več pozornosti bi bilo potrebno nameniti tudi tako imenovanim virtualnim svetovom, ki so vedno bolj priljubljeni oblika druženja na spletu za predšolske otroke, saj združujejo funkcijo spletnega igranja z neposrednim komuniciranjem med uporabniki (Holloway n drugi 2013, 17). V moji analizi sem naletela na dve takšni strani, ki sta obe imeli poleg človeške moderacije tudi tehnološko. Dobro bi bilo otroke in mladostnike povprašati, zakaj uporabljajo strani, ki so namenjene starejšim uporabnikom in kakšne strani bi si zase želeli. V Sloveniji ima tako 66 % otrok, starih od 10 do 15 let, svoj profil na socialnem omrežju, ki je namenjen tudi odraslim (Vehovar in drugi 2011, 10). Nadzor staršev in računalniških programov nad uporabo interneta otrok se sprva morda zdi učinkovit, vendar so razhajanja med željo po nadzoru in dejanskim nadzorom velika, kar je ugotovila tudi Sonia Livingstone (Livingstone in drugi 2011, 103–107).

Zanimivo bi bilo izvedeti kakšno uporabno izkušnjo bi si želeli otroci, zlasti predšolski. Na tej podlagi bi nato lahko ponudniki spletnih storitev ustvarili varno omrežje, ki bi ga otroci tudi uporabljali. Več raziskovanja bi bilo potrebnega na področju nadzora otrok na internetu in učinkovitost takšnega nadzora. Predvsem pa je pomembna sprememba mišljenja ponudnikov storitev. Ti morajo iz prelaganja odgovornosti na otroke in mladostnike preiti na večje zagotavljanje varnosti na spletnih straneh z moderiranjem vsebine in onemogočanjem zlonamernih oseb pri kontaktiranju in komuniciranju z mladoletnimi osebami. Varnostni ukrepi na otroških klepetalnicah in socialnih omrežjih so tako kljub hitrosti tehnološkega razvoja spletnih storitev, še zmeraj slabše razviti, kar je škoda, saj imajo velik potencial in so vredni nadaljnega proučevanja.

10 LITERATURA

Aftab, Perry. 2010. The realities and obstacles of child pronography reporting from trenches. V *Youth safety on a living internet: report of the online safety and technology working group*, ur. Hemanshu Nigam in Anne Collier, 96–99. Dostopno prek: http://www.aftab.com/index.php?page=child-pornography-ostwg (29. junij 2013).

Alexy, Eileen M., Ann W. Burgess in Timothy Baker. 2005. Internet Offenders: Traders, Travelers, and Combination Trader-Travelers. *Journal of Interpersonal Violence* 20 (7): 804–812. Dostopno prek: http://jiv.sagepub.com.nukweb.nuk.uni-lj.si/content/20/7/804.full.pdf+html (20. julij 2013).

Barak, Azy. 2005. Sexual Harassment on the Internet. *Social Science Computer Review* 23: 77–92. Dostopno prek: http://ssc.sagepub.com.nukweb.nuk.uni-lj.si/content/23/1/77.full.pdf+html (17. marec 2013).

Boonaert, Tom in Nicole Vettenburg. 2011. Young peopel's internet use: divided or diversified?. *Childhood* 18 (1): 54–66. Dostopno prek: http://chd.sagepub.com.nukweb.nuk.uni-lj.si/content/18/1/54.full.pdf+html (14. avgust 2013).

Boyd, Danah. 2011. Social network sites and networked publics V *A networked self: identity, community, and culture on social network sites*, ur. Zizzi Papacharissi, 37–58. New York: Routledge.

Briggs, Peter, Walter T. Simon in Stacy Simonsen. 2010. An exploratory study of internet-initiated sexual offenses and the chat room sex offender: has the internet enabled a new typology of sex offender?. *Sexual abuse: a journal of research and treatment* 23 (1): 72–91. Dostopno prek: http://sax.sagepub.com.nukweb.nuk.uni-lj.si/content/23/1/72.full.pdf+html (19. avgust 2013).

Buckingham, David. 2006. *After the death of childhood: growing up in the age of electronic media*. Cambridge: Polity Press.

Buckingham, David, Hannah Davies, Ken Jones in Peter Kelley. 1999. *Children's television in Britain*. London: British film institute publishing.

Cassell, Justine in Mag Cramer. 2008. High tech or high risk. Moral panics about girls online. V *Digital jouth, inovation and the unexpected*, ur. Tara McPherson, 53–75. Cambridge, MA: The MIT press.

Childnet international. 2009. *Chatting online and child safety: a guide for parents and carers on how to help children keep safe while chatting*. Dostopno prek: http://www.kidsmart.org.uk/downloads/chatGuide.pdf (20. september 2013).

Directorate General Information Society and Media. 2007. *Safer internet for children: Qualitative study in 29 european countries – Summary report*. Dostopno prek: http://ec.europa.eu/public_opinion/archives/quali/ql_safer_internet_summary.pdf (20. avgust 2013).

--- 2008. *Towards a safer use of theinternetforchildrenin the EU–a parents' perspective*. Dostopno prek: http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/analyticalreport_2008.pdf (2. sepmeber 2013).

European Commission. 2009. *Safer Social Networking Principles for the EU*. Dotopno prek: http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/sn_principles.pdf (20. september 2013).

Ebizmba. 2013. *Top 15 Most Popular Search Engines: September 2013*. Dostopno prek: http://www.ebizmba.com/articles/search-engines (4. september 2013).

Fontana-Rosa, Júlio C. 2001. Legal Competency in a Case of Pedophilia: Advertising on the Internet. *International Journal of Offender Therapy and Comparative Criminology* 45 (1): 118–128. Dostopno prek: http://ijo.sagepub.com.nukweb.nuk.uni-lj.si/cgi/reprint/45/1/118 (20. julij 2013).

Garton, Laura, Caroline Haythornthwaite in Barry Wellman. 1999. Studying on-line social networks V *Doing internet reasearch: critical issues and methods for examing the net*, ur. Steve Jones, 75–105. London: Sage publications.

Hick, Steven in Edward Harpin. 2011. Children's rights and the internet. *The ANNALS of the American Academy of Political and Social Science* 575: 56–70. Dostopno prek: http://ann.sagepub.com/content/575/1/56 (18. avgust 2013).

Hine, Christine. 2000. *Virtual ethnography*. London: Sage publications.

--- 2004. *Virtual ethnography revised*, 1. julij. Dostopno prek: http://www.restore.ac.uk/orm/background/exploringorms/rmf_hine_outline.pdf (23. julij 2013).

Helseth, Solvi in Ashild Slettebo. 2004. Research involving children: some ethical issues. *Nursing ethics* 11 (3): 298–308. Dostopno prek: http://nej.sagepub.com.nukweb.nuk.uni-lj.si/content/11/3/298.full.pdf+html (20. julij 2013).

Holloway, Donell, Lelia Green in Sonia Livingstone. 2013. *Zero to eight. Young children and their internet use.* LSE, London: EU Kids Online. Dostopno prek: http://eprints.lse.ac.uk/52630/1/Zero_to_eight.pdf (28. september 2013).

Home Office. 2008. *Home office task force on child protection on the internet*. Dostopno prek: http://www.manchesterscb.org.uk/docs/Home%20Office%20Task%20Force%20in%20CP%20on%20the%20Internet.pdf (15. september 2013).

Hughes, John R. 2007. Review of Medical Reports on Pedophilia. *Clinical Pediatrics* 46: 667–682. Dostopno prek: http://cpj.sagepub.com.nukweb.nuk.uni-lj.si/cgi/reprint/46/8/667 (20. julij 2013).

Hunter, Christopher D. 2000. Internet Filter Effectiveness: Testing Over- and Underinclusive Blocking Decisions of Four Popular Web Filters. *Social Science Computer Review* 18 (2): 214–222. Dostopno prek: http://ssc.sagepub.com.nukweb.nuk.uni-lj.si/content/18/2/214.full.pdf+html (20. julij 2013).

Jenkins, Philip. 2001. *Beyond tolerance: child pornography on the internet*. New York: New York university press.

Jones, Steve. 1999. Studying the net: intricacies and issues V *Doing internet reasearch: critical issues and methods for examing the net*, ur. Steve Jones, 1–27. London: Sage publications.

Kovačič, Matej. 2006. *Nadzor in zasebnost v informacijski družbi: filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu*. Ljubljana: Fakulteta za družbene vede.

Livingstone, Sonia, Leslie Haddon, Anke Görzig in Kjartan Olafsson. 2011. *Risks and safety on the internet: the perspective of european children*. *Full findings*. London: EU kids online. Dostopno prek: http://eprints.lse.ac.uk/33731/1/Risks%20and%20safety%20on%20the%20internet%28lsero%29.pdf (6. september 2013).

Livingstone, Sonia, Kjartan Olafsson in Elisabeth Staksrud. 2011. *Social Networking, Age and Privacy*. London: EU kids online http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20Online%20reports.aspx (23. julij 2013).

Lobe, Bojana, Sonia Livingstone in Leslie Haddon. 2007. *Researching children's experiences online across countries: Issues and problems in methodology*. London: EU kids online. Dostopno prek: http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20Online%20reports.aspx (23. julij 2013).

Malnar, Brina. 2010. Razisokovalna etika med znanostjo, zasebnostjo in birokracijo. *Družboslovne razprave* 64: 7–24. Dostopno prek: http://www.druzboslovnerazprave.org/media/pdf/clanki/64-malnar.pdf (20. julij 2013).

Mahoney, Debbie in Nancy Faulkner. 1997. Overview of Pedophiles on the Web. Gradivo za *Internet Online Summit: Focus on Children*. Dostopno prek: http://www.healthyplace.com/abuse/articles/pedophiles-on-the-web/ (28. avgust 2013).

Mcalinden, Anne-Marie. 2006. ‘Setting ’Em Up’: Personal, Familial and Institutional Grooming in the Sexual Abuse of Children. *Social Legal Studies* 15 (3): 339–362. Dostpno prek: http://sls.sagepub.com.nukweb.nuk.uni-lj.si/cgi/reprint/15/3/339 (20. julij 2013).

Meyrowitz, Joshua. 1986. *No sense of place*. New York: Oxford university press.

Mitra, Amanda in Elisa Cohen. 1999. Analyzing the web: directions and challenges V *Doing internet reasearch: critical issues and methods for examing the net*, ur. Steve Jones, 179–202. London: Sage publications.

Moinian, Farzaneh. 2006. The construction of identity on the internet. Oops! I’ve left my diary open to the whole world!. *Childhood* 13 (1): 49–68. Dostopno prek: http://chd.sagepub.com.nukweb.nuk.uni-lj.si/content/13/1/49.full.pdf+html (17. marec 2013).

MSPA North America. Dostopno prek: http://www.mysteryshop.org/ (20. september 2013).

Nigam, Hemanshu in Anne Collier. 2010. *Youth safety on a living internet: report of the online safety and technology working group*. Dostopno prek: http://www.ntia.doc.gov/legacy/reports/2010/OSTWG_Final_Report_060410.pdf (29. junij 2013).

O'Donnell, Ian in Clair Milner. 2007. *Child pornography: Crime, computers and society*. Cullopmton, Devon: Willan publishing.

Oswell, David. 1999. The Dark Side of Cyberspace: Internet Content Regulation and Child Protection. *Convergence* 5: 42–62. Dostopno prek: http://con.sagepub.com.nukweb.nuk.uni-lj.si/cgi/reprint/5/4/42 (20. julij 2013).

Pratt, John. 2009. From Abusive Families to Internet Predators?: The Rise, Retraction and Reconfiguration of Sexual Abuse as a Social Problem in Canada. *Current Sociology* 57 (1): 69–88. Dostopno prek: http://csi.sagepub.com.nukweb.nuk.uni-lj.si/cgi/reprint/57/1/69 (17. marec 2013).

Safe-si. Dostopno prek: http://www.safe.si/db/15/1822/ (18. avgust 2013).

Slovensko sociološko društvo. *Kodeks profesionalne etike SSD*. Dostopno prek: http://www.sociolosko-drustvo.si/wp-content/uploads/2011/01/Kodeks_profesionalne_etike_SSD-1992.pdf (20. julij 2013).

SURS - Statistični urad Republike Slovenije. 2012. *Uporaba informacijsko-komunikacijske tehnologije: Uporaba IKT v gospodinjstvih, Slovenija, 2012*. Dostopno prek: http://www.stat.si/ (17. marec 2013).

Taylor, Max in Ethel Quayle. 2003. *Child pornography: an internet crime*. East Sussex: Routledge.

Tynes, Brendesha M. 2007. Internet Safety Gone Wild?: Sacrificing the Educational and Psychosocial Benefits of Online Social Environments. *Journal of Adolescent Research* 22: 575–584. Dostopno prek: http://jar.sagepub.com.nukweb.nuk.uni-lj.si/content/22/6/575.full.pdf+html (20. julij 2013).

Vehovar, Vasja in Gregor Petrič. 2006. Družboslovna informatika: Disciplina v nastajanju. *Znanilci informacijske družbe. 20 let študija družboslovne informatike*. Ljubljana: FDV.

Vehovar, Vasja, Ajda Jerman Kuželički in Lea Lebar. 2011. *Socialna omrežja 2011*. Dostopno prek: http://www.ris.org/db/13/12076/RIS%20poro (3. september 2013).

Webb, Larry, Jackie Craissait in Steven Keen. 2007. Characteristics of Internet Child Pornography Offenders: A Comparison with Child Molesters. *Sex abuse* 19: 449–465. Dostopno prek: http://sax.sagepub.com.nukweb.nuk.uni-lj.si/content/19/4/449.full.pdf+html (20. julij 2013).

Yar, Mahid. 2006. *Cybercrime and society*. London: Sage publications.

Young, S. Kimberly. 2008. Internet Sex Addiction: Risk Factors, Stages of Development, and Treatment. *American Behavioral Scientist* 52 (1): 21–37. Dostopno na: http://abs.sagepub.com.nukweb.nuk.uni-lj.si/content/52/1/21.full.pdf+html (20. julij 2013).