

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Tim Grilc

(Ne)varnost mladih na spletu

Diplomsko delo

Ljubljana, 2017

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Tim Grilc

Mentor: izr. prof. dr. Samo Uhan

(Ne)varnost mladih na spletu

Diplomsko delo

Ljubljana, 2017

(Ne)varnost mladih na spletu

Moje diplomsko delo predstavlja poglobljen pogled na trenutno stanje seznanjenosti mladih z varnostjo na spletu. Mladi so na spletu najbolj izpostavljena starostna skupina. Zaradi svoje mladostne naivnosti so pogosto lahke tarče internetnih zlorab, ustrahovanj ali celo izsiljevanj. Ker so mladi praktično od rojstva obdani z elektroniko, je lahko zelo problematično, če se v mladosti ne seznanijo z nevarnostmi, ki so prisotne ob nepravilni in neprevidni rabi interneta. Nasilje, sovražni govor in grožnje so v družbenem okolju prisotne odkar štejemo leta, iz zunaj spletnega sveta (*offline*) pa so prišle tudi v spletne (*online*) skupnosti. Raziskovalcem to področje že od začetka spletnih skupnosti predstavlja zelo trd oreh, saj je težko povezati vzorce prenosa obnašanja iz *offline* na *online*. V delu so podrobno analizirane navade mladih pri uporabi spleta, s poudarkom na njihove pomanjkljivosti. Pri varnosti in seznanjenosti mladih o tveganjih igrajo največjo vlogo starši in institucije. V nadaljevanju naloge pa je analiziran tudi odnos staršev do varnosti njihovih otrok na spletu in predstavljena njihova dejanja, ki kljubujejo in ožijo nabor nevarnosti, ki so jim mladi izpostavljeni na spletu.

Ključne besede: mladi, internet, spletna varnost, izobraževalne institucije, spletno ustrahovanje.

Safety and risks of youth online

My BA dissertation is giving an in depth view on the current situation and awareness of young people's safety online. Youths are known to be the most vulnerable group on the internet. Due to their youthful naivety they are often targets of online abuse, harassment or even blackmail. Since they are surrounded with technology from young ages they need to be familiar with dangers of wrong and careless use of the internet. Violence, hate speech and other threats are present in our social environment since we count years but they are transferring from the »offline« world to the »online« communities. Researchers are very interested in this area since the beginning of online communities as it is very difficult to find connections within the patterns of behaviour in online and offline world. Parents and educational organizations play a significant role in delivering safety awareness and informing young people about the risks on the internet. Later in this paper I am keen to research whether parents are providing sufficient knowledge of their children's online safety to narrow risks to which young people are exposed to online.

Key words: youth, internet, online safety, educational organizations, cyberbullying.

KAZALO VSEBINE

1	UVOD	9
2	OPREDELITEV POJMOV	12
2.1	Mladi	12
2.2	Zasebnost in osebni podatki	12
2.3	Internet	14
2.4	Spletna skupnost.....	14
2.5	Kibernetsko nadlegovanje in sovražni govor med mladimi.....	15
2.6	Družbeno zaupanje	17
2.7	Phishing oziroma spletno ribarjenje	18
2.8	Spletno novačenje	19
2.9	Programi za starševski nadzor	21
2.10	Internet stvari	22
2.11	Kraja identitete.....	23
2.12	Samorazkritje	23
3	TVEGANJA MLADOSTNIKOV NA SPLETU	26
3.1	Zloraba osebnih podatkov	27
3.2	Razkrivanje osebnih podatkov neznancem	28
3.3	Zasvojenost z internetom in sodobno tehnologijo.....	29
3.4	Odprt dostop do interneta oziroma nenadzorovanost.....	30
3.5	Vohunski programi in virusi	33
3.6	Prenašanje nelegalnih ali piratskih vsebin	33
3.7	Medijska (ne)pismenost	34
3.8	Spletno nadlegovanje in sovražni govor	35
4	VLOGA INSTITUCIJ IN STARŠEV PRI IZOBRAŽEVANJU MLADIH O VARNI UPORABI SPLETA	36

4.1	Vloga izobraževalnih institucij pri informiranju mladih o varnosti na spletu.....	36
4.1.1	Projekt SAFE-SI	36
4.1.2	TOM.....	37
4.1.3	Spletno oko	37
4.1.4	Varni in internet	38
4.1.5	Log Out.....	38
4.1.6	Varni na internetu	39
4.2	Vloga staršev pri zagotavljanju informiranosti mladih o varnosti na spletu.....	39
5	RAZISKOVALNI NAČRT IN OPERACIONALIZACIJA.....	41
5.1	Enota analize in vzorec	42
5.2	Tehnično ozadje izvedbe	42
5.3	Zbiranje podatkov pri anketi za mlade	42
5.4	Zbiranje podatkov pri anketi za starše.....	43
5.5	Analiza rezultatov	43
5.5.1	Podatki pri anketi za mlade.....	44
5.5.2	Podatki vzorca pri anketi za starše.....	44
6	INTERPRETACIJA REZULTATOV IN UGOTOVITEV RAZISKAVE MED OTROKI IN STARŠI.....	46
6.1	Časovni in materialni okviri uporabe spleta.....	46
6.2	Objava osebnih podatkov na spletu.....	48
6.3	Aktivnost mladih na spletu in pametnih telefonih	51
6.4	Izpostavljenost tveganjem na spletu.....	52
6.5	Tehnična zaščita pri mladih.....	55
6.6	Informiranost in izobraževanje mladih o spletnih tveganjih ter uporabi pametne tehnologije.....	58
6.7	Omejitve dostopa.....	61
6.8	Kaj starše bolj skrbi, spletna ali zunaj spletna tveganja?	66

7	ANALIZA SEKUNDARNIH PODATKOV	70
7.1	Mladi na netu.....	70
7.2	EU Kids Online	71
7.3	Projekt »Nasvet za net«.....	71
8	ZAKLJUČEK.....	73
9	LITERATURA.....	76
	PRILOGE.....	84
	Priloga A: Kanali promocije ankete za mlade	84
	Priloga B: Kanali promocije ankete za starše	87
	Priloga C: Anketni vprašalnik za mlade	88
	Priloga Č: Anketa za starše	94
	Priloga D: Vabilo za mlade	99
	Priloga E: Tabele povezanosti pri anketi za starše	100
	Priloga F: Tabela korelacij med spremenljivkami pri anketi za starše	104
	Priloga G: Tabele povezanosti pri anketi za mlade	105
	Priloga H: Tabela korelacij med spremenljivkami pri anketi za mlade	109

KAZALO SLIK

Slika 3.1:	Mladi nenadzorovani uporabniki spleta v Evropi.....	30
Slika 4.1:	Potek prijave na portalu Spletno oko	38
Slika 6.1:	Opozarjanje na prekomerno uporabo spleta ali telefona	47
Slika 6.2:	Mnenje otrok o prekomerni uporabi spleta	47
Slika 6.3:	Ali so starši povedali, kateri podatki sodijo na splet?	50
Slika 6.4:	Omejitev prikaza objav na družbenih omrežjih	50
Slika 6.5:	Mladi uporabniki družbenih omrežij	51
Slika 6.6:	Število prijateljev oz. sledilcev na spletu	53

Slika 6.7: Virtualni prijatelji	53
Slika 6.8: Komunikacija z virtualnimi prijatelji	54
Slika 6.9: Spoznavanje virtualnih prijateljev v živo	54
Slika 6.10: Primerjava odgovorov - spletno ustrahovanje	56
Slika 6.11: Kam se mladi obrnejo na pomoč pri spletnem ustrahovanju.....	57
Slika 6.12: Kaj se je mladim že zgodilo na spletu	57
Slika 6.13: Kako se je otrok naučil uporabe spleta in tehnoloških naprav	59
Slika 6.14: Kdaj je otrok začel z redno uporabo računalnika oziroma dostopa do spleta	60
Slika 6.15: Predavanje o varnosti na spletu v šoli	61
Slika 6.16: Kaznovanje otroka z odvzemom računalnika ali tehnoloških naprav	62
Slika 6.17: Nadziranje otroka s pametno tehnologijo	63
Slika 6.18: Omejitve pri dostopu do računalnika in spletnih vsebin	64
Slika 6.19: Omejitve uporabe spleta s strani staršev – rezultati ankete za mlade.....	65
Slika 6.20: Kaj starši svojemu otroku dovolijo	66
Slika 6.21: Zanimanje za dejavnost otrok na spletu	67
Slika 6.22: Žrtev medvrstniškega spletnega nadlegovanja	67
Slika 6.23: Slaba družba.....	68
Slika 6.24: Uživanje alkohola ali drog.....	68
Slika A.1: Promocija TOM	84
Slika A.2: Promocija Safe.si	84
Slika A.3: Promocija MISSS	85
Slika A.4: Promocija Deskam varno	85
Slika A.5: Promocija Arnes	86
Slika A.6: Promocija SIO	86
Slika B.1: Promocija Za starše	87
Slika B.2: Promocija Safe.si - starši.....	87
Slika B.3: Promocija Safe.si Twitter.....	88

KAZALO TABEL

Tabela 5.1: Končni vzorec ankete za otroke pred analizo	44
Tabela 5.2: Končni vzorec ankete za starše pred analizo	45
Tabela 6.1: Ali je komunikacija po spletu res lažja?	49
Tabela E.1: Povezanost med kaznovanjem in spolom.....	100
Tabela E.2: Povezanost med kaznovanjem in spolom - hi-kvadrat	100
Tabela E.3: Povezanost med omejitvami in spolom	101
Tabela E.4: Povezanost med omejitvami in spolom - hi-kvadrat	101
Tabela E.5: Povezanost med omejitvami in spolom - Cramer.....	101
Tabela E.6: Povezanost med uporabo sodobne tehnologije in spolom - Cramer	102
Tabela E.7: Povezanost med omejitvami in spolom - hi-kvadrat	102
Tabela E.8: Povezanost med uporabo sodobne tehnologije in spolom - Cramer	102
Tabela E.9: Povezanost med zgodnjo uporabo sodobne tehnologije in spolom.....	103
Tabela E.10: Povezanost med zgodnjo uporabo tehnologije in spolom - hi-kvadrat	103
Tabela E.11: Povezanost med zgodnjo uporabo sodobne tehnologije in spolom - Cramer ..	103
Tabela F.1: Tabela korelacij med spremenljivkami pri anketi za starše	104
Tabela G.1: Povezanost med uporabo družbenega omrežja in spolom	105
Tabela G.2: Povezanost med uporabo družbenega omrežja in spolom - hi-kvadrat	105
Tabela G.3: Povezanost med neznanimi virtualnimi prijatelji in spolom.....	106
Tabela G.4: Povezanost med neznanimi virtualnimi prijatelji in spolom - hi-kvadrat.....	106
Tabela G.5: Povezanost med neznanimi virtualnimi prijatelji in spolom - Cramer	106
Tabela G.6: Povezanost med spoznavanjem virtualnih prijateljev v živo in spolom	107
Tabela G.7: Povezanost med spoznavanjem virtualnih prijateljev in spolom – hi-kvadrat..	107
Tabela G.8: Povezanost med spletnim nadlegovajem in spolom	108
Tabela G.9: Povezanost med spletnim nadlegovajem in spolom - hi-kvadrat.....	108
Tabela G.10: Povezanost med spletnim nadlegovajem in spolom - Cramer	108
Tabela H.1: Tabela korelacij med spremenljivkami pri anketi za mlade	109

1 UVOD

Živimo v hitro razvijajočem se svetu, kjer smo vsak trenutek izpostavljeni novim tehnološkim izumom in napravam, posledično pa tudi nenehno novim načinom uporabe tehnologij. Mladi so že od začetka življenja obdani s tehnologijo, ki je včasih tudi ne znajo uporabljati na ustrezen oziroma pravilen način. Družbena omrežja, spletni forumi in nove aplikacije predstavljajo za mlade nov vir in novo okolje preživljanja prostega časa, a nosijo s seboj tudi določena varnostna tveganja. Internet predstavlja zelo uporabno in skorajda nujno orodje za dostop, urejanje in deljenje podatkov za vsakršne namene, vseeno pa moramo danes bolj kot kdaj koli poznati njegovo delovanje in pasti, ki se tam pojavljajo. V svojem diplomskem delu bom podrobneje raziskal področje varnosti podatkov, ki jih mladi objavljajo na spletu, njihovo zavedanje o tveganjih na spletu, ter vlogo staršev in izobraževalnih institucij pri informiranju mladih o varnosti in pravilni rabi interneta. Glede varnosti je potrebno omeniti pomembne dejavnike, ki mladim pomagajo do regulacije objave osebnih podatkov, tj. preventiva in seznanjanje mladih o tveganjih javne objave podatkov oziroma medijska pismenost kot način, da pridemo do kritičnih in zdravih uporabnikov interneta. Višja stopnja participacije na spletu med mladimi je posledično povezana z večjo izpostavljenostjo nevarnostim in zasvojenosti z internetom, navade, ki jih v tem času mladi pridobijo, pa jih bodo po mnenju številnih raziskav spremljale vse življenje. Za zbiranje podatkov bom uporabil tako kvalitativni in kvantitativni pristop, kar je bilo tekom študija večkrat prakticirano.

V zadnjih letih čas, ki ga preživimo na spletu, konstantno narašča, prav tako narašča število ljudi, ki do spleta dostopa. Današnje otroke in mlade lahko poimenujemo tudi digitalna generacija, saj odraščajo s tehnologijo in so v stiku z njo praktično od rojstva. Mladi tako predstavljajo zelo pomembne medijske porabnike, predvsem zato, ker bodo s tehnologijo v stiku vse življenje. Včasih so si mladi želeli lego kocke, danes pa nov in zmogljiv mobilni telefon. Pri oblikovanju teh navad igrajo starši zelo močno vlogo, saj morajo na mlade prenesti svoje znanje iz področja digitalne pismenosti, predvsem pa podati svoj zgled zdrave in premišljene uporabe medijev, da bodo lahko mladi odgovorno in varno uporabljali internetno tehnologijo. V Sloveniji je imelo leta 2016 po podatkih Statističnega urada Slovenije (SURS) dostop do spleta 78 % gospodinjstev, kar nas uvršča v najvišjo skupino v primerjavi z drugimi državami Evropske unije (EU) (SURS 2015). Leta 2015 je računalnik

redno uporabljalo 1.135.842 Slovencev, starih 16–74 let, internet pa 1.136.008 (SURS 2015). V podatke pri uporabi interneta so vključeni tudi tisti, ki internet uporabljajo preko mobilnega telefona, televizije ali računalnika. Dostop do interneta preko mobilnih podatkov ima po zadnjih podatkih 91 % mladih (16–24 let). Ti podatki so sicer enaki povprečju vseh držav EU in nekoliko nižji kot v Baltskih državah, kjer mladi internet začnejo uporabljati kot najmlajši glede na ostale države. Po nekoliko starejših podatkih pa je internet v Sloveniji že leta 2008 uporabljalo 88 % mladih, starih 6–17 let (Eurobarometer v Vehovar in drugi 2009, 1). Zanimiv pa je tudi podatek, da je približno 9 % anketiranih (15.920) že kdaj izgubilo svoje osebne podatke, kar je bila posledica okužbe z računalniškim virusom, to pa je zaskrbljujoče visoka številka glede na starost (SURS 2015). Lahko predvidevamo, da je pri mlajših uporabnikih spleta ta številka še višja. Mladi mobilni internet uporabljajo predvsem za komunikacijo preko družbenih omrežij ter ogled avdio in video vsebin (SURS 2015). Časi, ko so se mladi družili zunaj, so minili, saj so se mladi v veliki meri preselili v svoje sobe, kjer se družijo v virtualnem svetu. Preživljanje prostega časa na spletu tako mladim nudi priložnost, da razvijejo prijateljstva in se na spletu družijo z vrstniki. V diplomski nalogi bom poudaril glavne pomanjkljivosti in tveganja, ki so jim mladi izpostavljeni na spletu. Predvsem se bom osredotočil na mero zasebnosti in varovanja osebnih podatkov. Prav tako želim preučiti navade rabe interneta in družbenih omrežij med mladostniki. Slovenski mladostniki so se že leta 2010 v primerjavi z drugo evropsko mladino nadpovprečno zgodaj odpravljali na splet, kjer tudi preživijo vse več časa (Mladina 2010). Uporaba informacijsko-komunikacijskih tehnologij (IKT) že nekaj časa predstavlja osrednji element sodobne družbe, zato bi bilo treba mladostnike oziroma že otroke vzgajati, kako jih pravilno uporabljati. Pa to počnemo? Osnovno znanje uporabe mladi dobijo v šoli, npr. uporaba orodij Microsoft Office, e-poštnega nabiralnika, brskanja po spletu itd. Vendar pa bi bilo mlade treba podučiti tudi o varnosti podatkov na spletu in uporabi družbenih omrežij ter portalov, kjer delijo svoje osebne podatke. Po podatkih britanske raziskave so mladi na spletu v prostem času približno štiri ure dnevno (Anderson 2015), Američani pa pravijo, da je njihova mladina v prostem času na spletu v povprečju devet ur dnevno (Wallace 2015). Podatkov za Slovenijo nisem našel, vendar pa je raziskava Mladina 2010 pokazala, da so mladi že nekaj let nazaj redno uporabljali internet in se na lestvici uvrstili nad povprečje EU (Eurostat v Lavrič in drugi 2010, 227). Skoraj vsi mladi uporabljajo družbena omrežja, ki so danes »norma« in popolnoma običajen način komuniciranja med mladimi, zaradi enostavne komunikacije s prijatelji in preživljanja prostega časa. Spletna družbena omrežja mnogim tudi olajšajo

komunikacijo z drugimi osebami, saj nas naredijo bolj samozavestne, če nismo v isti sobi kot oseba, s katero govorimo. Druga prednost pa je tudi instantna komunikacija z osebami, ki so lahko fizično zelo oddaljene med seboj. Pozitivni vplivi tehnologije na samozavest mladih so bili tudi znanstveno dokazani, predvsem na odprtost in odkritost pri spletnem pogovoru (Ehrenberg in drugi 2008, 740).

Za mlade kot ciljno skupino sem se odločil, ker po mojem mnenju sodijo v skupino, ki je bolj izpostavljena pastem na spletu. V ta namen bom s pomočjo spletne ankete preveril tako zavedanje mladih o varnosti podatkov, ki jih objavijo na spletu, kot tudi, koliko podatkov dejansko pustijo dostopnih tretjim osebam. S pomočjo zbranih podatkov bom skušal ugotoviti in opredeliti navade mladih na spletu v trenutnem času. Kot dodatno tehniko preučevanja pa bom izvedel tudi anketo med starši, katere namen je pridobitev in primerjava ujamenja podatkov. Glavni cilj moje diplomske naloge bo tako odkriti dejavnike, ki mlade spravljajo v položaj občutljivejših uporabnikov spleta, ter s pomočjo ankete analizirati njihovo obnašanje in splošno znanje uporabe spletnih omrežij. Želim tudi ugotoviti, ali institucije in starši igrajo dovolj pomembno vlogo pri izobraževanju oziroma seznanjanju o tveganjih objave osebnih podatkov na spletu. V zaključku diplomske naloge bom zapisal najpomembnejše ugotovitve ter podal predloge, kako danes izboljšati varnost uporabe spleta med mladimi.

2 OPREDELITEV POJMOV

Za podrobnejše razumevanje moramo najprej predstaviti koncepte in opredeliti pomene terminov, ki jih bomo uporabljali. V nadaljevanju bom najprej predstavil različne pojme, ki se bodo v moji diplomski nalogi velikokrat pojavljali, nadaljeval pa bom z umestitvijo pojma v problemski kontekst, ki ga preučujem.

2.1 Mladi

Mladi so po definiciji Urada za mladino RS stari od 15–29 (Bučar-Ručman 2004, 25). Ker se mi zdi takšno razslojevanje preširoko in neustrezno za namen raziskovanja določene starostne skupine (15-letnik in 29-letnik nimata praktično nič skupnega glede načina življenja), bom v svoji diplomski nalogi kot mlade opredelil osebe med 11 in 17 leti in tako s precej ožjo definicijo mladih prišel do bolj konsistentne ciljne skupine, pri kateri se navade uporabe tehnologij šele oblikujejo. S pojmom mladi se bom tako skliceval na osebe, ki predstavljajo to starostno skupino in so učenci zadnje triade osnovne šole (7, 8 in 9–ti razred) ali srednješolci (1. in 2. letnik). Za tako razdelitev sem se odločil, ker bi rad raziskal predvsem mlade, ki vstopajo na splet in za katere predvidevam, da so izpostavljenim številnim tveganjem.

Konkretnih raziskav, ki bi preučevale varnost objave podatkov na spletu, nisem našel. Najbolj uporabna pa se mi je zdel raziskava EU Kids Online, ki govori o splošni varnosti mladih Evropejcev in Evropejk na spletu. Potrebno je tudi omeniti pomembno vlogo izobraževalnih institucij in staršev glede seznanjanje mladih s pravilno in varno rabo in obnašanjem na spletu. Neka raziskava pa se bo dotaknila tudi povezanosti med varno uporabo spleta, medijsko pismenostjo in kritičnim razločevanjem novic (Toor 2016).

2.2 Zasebnost in osebni podatki

Zasebnost je pojem, ki je močno povezan z varnostjo na spletu. Bolj kot smo zasebni, manj podatkov pustimo na spletu in posledično smo tudi bolj varni pred različnimi pastmi. Na razkritje osebnih informacij, predvsem vrednotnega oziroma ocenjevalnega značaja s

poudarkom na čustvenih ali mnenjskih stališčih, pa lahko vplivajo tudi osamljenost, sramežljivost, zadovoljstvo z življenjem in zdravstveno stanje. Raziskava o skrbi za zasebnost je pokazala, da več kot so uporabniki razkrili opisnih ali ocenjevalnih informacij oziroma se zavedajo razkritja le teh, bolj bodo obiskovali točno določeno spletno skupnost (Staddon in drugi v Zlatolas in drugi 2015, 158). Ugotovitve kažejo, da so mladi ljudje, predvsem najstniki, bolj pripravljeni razkriti osebne informacije na spletu, motivacijo pa jim v veliki meri predstavlja želja po slavi in sprejetju.

Osebni podatki so vsi podatki, ki so povezani s posameznikom (npr. ime, datum rojstva, davčna številka itd.) ali pa podatki, ki jih je posameznik ustvaril (npr. e-poštno sporočilo, slika itd.). Vsak uporabnik spleta z obiskovanjem spletnih strani pušča digitalni odtis. Tega se veliko ljudi ne zaveda, kar seveda lahko zelo hitro pripelje do različnih spletnih zlorab, kot so izsiljevanje, kraja osebnih podatkov, zloraba gesel itd. Vsi uporabniki spleta objavljamo svoje osebne podatke na spletnih straneh, spletnih dnevnikih (blogih) in družbenih omrežjih, ne da bi se zavedali, da jih lahko skoraj kdorkoli uporabi. Do teh podatkov je zelo lahko priti, tudi če nismo žrtve vdora ali računalniških virusov. V mnogo primerih pa podatki ostanejo shranjeni na spletu, četudi jih izbrišemo. Samorazkritje zniža raven zasebnosti članov spletne skupnosti zaradi izpostavljanja osebnih podatkov in s tem dviguje in krepi »občutek domačnosti« v skupnosti. Zaupanje ima antagonistični odnos (vzajemen) do zasebnosti zato, ker hočejo ljudje vedeti podatke o drugih, da jim lahko v zameno verjamejo, slednje pa ima pozitiven učinek na spletno samorazkritje (Contena in drugi 2015, 31). Dokazana je bila tudi pozitivna povezanost med samorazkritjem in mladostniki, pri starejših ljudeh pa so bila vidna odstopanja (Christofides in drugi 2012, 53). To pomeni, da so mladi bolj pripravljeni deliti svoje osebne informacije na spletu kot starejši.

Milijoni uporabnikov socialnih omrežij razkrijejo svoje podatke, misli, izkušnje, fotografije in videoposnetke v družbenem okolju, ki ima nizko mero varnostnih standardov (med prijatelji se npr. skrivajo tudi osebe, ki jih ne poznajo). Nekateri celo zaupajo osebam, ki jih ne poznajo, in jim razkrijejo svojo identiteto, dajo osebne informacije, strokovno znanje in avtorsko delo, ali pa jim celo posodijo denar (Lai in Turban v Grabner-Krauter in Bitter 2015, 49).

Nekatere dobro organizirane spletne skupnosti in družbena omrežja pri uporabnikih krepijo socialne vrline, tj. vzajemnost, poštenost, dolžnosti, zanesljivost in nesebičnost oziroma altruizem (Hearn v Welch in drugi 2005, 11). Socialne vrline jih učijo skozi pravila, ki znotraj teh skupnosti določajo, kaj je pošteno, sprejemljivo, nagrajlivo ter kaj je deviantno in neželjeno. Prisotnost zaupanja med ljudmi odpira večje priložnosti za medsebojno pomoč, vzajemnost in solidarnost (Welch in drugi 2005, 25).

2.3 Internet

Internet ali medomrežje je mreža računalnikov, ki so med seboj povezani v omrežje. Internet danes ponuja veliko več vsebin in možnih definicij, kot jih je nekoč. Primarna naloga interneta je bila pošiljanje podatkov (npr. izmenjave e-poštnih sporočil). Danes pa je na voljo veliko več vsebin, ki so večinoma neposredno odvisne od delovanja omrežja oziroma interneta (Cohen-Almagor 2011). Internet danes pa se uporablja za ustvarjanje, deljenje in iskanje informacij. Vsak uporabnik interneta je hkrati tudi ustvarjalec vsebine, kar prinaša tako prednosti kot slabosti. Dejstvo, da je vsaka ustvarjena oziroma deljena informacija na spletu izpostavljena nepooblaščenim rabi in posredovanju drži. Iz tega pogleda lahko internet mladim predstavlja zelo nevarno orodje.

2.4 Spletna skupnost

Spletna oziroma virtualna skupnost je skupnost, ki je locirana na spletu v več možnih oblikah (forum, blog, skupina na družbenih omrežjih itd.). Za spletne skupnosti je značilno, da se člani skupnosti identificirajo s skupnostjo, vanjo vlagajo v dobro skupnosti in spoštujejo ter se podrejajo sistemu delovanja skupnosti oziroma predpisanim pravilom (McMillan in Chavis, 1986). Ker člani spletnih skupnosti vlagajo svoje znanje, energijo in čas v svoje delo je izredno pomembno spoštovanje pravil, saj se le tako dosežeta red in zaupanje v skupnosti. Zanimanje za spletne skupnosti je mogoče razložiti z vplivom porasta spletnih (2.0) aplikacij – virtualnih okolij, kjer si skupina ljudi izmenjuje družbene interakcije, ki temeljijo na skupnih vezeh (Sánchez-Franco in Roldán 2015, 394). Družbena omrežja kot je Facebook, Instagram, Snapchat in druga tako tvorijo spletno skupnost, ki med seboj povezuje ljudi in med njimi spodbuja interakcije.

2.5 Kibernetško nadlegovanje in sovražni govor med mladimi

Kibernetško nadlegovanje (ang. *cyberbullying*) predstavlja eno izmed najbolj pogostih zlorab mladih na spletu. Spletno ustrahovanje je zelo pogosta izsiljevalska metoda, ki preži nad uporabniki spleta. Poznamo več vrst spletnega ustrahovanja, ki je zelo pogosto med mladimi. Pojav kibernetškega ustrahovanja je predvsem med mladimi zelo razširjen in se manifestira na različne načine. Definiran je kot ustrahovanje, norčevanje ali nadlegovanje neke osebe preko spleta, na podlagi nekih (ne nujno) osebnih informacij. Lahko je tudi na podlagi osebnega videza, določene fotografije, mnenja glede neke zadeve, interesov ali hobijev neke osebe itd. Kibernetško nadlegovanje je zelo široko definirano: lahko gre le za komentar pod fotografijo nekega uporabnika in norčevanje iz oblačil, ki jih nosi, pa vse do bolj resnih groženj ali celo izsiljevanja preko zasebnih sporočil na spletu. Med spletno ustrahovanje sodijo tudi žaljenje, nadlegovanje, izsiljevanje in grožnje, uperjene v druge uporabnike spleta (Suzor 2012, 563). Med mladimi je predvsem razširjeno norčevanje preko spleta, ki lahko iz nedolžnega posmehovanja preraste v hudo težavo. Po podatkih SI-CERT-a in SURS-a je spletno ustrahovanje tudi bolj razširjeno oziroma pogosto kot ustrahovanje »v živo«. Vsekakor pa je spletno ustrahovanje zelo malokrat prijavljeno oziroma odpravljeno. Po slovenskem kazenskem zakoniku je sovražni govor ter direktno izkazovanje namere nasilja proti neki določeni skupnosti (manjšini) ali osebi kaznivo.

297. Člen Kazenskega zakonika (2012) pravi:

Javno spodbujanje sovraštva, nasilja ali nestrpnosti

297. člen

- (1) Kdor javno spodbuja ali razpihuje narodnostno, rasno, versko ali drugo sovraštvo, razdor ali nestrpnost, ali spodbuja k drugi neenakopravnosti zaradi telesnih ali duševnih pomanjkljivosti ali spolne usmerjenosti, se kaznuje z zaporom do dveh let.
- (2) Enako se kaznuje, kdor javno širi ideje o večvrednosti ene rase nad drugo ali daje kakršnokoli pomoč pri rasistični dejavnosti ali zanika, zmanjšuje pomen, odobrava, omalovažuje, smeši ali zagovarja genocid, holokavst, hudodelstvo zoper človečnost, vojno hudodelstvo, agresijo ali druga kazniva dejanja zoper človečnost.
- (3) Če je dejanje iz prejšnjih odstavkov storjeno z objavo v sredstvih javnega obveščanja, se kaznuje tudi urednik oziroma tisti, ki ga je nadomeščal, s kaznijo iz prvega ali drugega odstavka tega člena, razen če je šlo za prenos oddaje v živo in dejanj iz prejšnjih odstavkov ni mogel preprečiti.

Med spletno ustrahovanje sodijo tudi izsiljevalski virusi, ki od uporabnika zahtevajo plačilo za dostop do računalnika. Prav v zadnjih dveh letih so ti virusi zelo pogosti, saj kriminalci z njimi zelo preprosto pridejo do denarja. CryptoLocker je program, ki se namesti na

uporabnikov računalnik in od uporabnika v zameno za dostop do računalnika in s tem osebnih podatkov zahteva plačilo odkupnine, ki je največkrat v kriptovaluti, kot je Bitcoin. Razlog za plačilo preko virtualne valute je preprost, le-ta je namreč neizsledljiva. Proti plačilu približno 1500 evrov pa na okužen računalnik pošljejo novo datoteko, ki virus "odklene". V veliko primerih je celo slovenska policija predlagala plačilo odkupnine, saj virusov praktično ni mogoče odstraniti, virusi pa so prišli tudi na računalnike nekaj slovenskih upravnih organov, ki pa se z odkupninami niso ukvarjali, saj so imeli urejeno varnostno kopiranje podatkov.

Pri kibernetiskem ustrahovanju pomembno vlogo igrajo *pravila in norme*. Pravila se delijo na eksplicitna in implicitna (napisana ter samoumevna oz. nezapisana). Postavljena so z namenom ohranjanja pozitivnega vzdušja in reda v skupnosti in definiranjem, kakšno obnašanje je v skupnosti zaželeno in kakšno je prepovedano oziroma negativno. Zapisana so v formalnem dokumentu, ki je dostopen vsem članom (Burnett in drugi v Petrovčič in Petrič 2011). Dokument ima naslov »Pravila in pogoji« (*Terms and Conditions*), notri pa so zapisana pričakovanja, po katerih naj bi se člani skupnosti morali zgledovati in jih upoštevati. Sieckenius de Souza pravi, da morajo biti pravila jasno in eksplicitno zapisana ter razumljiva vsem članom (2004, 592), če naj nato uspešno delujejo. Kibernetiski pravni teoretiki (ang. *cyber law theorists*) pravijo, da je pravično izvrševanje pravil pomembno za vsebinsko pravičnost in avtonomijo skupnosti (Suzor 2012, 530). Pravilom morajo za vzpostavljjanje reda glede morebitnih kršitev pravil in norm slediti sankcije, ki so lahko formalne ali neformalne oziroma neuradne, določene pa so glede na stopnjo kršitve (npr. od suspendiranja uporabniškega računa do izbrisa uporabnika). Pravila so določena tako, da so pravična in enaka za vse uporabnike spletnih skupnosti. Primer pravila je npr., da se v javnih debatah ne sme preklinjati ali žaliti drugih članov, tisti, ki pravila ne bodo upoštevali, pa bodo kaznovani z začasno ukinitvijo možnosti komentiranja.

Kibernetisko ustrahovanje se lahko manifestira tudi kot zloraba razkritih informacij, npr. posmeh, ali pa celo grožnje posamezniku. Kibernetisko ustrahovanje je zaradi pogosto neznane identitete manjkrat odpravljeno in preganjano, saj se ustrahovalca znotraj spletne skupnosti težje sankcionira kot na primer ustrahovalca, ki je v šoli izzval pretep. Durante meni, da se skozi zaupanje na spletnih skupnostih razvije več socialnih vrlin, kot je npr.

odgovornost, ki so vidne tudi v zunaj spletnem okolju (2011, 596), slednje pa lahko velja tudi zrcalno.

Pod pojmom kibernetško ustrahovanje razumemo tudi razžalitev neke osebe oziroma posredne (indirektne) grožnje. Med slednje uvrščamo objavo posameznih vsebin ali podatkov, za katera določena oseba ni želela, da so objavljeni (npr. »smešnik«, sramotni video posnetki, slike, dejstva). Definicija kibernetškega nadlegovanja je zelo podobna nadlegovanju zunaj spleta, prisotno je takrat, kadar neka oseba drugo osebo pripelje do neprijetnih občutkov z ustrahovanjem, norčevanjem ali drugimi načini sovražnega govora. Žrtev kibernetškega nadlegovanja je lahko kdorkoli, saj lahko ostre besede in žalitve padajo že na podlagi navzkrižnih mnenj dveh ali več oseb v spletni skupnosti.

2.6 Družbeno zaupanje

Družbeno zaupanje (ang. *social trust*) je definirano kot prepričanje, da skupnost ustvarja v dobri veri in v skladu z zavezami in da ne (pretirano) izrablja drugih članov za dosego nekega cilja. V skupnostih se pojavlja družbeno zaupanje, med ljudmi pa individualno zaupanje. V spletnih skupnostih je prisotno družbeno zaupanje, ki nosi primarno pomembnost v spletnih interakcijah (Blanchard in drugi 2011). Družbeno zaupanje se manifestira s tem, ko neko osebo spustimo v krog svojih virtualnih prijateljev na družbenem omrežju.

Danes smo obdani z raznovrstnimi družbenimi omrežji, nekatera od teh pa so namenjena ravno natančno določenemu krogu ljudi in imajo boljši pristop k varovanju osebnih zadev (npr. fotografij, videov). Ena izmed takih platform je Snapchat, ki deluje od leta 2011. Objave tukaj so večinoma namenjene ožjemu krogu prijateljev in se po vnaprej določenem času izbrišejo, kar vpliva na varnost osebnih podatkov. Po drugi strani pa se Facebook trži kot spletna »spominska knjiga«, saj so podatki hranjeni, dokler jih uporabnik ne izbriše (na strežnikih Facebook-a pa ostanejo za vedno). Nova izbira Facebooka za oddajanje (ang. *streaming*) »v živo« se je že nekajkrat tudi na slovenskih tleh pokazala, kaj vse so ljudje pripravljeni narediti za všečke ali pa podporo virtualnih prijateljev.

Družbeno zaupanje v sedanjosti predstavlja pomemben dejavnik, saj se na družbenem zaupanju gradijo interakcije. Družbeno zaupanje je zaupanje celotni ali pa delu skupnosti, ki

se razvije na podlagi individualnega zaupanja in izkušenj (Blanchard in drugi 2011). Večje, kot je družbeno zaupanje v skupnosti, bolj bodo člani spletne skupnosti spoštovali pravila, saj lahko rečemo, da pravila predstavljajo smernike vedenja družbe, ki določajo, kaj je sprejemljivo vedenje in kaj ni. Ugotovljeno je bilo, da je družbeno zaupanje zelo generacijsko odvisno, starejše osebe so namreč na spletu bistveno bolj previdne in ne zaupajo drugim osebam, v primerjavi z mladimi, ki lažje ustvarijo zaupanje, tudi do neznancev. Ta dejavnik je prisoten tudi pri samorazkritju. Spletne skupnosti in družbena omrežja med drugim v ljudi vlivajo socialne vrline, tj. vzajemnost, poštenost, obveza, zanesljivost in altruizem (Hearn V Welch in drugi 2005, 11), ki pa so lahko s strani nekaterih posameznikov tudi zlorabljene. Rezultati raziskave iz leta 2009 kažejo, da se pri mladih zaradi razkritja osebnih informacij pogosto pojavlja kibernetško ustrahovanje, ki je preveč podcenjeno (Bryce in Klang 2009, 161). Družbeno zaupanje se mi zdi pomembno, saj ima zelo širok spekter in ni vezano le na spletne skupnosti, temveč na naše vsakdanje življenje. Z višjo stopnjo zaupanja se širijo koherentnost skupnosti, višja pripadnost in posledično višje spoštovanje pravil in norm, ki jih skupnost postavlja.

2.7 Phishing oziroma spletno ribarjenje

Spletno ribarjenje (ang. *phishing*) je kraja podatkov, ki tretji osebi omogočijo dostop do spletnih storitev (npr. e-banka, e-pošta, družbena omrežja itd.). Običajno gre za spletno ribarjenje takrat, ko prejmemo sumljivo sporočilo, da smo dobitniki neke nagrade ali pa celo sporočilo banke, da moramo spremeniti svoje geslo za dostop do e-banke. Namen spletnega ribarjenja je zbiranje gesel, podatkov o kreditnih karticah, sodelovanja v različnih plačljivih vsebinah itd. Kot neko vrsto spletnega ribarjenja sodijo tudi spletne strani, ki nas »izberejo« za »srečnega« nagrajenca in nam obljubljajo privlačno nagrado, ki jo dobimo le z vnosom svoje telefonske številke in e-poštnega naslova.

Pri lažnih spletnih straneh je namen dobiti resnične podatke uporabnika (geslo in uporabniško ime) ter te podatke zlorabiti. Po vnosu gesla v obrazec na lažni strani banke, se podatki za dostop posredujejo tretji osebi, ki jih lahko izrabi (SI-CERT 2017). Tarče spletnega ribarjenja smo vsi uporabniki spleta. Največ poskusov kraje podatkov pa se dogaja na strežnikih poštnih odjemalcev, kamor prihaja neželena pošta (SPAM). Poštni odjemalci imajo ščite, ki zaznajo takšna sporočila in jih premaknejo v drug nabiralnik, vendar pa včasih kakšno sporočilo tudi

spregledajo, zato je nujna previdnost uporabnikov. Mladi so tukaj najbolj izpostavljeni, saj pogosto ne znajo prepoznati spletnega ribarjenja. Trenutno so v porastu zlorabe z lažnimi spletnimi stranmi na družbenih omrežjih (Facebook), kjer v zameno za všečkanje strani in pošiljanje vabila prijateljem obljublajo bogate nagrade. Velikokrat se na takšnih straneh nato sledilec vsiljuje povezava do virusa, ki uporabnikom prevzame nadzor nad njihovim računom in širi virus še naprej. Na SI-CERT-u svetujejo upoštevanje preprostih navodil za razločitev poskusa ribarjenja. Vsak uporabnik, ki prejme sumljivo sporočilo, bi moral torej preveriti pošiljateljev e-naslov, slovnično pisanje (pogosto je narejen le prevod, z veliko slovničnimi napakami). Ob kliku na povezave pa moramo biti prepričani tudi, da so varne (protokol »https« in certifikat SSL), predvsem takrat, ko gre za vpisovanje osebnih ali plačilnih podatkov.

Obstaja tudi veliko spletnih trgovin, ki prodajajo dobrine, a v resnici le ukradejo uporabnikove podatke (npr. številko kreditne kartice, PayPal vpisne podatke itd.). Kljub temu pa ni nujno, da je vsaka spletna stran, ki nima sodobnega protokola »https«, postavljena v te namene. Ponekod na svetu se ta protokol šele uvaja v sisteme, na primer na Kitajskem, Rusiji in podobno. Protokol je tudi povezan z zmogljivostjo računalnikov, ki zahtevajo za optimalno delovanje močnejše in sodobnejše naprave.

2.8 Spletno novačenje

Spletno novačenje ima za cilj bodisi reklamo za hiter zaslužek ali pa angažiranje novih članov terorističnih organizacij – oboje privlači ogleda, nevarno pa je, ko takšne spletne strani do te mere pritegnejo zanimanje ljudi, da se ti včasih celo poistovetijo s prikazanim. Spletno novačenje je sodobna oblika pranja možganov. Različne teroristične skupine so se izkazale kot zelo uspešne pri spletnem promoviranju in novačenju novih privržencev, saj s svojimi izzivalnimi prispevki dosežejo veliko število ogledov. Njihova izobraževanja potekajo preko spleta, kar ponovno nakazuje, da so te osebe visoko medijsko pismene in da imajo načrtan nekakšen model, katerega namen je prepričevanje ljudi, da se jim pridružijo.

Anonymous, skupina aktivističnih hakerjev, ki si je pridobila tudi naziv "etični hakerji", je že pred leti naznanila kibernetško vojno terorističnim skupinam. Aktivno sodelujejo pri razkrivanju članov terorističnih skupin preko IP-naslovov in predajajo informacije državnim

oblastem. S svojim delom skušajo opozarjati na pomanjkljivosti in luknje v sistemih. V ta namen so ustvarili tudi spletno stran, preko katere lahko kdorkoli naredi prijavo osebe ali pa vsebine na spletu, ki jo oni preverijo in posredujejo naprej. Spletna povezava se glasi: "http://www.ghostsec.info". Spletna stran »uradno« ne obstaja. Vsaj tako pravijo programi, kjer sta vidna tehnični vzdrževalec in podjetje, ki gostuje domeno. In to je bilo tudi pričakovati od skupine Anonymous, ki s svojim delom krši marsikateri zakon, vendar kljub temu stoji na pravi strani, nas strani povprečnih prebivalcev Zemlje. Med drugim so bili obtoženi več vdorov v informacijske sisteme vladnih organov in posredovanja zaupnih dokumentov medijem. Na spletni strani je javno dostopnih tudi veliko intervjujev z različnih področij. Člani terorističnih organizacij so zelo aktivni na omrežjih, kot sta Facebook in Twitter, ki na žalost pri razkrivanju podatkov uporabnikov ne sodelujeta dovolj hitro. Sicer pa imajo teroristične skupine svoje spletne strani, kjer objavljajo propagandni video material in tudi nekakšna »spletna predavanja«, s katerimi novačijo nove pripadnike. Takšne strani so seveda odstranjene, a vsebina videov zelo hitro konča pri medijskih hišah, ki jih teroristične skupine posredno uporabljajo za promocijo svojega »dela«. Teroristične skupine, kot je ISIS, dobro vedo, kaj motivira ljudi, da se jim pridružijo. Nezaposlenost, pomanjkanje izobrazbe in razslojenost družbe tako mlade, a tudi vse druge naredi veliko bolj naivne in dojemljive za manipulacije. Svoja dejanja opravičujejo v imenu vere. Teroristi ustvarjajo in širijo svoje ideologije z novačenjem manipulativnih (predvsem mladih) oseb preko spleta, nato pa jih prepričajo, da pridejo na vojaška urjenja, kjer jim dokončno operejo možgane z lažnimi obljubami.

V priročniku, ki ga skupina ISIS po spletu pošilja predvsem mladim, je o ljudeh, ki niso muslimani, zapisano slednje spodnje besedilo.

Izvorno besedilo: »This is the sector that I prefer. This is because you will be the one to guide him (i.e. this non-religious Muslim) to the right path. This sector (contains candidates) without limit, especially the youths, who are the safest people (for recruitment), and all praise to Allah. However, we must be careful, too...« (Engel 2015, 10).

»Ta del mi je najbolj všeč. To pa zato, ker boste vi tisti, ki boste (nevernika) vodili na pravo pot. Ta del je (za kandidate) brez omejitev, namenjen predvsem mladim, ki so najvarnejši ljudi (za novačenje), in čaščenje Alaha. Vendar pa moramo biti kljub temu previdni...« (Lasten prevod po Engel 2015, 10).

Predvsem iščejo mlade, izolirane ljudi, ki ne živijo v velikih mestih, splet pa jim predstavlja najpreprostejši komunikacijski kanal za dostop do mladih (Engel 2015). Seveda pa novačenje otrok v terorizem ni edina stvar, lahko gre tudi za nagovarjanje v prostitucijo ali trgovino z belim blagom.

2.9 Programi za starševski nadzor

Programi za starševski nadzor staršem omogočajo omejitve (časovno kot tudi vsebinsko) dostopnosti do spletnih vsebin svojim otrokom. Mladi v Sloveniji po poročanju raziskave EU Kids Online neomejeno, brez nadzora staršev ali različnih programov dostopajo do svetovnega spleta in vseh vsebin, ki so tam na voljo. Programi, ki onemogočajo ali omejujejo dostop do spleta, so sicer vsakdanja praksa čez lužo, v Ameriki. Programi so na voljo tako v brezplačni kot tudi v plačljivi različici in se razlikujejo v naboru funkcij, ki jih omogočajo. Plačljive in bolj popularne izbire so npr. F-Secure, Norton Family in Kaspersky Family. V Sloveniji po poročanju Arnesa ti programi niso priljubljeni, čeprav so zelo priročna zadeva, ki staršem omogoči, da svojega otroka nadzorujejo na spletu. To potrjujejo tudi ugotovitve raziskave EU Kids Online, kjer se je izkazalo, da starši svojih otrok v večini primerov ne nadzorujejo. Starši pri nas predvsem nadzorujejo, *koliko* časa njihovi otroci preživijo na spletu, to pa jih tudi bolj zanima kot dejstvo, *kaj* takrat otroci na spletu počno (Šterk in Petek 2016, 11). Časovne omejitve žal ne omogočajo nikakršne zaščite na spletu. Geografsko je starševski nadzor najbolj popularen na Kitajskem, v ZDA, Nemčiji, Veliki Britaniji in Rusiji (Kaspersky 2015). Merljivost popularnosti je bila izvedena glede na število prodanih licenc spletnih programov (Kaspersky 2015). Poleg programov za računalnik je trenutno na voljo tudi množstvo programov za mobilne telefone, med katerimi so najbolj priljubljeni NetNanny, SecureTeen, Family Time, Screen Time, Kids Place, Family Locator. Ti programi imajo številne funkcije, med drugim tudi takšne, ki so bile s strani strokovnjakov označene kot nelegitimne, saj so posegale dobesedno v »vsak digitalni korak« otroka. To so npr. dostop do vseh poslanih in prejetih sporočil, zgodovine brskanja po spletu, vklop mikrofona, dostop do trenutne lokacije ter zgodovina lokacij, kjer se je otrok nahajal in še mnogo drugih.

2.10 Internet stvari

Druga izpostavitve potrebna tema je *internet stvari* (ang. *internet of things*), ki predstavlja zelo vročo temo v svetovnih medijih, ki si o tem drznejše pisati. Danes so praktično vse moderne naprave med seboj povezane in posledično pošiljajo različne metapodatke na splet, kar je lahko tvegano v smislu zlorabe podatkov, ki jih naprave beležijo. Povprečnemu človeku se to sicer ne zdi problematično, saj večina ljudi tega preprosto ne ve.

Sodobni avtomobili beležijo lokacije in ure voženj, ki jih posredujejo telefonu, ki je povezan z multimedijским vmesnikom. Telefon pa te podatke posreduje tretjim osebam, bodisi proizvajalcem avtomobila, zavarovalnicam ali pa drugim organom. Kar se tiče mladih, se vse več staršev odloča za njihov nadzor s pomočjo pametnih naprav, kot so pametni telefoni, pametne ure, GPS sledilniki in drugo. Nekatere pametne ure se tržijo s sloganom »Naučite svoje otroke odgovornosti« in delujejo kot nekakšni interaktivni opomniki, da si morajo otroci vsak dan ob določeni uri umiti zobe, pospraviti posteljo, jesti. Obstajajo pa tudi bolj srhljive naprave, ki dejansko omogočajo lociranje otroka, kadarkoli in kjerkoli je na voljo omrežje. Nekatere naprave omogočajo celo vklop »v živo« in poslušanje mikrofona, ki je npr. na otrokovi uri (Keating 2016). Ameriška in prav tako naša zakonodaja sicer dovoljuje snemanje in poslušanje klicev ob slutnji, da je neka oseba povezana s teroristično ali drugo kriminalno dejavnostjo, vendar ne to ne vključuje prisluškovanja napravam, saj se je ta tehnologija razvila šele s porastom pametnih telefonov. Zelo podobno je s podatki, ki so objavljeni na spletu. Ker je družbeno omrežje Facebook ameriško podjetje, se lahko vsi podatki, ki jih katerikoli uporabnik (ne glede na njegovo lokacijo) ustvarja (tudi zasebna sporočila) izročijo ameriškim preiskovalnim organom, brez potrebne privolitve kateregakoli drugega organa. To nas pripelje do kontradiktosti – kdo je torej lastnik podatkov, oseba, ki jih ustvari, ali stran, na kateri so podatki objavljeni? Podobno je tudi s primerom družbenega omrežja za deljenje slik, ki v pogojih uporabe navaja, da z objavo slike na njihovem omrežju tudi sami pridobijo delne avtorske pravice do objavljene vsebine, saj je slika objavljena na njihovi spletni strani, poleg tega pa se po navadi uporabijo tudi »filtri« za slike, ki so last podjetja.

Nekoč ni bilo možno dostopati do vseh podatkov, imenovanih »big data«. Danes, ko imamo dostop do njih, pa jih ne znamo analizirati. S tem se soočajo marsikatera podjetja, ki imajo na voljo preveč podatkov in ne najdejo pristopa, kako bi se analize le-teh lotili. Večina teh

podatkov legalno ne bi smela biti posredovana oziroma uporabljena v marketinške ali druge namene. Tak primer sta na primer nakupovanje in sistem kartic zvestobe, ki trgovcem omogočajo izdelavo profila osebe, na podlagi česar potem tej osebi pošiljajo personalizirane nasvete in popuste. Enako velja za spletno nakupovanje. Ob brskanju po spletu za nekimi stvarmi, kot je lahko knjiga, letalska vozovnica, ali pa hotel, nam bo Facebook s sponzoriranimi vsebinami ponujal iskano storitev ali dobrino, lahko tudi pri konkurenčnem ponudniku. To sicer ni nič spornega, saj je to cena, ki jo plačamo za »brezplačno uporabo« storitev.

2.11 Kraja identitete

Pri *kraji identitete* gre lahko za uporabo osebnih podatkov tretje osebe, pogosto pa je v ozadju pridobitev finančnih ali drugih dobrin. To je na primer nakup s kartico neke druge osebe, nepooblaščen dostop do osebnih podatkov tretje osebe (e-pošta, spletna omrežja itd.). Pri nakupovanju s kreditnimi karticami se zgodovina beleži, beleži se tudi lokacija telefona s pomočjo oddajnega omrežja (Oppmann 2010). Prav tako se beležijo vsi podatki, ki so narejeni na računalniku, kadar pa je računalnik prijavljen na splet, so ti podatki izpostavljeni potencialnim hekerjem, ki lahko do podatkov nepooblaščno dostopajo in jih ukradejo. Kraja podatkov, kot je zgodovina brskanja, se najpogosteje uporabi v komercialne namene, medtem ko je lahko kraja osebnih podatkov, kot je identiteta, veliko bolj nevarna. Zelo pogoste so tudi t. i. »nigerijske prevare«, ki uporabnika zavedajo na način, da je zadel veliko vsoto denarja ali pa da nujno potrebujejo njegove podatke za prenos denarja. Nepridipravi pa potem v imenu žrtve lahko sklenejo posojila ter odtujijo denar. Taka tveganja so sicer bolj usmerjena v starejše ljudi. Mladi pa so tveganjem zlorabe osebnih podatkov še posebej izpostavljeni, saj so na spletu bolj pripravljeni deliti svoje osebne podatke, kot starejši. Kraja identitete je sicer zelo redka, saj hekerji ponavadi izbire ne prepuščajo naključju in ciljajo na znane oziroma vplivne osebe. Vseeno pa je glaven del za zaščito odvisen od uporabnika, ki mora za zagotavljanje varnosti na spletu uporabljati različna in zahtevna gesla.

2.12 Samorazkritje

Samorazkritje je pojem, ki bo pogosto uporabljan v nadaljevanju, predstavlja pa razkritje osebnih podatkov, mišljenja, osebnih fotografij in videov. Samorazkritje (*self-disclosure*) je

definirano kot prostovoljno in namerno razkrivanje osebnih informacij ostalim članom spletne skupnosti (Archer v Li in drugi 2015). Poznamo *opisno samorazkritje* (osebna dejstva) in *ocenjevalno samorazkritje* (čustva, mnenja in sodbe) (Derlega in drugi v Li in drugi 2015). Pri opisnem samorazkritju gre za razkrivanje osebnih dejstev (tj. rojstni datum, domač naslov, identiteta, kontaktni podatki, družinsko drevo), pri ocenjevalnem pa gre za izražanje čustev, mnenj, prepričanj in sodb (tudi osebne preference – npr. okus glasbe, sojenje drugih ljudi, dogodkov itd.) (Derlega in drugi v Li in drugi 2015). Samorazkritje na spletu lahko poteka pasivno (objava na profilu, straneh, blogih) ali pa interaktivno (spletne interakcije med drugimi uporabniki – pogovori preko zasebnih sporočil, e-pošte in tudi pogovori v komentarjih) (Bryce in Klang 2009, 162). Samorazkritje obeh vrst naj bi vplivalo tudi na večjo samozavest in družbeno kohezijo, ki izraža pripadnost večji skupnosti. Pojavi se zanimiva razlika med spoloma: moški naj bi razkrili več osebnih informacij (opisnih), ki so objavljene na profilu – torej dostopne vsem, kot pa ženske (Hollenbaugh in Ferris 2015, 457).

Samorazkritje velja kot pomemben dejavnik pri medosebnem zaupanju, med drugim pa je zelo pomembno tudi v trženjskem oziroma marketinškem smislu, v odnosu med uporabnikom in podjetjem. Pripravljenost posameznika, da razkrije informacije, ima namreč tudi neposreden učinek potrditve zaupanja določeni organizaciji ali skupnosti (Loiacono 2014, 67). Obstaja tudi tveganje, ki so mu osebe izpostavljene, če razkrijejo občutljive oziroma osebne informacije. Predvsem to velja za razkrivanje informacij marketinški organizaciji, saj lahko tako na podlagi osebnih karakteristik in zanimanj le-te ustvarijo nabor stvari, ki so vredne promoviranja pri taki osebi in tako nekako predvidevajo oziroma ugotavljajo posameznikove preference. Pojavljajo se dileme, kjer se posamezniki sprašujejo, ali je vsebina primerna za objavo in ali bi lahko imela negativne posledice ter kakšne bi te bile. Göritz (2007, 42) pravi, da zavedanje tveganja zmanjšuje namero osebe, da bi opravila nakup na spletu, sledila prodajalčevim nasvetom in razkrila osebne informacije.

Nespametno ali neprimerno samorazkritje na spletu lahko na primer negativno vpliva na možnost zaposlitve, lahko ima posledice za osebno življenje posameznika in samorazkrita osebo spremlja vse življenje. Primer predstavlja samomor osebe, ki je poslala erotičen video svojemu nekdanjemu fantu, da bi vzbudila ljubosumje. Posnetek je bil kasneje deljen po svetovnem spletu in dosegel veliko število ogledov, dekle pa si je zaradi tega vzelo življenje (Sanghani 2016). To je predvsem problematično pri mladih, ki se posledic previsoke stopnje

samorazkritja ne zavedajo. Pri opisnem in ocenjevalnem samorazkritju se med člani razvije višja stopnja medosebnega zaupanja, saj ta temelji na izmenjavi podatkov. Pri opisnem samorazkritju gre za razkrivanje osebnih dejstev, pri ocenjevalnem pa gre za izražanje čustev, mnenj, prepričanj in sodb (Derlega in drugi v Li in drugi 2015). Samorazkritje na spletu pogosto poleg objave sporočila na forumu zajema tudi objavo podatkov na svojem profilu (kontaktni telefon, naslov, hobiji oziroma konjički itd.), objavo fotografij, mnenja itd. Loiacono (2014, 66) pravi, da informacijski sistemi spodbujajo interakcije med osebami, forumi in spletne skupnosti pa le-te omogočajo.

Loiacono ugotavlja, da so ljudje iz držav, kjer je prisoten močan vpliv vere, manj pripravljeni posredovati svoje osebne podatke oziroma se javno samorazkriti. Bryce in Klang pravita, da so mlade osebe bolj izpostavljene in občutljive pri obeh vrstah samorazkritja, saj nad njimi preži grožnja kibernetkega ustrahovanja (*cyberbullying*) in spolnega izkoriščanja v višji meri kot nad drugimi starostnimi skupinami (2009, 164). Mladostniki na spletu največkrat razkrijejo osebne informacije, kot so spolna usmerjenost, zasebna lastnina (fotografije novih materialnih dobrin, potovanj), razkritje hobijev ter drugih preferenc (npr. stil glasbe), pa tudi občutljivejše podatke, kot so domač naslov, telefonska številka, rojstni datum, družinsko drevo.

3 TVEGANJA MLADOSTNIKOV NA SPLETU

V tem delu bom na kratko predstavil najpogostejša tveganja na spletu, ki so jim izpostavljeni mladi. Predstavil bom tudi vpliv spleta na zasebnost oziroma skušal utemeljiti, kako nam splet krati zasebnost oziroma zasebno spreminja v javno. Obenem bom predstavil načine reguliranja otrok na spletu, ki so na voljo staršem (programi, naprave in pripomočki). Splet je okolje, kamor se je večina stvari prenesla, kljub temu, da starši pogosto mislijo, da je bolj varen kotiček kot zunaj spletni, »offline« svet. Nasilje, sovražni govor, grožnje in izsiljevanje so v družbenem okolju prisotni odkar štejemo leta, v spletnih skupnostih (ang. *online communities*) pa so se te nevarnosti preselile iz zunaj spletnih (*offline*). Splet predstavlja tudi nekakšen medij, s katerim je možno deliti in prikazovati nasilje v različnih oblikah, največkrat pa se pojavlja v videih in fotografskem prikazu nasilja. Video igre lahko prav tako prikazujejo nasilje in vplivajo na posameznikovo osebnost, saj se v večini iger mladi poistovetijo z virtualno ikono sebe in z njo sami ustvarjajo nasilne prizore. Glede nasilnih iger Šterk in drugi nazorno predstavijo različne, nasprotujoče si teorije. Stimulacijska teorija tako pravi, da računalniške igre pripomorejo k temu, da so igralci bolj agresivni tudi v zunanjem svetu, nasprotno pa trdi inhibicijska teorija, po kateri naj bi bili ljudje, ki igrajo nasilne igre, v zunanjem svetu manj agresivni. Tretja, habitualizacijska teorija pravi, da igre nimajo nobenih vplivov na zunanje vedenje ljudi, katarzijska teorija pa zagovarja stališče, da nasilne igre sproščajo in s tem zmanjšujejo nasilnost igralcev (Šterk in drugi 2006, 72). Navade uporabe spleta gotovo prinašajo tudi razlike med spoloma in seveda je marsikaj odvisno od starostne skupine. Fantje se tako verjetno bolj zanimajo za računalniške igrice, dekleta pa za glasbo, video vsebine, spletne skupnosti in spletne interakcije oz. pogovore. Na vprašanje, zakaj so na internetu, večina mladih odgovarja, da zato, ker se pogovarjajo s prijatelji, da se zabavajo, sproščajo in zaradi dolgčasa (Fornazarič 2010, 102). Do enakih ugotovitev so pripeljali tudi rezultati ameriške raziskave. Dodajajo pa še ugotovitve, da pretirana uporaba interneta lahko povzroči družbeno izolacijo in depresijo, predvsem med mladimi. Ugotavljajo tudi, da so mladi bolj zaupljivi s svojimi podatki na spletu, medtem ko skušajo starejši podatke čimbolj zakriti in jih ne podajajo prostovoljno (Gross 2004, 633). Starši, ki so sodelovali v tej raziskavi, so izrazili skrb, da njihovi otroci na internet zahajajo prepogosto in da imajo zaradi tega tudi slabše rezultate v šoli (Gross 2004, 635).

3.1 Zloraba osebnih podatkov

Tveganja zlorabe podatkov stalno naraščajo, saj se podatki shranjujejo na strežnikih, ki so locirani v državah sedeža podjetja. Po zakonih, ki jih država predpisuje, je možno do podatkov dostopati. Primer so strežniki Facebooka, ki so locirani v Ameriki: posledično je možno dostopati do podatkov uporabnikov po pravilih, ki jih postavljajo ZDA. Predvsem se bom osredotočil na varnost objavljanja osebnih podatkov (npr. Facebook, Instagram, blogi in druga spletna mesta), ki so priljubljeni med mladimi. Z objavo osebnih podatkov se večina ljudi, predvsem mladih niti ne zaveda, kako enostavno se da podatke izrabiti in jih uporabiti v "zle" namene. Kot primer tega bi izpostavil rop hiše po tem, ko je neko dekle na FB objavilo status, da gre na koncert z zaročencem, med drugim pa je bil pod osebnimi podatki viden njen domači naslov. Roparji oziroma nekdo izmed njenih Facebook prijateljev je odsotnost izkoristil in oropal hišo. Tukaj pridemo do prvega vprašanja – ali so virtualni prijatelji vredni našega zaupanja oziroma kako presodimo, komu bomo dovolili dostop do svojih osebnih podatkov? Študija, ki se je ukvarjala s težavo razkritja informacij na Facebooku (Zlatolas in drugi 2015, 161), je pokazala, da v nekaterih primerih posamezniki razkrijejo informacije (predvsem opisne) osebnega značaja, za katere niso vedeli, da so jih razkrili. To lahko ponazorimo s primerom vpisa telefonske številke na Facebook, ki naj bi delovalo kot varnostna zanka, vendar je lahko številka ob prehitrem kliku na gumb »shrani« vidna vsem prijateljem, včasih pa je bila lahko vidna celo vsem uporabnikom Facebooka. Obstajajo tudi ljudje, ki se na varnost ne ozirajo in objavijo osebne podatke brez zadržkov in brez ozira na morebitne posledice.

Pogoste pa so tudi zlorabe podatkov v namen norčevanja oz. ustrahovanja (ang. *bully*) iz določene zadeve ali objave na spletu. Glede na to, da bomo internet uporabljali praktično celo življenje, menim, da bi morali otroke poučevati o posledicah objav vsebine na spletu oziroma o uporabi spleta na splošno. Problematiko nevedenja oziroma neznanja uporabe spletnih vsebin je potrdila tudi nedavna raziskava, izvedena na Stanfordu, kjer so ugotovili, da večina (82 %) študentov in srednješolcev ne loči lažnih objav oziroma novic na Facebooku (Shellenbarger 2016). Izpostavljajo pomembnost medijske pismenosti, saj mladostniki preživljajo vse več časa na spletu – po zadnjih podatkih je to približno 8 ur dnevno.

3.2 Razkrivanje osebnih podatkov neznancem

Desjarlais ugotavlja, da je samorazkritje neznancem bolj pogosto na spletu, ker so ljudje tam bolj sproščeni, saj je prisotna fizična distanca, ki med ljudmi ustvari večjo stopnjo odprtosti, predvsem pri stvareh, o katerih v živo ne bi govorili (2015, 718). Na podlagi prejšnjih raziskav ugotavljajo, da je pri dejavniku samorazkritja zelo pomembna starostna skupina, saj mladi razkrijejo več intimnih ali osebnih informacij. Glede dejavnika spola so bile raziskave preveč variabilne, da bi lahko trdili, kateri spol je bolj nagnjen k razkritju osebnih informacij. Spletno samorazkritje je na podlagi raziskav pokazalo pozitivno povezanost z ustvarjanjem in vzdrževanjem spletnih in izven spletnih prijateljskih zvez, pripravljenost pomagati (altruizem) in zaupanje (Desjarlais in drugi 2015, 724). »Doxing« je angleški izraz, ki nima slovenskega prevoda, gre pa za spletno iskanje in posredovanje osebnih ali identifikacijskih podatkov neke osebe ali organizacije večjemu številu ljudi. Pomeni narediti zasebne podatke in informacije javne z namenom neko osebo javno izpostaviti – tukaj gre predvsem za znane osebe, ki jih želi nekdo izpostaviti medijskemu pritisku (McIntyre 2016, 113). Ponovno se nam odpre vprašanje, kdo ali kaj mlade na spletu najbolj ogroža in izkorišča. To so lahko korporacije s prikritimi oglaševalskimi ali marketinškimi prijemi, ki mladim sponzorirajo vsebino na podlagi »zlorange« ali pa zavestnega posredovanja osebnih podatkov in preferenc. Lahko pa so tudi ekstremisti, ki preko spleta širijo svoja skrajna stališča in ideološko propagiranje, ali pa kriminalne združbe oz. kriminalni posamezniki.

Raziskovalci poročajo, da so pomisleki glede varnosti negativno povezani z opisnim razkritjem informacij in da člani skupnosti podatke pogosto razkrijejo, vendar raje uporabijo možnost omejitve prikaza podatkov le določenim osebam, tj. skrijejo podatke pred gosti, neregistriranimi uporabniki in osebami, ki niso njihovi prijatelji na družbenem omrežju (Varnali in Toker 2015, 2). Še ena zanimiva raziskava, ki se je zopet ukvarjala s primerom Facebooka, je postavila teorijo, da bodo ljudje z višjo željo po pripadnosti neki skupnosti bolj spoštovali pravila ter se razkrili v večji meri kot druge osebe. Pri tem imajo, kot smo že poudarili, velik vpliv tudi zaupanje, želja po popularnosti in samozavest posameznika (Christofides in drugi 2012, 49).

3.3 Zasvojenost z internetom in sodobno tehnologijo

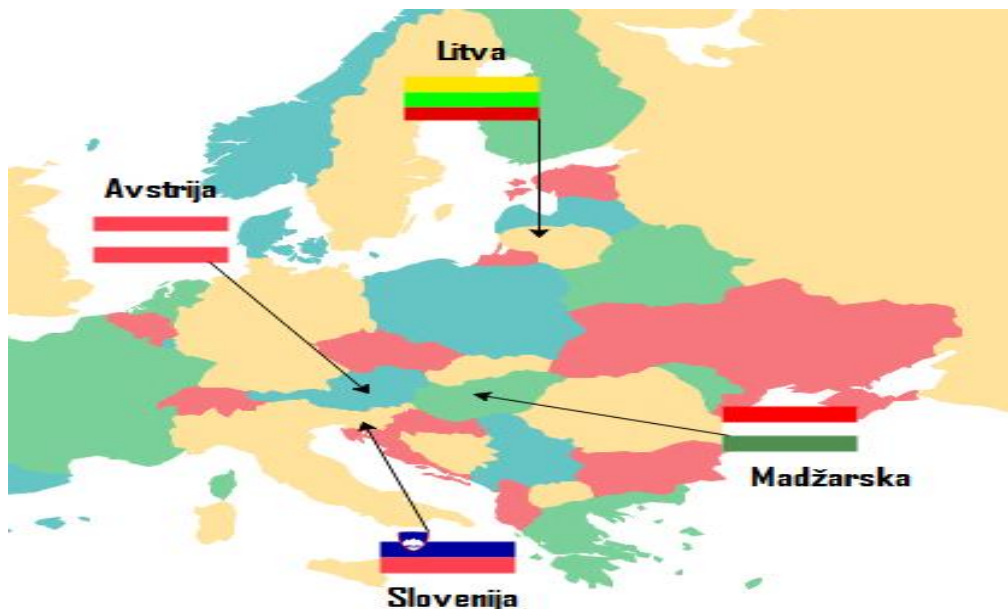
Internet je danes nepogrešljivo orodje za življenje, obenem pa lahko zaradi vsakdanje povezanosti z njim hitro vodi v zasvojenost. *Zasvojenost* delimo na fizično in psihično, pri definiranju zasvojenosti pa gre pogosto za neko vrednost, ki se dogaja bolj pogosto, kot je normalno. Pri uporabi interneta (koliko, kdaj, na kakšen način uporabljamo internet) normalna vrednost ne obstaja. Uradno tako težave, povezane z internetom, še ne obstajajo. Kar pa ne pomeni, da nekateri ekstremni pojavi zasvojenosti z internetom niso dobili različnih odgovorov.

Na Kitajskem je bila leta 2005 odprta prva klinika na svetu, ki ponuja zdravljenje zasvojenosti z internetom, tehnologijo in igranjem računalniških igrar. V Južni Koreji, kjer stopnja zasvojenosti z internetom oziroma sodobno tehnologijo (14 %) velja za najvišjo, se te »bolezni« preko javnega zdravstvenega sistema zdravi približno 8 % prebivalstva (Suisa 2015, 29). Na Hrvaškem so ravno v letu 2017 odprli prvo kliniko za zdravljenje odvisnosti od interneta, sodobnih tehnologij ter naprav. Pobuda je prišla s strani raziskave, ki je ugotovila, da hrvaški srednješolci na računalniku vsak teden preživijo isto količino časa, kot njihovi starši v službi (Karačić in Orešković 2017, 9). V Sloveniji zasvojenost z internetom uradno še ni prepoznana, zato se tudi ne odpravlja oziroma zdravi v okviru javnega zdravstvenega sistema, so pa glede tega zelo dejavne nekatere nevladne organizacije. Center Log Out je prvi specializirani center za pomoč pri prekomerni rabi interneta, ki omogoča brezplačne pogovore s strokovnjaki s tega področja. Težava pri definiranju zasvojenosti z internetom, računalnikom oziroma sodobno tehnologijo nastane tudi zato, ker večina ljudi danes po 8 ur dnevno uporablja računalnik in se to sprejema kot normalno in sprejemljivo vedenje. Med mladimi se je v zadnjih treh letih raba interneta več kot potrojila (Ofcom 2015, 108). Kljub temu poteka uporaba sodobnih tehnologij tudi v prostem času, kar na koncu predstavlja praktično ves dan. Internet tako izjemno determinira vedenje, obnašanje in način življenja takšnega posameznika. Tehnologija nas po mnenju strokovnjakov iz centra Log Out naredi asocialne, kljub temu, da sami mislimo, da smo družabni. To pa predstavlja nekakšen začaran krog, v katerem se znajdejo prav vsi uporabniki sodobnih tehnologij – najbolj pa so temu podvrženi mladi (Duggan 2014). Na mlade pa ima močan vpliv tudi sodobna tehnologija, kot so telefoni. Zato veliko mladih telefone menjava pogosto le zato, da bi imeli najsodobnejšo in najboljšo napravo, kljub temu, da star telefon še vedno deluje.

Višja stopnja participacije na spletu med mladimi je posledično povezana z večjo izpostavljenostjo nevarnostim in zasvojenosti z internetom. Zasvojenost brez dvoma predstavlja obširen problem med mladimi, saj je eden izmed dejavnikov, ki so povezani z varnostjo mladih na spletu. Raziskava o skrbi za zasebnost na spletu je pokazala, da več kot so uporabniki razkrili opisnih ali ocenjevalnih informacij oziroma se zavedajo razkritja le teh, bolj bodo obiskovali točno določeno spletno skupnost (Staddon in drugi V Zlatolas in drugi 2015, 158). Iz tega lahko sklepamo, da bolj kot uporabniki skrbijo za svoj profil, večkrat bodo prisotni na spletu, kar lahko nakazuje k zasvojenosti. Obenem pa se tudi briše meja med resničnim in ljudje v ospredje postavljamo virtualne interakcije, osebni stiki pa vse bolj izginjajo.

3.4 Odprt dostop do interneta oziroma nenadzorovanost

Prost dostop do spletnih vsebin slovensko mladino po mnenju strokovnjakov izpostavlja večjim nevarnostim. To velja predvsem za najmlajše, ki se s spletom še spoznavaajo. Te ugotovitve so bile potrjene tudi z izvedbo raziskave EU Kids Online, kjer je bila slovenska mladina uvrščena med ne-nadzorovane uporabnike spleta. To pomeni, da lahko otroci neomejeno, brez nadzora staršev ali različnih programov dostopajo do svetovnega spleta in vseh vsebin, ki so tam na voljo.



Slika 3.1: Mladi nenadzorovani uporabniki spleta v Evropi
(Lastna izdelava slike)

Programi, ki onemogočajo, ali pa omejujejo dostop do spleta, so sicer vsakdanja praksa čez lužo, kjer starši ameriške mladine s pomočjo brezplačnih in tudi plačljivih programov omejujejo količino časa na spletu in vsebine, do katerih njihovi otroci dostopajo. Skoraj vsa družbena omrežja so brezplačna ter imajo tudi zaradi tega veliko število rednih uporabnikov. Vendar večina povprečnih uporabnikov ne ve, da uporabo omrežij plačajo s svojimi podatki. Več kot objavijo – več so vredni v očeh oglaševalcev in posledično prinesejo večji donos oglaševalcem. Zaradi oglaševalskih zakonov imajo tudi družbena omrežja določeno minimalno starost uporabnikov, saj Facebook dejansko beleži obiske spletnih strani v času, ko smo prijavljeni vanj in nam promovira podobne stvari, ki so od ponudnikov, ki za oglaševanje plačajo. Iz prakse pa vidimo, da to mladih ne ovira pri ustvarjanju profila na Facebooku, saj pogosto izberejo drugo letnico rojstva, da se lahko registrirajo. Slovenski mladostniki niso deležni izobraževanj o varni rabi spleta v sklopu rednega učnega načrta osnovnih ali srednjih šol. Nekatere šole organizirajo posebne delavnice, ki pa niso obvezne za vse učence in pogosto niso deležne pretiranega zanimanja. Pri nas primanjkuje konkretnega seznanjanja mladih o varni rabi interneta, zatrjujejo strokovnjaki, ki se ukvarjajo s preučevanjem mladih na spletu. Mladi pri nas se sicer vedno bolj zavedajo tveganj objave osebnih informacij na spletu, kar kažejo rezultati raziskave EU Kids Online ter društva Log Out. Vseeno pa izredno pomembno vlogo igrajo starši in učitelji, ki naj bi mlade seznanjali s tveganji in nevarnostmi na spletu. Zasvojenost s spletom predstavlja posledico rabe interneta, najbolj so izpostavljeni mladi, ki jih tehnologija obdaja na vsakem koraku. Starejši kljub uporabi interneta v službi niso tako kritična skupina kot mladi, pravijo na centru Log Out.

Nedavni dogodki, povezani s spolnimi zlorabami mladih in otrok preko spleta, so dobili veliko medijsko in javno pozornost, vendar za zdaj ni bilo podanih nobenih konkretnih rešitev ali predlogov. Ko gre za takšno temo, se poraja vprašanje o tem, kako daleč novinar sme iti z zgodbo in kakšne podatke lahko objavi, da ne razkrije identitet žrtev zlorab, zaradi dostojnosti oziroma občutljive teme, ki je za mlade že zaradi samega dogodka destruktivna. Glede preprečevanja zlorab mladih na spletu je Slovenija še v fazi razvoja, vendar aktivno sodeluje z mednarodnimi agencijami in drugimi državami (Europol). Kar se tiče nadlegovanja na spletu, ga je težko ustaviti, saj je pogosto primer tak, da se neka oseba izdaja za drugo osebo, ki naj bi bila iz iste starostne skupine kot žrtev, mladi pa takšne prevare stežka zaznajo. Glavno vlogo pri preprečevanju zlorab mladih na spletu igra projekt, podprt s strani Evropske komisije, imenovan Police2Peer, ki identificira osebe, ki na splet posredujejo

ali pa si ogledujejo posnetke zlorab otrok. O tem jih obvesti ter opozori, da se dogaja kaznivo in ilegalno dejanje, uporabnikove podatke pa posreduje tudi lokalnim organom pregona.

Spletna nadlegovanja so v zadnjih letih krepko narasla in izkoriščajo naivnost in nevednost mladih uporabnikov spleta. Na portalu Spletno oko so v letu 2016 obravnavali 185 prijav posnetkov spolnih zlorab otrok in 1273 prijav sovražnega govora. Na nacionalnem odzivnem centru za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (SI-CERT) podatkov za leto 2016 še nimajo, lahko pa z gotovostjo trdijo, da je bilo v tem letu daleč največ prijav incidentov. Mladi so na spletu predvsem hitrejši, vendar ne tudi previdnejši. Z leti pridobimo tudi več življenjskih izkušenj, ki vplivajo na naš spletni (ang. *online*) in zunaj spletni (*offline*) svet. Številka po mnenju predstavnice centra za leto 2016 zagotovo presega 3000 različnih prijav, ki so jih posredovali uporabniki spleta v Sloveniji. V letu 2016 pa je bilo največ intervencij pri izsiljevalskih virusih (SI-CERT 2017).

Na spletnem seminarju Varna raba interneta in naprav (*Massive Open Online Courses – MOOC-V*) je bila odprta zanimiva tema, ki zaenkrat še ni bila rešena in ima zelo nasprotujoča si mnenja. Učiteljica je opozorila, da ima nekaj osnovnošolcev na sebi pametno uro, ki staršem omogoča sledenje vsakega koraka, ki ga naredijo, in tudi snemanje ter poslušanje »v živo«. Nekateri učitelji osnovnih šol so izrazili prepričanje, da je to prepovedano in kaznivo, drugi pa so označili to kot sprejemljivo in pametno, saj staršem omogoča sledenje in nadzor njihovih otrok. Nekateri so to opravičevali kot nujno potrebno, vsaj za najstnike v »težavnih« letih, drugi pa so trdili, da je to sporno iz vseh pogledov in da morajo tudi otroci imeti nekaj zasebnosti. Nadzor je po mnenju strokovnjakov potreben toliko časa, dokler otrok ne pride do stopnje, da lahko sam odgovorno presodi, ali mu določeno dejanje na internetu lahko povzroči škodo ali ne. Pri mlajših otrocih morajo starši redno opazovati, kaj otroci počnejo na internetu, in jih opozarjati na nevarnosti in napačna ravnanja. Pri mladostnikih je bolj kot spremljanje njihovega početja na spletu pomembno opaziti spremembe v vedenju, ki so povezane z uporabo interneta, računalnika, tablic in telefonov (povzeto po Kemperle 2016). Zato so programi, ki omogočajo spremljanje otrokovega početja na spletu, zelo uporabni in priporočljivi.

3.5 Vohunski programi in virusi

Vohunski (ang. *spyware*) programi se lahko na računalnik namestijo z virusom ali pa z obiskom okužene spletne strani. Včasih se ti programi skrivajo tudi v okuženih datotekah. Ti programi sicer za računalnik niso nevarni (tako kot npr. virusi), vendar so ustvarjeni za vohunjenje in krajo osebnih podatkov, kot so gesla, datoteke in osebni dokumenti. Te podatke program preko interneta posreduje osebi, ki je ustvarila program. Programi so lahko namenjeni tudi sledenju obiska spletnih strani ali v marketinške namene (promocija spletne strani ali izdelka). Takšno oglaševanje sicer ni dovoljeno, vendar se zelo redko odkrije, saj povprečen uporabnik takšnega vsiljenega oglaševanja pogosto sploh ne zazna. Trenutno so v porastu t. i. Facebook virusi, ki se namestijo le s klikom na povezavo. Ker vohunski program s pomočjo Facebooka in preferenc uporabnika (všečki ali ang. *likes*) izgradi profil osebe, so dobički visoki, saj uporabnik dobiva le oglase za stvari, ki naj bi ga zanimala.

3.6 Prenašanje nelegalnih ali piratskih vsebin

Po zadnjih podatkih agencije za intelektualno lastnino EU (*European Union Intellectual Property Office* – EUIPO) 30 % mladih (15–24 let) v Evropi preko spleta redno namerno kupuje ponaredke (oblačil, telefonov, čevljev ipd.) in redno prenaša piratske vsebine kot so filmi, glasba in serije (Deloitte 2017, 18). EUIPO državam članicam predlaga večji nadzor nad posredovanjem in deljenjem avtorsko zaščitene vsebine po spletu in izvajanje preventivnega izobraževanja nad mladimi uporabniki spleta.

S prenašanjem avtorsko zaščitene vsebine se krši zakon o intelektualni vsebini, ki je v nekaterih državah zelo strog (npr. Nemčija), ponekod pa se to področje niti ne nadzoruje oziroma izvaja. Med drugim je zakon manj strog v Sloveniji, kjer prenos digitalnih vsebin brez dovoljenja sicer ni dovoljen, vendar se nadzor in kaznovanje kršiteljev zaenkrat še ne izvajata. Po zakonu je dovoljeno gledanje piratskih vsebin preko spleta (ang. *stream*), ni pa dovoljeno vsebin prenesti na računalnik. Prenos nelegalnih vsebin, kot so filmi, je sicer popularen tudi med starejšimi, zaradi katerih mladi tudi najbolj pogosto opravičujejo svoja tovrstna dejanja, saj je pogosto zgledujejo po starejših. V Evropi tako kar 68 % ljudi prenaša ali gleda piratske vsebine (Evropska komisija 2014, 22).

V prenesenih vsebinah pa se pogosto skrivajo virusi in vohunski programi, ki lahko prinesejo gromozanske stroške zlorabe osebnih podatkov, izsiljevalskih virusov ali pa uničenega računalnika. Če mladi (oziroma uporabniki spleta) nimajo dovolj velike seznanjenosti s tveganji, pa takih virusov velikokrat niti ne opazijo, saj delujejo v ozadju programa.

3.7 Medijska (ne)pismenost

Glede varnosti je potrebno omeniti pomembne dejavnike, ki mladim pomagajo do regulacije objave osebnih podatkov, tj. preventive in seznanjanja mladih o tveganjih javne objave podatkov. *Medijska pismenost* je način, da pridemo do kritičnih in zdravih uporabnikov interneta. Klasična pismenost je danes tako nujno potrebna za razumevanje medijske pismenosti, ki predstavlja »novo dimenzijo«. Medijska (ne)pismenost tako mladih, kot tudi starejših predstavlja vse večjo nevarnost, da ogrozi razvoj sodobne, pametne družbe.

Medijska pismenost se navezuje na objavo osebnih podatkov in tudi na bolj vsakdanje stvari, kot je kritično branje novic. Predvsem mladi in starejši ljudje imajo težave s prepoznavanjem lažnih novic (ang. *fake news*) in prav tako oglasnih reklam ter »pravih« novic. Medtem ko so mladi vse bolj vešči uporabe tehnologije, jim drastično primanjkuje kakih drugih veščin, kot sta denimo splošna razgledanost in razsodnost. Zakaj bi se sploh kaj učili, ko pa nam lahko vse v hipu pove stric Google? Številni poudarjajo pomembnost tehnološkega razvoja za družbo, po drugi strani pa »digitalizacija« predstavlja nejasno prihodnost posameznikov, ki tehnologije ne uporabljajo oziroma so medijsko nepismeni. Uporabniki tehnologije so lahko derivirani zaradi finančnega položaja, fizičnih ovir ali pa iz lastnih prepričanj. Vse to ustvarja nekakšno ločnico med digitalno izobraženimi in digitalno neizobraženimi. Seznanjenost z mediji in informacijska družba sta tako danes pozitivna kazalnika oziroma indikatorja razvite družbe ali posameznika. Uporaba spleta v mladih letih izkazuje tudi hitrejši kognitivni razvoj pri otrocih (Norris in Inglehart 2009, 47).

Kar nekaj raziskav poudarja, da mladi, ki uporabljajo splet, tudi dosegajo boljše rezultate v šoli. Po drugi strani pa vsi vemo, da obstajajo tudi negativni vplivi rabe interneta med mladimi, kot so zasvojenost, pretirano igranje računalniških iger, lažja podrejenost zasvojenosti z različnimi substancami itd. Problematika uporabe interneta je tesno povezana s stanjem medijske pismenosti in kritičnega razločevanja novic.

3.8 Spletno nadlegovanje in sovražni govor

Spletno nadlegovanje se lahko pojavi v različnih oblikah, kot je draženje, pošiljanje zlobnih sporočil ali pa je bolj podobno spletnemu ustrahovanju. Vsekakor predstavlja neko dejanje, ki si ga vsaj ena oseba v skupini ne želi. Po podatkih raziskave Mladi na netu se mladi na zlobna sporočila odzovejo negativno in »udarec« z žaljivim komentarjem vrnejo osebi, kar ima pogosto še slabši končni učinek (Lobe in Muha 2011, 39). Prav zaradi sovražnega govora in vsebine pa so za otroke zelo priporočljivi programi, ki omejujejo prikaz vsebine in omogočajo blokiranje oziroma filtriranje sporne vsebine.

Sovražni govor je pri mladih bolj redek, vendar je večinoma usmerjen v ožje skupine, ki so pogosto stereotipizirane, ksenofobične ali rasistične. Sovražni govor je najbolj pogost na forumih in spletnih straneh, kjer se otroci ne zadržujejo prav pogosto. Nekoliko manj sovražnega govora je mogoče videti na družbenih omrežjih, saj tam ni mogoče neki osebi pisati, če z njo nisi prijatelj, poleg tega pa ima vsak posameznik dovoljenje za izbris vsebine, v forumih pa to vlogo prevzema moderator. Večinoma pa sovražni govor in spletno ustrahovanje sovpadata, saj gre za namero neko osebo prestrašiti z grožnjami.

4 VLOGA INSTITUCIJ IN STARŠEV PRI IZOBRAŽEVANJU MLADIH O VARNI UPORABI SPLETA

V tem delu bom predstavil možnosti izobraževanja mladih o spletu in IKT. V primerjavi s starejšimi prebivalci (Simbioza je nemara najbolj znan tovrstni projekt izobraževanja starejših) imajo mladi precej več možnosti za izobraževanje o uporabi spleta in IKT. Med drugim se o uporabi učijo že v osnovni šoli, kjer je računalništvo obvezen predmet. Po podatkih raziskave Eurobarometer skoraj 90 % slovenskih staršev trdi, da njihovi otroci v šoli niso deležni zadostne vzgoje o varni rabi interneta. Ti pa tudi trdijo, da tudi sami (starši) potrebujejo več ozaveščanja o tveganjih na spletu (Eurobarometer 2008 v Vehovar in drugi 2009). V nadaljevanju bom predstavil nekaj programov oziroma dejavnosti društev, ki se ukvarjajo z izobraževanjem mladih oziroma zagotavljajo varnost mladih na spletu.

4.1 Vloga izobraževalnih institucij pri informiranju mladih o varnosti na spletu

Šole vzgajajo mlade in jih učijo za njihovo življenje. Kljub temu številne izobraževalne institucije svojih učencev ne naučijo osnov varne uporabe računalnika in sodobnih tehnologij. Učenci v četrtem in petem razredu imajo na voljo kot izbirni predmet računalništvo, v šestem razredu pa je računalništvo obvezno. A velika večina učencev je računalnik uporabljala že pred tem, zato mislim, da bi morali starši svojim otrokom med prvimi pojasniti tveganja oziroma nevarnosti na spletu, v kolikor se učni programi izobraževalnih ustanov ne bodo prilagodili t. i. vsesplošni digitalizaciji.

4.1.1 Projekt SAFE-SI

Projekt SAFE-SI izvajajo Fakulteta za družbene vede, Zavod Arnes, Zveza prijateljev mladine Slovenije in Mladinsko informativno svetovalno središče Slovenije (Zavod MISSS). Financiran je s sredstvi Agencije INEA in Direktorata za informacijsko družbo pri Ministrstvu za javno upravo (Safe.si 2016). S svojo spletno prisotnostjo dosežejo več ciljnih skupin na spletu in jih obveščajo o varni rabi interneta po različnih družbenih omrežjih in na spletni strani. Nudijo razne nasvete, e-učilnice in gradiva, povezana z varno rabo interneta.

Predstavljajo točko osveščanja o varni rabi interneta in mobilnih naprav za otroke, najstnike, starše in učitelje (Safe.si 2016).

4.1.2 TOM

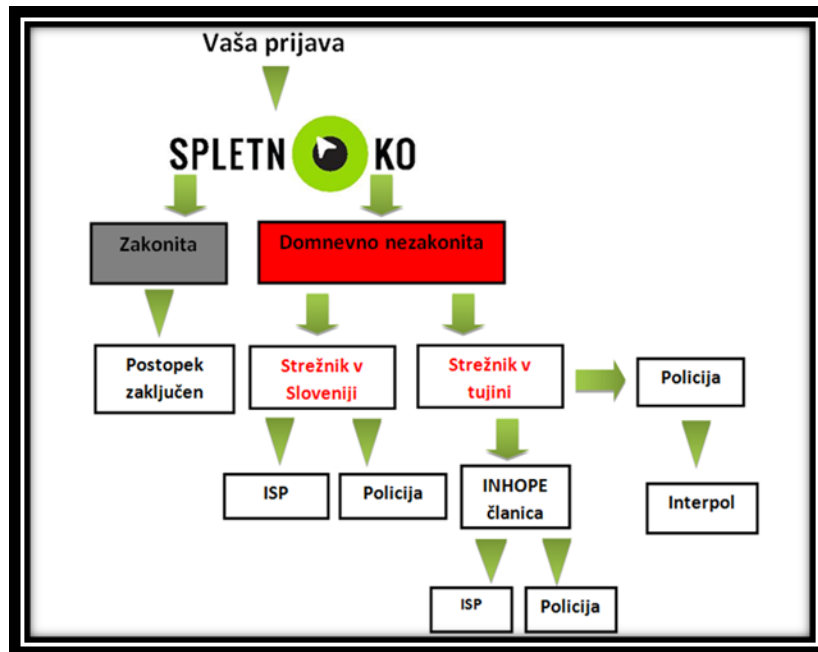
Telefon otrok in mladostnikov – TOM je projekt razvit v sklopu projekta SAFE-SI in mladostnikom zagotavlja 24 urno telefonsko podporo. Operaterji so mladim na voljo za kakršnakoli vprašanja, ki niso nujno povezana s spletom.

4.1.3 Spletno oko

Projekt Spletno oko je platforma, razvita s strani Centra za varnejši internet (SAFE-SI). Spletno oko tako zbira anonimne prijave sovražnega govora in otroške pornografije. Zbrane prijave najprej pregleda in jih v primeru resnih kršitev posreduje policiji (Spletno oko 2017). Prav letos (2017) pa mineva 10 let delovanja centra, ki navaja, da je v svojih letih delovanja prejel več kot 21 tisoč prijav.

Anonimno prijavo na njihovi strani lahko poda kdorkoli. Ključni podatek, ki ga mora prijavitelj podati je naslov spletne strani, na kateri se nezakonita vsebina nahaja. Če se vsebina nahaja na strežnikih druge države članice INHOPE omrežja, pa je prijava poslana tudi lokalnim organom te države. INHOPE je organizacija vseh spletnih prijavnih točk za nezakonite vsebine na internetu in skrbi za povezovanje in sodelovanje med točkami (Vehovar in drugi 2009). Največ prijav sovražnega govora pa je glede splene usmerjenosti, narodnosti in verskega prepričanja (Motl 2017).

V celotnem postopku, torej od prijave nezakonitih spletnih vsebin do ustreznega ukrepanja, se prijavna točka in Policija ukvarjata izključno z vsebino prijave, podatki o prijavitelju pa se ne hranijo (Spletno oko 2017).



Slika 4.1: Potek prijave na portalu Spletno oko
Vir: Safe.si 2016

4.1.4 Varni in internet

Varni in internet je organizacija, ki nudi izobraževalne programe o varnosti na internetu in pri uporabi sodobne tehnologije. Pripravljajo delavnice za otroke (6–11let), najstnike (12–15 let), mladostnike, odrasle, pedagoške delavce in tudi za podjetja oz. organizacije. S svojimi izobraževanji o spletu posameznikom pomagajo do nujno potrebnih znanj, ki so v sodobni dobi digitalne tehnologije potrebna za varno, odgovorno in učinkovito brskanje po spletu. Izobraževanja tudi prilagodijo glede na predznanje in potrebe posameznika (Varni in internet 2017).

4.1.5 Log Out

Center Log Out je prvi specializirani center za pomoč pri prekomerni rabi interneta, ki omogoča brezplačne pogovore s strokovnjaki iz tega področja. Deluje na dveh lokacijah v Sloveniji, in sicer v Ljubljani ter Izoli, kjer so svetovalci na voljo tudi za osebni pogovor. Na njihovo pomoč se največkrat obrnejo starši, katerih otroci prekomerno uporabljajo splet. Preventivno izvajajo tudi delavnice za starše v vrtcih, šolah in srednjih šolah, kjer staršem ponujajo izobraževanja v zvezi z zasvojenostjo z internetom in zmerno uporabo.

4.1.6 Varni na internetu

Varni na internetu je informativni in interaktivni portal za izobraževanje in prijavo vsebine ter oddajo zahtevka za pomoč pri težavah na spletu. Portal vzdržuje Slovenski center za posredovanje pri omrežnih incidentih SI-CERT, ki deluje pod okriljem javnega zavoda Arnes. SI-CERT predstavlja nacionalno kontaktno točko, ki opravlja posredniško in svetovalno vlogo ter prevzema tudi koordinacijo projekta osveščanja javnosti o informacijski varnosti. Projekt v celoti financira Ministrstvo za izobraževanje, znanost in šport - Direktorat za informacijsko družbo (Varni na internetu 2017). Ponuja vsakdanje nasvete pri uporabi spleta, rešitve za zaščito in nasvete, kako ravnati ob vdoru v e-poštni naslov, družbena omrežja ali po namestitvi virusov.

4.2 Vloga staršev pri zagotavljanju informiranosti mladih o varnosti na spletu

Starši igrajo glavno vlogo pri informiranju svojih otrok o spletnih nevarnostih. So večinoma prvi, ki svojemu otroku omogočijo dostop do spleta oziroma mu kupijo pametni telefon. Otroci imajo danes do tehnologije potrošniški odnos. Nov telefon ali računalnik sta zanje uporabna, vendar se po letu ali dveh pojavi potreba po novem, zmogljivejšem, in to kljub temu, da star telefon še vedno dela popolnoma brezhibno. To je danes še toliko bolj izrazito, saj vsak dan na trg pride kak nov telefon. Pametni telefoni počasi, a vztrajno izrivajo pomembnost računalnika, saj se mladi raje odločijo za malo boljši pametni telefon, ki dejansko omogoča večino funkcij, ki so na voljo na računalniku. Pri tem se tudi viša dnevna uporaba, ki je pri mobilnih telefonih težko ocenljiva oz. ranžirana, saj večina ljudi pametni telefon uporablja ves dan in nanj pogleda vsake toliko časa. Rezultati britanskega eksperimenta so pokazali, da povprečen človek preživi približno 6 ur dnevno na telefonu, na katerega pogleda najmanj 85-krat. To predstavlja približno tretjino dneva, če odštejemo čas nedejavnosti oz. spanja (Andrews in drugi 2015, 5).

Starši se morajo tudi sami poučiti o uporabi spleta in pametnih tehnologij, ta znanja pa jim ponujajo institucije, ki pripravljajo različne delavnice za starše. Po mnenju raziskovalcev so starši premalo poučeni o pomembnosti izobraževanja mladih glede varnosti na spletu. Ko gre za informiranje mladih o varni uporabi spleta, je zelo pomembno, da se zlasti najmlajše o tem pouči. Z leti pa se mladi tudi sami naučijo novih stvari in do 18. leta po navadi celo prehitijo starše v informiranosti o varni rabi interneta (Christofides in drugi 2012, 49). Obstajajo zelo

velike razlike med količino deljenih informacij preko spleta glede na starost. Mladi bolj pogosto javno delijo svoje osebne podatke kot starejši, saj se z leti spreminjata tudi način in namen uporabe spleta (Christofides in drugi 2012, 52). Starši otrokom kupujejo računalnike zato, ker jim želijo omogočiti nove možnosti za izobraževanje. Posledično so zelo razočarani, ko otroci računalnik uporabljajo za igranje iger in krajšanje prostega časa (Subrahmanyam 2001, 8). Starši poročajo tudi o povečani navezanosti na računalnik in na uporabo spleta, kar je bilo izrazito ob poizkusu odvzema računalnika oziroma omejitve rabe interneta (Subrahmanyam 2001, 17). V času izvajanja raziskave je bila zelo popularna igra Sims (tudi SimCity, SimLife), ki je bila po mnenju staršev glavni krivec za zasvojenost otrok z računalnikom. Razlog za to je, da so otroci živeli v virtualnem svetu in so po prihodu iz šole hiteli na računalnik, da so lahko čim prej gradili svojo virtualno družino in opravljali virtualna gospodinjska dela (Subrahmanyam 2001, 22). Kot je bilo že omenjeno, pri temi nasilnih iger obstaja deljeno mnenje strokovnjakov. Starši pa so opazili, da je kar 80 % iger, ki so jih igrali njihovi otroci, nasilnih. Povezave z zunanjim nasiljem ni bilo mogoče opaziti, kljub temu, da se je kar nekaj mladostnikov grdo vedlo do sovrstnikov in jim pogosteje grozilo (Subrahmanyam 2001, 25). Dokazana pa je tudi povezava, da bolj agresivne osebe tudi raje igrajo nasilne računalniške igre (Appelbaum in drugi 2015, 11).

5 RAZISKOVALNI NAČRT IN OPERACIONALIZACIJA

Za empirični del svoje diplomske naloge sem napravil dve kvantitativni in eno kvalitativno tehniko preučevanja. Orodje za zbiranje podatkov je predstavljala spletna anketa, ustvarjena na mestu za spletno anketiranje 1ka.si. Spletna anketa se mi je zdela najbolj primerna za zbiranje takšnih podatkov, saj mislim, da lahko s kvantitativnimi podatki dobim bolj natančen pogled v dejansko stanje glede varnosti na spletu. Vsebinsko pa bom svoje ugotovitve podprl tudi s predlogi in odgovori strokovnjakov na tem področju. Spletna anketa tudi predstavlja cenovno ugodno izhodiščno metodo za raziskovanje in proučevanje družbe.

Prvi del je predstavljala spletna anketa za mlade, ki je bila poslana šolam in promovirana na različnih kanalih, kot je Facebook stran Deskam varno. Vabilo k sodelovanju v anketi je bilo poslano na več 100 šol in na dijaške domove, katerih poštni naslovi so bili zbrani na spletni strani Ministrstva za izobraževanje, znanost in šport. Vabilo je bilo tudi natisnjeno in predano Zavodu MISSS, ki je vabila predalo udeležencem svojih delavnic po različnih slovenskih šolah. Za pomoč pri posredovanju anket mladim sem prosil tudi Majo Vreča, ki je sodelavka Arnesa, Centra za varnejši internet SAFE-SI in Slovenskega izobraževalnega omrežja (SIO). Med drugim tudi izvaja delavnice za učitelje osnovnih šol na temo varnost mladih na spletu - MOOC-V.

Drugi del je sestavljal spletni vprašalnik za starše otrok, v katerem sem se zanimal predvsem za nadzor mladih na spletu in preko različnih kanalov. Anketa je bila oglaševana interno in po drugih medijskih kanalih, kot so spletna stran MedOver.net, portal »Za starše« in Facebook. Med drugim pa je bila anketa poslana tudi na e-poštne naslove zveze aktivov svetov staršev z različnih koncev Slovenije.

Tretji način zbiranja podatkov je vključeval analizo sekundarnih podatkov oziroma že končanih raziskav drugih avtorjev in odgovore strokovnjakov na določena vprašanja, povezana s področjema varnosti mladih na spletu.

5.1 Enota analize in vzorec

Enota analize v moji raziskavi za mlade je en učenec oz. učenka zadnje triade osnovne šole oz. dijak oz. dijakinja srednje šole. Izbrane so bile vse šole, katerih e-poštni naslovi so dostopni na strani Ministrstva za znanost izobraževanje in šport, žal se je le nekaj šol je odzvalo povabilu. Na podlagi poslanih prošenj za sodelovanje v anketi sem šolam poslal navodila za izvedbo ankete oziroma jih prosil za posredovanje povezave do spletne ankete svojim učencem in dijakom.

Pri raziskavi za starše je enota analize en starš, ki izpolni anketo o navadah svojega otroka, ki je star med 11 in 17 let, ter odgovori na vprašanja v povezavi z nadzorom svojega otroka na spletu.

5.2 Tehnično ozadje izvedbe

Obe anketi sta bili narejeni s pomočjo orodja En Klik Anketa (www.1ka.si). Pred odprtjem ankete sem prosil več ljudi za mnenje in pripombe ter za približno 10 dni omogočil tudi testno obdobje. Po koncu testnega obdobja sem pripombe in nasvete uporabil za optimiziranje svojih vprašalnikov. Končna anketa med mladimi je bila po podatkih orodja 1KA dolga dobrih 10 minut, anketa med starši pa okoli 7 minut.

5.3 Zbiranje podatkov pri anketi za mlade

Zbiranje podatkov s spletnim vprašalnikom za mlade se je začelo 10. aprila 2017 in končalo 15. maja 2017. En mesec pred zbiranjem podatkov sem izbranim šolam poslal prošnjo za sodelovanje njihovih učencev v anketi. Ob odprtju ankete sem ponovno poslal prošnjo za sodelovanje oziroma posredovanje ankete mladim in kratek dopis za mlade. Ankete so bile poslane tudi na dijaške domove, zraven pa je bila tudi QR koda, ki je omogočala dostop do ankete preko pametnega telefona, saj je bilo vabilo objavljeno na oglasni deski. V tiskani obliki so vabilo dobili tudi udeleženci izobraževalnih delavnic, ki jih je organiziral zavod MISSS. Kar nekaj šol je upoštevalo moje predloge za zbiranje podatkov med uro računalništva, ko je vsak učenec na svojem računalniku, ki ima omogočeno povezavo do spleta. Anketa je ponekod tudi predstavljala nekakšen uvod v uro predavanja o spletni

varnosti. Učiteljem sem za primere težav posredoval tudi svoj elektronski naslov, na katerem sem bil na voljo za kakršnakoli vprašanja, vendar ni bilo nobenih zapletov med samo izvedbo anketiranja. Ostali kanali promocije ankete za mlade pa so v Prilogi A.

5.4 Zbiranje podatkov pri anketi za starše

Zbiranje podatkov za starše, ki vzgajajo otroka, starega med 11 in 17 let, se je začelo 18. aprila 2017 in končalo 6. maja 2017. Anketni vprašalnik je bil poslan na e-poštne naslove sveta staršev različnih osnovnih šol in deljen preko različnih kanalov na spletu in družbenih omrežjih. Staršem sem na zadnji strani omogočil tudi vpis e-poštnega naslova, če bi želeli prejeti ugotovitve moje raziskave. Za to se je odločilo 58 oseb. S tem, da sem staršem omogočil prejem rezultatov sem skušal vplivati na njihovo razmišljanje in prispevanje k varni uporabi spleta in sodobnih tehnologij njihovih otrok. Obenem pa mislim, da je imelo to tudi motivacijski vpliv za dokončanje ankete. Vsi kanali promocije ankete za mlade se nahajajo v Prilogi B.

5.5 Analiza rezultatov

Analizo rezultatov, ki bo predstavljena v naslednjem poglavju, sem opravil s programom IBM SPSS Statistics 22 za programsko okolje Windows. Iz spletnega strani 1ka.si sem najprej opravil izvoz v SPSS datoteko, nakar sem v programu SPSS podatke uredil in izločil neveljavne in neuporabne vnose (manjkajoče odgovore, odgovore z neveljavno vrednostjo starosti in podobno). Preveril bom tudi prisotnost statistično značilnih povezanosti med spremenljivkami. Za statistično značilno šteje spremenljivka, katere signifikanca je manjša od vrednosti 0.05. Moč povezanosti pa merimo s Paersonovim (intervalne), Cramerjevim (nominalne) ali Spearmanovim koeficientom povezanosti, ki se raztezajo med 0 in 1. Zaradi velikega števila nominalnih spremenljivk in doseženega cilja že z enostavnimi statističnimi analizami bolj naprednih analiz tudi nisem izvajal, saj sem dobil dovolj podatkov za kvalitetno delo. Veliko število nominalnih spremenljivk je bilo potrebnih in neizogibnih za podroben vpogled v dejansko stanje glede varnosti na spletu pri mladih.

5.5.1 Podatki pri anketi za mlade

Takoj po izvozu podatkov sem vzorec uredil (rekodiral in pod manjkajoče spremenil odgovore oseb, ki niso izhajale iz mojega vzorca), tako da nepopolne in neveljavne enote ne bodo uporabljene v nadaljnji analizi. Pri anketi za mlade sem dobil 1285 odgovorov, od tega je bilo za končno analizo primernih 571. Upošteval sem tudi delno izpolnjene ankete, tako da je bilo pri nekaterih vprašanjih več enot. Iz vzorca sem odstranil tiste, za katere je bilo vidno, da ankete niso vzeli resno (16).

Tabela 5.1: Končni vzorec ankete za otroke pred analizo
(Lastna izdelava tabele)

STAROST OTROKA		
VELJAVNI ODGOVORI	Število	Veljaven delež (%)
11	3	0,5
12	4	0,7
13	48	8,4
14	80	14,0
15	67	11,7
16	206	36,1
17	163	28,5
SKUPAJ VELJAVNI	571	100
MANKAJOČI	698 (55 %)	
SKUPAJ	1269	

5.5.2 Podatki vzorca pri anketi za starše

Pri anketi za starše sem dobil 2295 odgovorov, vendar je bilo od teh le 267 ustreznih za končni vzorec. Takoj po izvozu podatkov sem podatke uredil in pod manjkajoče spremenil odgovore oseb, katerih starosti otrok niso bile ustrezne mojemu vzorcu (npr. starejši od 17 let in mlajši od 11 let), tako da teh odgovorov pri nadaljnji analizi nisem upošteval. V moji anketi je sicer sodelovalo več žensk (74 %), večina anketirancev pa ima končano 6. stopnjo izobrazbe in je zaposlenih.

Največ prekinitev je bilo takoj po kliku na nagovor. Razlog za to je po mojem mnenju uporaba mobilnega telefona, saj je večina ljudi, ki so odprli povezavo na družbenih omrežjih, po podatkih na IKA dostopala preko mobilnega telefona in verjetno zato niso želeli izpolniti vprašalnika. Druga možna razlaga pa je, da so odgovarjanje prekinili zato, ker niso ustrezali kriterijem, kar pomeni, da osebe, ki so kliknile na anketo, nimajo otroka, starega med 11 in 17 let.

Tabela 5.2: Končni vzorec ankete za starše pred analizo
(Lastna izdelava tabele)

STAROST OTROKA		
VELJAVNI ODGOVORI	Število	Veljaven delež
11	18	6,7
12	49	18,4
13	42	15,7
14	75	28,1
15	13	4,9
16	58	21,7
17	12	4,5
SKUPAJ VELJAVNI	267	100
MANKAJOČI	2028 (88,68 %)	
SKUPAJ	2295	

6 INTERPRETACIJA REZULTATOV IN UGOTOVITEV RAZISKAVE MED OTROKI IN STARŠI

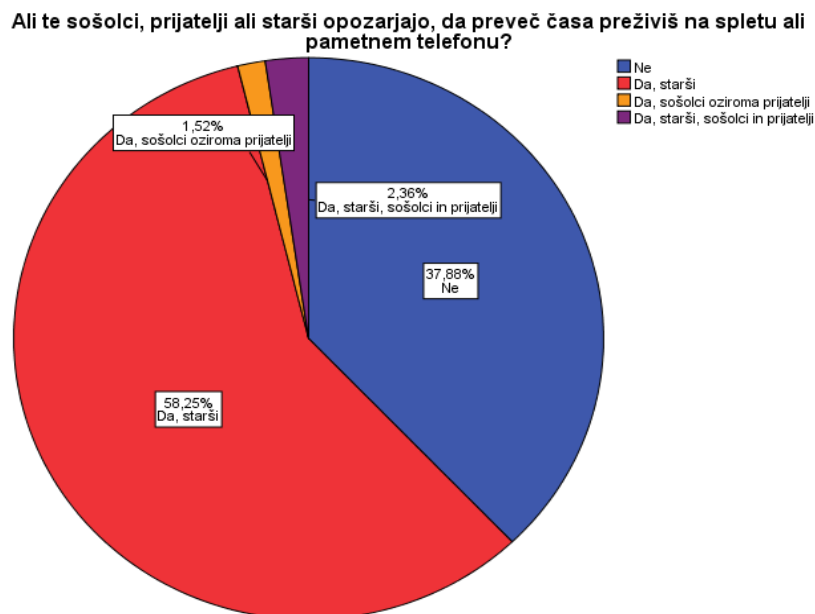
Empirični del moje diplomske naloge sta sestavljala dva anketna vprašalnika (Priloga C in Priloga Č), eden je namenjen starejšim osnovnošolcem in srednješolcem, drugi pa je namenjen staršem, ki imajo otroke iz te starostne skupine (11–17 let). V svojo diplomsko nalogo pa sem vključil tudi analizo sekundarnih podatkov oziroma že izvedenih raziskav, ki so bile podobne moji. Za pomoč pri posredovanju vprašalnika sem elektronsko naslovil prošnje na več kot 500 slovenskih izobraževalnih ustanov ter na dijaške domove. Seveda pozitivnih odgovorov glede posredovanja vprašalnika nisem dobil z vseh šol, kar je bilo tudi pričakovati. Šolam sem v vabilu svetoval, da v kolikor bodo posredovale vprašalnik, ob tej priložnosti kot izhodišče namenijo nekaj časa za nadaljnji pogovor o varni uporabi interneta. To bi bilo pametno predvsem za otroke, saj jih večina ni dovolj seznanjenih s tem, kajti učni proces podobnih izobraževanj ne vključuje. S pomočjo ljudi, ki se ukvarjajo z varnostjo mladih na spletu, je moj anketni vprašalnik dosegel še večji krog mladih, saj so bile pobude dane tudi vsem udeležencem spletnega izobraževanja o varnosti na spletu za učitelje računalništva, ki je zajemalo več kot 500 sodelujočih. Glede na to, da je bil moj vprašalnik precej dolg, sem z rezultatom zadovoljen.

6.1 Časovni in materialni okviri uporabe spleta

Starši, ki so sodelovali v anketi, pravijo, da imajo njihovi otroci omogočen dostop do spleta preko telefona (81,5 %). Le 9,6 % jih pravi, da imajo njihovi otroci telefon, ki nima dostopa do spleta. Pri lastništvu oziroma souporabi računalnika so rezultati deljeni – polovica staršev pravi, da imajo njihovi otroci svoj osebni, prenosni ali tablični računalnik, druga polovica pa, da uporabljajo napravo, ki je v skupni rabi. Razen treh odstotkov imajo vsi mobilni ali pametni telefon z dostopom do interneta.

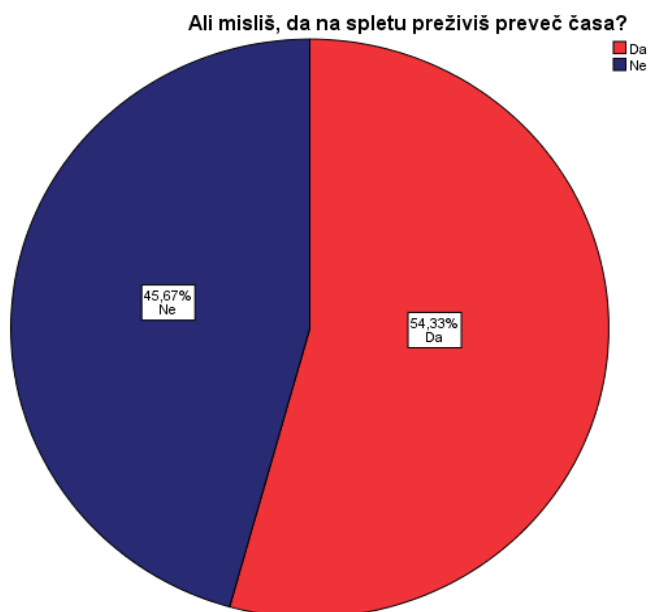
Časovni okvir uporabe računalnika in spleta je zelo težko oceniti, saj je podobno kot pri uporabi telefona, ki ga uporabljamo čez ves dan po malo, kljub temu pa lahko to skupaj seštejemo v več ur dnevno. Največji del staršev pravi, da njihovi otroci računalnika ne

uporabljajo vsak dan (41 %), 27 % pa jih pravi, da na računalniku preživijo manj kot dve uri dnevno.



Slika 6.1: Opozarjanje na prekomerno uporabo spleta ali telefona
(Lastna izdelava slike)

Otroci po samooceni pravijo, da pred tehnološkimi napravami preživijo kar nekaj časa. Več kot polovica (54,33 %) jih celo pravi, da na spletu preživijo preveč časa. Največ otrok pa na prekomerno uporabo spleta in telefona opozarjajo starši (58,25 %). Trendi se spreminjajo, pametni telefoni so prevzeli vodstvo računalnikom, ki jih 60 % mladih ne uporablja vsak dan.



Slika 6.2: Mnenje otrok o prekomerni uporabi spleta
(Lastna izdelava slike)

Po drugi strani ima pametni telefon z dostopom do spleta kar 98 % sodelujočih v anketi. Uporabo je časovno težko oceniti, ampak mladi pravijo, da telefone uporabljajo zelo pogosto. Kar 68 % jih pravi, da so preko telefona dosegljivi skoraj ves čas, tudi čez noč. Telefon največkrat uporabljajo za klicanje in pisanje sporočil, brskanje po spletu, dostop do družbenih omrežij in igranje igrice. Strah, da bi nekaj zamudili (*Fear of Missing Out* – FoMO) je izraz, ki je povezan s psihično navezanostjo na tekoče informacije s strani virtualnih prijateljev. Ta simptom sicer ni klinično priznan, ampak je redno omenjen in razložen s strani priznanih raziskovalcev že od leta 2004. Zato bi tudi večina mladih raje doma pustilo denarnico, kot pa telefon (Frenkel 2014).

6.2 Objava osebnih podatkov na spletu

Raziskave in mnenja strokovnjakov kažejo, da naj bi bili mladi na spletu bolj odprti za pogovor o neprijetnih stvareh, saj naj bi bilo komuniciranje preko spleta nekoliko lažje zaradi fizične oddaljenosti od sogovornika. Mladi so na spletu zato tudi bolj »pogumni«, saj jih skrivanje za računalnikom naredi bolj samozavestne, odprte za pogovor ali celo za prepir. Kljub temu, da računalnik ter predvsem splet nista ravno sinonima za anonimnost (čeprav včasih na prvi pogled deluje tako), imajo mladi takšno mnenje, kadar se ne podpišejo s svojim imenom in priimkom.

Rezultati ankete kažejo, da to ne drži. Mladi pravijo, da preko spleta ne komunicirajo lažje (41 %) oziroma da o svojih osebnih stvareh preko spleta ne govorijo lažje kot v živo (62 %). Prav tako jih 76 % pravi, da zaupanje neki osebi preko spleta ni lažje. V večji meri se strinjajo le z eno trditvijo – na spletu ostajajo dlje, kot je bilo načrtovano (46 %).

Nekoliko več fantov kot deklic pa se strinja s trditvijo, da na spletu ostajajo dlje, kot je bilo pričakovano. To ugotovitev prikazuje tabela korelacij (glej Prilogo H, Tabela 26).

Tabela 6.1: Ali je komunikacija po spletu res lažja?

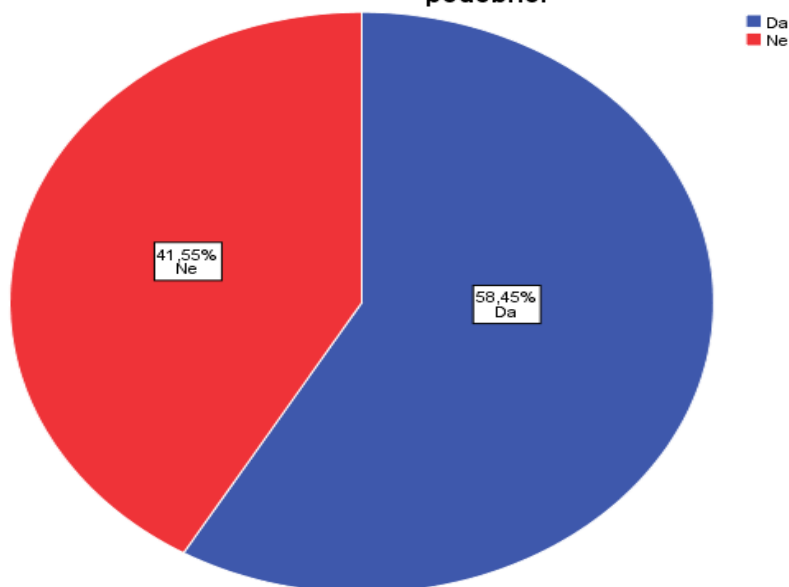
(Lastna izdelava tabele)

	1 - SPLOH SE NE STRINJAM	2 - SE NE STRINJAM	3 - NITI NITI (VČASIH)	4 - SE STRINJAM	5 - ZELO SE STRINJAM	SKUPAJ
NA SPLETU LAŽJE KOMUNICIRAM KOT V POGOVORU V ŽIVO.	134	125	216	100	53	628
	21%	20%	34%	16%	8%	100%
NA SPLETU LAŽJE GOVORIM O OSEBNIH ZADEVAH.	232	159	138	61	38	628
	37%	25%	22%	10%	6%	100%
NA SPLETU SE LAŽJE Zaupam neki osebi kot v pogovoru.	310	163	90	38	23	624
	50%	26%	14%	6%	4%	100%
SVOJ PROSTI ČAS PREŽIVLJAM NA INTERNETU ALI V DRUŽBI MOBILNE NAPRAVE.	68	106	244	159	48	625
	11%	17%	39%	25%	8%	100%
NA INTERNETU OSTAJAM DLJE, KOT JE BILO NAČRTOVANO.	61	65	209	187	103	625
	10%	10%	33%	30%	16%	100%

Večina mladih na spletu deli svoje slike (76,5 %), slike s prijatelji (67,4 %), datum rojstva (53,7 %) in svoje pravo ime (72,2 %). Manj pogosto, a vseeno pa na spletu uporabljajo vzdevek (33 %). To sicer predstavlja tretjino mladih, kar je precejšen del. S tem si zakrijejo lastno resnično ime, vendar pa kljub temu prijatelji, katere imajo na svojem omrežju vedo njihovo pravo ime. E-poštni naslov deli 40,9 odstotka mladih, najmanj pa jih deli telefonsko številko (14,8 %).

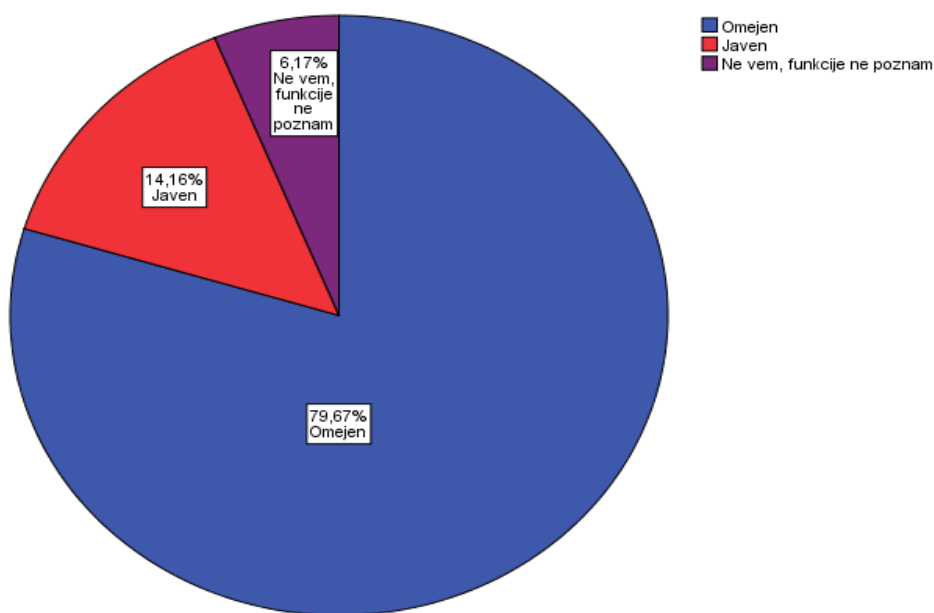
Dobra polovica staršev (58,45 %) je svojim otrokom povedala, kaj lahko in česa ne smejo objaviti na spletu. Vseeno pa je to relativno majhna številka, glede na to, da skoraj vsi uporabljajo družbena omrežja ter so s tem posledično izpostavljeni tveganjem na spletu. Pri prijavi in uporabi spletnih družbenih omrežij je otrokom pomagalo le 30,8 % staršev.

Ali so ti starši povedali, katere podatke in vsebino lahko objaviš na spletu in katerih ne smeš? Npr. osebni podatki, telefonska številka, vaše osebne slike in podobno.



Slika 6.3: Ali so starši povedali, kateri podatki sodijo na splet?
(Lastna izdelava slike)

Kakšne so nastavitve tvojega prikaza podatkov na družbenih omrežjih? Omejen (določene podatke vidijo samo moji prijatelji) ali javen (podatki so na voljo vsem).



Slika 6.4: Omejitev prikaza objav na družbenih omrežjih
(Lastna izdelava slike)

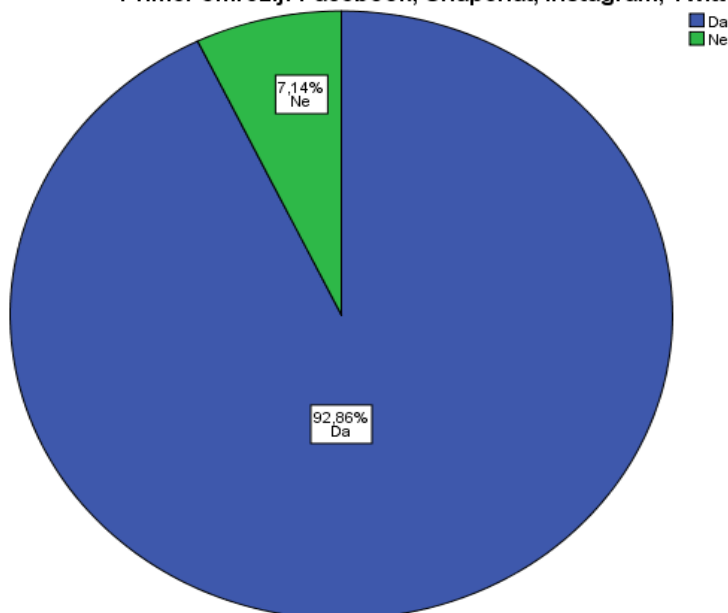
Pri načinu objave vsebine na družbenih omrežjih ima javen prikaz podatkov na spletu 14,16 % mladih, 6,17 % pa te funkcije ne pozna. Ker ima Facebook privzete nastavitve, da so

objave javne, lahko tako upravičeno sklepam, da ima javno dostopen profil 20,33 % mladih. Za tiste, ki so odgovorili, da ne poznajo funkcije omejitve prikaza vsebine, sem na koncu dodal še eno stran, na kateri je bil video s strani Safe.si, ki vodi skozi proces omogočanja funkcije. Prikaz vsebine pa na svoj krog prijateljev omejuje kar velik del mladih (79,67 %).

6.3 Aktivnost mladih na spletu in pametnih telefonih

Družbena omrežja uporablja velika večina mladih, saj predstavljajo preprost kanal za komuniciranje in obveščanje o novostih, obenem pa ponujajo tudi možnost za zabavo in preživljanje prostega časa. Do uporabe najbolj popularnega družbenega omrežja Facebook so upravičene vse osebe, starejše od 13 let, ki imajo napravo za dostop do spleta in omrežno povezavo. Med sodelujočimi v moji anketi se med uporabniki družbenega omrežja Facebook nahajajo tudi 12-letniki, ki jim sicer uporaba še ni dovoljena. Ker je registracija relativno enostavna, mladi kmalu ugotovijo, da lahko spremenijo letnico rojstva in tako dostopajo do polne vsebine. Tisti, ki so stari med 13 in manj kot 18 let, imajo tudi bolj omejen dostop do vsebin, ki so na omrežju. Vse vsebine, ki niso primerne za mlade, so zanje namreč nedostopne.

Ali si uporabnik/ca vsaj enega družbenega omrežja, ki ga dnevno spremljaš?
Primer omrežij: Facebook, Snapchat, Instagram, Twitter itd.



Slika 6.5: Mladi uporabniki družbenih omrežij
(Lastna izdelava slike)

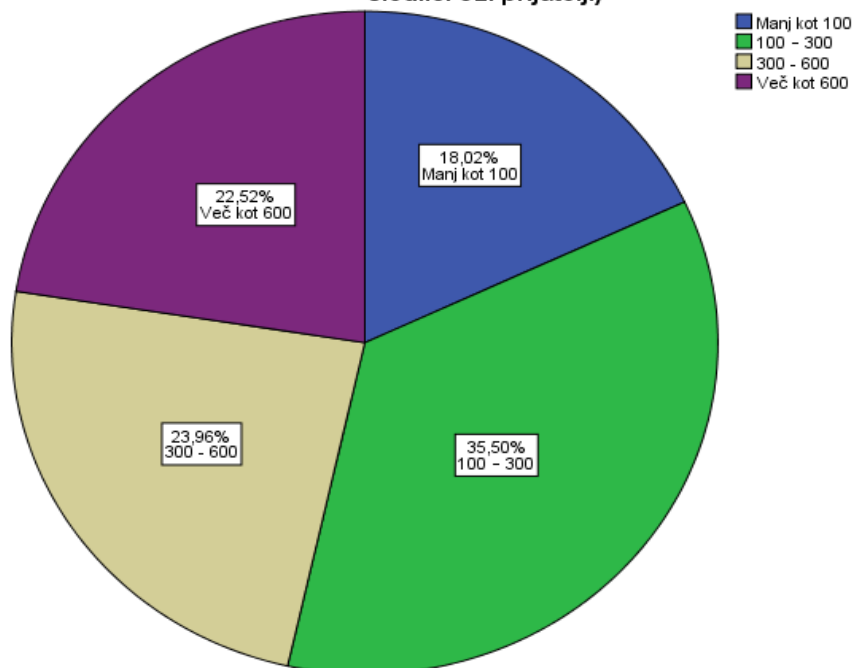
Izmed uporabnikov omrežja Facebook in drugih omrežij jih 53 % pravi, da vsebine (statuse in fotografije) objavljajo približno enkrat tedensko, 37 % pa jih pravi, da informacij (statusov in fotografij) nikoli ne delijo. Takšnim uporabnikom družbenih omrežij se v spletni terminologiji reče tudi »lurkerji«, saj vsebine spremljajo, ne da bi sami aktivno sodelovali v ustvarjanju le-teh (Mousavi in drugi 2017, 377).

Zasvojenost s tehnologijo, ki sicer včasih predstavlja nekakšno družbeno sprejeto in neizogibno stvar vsakega mladega, je med mladimi precejšnja. To lahko sklepamo že iz dejstva, da jih je več kot polovica (68 %) na telefonu dosegljivih skoraj ves čas, med drugim tudi ponoči. Nova ugotovitev je tudi ta, da kar 64 % mladih telefon vzame v šolo in ga tam tudi uporablja. Le 23 % mladih telefon pusti doma, 6 % pa ga v šolo vzame občasno. Po mnenju strokovnjakov uporaba pametnih telefonov ljudem prinaša veselje oziroma sprošča občutek lagodja na podoben način, kot se zgodi pri prejemanju denarja, daril ali prehranjevanju (Frenkel 2014).

6.4 Izpostavljenost tveganjem na spletu

Uporaba družbenih omrežij med fanti in dekleti je praktično enaka in večinska (92 %). Večina mladih (35,5 %) pravi, da ima na spletu med 100 in 300 prijateljev. Kar 22,52 % mladih pa pravi, da ima na spletu več kot 600 prijateljev. V komentarjih so tudi zapisane številke, ki pogosto segajo čez 1000, vse do 5000 (toliko je tudi omejitev na Facebooku).

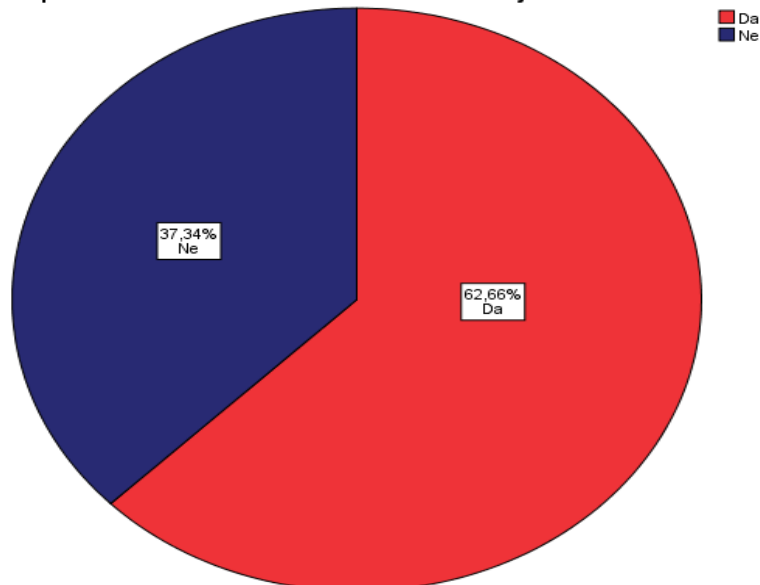
Koliko prijateljev oziroma sledilcev imaš na spletu?(Facebook, Twitter, Instagram sledilci oz. prijatelji)



Slika 6.6: Število prijateljev oz. sledilcev na spletu
(Lastna izdelava slike)

Nemogoče je, da bi tako mladi ljudje tako dobro poznali 1000 oseb, da bi z njimi delili osebne informacije. Kljub temu pa jih kar 62,66 % pravi, da imajo med prijatelji tudi osebe, ki jih niso nikoli spoznali (virtualni prijatelji).

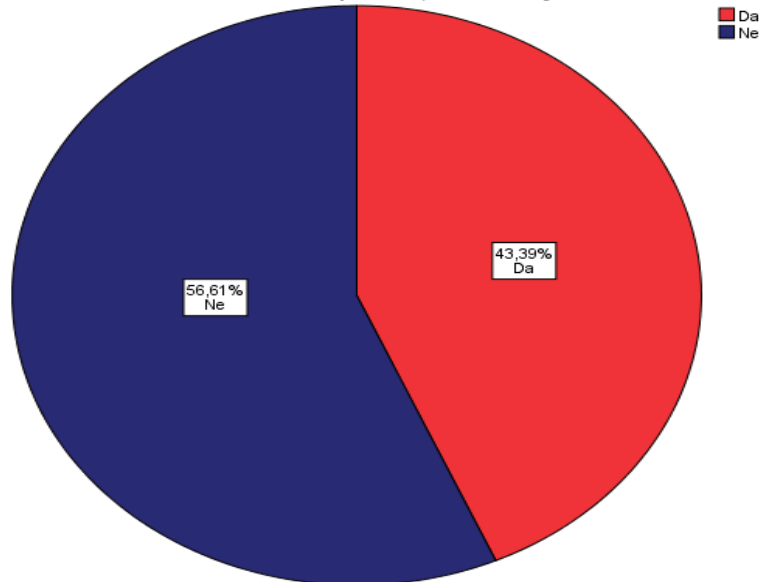
Ali imaš na svojih družbenih (socialnih) omrežjih prijatelje, ki jih nisi nikoli spoznal/a v »offline« svetu oziroma se z njimi v živo nikoli nisi pogovarjal/a?



Slika 6.7: Virtualni prijatelji
(Lastna izdelava slike)

Zaskrbljujoče je dejstvo, da 43,39 s temi osebami komunicira (verjetno to niso znanci iz šole, ki jih poznajo na videz, temveč popolni neznanci).

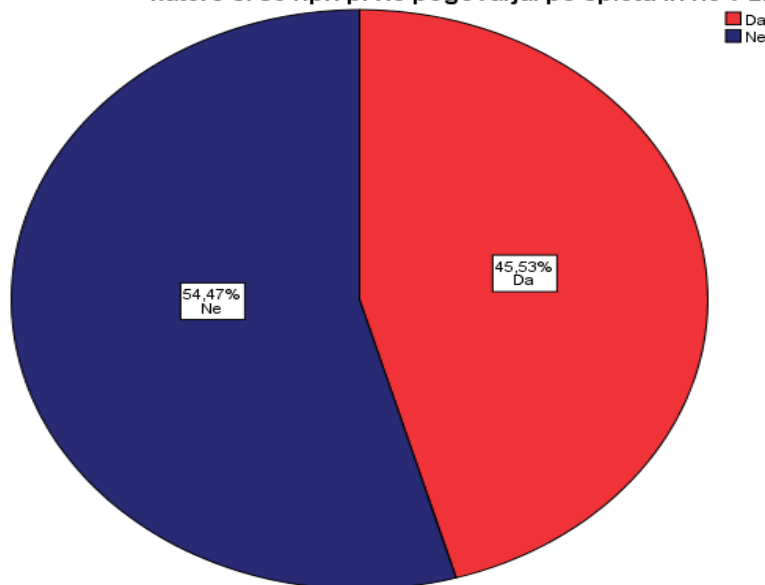
Ali s temi ljudmi, ki jih poznaš le preko spleta, kdaj komuniciraš? Preko zasebnih sporočil, komentarjev itd.



Slika 6.8: Komunikacija z virtualnimi prijatelji
(Lastna izdelava slike)

Tukaj gre ponovno za relativno nevarno in varnostno skrb vzbujajočo ugotovitev, saj se je kar 45,53 % mladih z virtualnim prijateljem spoznalo tudi v živo. To je sicer še večje število kot pri prejšnjem vprašanju (43,39 % mladih se preko spleta pogovarja z neznanci).

Si kdaj "virtualnega" prijatelja spoznal/a v živo? Virtualni prijatelj je oseba, s katero si se npr. prvič pogovarjal po spletu in ne v živo.



Slika 6.9: Spoznavanje virtualnih prijateljev v živo
(Lastna izdelava slike)

Pri uporabi družbenih omrežij ni mogoče ugotoviti statistično značilne povezanosti med skupinami (glej Prilogo G, Tabela 16 in 17).

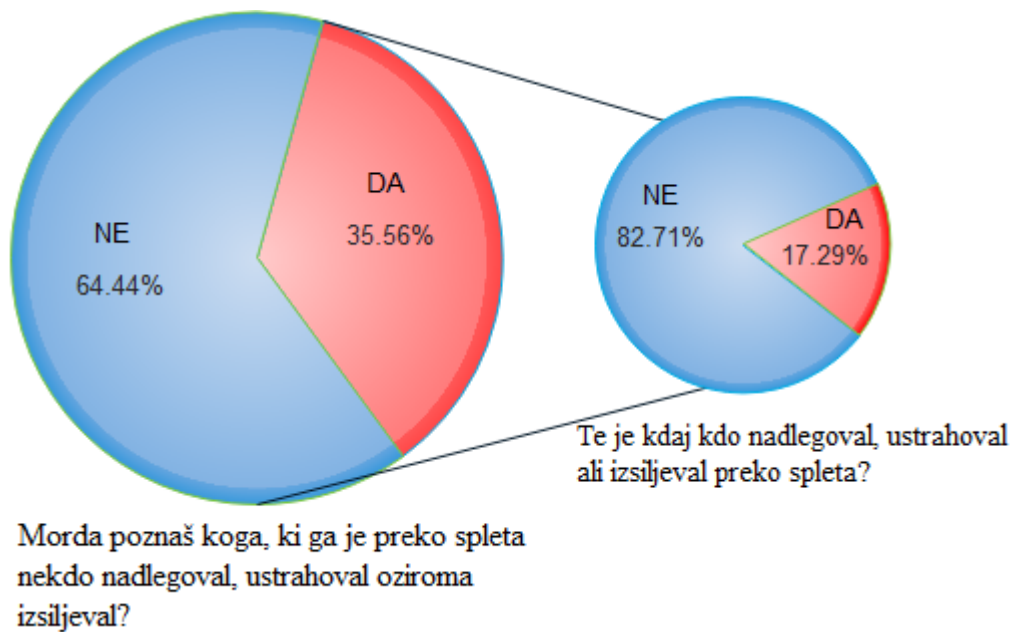
Enako je z virtualnimi (nepoznanimi) prijatelji, ki jih imajo tako fantje kot dekleta (glej Prilogo G, Tabela 18). Tudi pri spoznavanju virtualnega prijatelja ni razvidnih razlik med fanti in dekleti (glej Prilogo G, Tabela 21).

6.5 Tehnična zaščita pri mladih

Kot je bilo ugotovljeno že v raziskavi Mladi na netu, so mladi bolj izpostavljeni nevarnostim na spletu tudi zaradi tehnične oziroma varnostne neseznanjenosti.

Med mladimi, ki so sodelovali v anketi, jih je 17,3 % odgovorilo, da so bili nekoč nadlegovani, ustražovani ali izsiljevani preko spleta, 35,6 % pa pozna nekoga, ki je bil žrtev spletnega nasilja. Vprašanje je bilo preprosto, zato nisem želel vpletati teže dejanja, katerega žrtev so bili. Sem pa zato ustvaril novo, odprto vprašanje, kamor so lahko zapisali svoje izkušnje. Nekatere izmed izkušenj se glasijo takole:

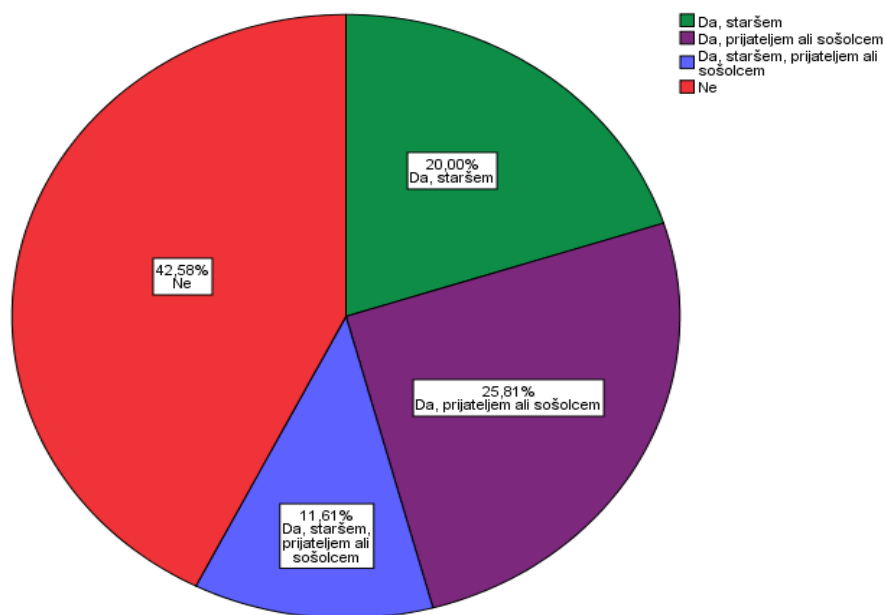
- *»phishing, do Facebook računa nisem mogel dostopati za 12 ur,*
- *virusi na računalniku,*
- *enkrat se mi je zgodilo, da sem prišel na Facebook in se nekaj časa dopisoval z nekim tipom, nakar mi pošlje neko povezavo, ki sem jo kliknil in nato dobil izsiljevalski virus, ki mi je uničil računalnik,*
- *na spletu so izkoriščali moje slike in se norčevali iz mene,*
- *nekdo je izvedel moje geslo in pisal grde stvari mojim prijateljem,*
- *sošolci so se norčevali iz mojih slik in delali memes,*
- *igral sem igrice in mi je nekdo vdrl v računalnik preko IP-ja in potem hotel denar,*
- *vdrt Yahoo račun«.*



Slika 6.10: Primerjava odgovorov - spletno ustrahovanje
(Lastna izdelava slike)

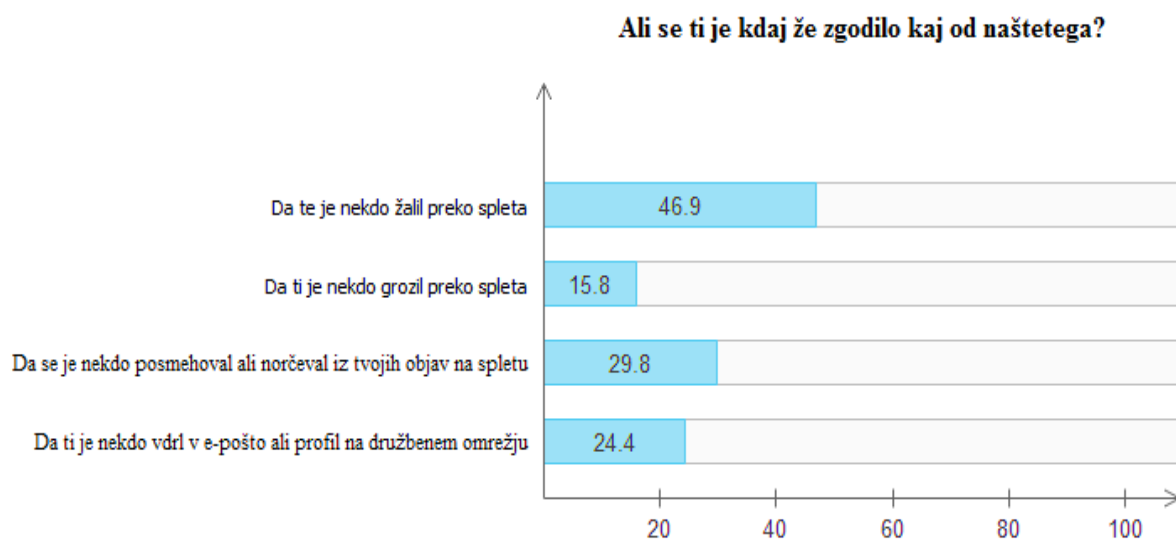
Izmed teh, ki so bili nadlegovani je kar 42,58 % to zadržalo zase in o dogodku ni povedalo nikomur. Ostali pa so največkrat povedali prijateljem ali sošolcem (25,81 %) in staršem (20 %).

Nekoliko bolj izrazita pa je razlika med izkušnjami z ustrahovanjem na spletu. Nekoliko več deklic (67), kot fantov (33) pravi, da so že bile ustrahovane ali izsiljevane preko spleta (glej Prilogo G, Tabela 23).



Slika 6.11: Kam se mladi obrnejo na pomoč pri spletnem ustrahovanju
(Lastna izdelava slike)

Najpogostejši odziv mladih, ki so bili nadlegovani preko spleta je, da osebo blokirajo in s tem prekinajo stike (48 %). To osebo je 24 % mladih prosilo, da jih preneha nadlegovati, 18 % pa jih je za pomoč prosilo starše in prijatelje. Ostali (10 %) pravijo, da niso naredili ničesar.



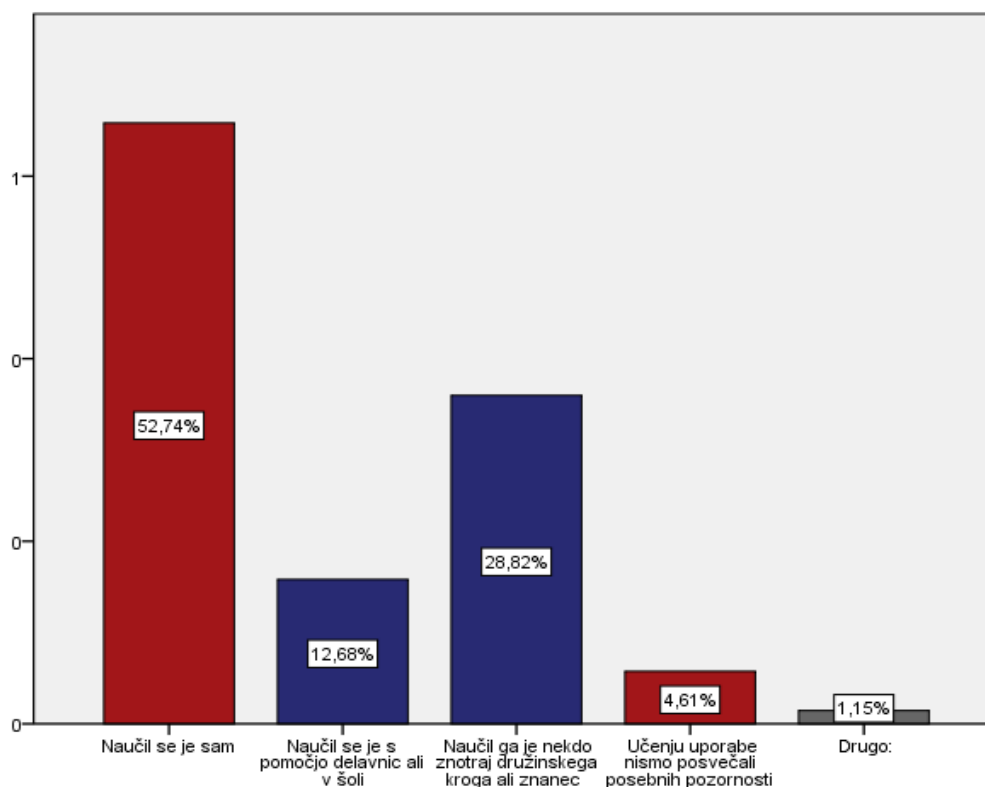
Slika 6.12: Kaj se je mladim že zgodilo na spletu
(Lastna izdelava slike)

Rezultati ankete kažejo, da mladi niso dovolj seznanjeni s tveganji na spletu in niti z nekaterimi preprostimi pojmi. Mladi so najbolj seznanjeni s pojmom spam pošta (72 %), spletno ustrahovanje (ang. *cyberbullying*), mocking in zlonamerna koda. Pojem spletno ustrahovanje je bil sicer tudi razložen med vprašanji v moji anketi. Nekoliko manj so seznanjeni s pojmi požarni zid (31 %), spletno ribarjenje (ang. *phishing*) (30 %) in virus Locky – CryptoLocker (26 %).

6.6 Informiranost in izobraževanje mladih o spletnih tveganjih ter uporabi pametne tehnologije

Rezultati ankete kažejo, da otroci na splet vstopajo nepoučeni oziroma neseznanjeni s pravilno uporabo, kar so bile tudi ugotovitve raziskav EU Kids Online in Mladi na netu. Otroci se večinoma sami naučijo uporabe računalnika oziroma pametne tehnologije (52,74 %), včasih pa jim pomaga tudi nekdo iz družinskega kroga (28,82 %). Zelo malo staršev (12,68 %) je označilo odgovor, da se njihovi otroci uporabe pametne tehnologije naučijo v šoli, kar kaže na izključenost učenja računalniške (predvsem varne uporabe spleta) pismenosti iz učnega programa.

Zaradi stalne navezanosti na digitalno tehnologijo pa se zmanjšuje tudi vnos kreativnosti oziroma ustvarjalnosti ter idej med uporabniki, saj je sanjarjenje, kot so ga prakticirali priznani izumitelji (npr. Einstein) stvar preteklosti. Sanjarjenje pa je pomembno tudi za sprostitvev možganov in ima tako tudi kognitivne prednosti (pozitiven vpliv na spomin). Le malo kdo si vsak dan vzame nekaj časa za razmišljanje v naravi, brez, da bi bil obdan s tehnologijo. Po drugi strani pa se kreativnost vidi v novih izumih, ki pa večinoma temeljijo na tehnologiji (Frenkel 2014).



Slika 6.13: Kako se je otrok naučil uporabe spleta in tehnoloških naprav
(Lastna izdelava slike)

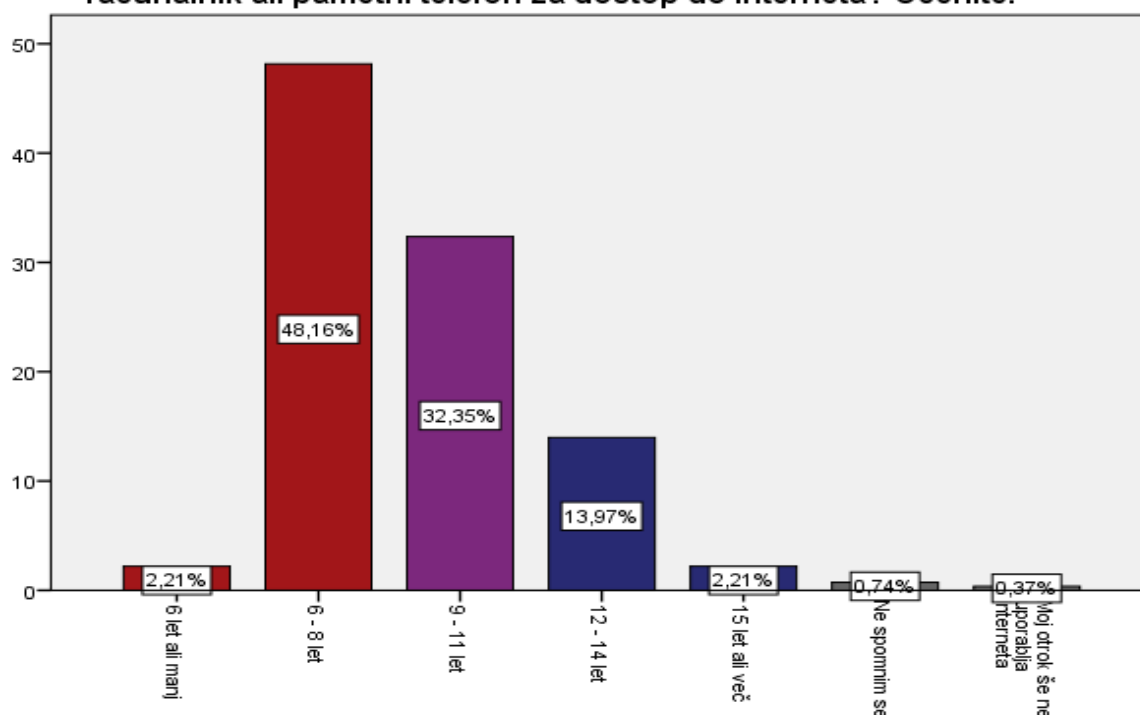
Mnenje o tem, ali so njihovi otroci zasvojeni z internetom in uporabo tehnoloških naprav oziroma ali pretiravajo z uporabo le-teh, je zelo deljeno. 41,7 % staršev pravi, da so njihovi otroci prekmalu začeli z uporabo spleta in da so celo zasvojeni z internetom, 58,3 % pa se jih s tem ne strinja in pravi, da so začeli ob pravem času in da niso zasvojeni z uporabo. Izkazalo se je, da predvsem ženske v večji meri trdijo, da so njihovi otroci prekmalu začeli z uporabo računalnika in spleta, moški pa ravno nasprotno. Starši pravijo tudi, da ima uporaba spleta tako pozitiven kot negativen učinek na uspešnost učenja.

Mnenju o vplivu sodobne tehnologije na učenje prinaša podobne rezultate kot pri prejšnji spremenljivki. Ponovno ima velik vpliv na rezultate vzorec, zaradi premajhnega števila moških, ki so sodelovali v anketi. Možno je razbrati statistično značilno povezanost med vplivom spola na oblikovanje mnenja. Veliko več žensk je namreč mnenja, da uporaba sodobne tehnologije lahko včasih pozitivno vpliva na učenje. Povezanost med spremenljivkama je šibka, vendar statistično značilna (glej Prilogo E, Tabela 9).

Največ otrok je začelo z redno uporabo računalnika in dostopa do spleta, ko so bili stari 6–8 let. Po mnenju 79 % staršev pa pretirana raba pametnega telefona ali računalnika vodi v slabše rezultate v šoli.

Mnenja, da je otrok prekmalu začel z uporabo sodobne tehnologije je sorazmerno uravnovešeno med moškimi in ženskami. Se pa zato nekoliko razlikuje pri odgovorih »ne« in »ne vem«, ki jih je izbralo več žensk kot moških. Povezanost je ponovno statistično značilna in šibka (glej Prilogo E, Tabela 12, 13 in 14).

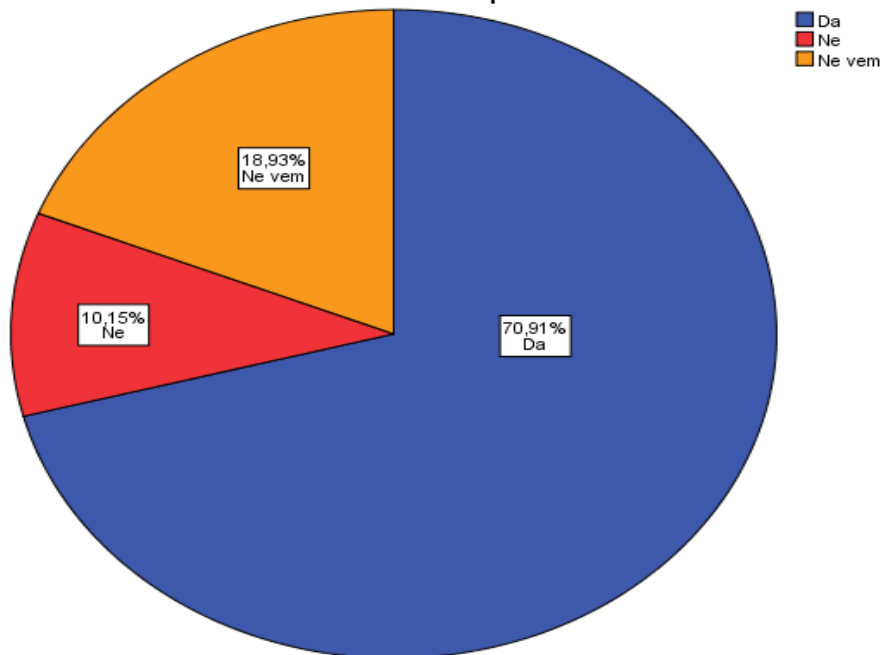
Se morda spomnite, pri kateri starosti je vaš otrok začel redno uporabljati računalnik ali pametni telefon za dostop do interneta? Ocenite.



Slika 6.14: Kdaj je otrok začel z redno uporabo računalnika oziroma dostopa do spleta
(Lastna izdelava slike)

Po mnenju večine mladih (70,91 %) je šola zanje organizirala predavanje o varnosti na spletu, kar je zanimivo predvsem zaradi navzkrižnih podatkov s strani staršev, ki v večini pravijo, da šola ni organizirala nikakršnih predavanj o varnosti na spletu.

Ali je bilo za učence v sklopu šole organizirano kakšno predavanje o varnosti na spletu?

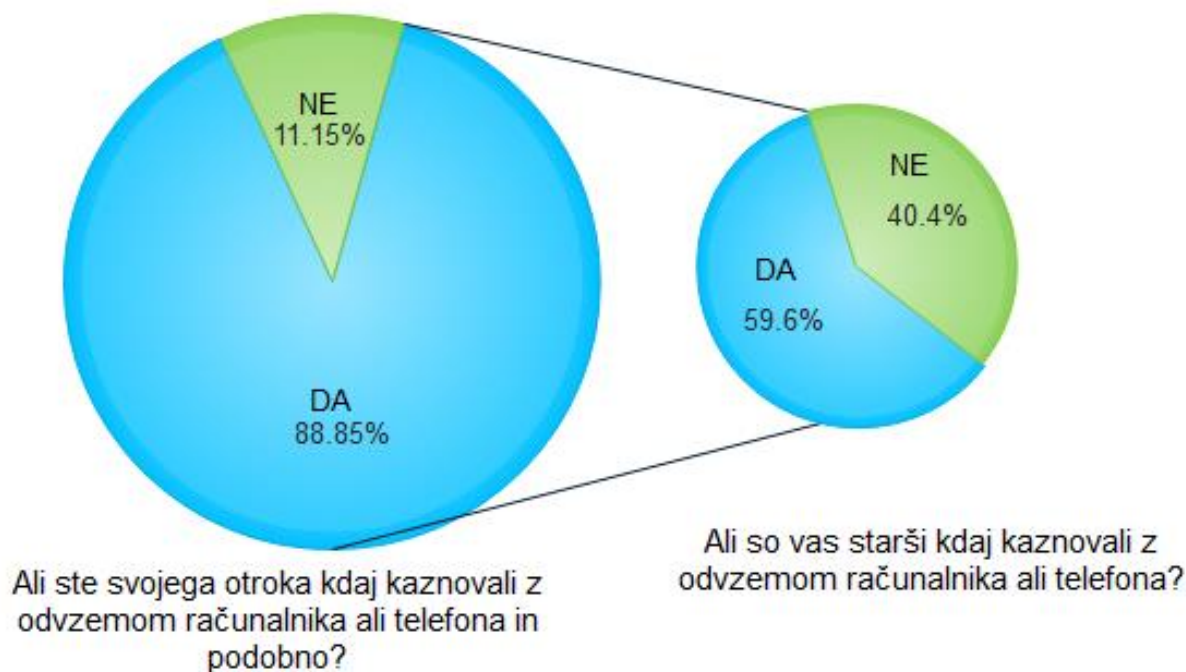


Slika 6.15: Predavanje o varnosti na spletu v šoli
(Lastna izdelava slike)

6.7 Omejitve dostopa

Težave pri definiranju zasvojenosti z internetom, računalnikom oziroma sodobno tehnologijo nastanejo tudi zato, ker večina ljudi danes po 8 ali več ur dnevno uporablja računalnik in se to nekako sprejema kot normalno in sprejemljivo dejanje. Kljub temu vsi ti uporabniki sodobne tehnologije uporabljajo tudi v prostem času, kar na koncu predstavlja praktično ves dan. Zasvojenost z računalnikom in pametnimi napravami je skorajda neizogibna med mladim, saj je pogosta uporaba naprav družbeno sprejemljiva, če ne celo zaželena. Če mladi niso aktivni in prisotni na družbenih omrežjih, je to podobno, kot da ne bi obstajali.

Starši, zajeti v vzorec, svojim otrokom postavljajo omejitve pri uporabi družbenih omrežij in jim npr. prepovedujejo objavo osebnih družinskih fotografij, domačega naslova, telefonske številke ipd., kar je potrdilo 83 % staršev. Kljub temu je pri prijavi v družbena omrežja svojim otrokom pomagalo le 30,8 % staršev.

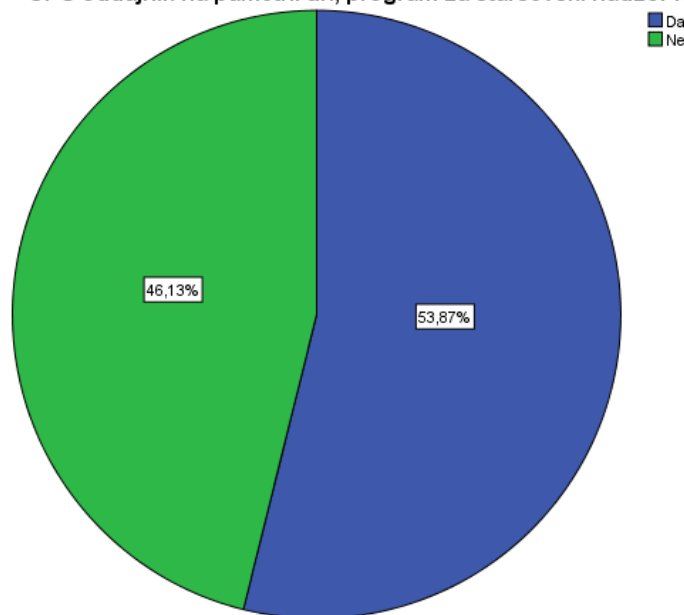


Slika 6.16: Kaznovanje otroka z odvzemom računalnika ali tehnoloških naprav
(Lastna izdelava slike)

Na vprašanje, ali so svojega otroka kdaj kaznovali z odvzemom tehnološke naprave oziroma omejitvijo dostopa do spleta, je 88,85 % staršev odgovorilo pritrdilno. Kot dodatno informacijo so navedli, da se to po navadi zgodi, ko dobi slabo oceno. Razlik glede na spol ni bilo - moški in ženske so enotni pri kaznovanju z odvzemom naprav. Zanimivo pa je, da otroci odgovarjajo nekoliko drugače. 59,6 % jih namreč trdi, da so kdaj bili kaznovani z odvzemom telefona ali računalnika. Kar precejšen del pa jih pravi, da še nikoli niso bili kaznovani z odvzemom telefona ali računalnika.

Pri kaznovanju z odvzemom telefona ali naprave ni bilo prisotnih statistično značilnih razlik med moškimi in ženskami. Mlade je sicer z odvzemom telefona ali naprave kaznovalo veliko več žensk kot moških. To pa je posledica nekoliko neuravnovešenega vzorca, saj je v anketi sodelovalo več žensk (75 %) kot moških (glej Prilogo E, Tabela 4).

Ali svojega otroka morda nadzirate s pomočjo pametne tehnologije? Npr. z aplikacijo na pametnem telefonu, poraba na telefonu (SMS sporočila in klici), GPS oddajnik na pametni uri, program za starševski nadzor na spletu ipd.

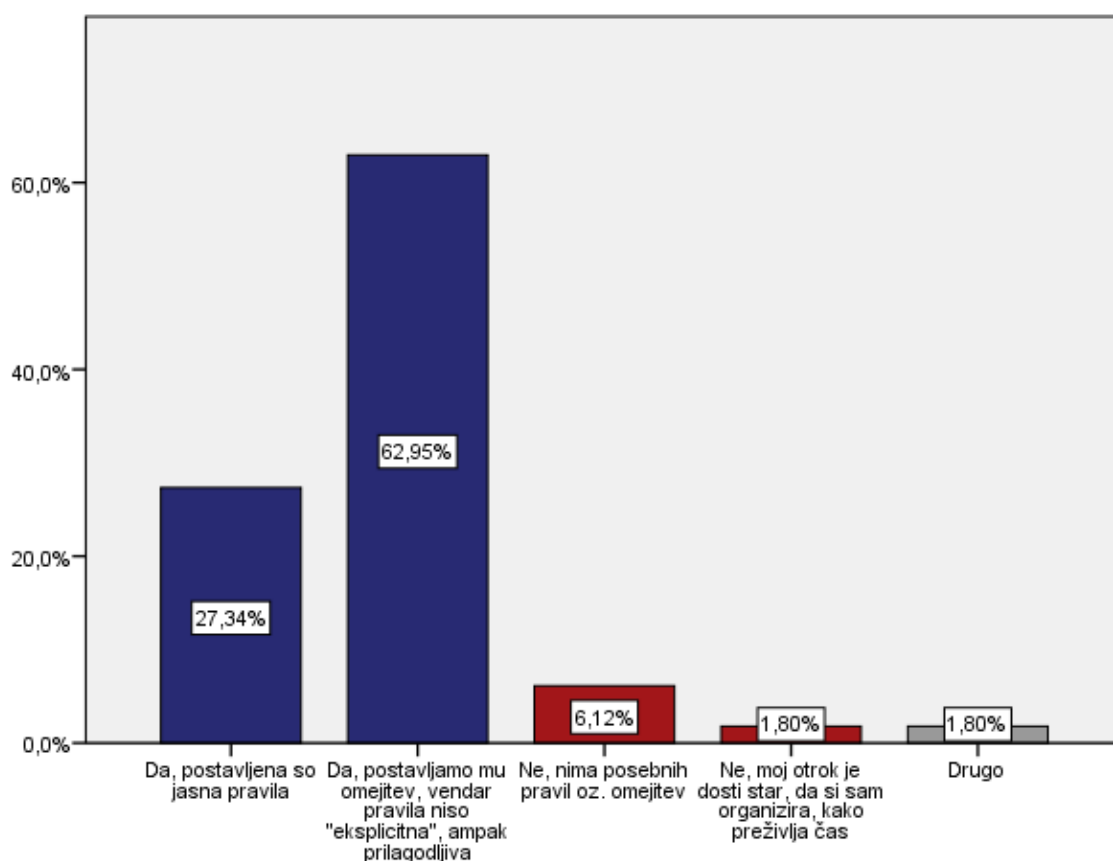


Slika 6.17: Nadziranje otroka s pametno tehnologijo

(Lastna izdelava slike)

Starši so glede nadzora nad svojimi otroki odgovarjali s precej deljenim mnenjem. 53,87 % staršev svoje otroke nadzira s pomočjo pametne tehnologije. Izmed teh, ki svoje otroke nadzirajo, je najbolj pogost način izvajanja nadzora dostop do družbenih omrežij in e-pošte otroka (51 % staršev ima geslo za dostop), spremljanje otrokovih SMS sporočil in klicev in aplikacije na računalniku, pametnem telefonu ali tablici. Večina staršev izvaja celo več načinov nadzora, saj jih je veliko označilo več možnih odgovorov. Izmed vseh staršev jih 32 % omejuje dostop do spletnih strani s programi za starševski nadzor.

Med rezultati ankete je bilo zapisano, da otroke spremljajo tudi s pomočjo e-Redovalnice oziroma e-Asistenta, ki omogoča pošiljanje SMS obvestil, ko otrok manjka v šoli, dobi slabo oceno, ko je brez opreme za športno vzgojo ali podobno. Ta obvestila omogoča uporaba e-redovalnice, dostop in uporaba le-te pa je odvisna od šole. Mnenja o uporabi spletne redovalnice so deljena, nekateri pravijo, da je zelo priročno orodje, ki poskrbi, da otroci doma govorijo resnico, drugi pa, da jih ne zanima, kaj je otrok danes delal v šoli.



Ali svojemu otroku postavljate omejitve glede dostopa do spletnih vsebin oziroma uporabe računalnika? Označite odgovor, ki drži.

Slika 6.18: Omejitve pri dostopu do računalnika in spletnih vsebin
(Lastna izdelava slike)

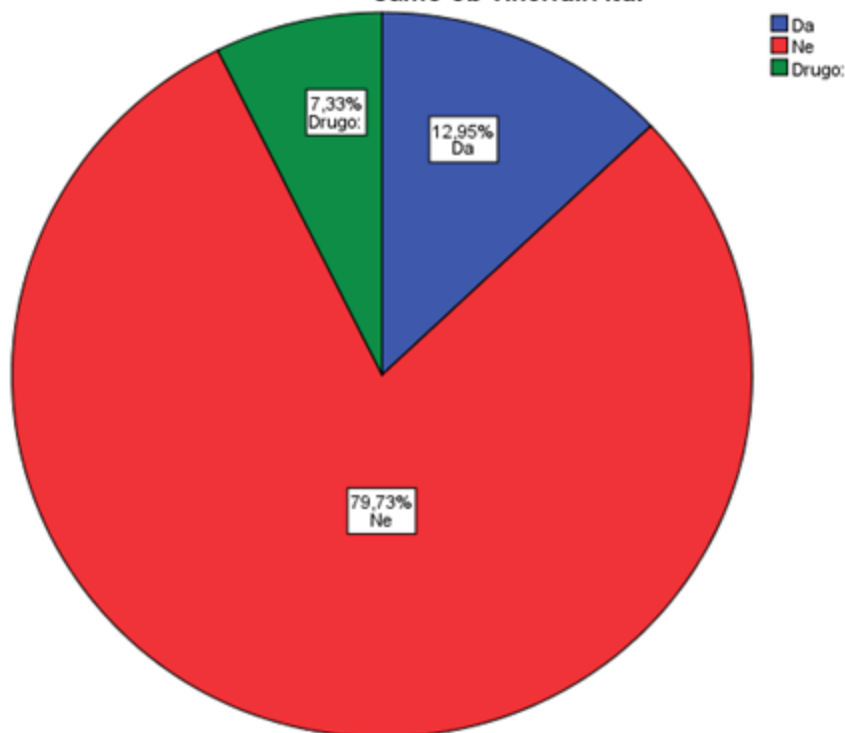
Pri časovnih omejitvah pravijo, da so pravila postavljena, vendar se prilagajajo. Pri odgovorih je bila tudi možnost drugo, kjer so bili bolj podrobni odgovori:

»Ob 23h je konec z internetom pri naši hiši; večinoma ne, če pa je potreba, čas na računalniku za nekaj časa omejimo; ne, ker na računalniku porabi zelo malo časa (igrice ipd. je sploh ne zanimajo), vsebine, ki jih pregleduje, pa so skoraj izključno povezane s šolo; ji zaupam, ker ima dovolj samokontrole, če raziskuje "mejne" vsebine, pa je to njena svoboda«.

Postavljanje omejitev glede dostopa do spletnih vsebin po skupinah se je pokazalo kot statistično značilno ($p = 0.002$). To pomeni, da nekoliko več žensk (58) pravi, da so postavljena jasna pravila kot moških (11). Cramerjev koeficient povezanosti znaša 0.253, kar kaže na šibko do zmerno povezanost (glej Prilogo E, Tabela 6, 7 in 8).

Zanimivo je, da mladi odgovarjajo nekoliko drugače. Večina jih namreč pravi, da omejitve s strani staršev nimajo. Le 12,95 % mladih pravi, da jim starši postavljajo omejitve glede uporabe spleta, 7,33 % pa pravi drugo (oziroma včasih). To pomeni, da jih je 79,73 % na spletu lahko časovno neomejeno dolgo, po lastni presoji, kar predstavlja izjemno velik del mladih. Kar nekaj otrok pa pravi, da jim starši omejitve sicer postavljajo, vendar jih sami ne upoštevajo. V primeru uporabe programov za starševski nadzor bi to poenostavilo delo staršem, saj je mogoče izbrati možnost, da je računalnik dnevno na voljo le za določen čas oziroma v določenem časovnem obdobju. Rezultati ankete med mladimi in starši so ponovno nasprotujoči, kar to vprašanje naredi še bolj zanimivo.

Ali ti starši določijo, koliko časa si lahko na spletu? Npr. največ dve uri dnevno, samo ob vikendih itd.

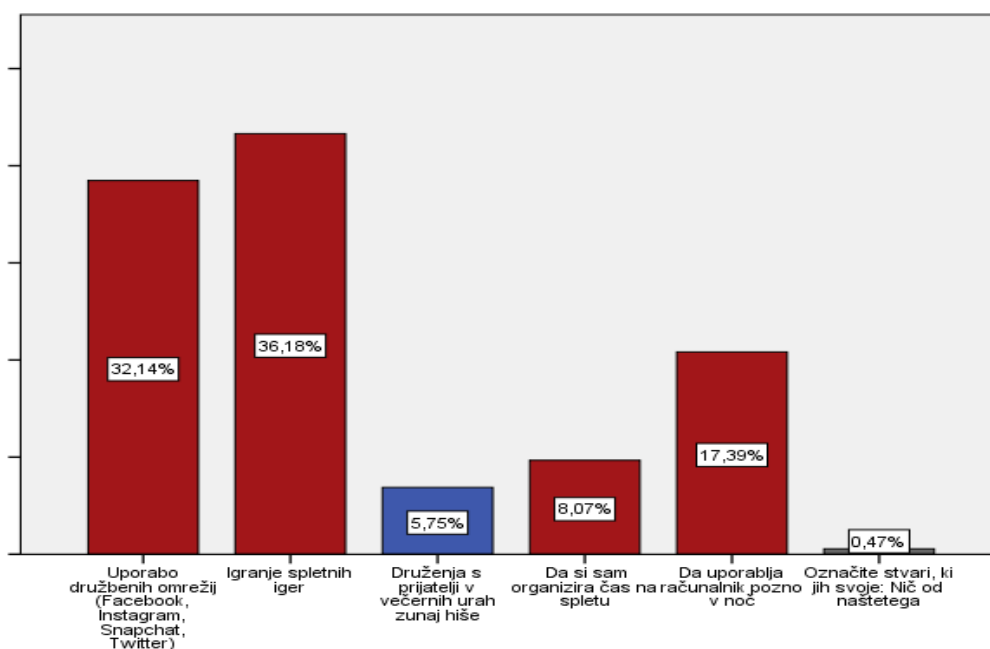


Slika 6.19: Omejitve uporabe spleta s strani staršev – rezultati ankete za mlade
(Lastna izdelava slike)

Pri 17 odstotkih otrok se je že zgodila neka neprijetna situacija. Starši so te neprijetne situacije lahko tudi zapisali v okvirček. Zabeleženo je bilo: »Posmehovanje na družbenih omrežjih; grožnje sošolk; grde besede sošolke (sovražni govor) in verbalno nasilje preko aplikacije Viber; izzivanje, nadlegovanje in norčevanje s strani vrstnikov; množično deljenje lažnih sporočil (deli to, drugače se bo zgodilo nekaj slabega); neprimerne objave sovrstnikov in okužba z virusom.«

6.8 Kaj starše bolj skrbi, spletna ali zunaj spletna tveganja?

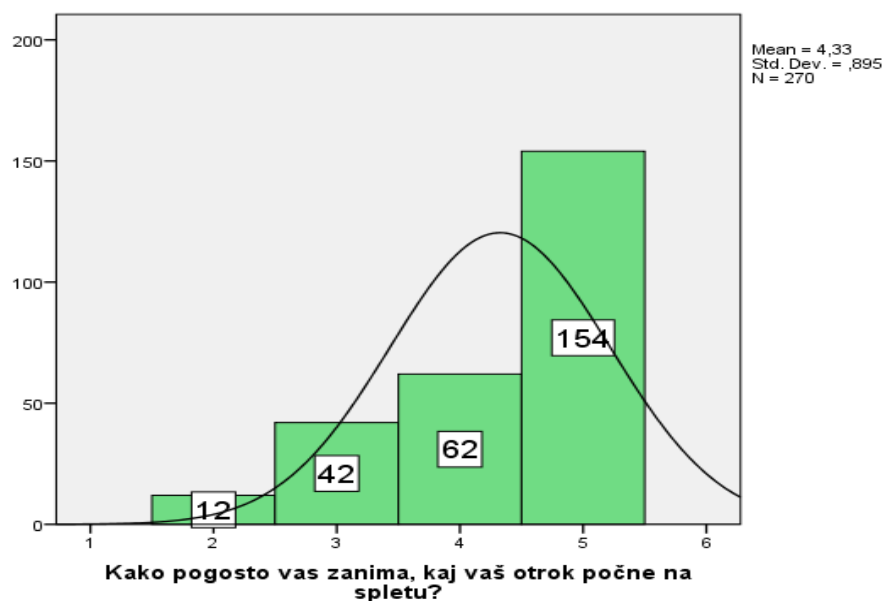
Eden izmed sklopov v vprašalniku je bil povezan s spletnimi (ang. *online*) in zunaj spletnimi (ang. *offline*) tveganji. Zanimalo me je, katere stvari starši svojim otrokom dovolijo in kaj zanje predstavlja večje tveganje. Starši svojim otrokom najpogosteje dovolijo igranje spletnih iger (36,18 %) in uporabo družbenih omrežij (32,14 %). Slaba petina staršev (17,39 %) pa svojim otrokom dovoli uporabo interneta pozno v noč, medtem ko jih le 5,75 % dovoli večerno druženje s prijatelji zunaj hiše.



Slika 6.20: Kaj starši svojemu otroku dovolijo
(Lastna izdelava slike)

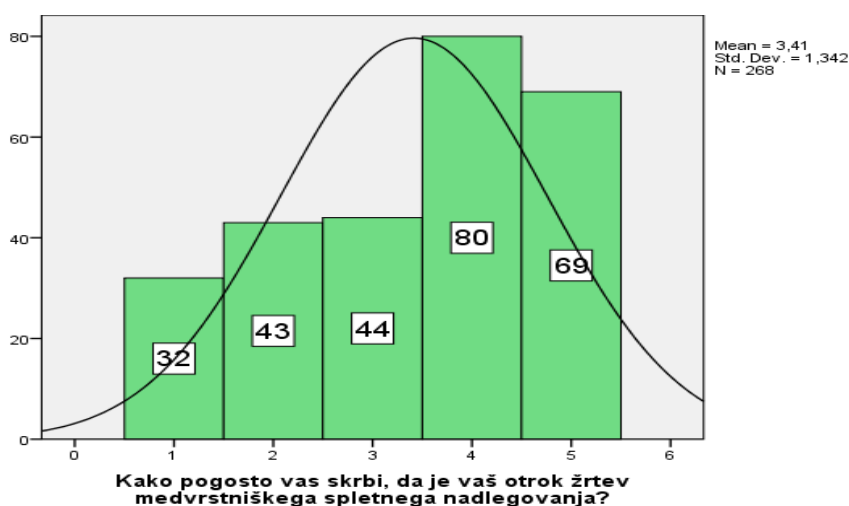
Za spodnji prikaz sem izbral histogram glede na število enot in ne odstotkov, saj se mi je ta zdel bolj pregleden.

Histogram predstavlja pogostost, ko starše zanima, kaj njihovi otroci počnejo na spletu. Merska lestvica znaša od 1 (»nikoli«) do 5 (»zelo pogosto«). Kot je razvidno s slike, starše zelo pogosto zanima, kaj njihovi otroci delajo na spletu (povprečje znaša 4,33), porazdelitev pa je asimetrična v levo.



Slika 6.21: Zanimanje za dejavnost otrok na spletu
(Lastna izdelava slike)

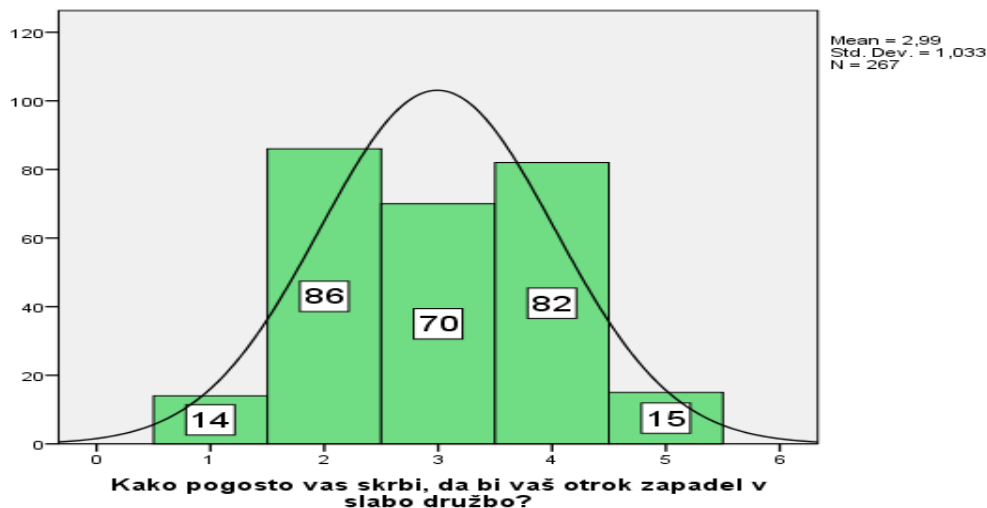
Spodnji histogram predstavlja pogostost, ko starše skrbi, da je njihov otrok žrtev medvrstniškega spletnega nadlegovanja. Merska lestvica znaša od 1 (»nikoli«) do 5 (»zelo pogosto«). Povprečje znaša 3,41, kar pomeni, da starše v povprečju včasih oziroma pogosto skrbi, da je njihov otrok žrtev medvrstniškega spletnega nadlegovanja.



Slika 6.22: Žrtev medvrstniškega spletnega nadlegovanja
(Lastna izdelava slike)

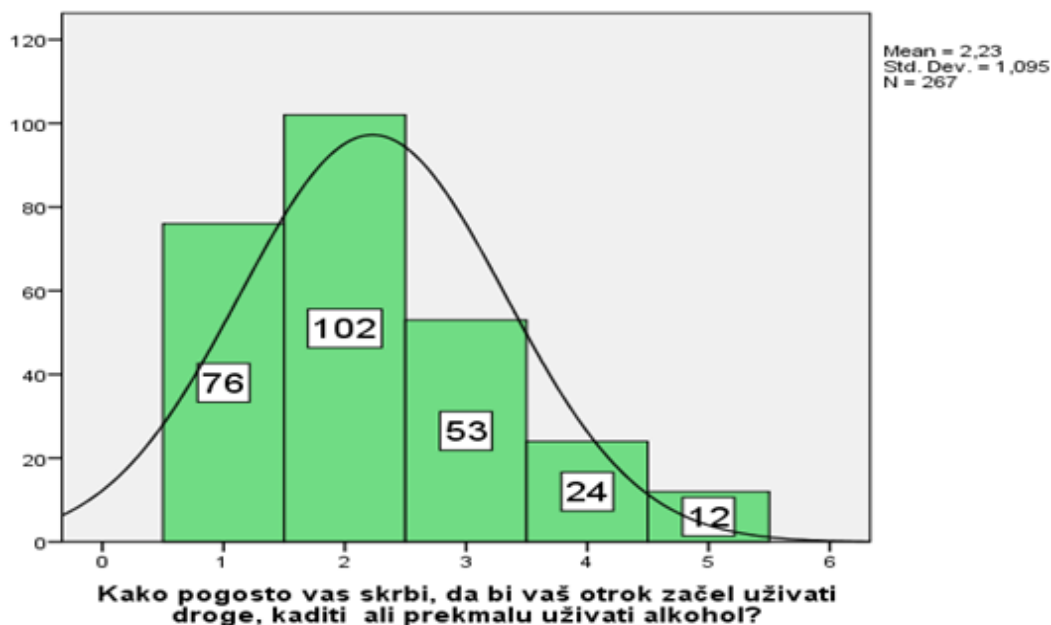
Histogram predstavlja pogostost, ko starše skrbi, da bi njihov otrok zapadel v slabo družbo. Merska lestvica znaša od 1 (»nikoli«) do 5 (»zelo pogosto«). Kot je razvidno iz slike, starše včasih skrbi, da bi njihov otrok zapadel v slabo družbo (povprečje je 2,99). Ta spremenljivka je zelo občutljiva na starost. Starši mlajših otrok so večinoma izbrali vrednost 4 in 5, kar

pomeni, da jih bolj skrbi kot starše starejših otrok, ki so izbrali nasprotno vrednost. Razlog za to je verjetno tudi, da si mlajši ravno takrat oblikujejo svoj družbeni krog in spoznajo prijatelje.



Slika 6.23: Slaba družba
(Lastna izdelava slike)

Spodnji histogram predstavlja pogostost, ko starše skrbi, da bi njihov otrok začel kaditi, uživati droge ali alkohol. Merska lestvica znaša od 1 (»nikoli«) do 5 (»zelo pogosto«). Kot je razvidno iz slike, starše malokrat skrbi, da bi njihov otrok začel kaditi, uživati droge ali alkohol (povprečna vrednost znaša 2,23), vrednosti pa so asimetrične v desno.



Slika 6.24: Uživanje alkohola ali drog
(Lastna izdelava slike)

Nekoliko več žensk je v strahu, da je njihov otrok žrtev medvrstniškega nasilja ali pa da bi njihov otrok zapadel v slabo družbo. Te povezanosti je pokazala tabela korelacij (glej Prilogo F, Tabela 15).

Oblike in načini medvrstniškega nadlegovanja in nasilja se spreminjajo skupaj z družbo, ki ji lahko rečemo tudi informacijska družba. Ker se nasilje in nadlegovanje iz zunaj spletnega oziroma (ang. *offline*) prenaša tudi v spletno (ang. *online*), je pomembno zavedanje tega problema. Večina staršev je odgovarjala, da jih bolj zanima, kaj njihov otrok počne na spletu, kot pa skrbi, da bi njihov otrok začel uživati droge, kaditi ali uživati alkohol. Ker se digitalizacija stalno širi, se spreminjajo tudi naši načini uporabe sodobnih naprav, pri tem pa nastajajo nove skrbi, stroški in tveganja, ki pred tem niso obstajala.

7 ANALIZA SEKUNDARNIH PODATKOV

V svoje diplomsko delo vključujem tudi pregled že izvedenih raziskav na temo (ne)varnosti mladih na spletu. Iskal sem raziskave, ki so bile izvedene v Sloveniji in tudi v tujini. Spletnih raziskav nisem našel, saj so po mnenju strokovnjakov tudi manj primerne zaradi težav pri vzorčenju – pri spletnih anketah namreč ni mogoče vnaprej določiti nekega vzorca, ampak je ta odvisen od zanimanja ljudi. Zanimanje za reševanje anket oz. proaktivnost mladih pa je zanemarljivo. Drug problem predstavlja razumevanje terminov pri mladih, saj se pogosto porajajo dodatna vprašanja, ki jih pri spletni anketi ni mogoče razjasniti. Zato se tudi večina »bolj resnih« raziskav še vedno izvaja na papirju.

7.1 Mladi na netu

Raziskava Mladi na netu je bila opravljena med januarjem in aprilom 2010, in sicer terensko (na domu), kjer je sodelovalo 31 anketarjev. V raziskavi je sodelovalo 691 otrok, starih med 8 in 19 let, in nekoliko več deklic (355) kot dečkov (336) (Lobe in Muha 2011, 16). Glavne ugotovitve raziskave so bile, da se je 35 % mladih že srečalo z osebo, ki so jo spoznali preko spleta. Med njimi so nekoliko bolj neprevidni dečki, saj se jih je kar 42 % že srečalo z neznancem, ki so ga spoznali na spletu, med deklicami pa se jih je srečalo 29 % (Lobe in Muha 2011, 5).

Če pa negativne stvari srečanja z neznanci pogledamo še s pozitivne strani, lahko pridemo do drugačnih ugotovitev. Med mladimi, starimi med 15 in 19 let, se jih je kar 55 % srečalo z neznancem, ki so ga spoznali na internetu, vendar jih je imela s srečanjem velika večina (88 %) zelo dobro izkušnjo (Lobe in Muha 2011, 46). Med mladimi je bila ugotovljena tudi manjša digitalna pismenost, predvsem pri varnosti, saj je 42 % mladih odgovorilo, da ne bi znali odstraniti virusa s svojega računalnika. Kljub temu jih kar 45 % pravi, da so sami najbolj spretni pri uporabi spleta in računalnika v primerjavi z ostalimi družinskimi člani. Ugotovljeno je bilo tudi, da se mladi na spletu (ang. *online*) počutijo bolj samozavestno in so pripravljeni deliti več informacij kot pa v živo oz. zunaj spletno (ang. *offline*). Kljub temu jih 62 % pravi, da se o pomembnih stvareh raje pogovorijo v živo, in to z nekom, ki ga poznajo. Neprijetne komentarje ali grožnje je preko spleta dobilo 53 % otrok, izmed teh pa jih je

skoraj polovica odgovorila z enako neprijetnim ali bolečim komentarjem. Zanimivo je tudi to, da splet za iskanje podatkov za šolo uporablja le 17 % anketiranih, največ pa jih splet uporablja za zabavo (Lobe in Muha 2011, 25).

7.2 EU Kids Online

EU Kids Online je mednarodni projekt, delno financiran s strani EU, pri katerem so sodelovale vse države, ki so bile leta 2010 članice EU (25). Glavna institucija, ki je bila zadolžena za urejanje podatkov pri raziskavi, je bila London School of Economics and Political Science. Namen projekta sta bila združitev in primerjava vseh podatkov med državami, ki so bili zbrani v lokalno izvedenih raziskavah »Mladi na netu« (O'Neill 2014, 4).

Ugotovitve raziskave slovenske otroke uvrščajo med nezaščitene uporabnike spleta, kar pomeni, da lahko sami že pri mladih letih dostopajo do spleta. Starši otrokom ne postavljajo omejitev dostopa do vsebine na spletu, niso intenzivno vključeni v uporabo interneta svojih otrok (Safe.si 2014) in jim starši ne postavljajo posebnih omejitev. V to kategorijo, ki je zadnja izmed štirih, so uvrščeni tudi otroci iz Avstrije, Madžarske in Litve. Mladi iz vseh držav, vključenih v raziskavo, pa do spleta začenjajo dostopati vse hitreje, tam ostajajo dlje in do spleta dostopajo s pomočjo različnih naprav, kot so računalnik, telefon, televizija.

7.3 Projekt »Nasvet za net«

Projekt Nasvet za net je organizirala Zveza potrošnikov Slovenije (ZPS), ki je mladim s pomočjo spletne klepetalnice in brezplačne telefonske številke ponujala brezplačne nasvete, povezane z uporabo spleta. Projekt sta v okviru programa Varnejši internet Plus sofinancirala Evropska komisija in Ministrstvo za šolstvo, znanost in tehnologijo. V treh letih delovanja projekta (2009–2012) je do njihovih nasvetov prišlo več kot 500 posameznikov, predvsem mladostnikov. Zabeležili so tudi kar nekaj (približno 1/3) vprašanj in prošenj za nasvete s strani staršev, ki mladostnike trenutno vzgajajo (povzeto po Med.Over.Net 2012). Najbolj vsakdanji in praktični nasveti oz. odgovori na vprašanja so bili večkrat anonimno objavljeni tudi v reviji PIL, ki je namenjena najstnikom.

Najpogostejša vprašanja, ki so jih mladi in njihovi starši zastavljali so bila v povezavi z:

- odvisnostjo od spleta in spletnih iger
- visokimi stroški računa za (pametne) telefone
- odstranjevanjem neželenih fotografij in videov iz družbenih omrežij
- odstranjevanjem in prijavo žaljivih komentarjev
- nasveti pri kraji osebnega gesla za družbena omrežja, e-pošto itd.

Svetovalci so posameznike tudi napotili do pristojnih centrov za nadaljnjo pomoč in prijavo hujših kršitev (Med.Over.Net 2012).

8 ZAKLJUČEK

Na podlagi rezultatov ankete in prebrane literature sem prišel do zanimivih ugotovitev in uporabnih podatkov. Spletna anketa je bila po mojem mnenju ustrezna izbira, saj sem s pomočjo pridobljenih podatkov dobil podroben vpogled v navade mladih in njihovih staršev. Intenziven razvoj digitalizacije na vseh področjih je neizogiben, zato je pomembno uporabnike sodobnih tehnologij poučiti o pravilni in varni uporabi. Mladi pri tem predstavljajo pomembno skupino, ki potrebuje znanje, saj bodo tehnologijo uporabljali skozi vse življenje. Naložba v mlade se v tem smislu večkratno obrestuje. Po rezultatih ankete kar 98 % mladih uporablja pametni telefon, ki ima dostop do spleta, in 92,9 % jih uporablja družbena omrežja vsak dan. Skoraj polovica jih telefon prinese ter uporablja tudi med šolo. Strah, da bi nekaj zamudili, je torej prisoten pri večini mladih, saj jih je večina na splet povezanih in dosegljivih skoraj ves čas. Ta psihična navezanost pa na mlade velikokrat negativno vpliva, saj zavira sanjarjenje, ki naj bi bilo po mnenju znanstvenikov tesno povezano s kognitivnim razvojem, kreativnostjo in spominom (Frenkel 2014).

Pojem zasebnost pri mladih ni preveč priljubljen in mu glede na zbrane podatke posebne pozornosti ne posvečajo, kar je zaskrbljujoče dejstvo. Zakaj bi se pred svetom »skrivali«, če pa lahko vse podatke delimo in se s tem počutimo dobro in zaželeno? Vsaj takšno je prepričanje sodobne mladine. Všečki in podpora virtualnih prijateljev (včasih popolnih neznancev) današnji mladini predstavlja potrdilo, da so popularni in sprejeti v družbo. Kljub vsemu pa v resničnosti temu ni tako, saj se večina stvari, ki jih ljudje opravijo, ne meri s številom všečkov. Na podlagi tega lahko sklepamo, da zasebnost mladim predstavlja nekaj nezaželenega, ravno obratno pa je pri starejših, ki si zasebnost želijo. Zasebnost na spletu pa je izjemnega pomena prav za mlajše generacije, saj se vsi podatki, objavljeni na spletu, beležijo in tam ostajajo, zato je pomembno izobraževanje, ki vzgaja in formira zrele uporabnike spleta. Objavljanje vsebin mladim predstavlja nekakšno vsakdanjo rutino, saj med njimi vlada narcisoidno oziroma samovšečno prepričanje, da se je za svoj družbeni status potrebno boriti s fotografijami, objavljenimi na družbenih omrežjih (Facebook, Instagram) in z zbiranjem všečkov. Bahanje pred drugimi tako predstavlja življenjski stil današnje mladine – pa naj bo to bahanje z novim telefonom ali pa fotografijo kosila, ki so ga tisti dan pojedli. To kaže, da je naša družba vse bolj narcisoidna, vpliv te samovšečnosti pa je močan na spletnih družbenih omrežjih, ki mladim danes predstavlja že kar samoumevno platformo

sodobnega načina življenja. Vsak dan računalnik uporablja le približno polovica anketiranih otrok, pri čemer pravijo, da v večji meri uporabljajo pametni telefon, to pa pravijo praktično vsi. Kar 68 % jih pravi, da imajo telefon ves čas pri sebi in so preko njega dosegljivi kadarkoli, tudi ponoči. To kaže, da je danes pomembno predvsem to, da si dostopen in na voljo ves čas, drugače si lahko izobčen iz družbenega kroga. Naj gre za učenje uporabe pisarniških programov, namestitvev antivirusnega programa ali prijavo na družbeno omrežje – povsod obstajajo pravila in navodila za pravilno in varno uporabo. Ta pravila in navodila za varno uporabo morajo institucije ali starši prenesti na mlade, da bodo postali informacijsko pismena generacija. Šole že delajo korak naprej glede računalništva, vendar sklepajoč po rezultatih ankete, mlade izobražujejo predvsem o uporabi orodij ter programov, o varnosti na spletu pa pri skoraj polovici anketirancev ni govora. Mladi se sicer v veliki meri tudi sami naučijo takih stvari, vendar včasih po napačni poti, z bridko izkušnjo. Ugotovil sem tudi, da ima veliko staršev gesla za dostop do družbenih omrežij in e-pošte svojih otrok, predvsem za otroke, mlajše od 15 let. Ali je to poseganje v otrokovo zasebnost, je kontradiktno vprašanje, ki ima lahko tako pozitivne kot negativne posledice. Zanimiva pa je tudi ugotovitev, da bolj izobraženi starši tudi v večji meri nadzorujejo aktivnosti svojih otrok na spletu. Nadzor naj bi bil po njihovem mnenju pomemben, da se oblikuje zdrav in odgovoren odnos do uporabe interneta. Ker se otroci zelo malokrat po pomoč obrnejo na starše, kadar imajo težavo, imajo tu starši prednost, saj jih lahko napotijo v pravo smer. Načini preživljanja prostega časa se spreminjajo in mladostniki se z igrišč vse bolj selijo pred računalnike in pametne telefone, kjer s prijatelji komunicirajo in se virtualno zabavajo na primer z igranjem spletnih iger. Starši pa pri spletu ne postavljajo dovolj omejitev in otrokom dopuščajo zelo odprt dostop do spleta, kjer je kriminal nad otroki vse pogostejši. Mladi tako v večji meri odgovarjajo, da jim starši ne postavljajo časovnih omejitev pri uporabi spleta, kar pomeni, da je njihova spletna aktivnost prepuščena naključju in lastni presoji, kdaj je interneta dovolj. Mladi tudi težko ocenjujejo, koliko časa na spletu dejansko preživijo, saj se načini rabe spleta menjajo. Na spletu so v manjših časovnih obdobjih, vendar večkrat dnevno, kadar dobijo obvestilo. Po rezultatih angleške raziskave naj bi povprečen človek na telefon pogledal več kot 85-krat dnevno, pri mladih pa naj bi bila ta številka še višja (Andrews in drugi 2015, 5). Pojem zasebnosti med mladimi torej izginja in se zabrisuje z uporabo spletnih družbenih omrežij za samopromocijo in z namenom pridobitve družbenega odobravanja s strani vrstnikov. Internet pa prav vsem uporabnikom ponuja dodatne možnosti za komunikacijo, zabavo, delo in izobraževanje, hkrati pa nas postavlja pred nova tveganja. Ker pa smo z internetom vse bolj

obsedeni, lahko zabriše tudi osebne stike z ljudmi, ter v ospredje postavlja virtualna prijateljstva. Zanimivi so tudi nasprotujoči si odgovori otrok in staršev. Namen mojega diplomskega dela je bil tudi odpreti nova vprašanja, ki se porodijo s primerjavo odgovorov staršev in otrok. Prav s tem namenom pa sem staršem, ki so v anketi sodelovali omogočil, da prejmejo analizo podatkov, če v okvirček na koncu ankete vpišejo svoj e-poštni naslov. Kot razlog za nasprotujoče odgovore otrok bi lahko prišteli pristranskost odgovorov otrok, ki menijo, da so sami dovolj odgovorni in ne potrebujejo omejitev s strani staršev, ali pa nepristranskost staršev, ki želijo vzgojo svojih otrok prikazati čimbolj popolno in v dobri luči.

Uporaba tehnoloških naprav pa je močno zaznamovala kulturo, v kateri živimo. Brez znanja uporabe tehnologije, s katero se srečujemo na vsakem koraku, bi bilo življenje v naši kulturi zelo ovirano oziroma praktično nemogoče. Že za potovanje z mestnim avtobusom moramo biti seznanjeni s pametno kartico Urbana, na katero naložimo »virtualni denar« in z njo potujemo po Ljubljani. Ta tehnološki napredek počasi, pa vendar drastično zaznamuje človeški razvoj in staro nadomešča z novim. Tehnologija tako preureja življenje, z modernizacijo človeštva pa tudi preoblikuje kulturo, v kateri živimo. Zato je izobraževanje mladih o varni in pravilni uporabi interneta ter naprav prioriteta za optimalno življenje v sodobni družbi. Danes večina uporabnikov ne namenja zadostnega pomena varnosti svojih naprav, vse dokler se jim računalnik ne okuži in s tem tvegajo izgubo svojih podatkov. Tudi mladi so v anketi odgovarjali, da so se že srečali z virusi in to tudi z najnovejšimi, ki zahtevajo odkupnino. To prikazuje, kako hitro lahko splet postane nevaren tudi za najmlajše, starši pa morajo igrati močnejšo vlogo pri preprečevanju nastajanja takih primerov z ustreznim pristopom in učenjem varne uporabe spleta in tehnoloških naprav.

9 LITERATURA

1. Anderson, Elizabeth. 2015. Teenagers spend 27 hours a week online: How internet use has ballooned in the last decade. *The Telegraph*, 11. maj. Dostopno prek: <http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/digital-media/11597743/Teenagers-spend-27-hours-a-week-online-how-internet-use-has-ballooned-in-the-last-decade.html> (9. december 2016).
2. Andrews, Sally., David A. Ellis, Heather Shaw in Lukasz Piwek. 2015. Beyond Self-Report: Tools to Compare Estimated and Real-World Smartphone Use. *Public Library of Science* 10 (10): 1–9.
3. Appelbaum, Mark., Sandra Calvert, Kenneth Dodge, Sandra Graham, Gordon Nagayama Hall, Sherry Hamby, Lawrence Hedges, Lauren Caldwell, Amani Chatmman in Dan Galloway. 2015. *Technical Report on the Review of the Violent Video Game Literature*. Washington: The American Psychological Association.
4. Blanchard, Anita., Jennifer L. Welbourne in Marla D. Boughton. 2011. A model of online trust: The mediating role of norms and sense of virtual community. *Information, Communication & Society* 14 (1): 76–106.
5. Bučar-Ručman, Aleš. 2004. *Nasilje in mladi*. Novo mesto: Klub mladinski kulturni center Novo mesto.
6. Bryce, Jo in Mathias Klang. 2009. Young people, disclosure of personal information and online privacy: Control, choice and consequences. *Information security Technical Report* (14): 160–166.
7. Christofides, Emily, Amy Muise in Serge Desmarais. 2012. Hey mom, what's on your Facebook? Comparing Facebook disclosure and privacy in adolescents and adults. *Social Psychological and Personality Science* 3 (1): 48–54.

8. Cohen-Almagor, Raphael. 2011. Internet history. *International Journal of Technoethics* 2 (2): 45–64.

9. Contena, Bastianina., Yura Loscalzo in Stefano Taddei. 2015. Surfing on Social Network Sites: A comprehensive instrument to evaluate online self-disclosure and related attitudes. *Computers in Human Behavior* 49: 30–37.

10. Desjarlais, Malinda., Jillian Gilmour, Jasmine Sinclair, Katilyn B. Howell in Alyssa West. 2015. Predictors and Social Consequences of Online Interactive Self-Disclosure: A Literature Review from 2002 to 2014. *Cyberpsychology, Behavior, and Social Networking* 18 (12): 718–725.

11. Deloitte. 2017. *European citizens and intellectual property: Perception, awareness and behaviour*. European Union Intellectual Property Office. Alicante. Dostopno prek: http://euipo.europa.eu/tunnelweb/secure/webdav//documentlibrary/observatory/documents/IPContributionStudy/2017/european_public_opinion_study_web.pdf (22. april 2017).

12. Duggan, Maeve. 2014. *Online Harassment: Summary of Findings*. Washington: Pew Research Centre. Dostopno prek: <http://www.pewinternet.org/2014/10/22/online-harassment/> (3. junij 2017).

13. Durante, Massimo. 2011. The Online Construction of Personal Identity through Trust and Privacy. *Information* (2): 594–620.

14. Ehrenberg, Alexandra., Suzanna C. Juckes, Katherine M. White, Shari P. Walsh. 2008. Personality and Self-Esteem as Predictors of Young People's Technology Use. *Cyber Psychology and Behavior* 11 (6): 739–741.

15. Engel, Pamela. 2015. Here's the manual that Al Qaeda and now ISIS use to brainwash people online. *Business Insider: Military & Defence*, 2. julij. Dostopno prek: <http://www.businessinsider.com/the-manual-al-qaeda-and-now-isis-use-to-brainwash-people-online-2015-7> (8. maj 2017).

16. Evropska komisija. 2014. *A profile of current and future audiovisual audience: Final report*. Luxembourg: European Union. Dostopno prek: http://bookshop.europa.eu/is-bin/INTERSHOP.enfinity/WFS/EU-Bookshop-Site/-en_GB/-EUR/ViewPublication-Start?PublicationKey=NC0414085 (22. april 2017).
17. Fornazarič, Milena. 2010. *Stališča do spletnega oglaševanja in vpliv na vedenje mladih*. Doktorska disertacija. Ljubljana: Ekonomska fakulteta.
18. Frenkel, Lior. 2014. *Why we should rethink our relationship with the smartphone, TEDx Bulgaria*. Dostopno prek: <http://undigitize.me/2014/08/24/lior-frenkel-ted/> (1. junij 2017).
19. Gross, Elisheva. 2004. Adolescent Internet use: What we expect, what teens report. *Applied Developmental Psychology* (25): 633–649.
20. Göritz, Anja. 2007. The induction of mood via the WWW. *Motivation and Emotion* 31 (1): 35–47.
21. Grabner-Krauter, Sonja in Sofie Bitter. 2015. Trust in online social networks: A multifaceted perspective. *Forum for Social Economics* 44 (1): 48–68.
22. Hollenbaugh, Erin in Amber L. Ferris. 2015. Predictors of honesty, intent, and valence of Facebook self-disclosure. *Computers in Human Behaviour* (50): 456–464.
23. Karačić, Silvana in Stjepan Orešković. 2017. Internet Addiction Through the Phase of Adolescence: A Questionnaire Study. *Journal of Medical Internet Research* 4 (2): 1–11.
24. Kaspersky. 2015. *Two-thirds of Users Encountered Content Dangerous to Children on Internet in 2014*. Dostopno prek: <http://www-old.kaspersky.com/about/news/business/2015/Two-thirds-of-Users-Encountered-Content-Dangerous-to-Children-on-the-Internet-in-2014> (7. december 2016).

25. *Kazenski zakonik* (KZ-1). Uradni list Republike Slovenije, št. 50/2012. Ljubljana: Uradni list Republike Slovenije. Dostopno prek: <https://zakonodaja.com/zakon/kz-1/297-clen-javno-spodbujanje-sovrastva-nasilja-ali-nestrapnosti> (9. april 2017).
26. Keating, Lauren. 2016. The Octopus Smartwatch for kids teaches them responsibility so parents don't have to. *Tech Times*, 23. junij. Dostopno prek: <http://www.techtimes.com/articles/166729/20160623/octopus-smartwatch-kids-teaches-responsib-parents-don-t.htm> (11. april 2017).
27. Kemperle, Tia. 2016. Skrite pasti in prežeče nevarnosti interneta. Dostopno prek: <http://www.bogastvozdravja.si/odnosi-in-druzina/otroci/1316-skrite-pasti-in-prezece-nevarnosti-interneta> (10. april 2017).
28. Lavrič, Miran., Sergej Flere, Marina Tavčar Krajnc, Rudi Klanjšek, Bojan Musil, Andrej Naterer, Andrej Kirbiš, Suzana Mihelin, Darja Ivanuša, Marko Divjak, Urška Antolin in Petra Lešek. 2010. *Mladina 2010: Končno poročilo o rezultatih raziskave*. Ljubljana: Ministrstvo za šolstvo in šport, Urad za mladino. Dostopno prek: http://www.ris.org/uploadi/editor/1298839714Mladina_2010_Koncno_porocilo.pdf (10. december. 2016).
29. Li, Siyue., Bo Feng, Na Li in Xuan Tan. 2015. How Social Context Cues in Online Support Seeking Influence Self-Disclosure in Support Provision. *Communication Quarterly* 63 (5): 586–602.
30. Livingstone, Sonia., Leslie Haddon, Anke Görzig in Kjartan Ólafsson. 2011. *Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9–16 year olds and their parents in 25 countries*. London: Kids Online Network.
31. Loiacono, T. Elanor. 2014. Self-Disclosure Behaviour on Social Networking Web Sites. *International Journal of Electronic Commerce* 19 (2): 66–94.

32. Lobe, Bojana in Sandra Muha. 2011. *Internet v vsakdanjem življenju slovenskih otrok in mladostnikov: Prvo poročilo raziskave Mladi na netu*. Ljubljana: Fakulteta za družbene vede: Center za metodologijo in informatiko. Dostopno prek: https://safe.si/sites/default/files/mladinanetu_porocilo_0_0.pdf (15. april 2017).
33. McIntyre, Victoria. 2016. Do(x) You Want to Hurt Me? Adapting IIED as a Solution to Doxing by Reshaping Intent. *Tulane Journal of Technology & Intellectual Property* (19): 111–134.
34. McMillan, W. David in David M. Chavis. 1986. Sense of community: A definition and theory. *Journal of Community Psychology* 14 (1): 6–23.
35. Med.Over.Net. 2012. Kako varno se počutijo mladi na internetu? Dostopno prek: <https://med.over.net/kako-varno-se-pouutijo-mladi-na-internetu/> (15. april 2017).
36. Motl, Andrej. 2017. *Desetletnica delovanja prijavnice točke Spletno oko*. Ljubljana: Fakulteta za družbene vede.
37. Mousavi, Sahar., Stuart Roper in Kathleen A. Keeling. 2017. Interpreting social identity in online brand communities: Considering posters and lurkers. *Psychology and Marketing* 34 (4): 376–393.
38. Norris, Pippa in Ronald Inglehart. 2009. *Cosmopolitan communications: cultural diversity in a globalized world*. Cambridge: Cambridge University Press.
39. O'Neill, Brian. 2014. *Policy Influences and Country Clusters: A Comparative Analysis of Internet Safety Implementation*. London: London School of Economics and Political Science. Dostopno prek: <http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/D6.3-Policy-Influences-May-2014-Final.pdf> (16. april 2017).

40. Oppmann, Patrick. 2010. In digital world, we trade privacy for convenience. *CNN*, 14. april. Dostopno prek: <http://edition.cnn.com/2010/TECH/04/14/oppmann.off.the.grid/index.html> (11. april 2017).
41. Ofcom. 2015. *Children and Parents: Media Use and Attitudes Report*. London: Ofcom. Dostopno prek: https://www.ofcom.org.uk/__data/assets/pdf_file/0024/78513/childrens_parents_nov_2015.pdf (3. junij 2017).
42. Petrič, Gregor in Andraž Petrovčič. 2014. Elements of the management of norms and their effects on the sense of virtual community. *Online Information Review* 38 (3): 436–454.
43. *Safe.si*. 2014. EU KIDS ONLINE: Slovenski otroci so nezaščiteni uporabniki interneta. Dostopno prek: <https://safe.si/novice/eu-kids-online-slovenski-otroci-so-nezasciteni-druzabni-uporabniki-interneta> (16. april 2017).
44. *Safe.si*. 2016. O Centru za varnejši internet. Dostopno prek: <http://www.safe.si/center-za-varnejsi-internet/o-centru> (10. december 2016).
45. Sánchez-Franco, Manuel in José L. Roldán. 2015. The influence of familiarity, trust and norms of reciprocity on an experienced sense of community: an empirical analysis based on social online services. *Behaviour & Information Technology* 34 (4): 392–341.
46. Sanghani, Radhika. 2016. Leaked sex tapes aren't a joke - they're deadly. *The Telegraph*, 16. september. Dostopno prek: <http://www.telegraph.co.uk/women/life/tiziana-cantone-suicide-leaked-sex-tapes-arent-a-joke---theyre-d/> (7. maj 2017).
47. SI-CERT. 2017. *Phishing*. Dostopno prek: <https://www.cert.si/si/varnostne-groznje/phishing/> (29. marec 2017).
48. Sieckenius de Souza, Clarisse in Jenny Preece. 2004. A framework for analyzing and understanding online communities. *Interacting with Computers* (16): 579–610.

49. Subrahmanyam, Kaveri., Patricia Greenfield, Robert Kraut in Elisheva Gross. 2001. The impact of computer use on children's and adolescents' development. *Applied Developmental Psychology* (22): 7–30.
50. SURS. 2015. *Uporaba informacijsko-komunikacijske tehnologije v gospodinjstvih in pri posameznikih v zadnjih treh mesecih*. Ljubljana: Statistični urad Republike Slovenije. Dostopno prek: http://pxweb.stat.si/pxweb/Database/Ekonomsko/23_29_informacijska_druzba/11_IKT_posamezniki/02_29741_uporaba_rac/02_29741_uporaba_rac.asp (16. april 2017).
51. Suissa, A. Jacob. 2015. Cyber addictions: toward a psychosocial perspective. *Addictive Behaviours* (43): 28–32.
52. Suzor, Nicolas. 2012. Order Supported by Law: The Enforcement of Rules in Online Communities. *Mercer Law Review* (63): 523–595.
53. Šterk, Tanja in Ajda Petek. 2016. *Pomoč staršem v vrtincu novih tehnologij: Napotki za otrokom prijaznejši internet*. Ljubljana: Fakulteta za družbene vede. Dostopno prek: http://www.osnovna-sola-idrija.si/files/2016/04/safe_si_brosura_starsi_ponatis_feb_2016_e_verzija.pdf (9. april 2017).
54. Šterk, Tanja., Tina Zupanič, Matej Kovačič in Tomi Dolenc. 2006. *Kako varno uporabljati internet? Gradivo za učitelje*. Ljubljana: Fakulteta za družbene vede. Dostopno prek: http://uploadi.safe.si/editor/1157005150gradiva_za_ucitelje_final.pdf (22. april 2017).
55. Toor, Amar. 2016. Most students can't tell the difference between sponsored content and real news. *The Verge*, 22. november. Dostopno prek: <https://www.theverge.com/2016/11/22/13712996/fake-news-facebook-google-sponsored-content-study> (3. marec 2017).
56. Varni in internet. 2017. *Rubrika O nas*. Dostopno prek: <https://www.varniinternet.si/zavod> (17. april 2017).

57. Varnali, Kaan in Aysegul Toker. 2015. Self-disclosure on Social Networking Sites. *Social behaviour and personality* 43 (1): 1–14.
58. Varni na internetu 2017. *Zavihek Kdo smo*. Dostopno prek: www.varninainternetu.si/kdo-smo/ (14. april 2017).
59. Vehovar, Vasja, Tanja Šterk, Andreja Pestotnik in Urša Šmid Božičevič. 2009. *Za varen internet: Predstavitev projektov za zaščito otrok pri uporabi interneta*. Mednarodna konferenca o otrokovih pravicah in zaščiti pred nasiljem, dne 6. avgust 2009, Ljubljana, Državni zbor.
60. Wallace, Kelly. 2015. Teens spend a 'mind-boggling' 9 hours a day using media, report says. CNN, 4. november. Dostopno prek: <http://edition.cnn.com/2015/11/03/health/teens-tweens-media-screen-use-report/index.html> (9. december 2016).
61. Welch, R. Michael, Roberto E. N. Rivera, Brian P. Conway, Jennifer Yonkoski, Paul M. Lupton in Russell Giancola. 2005. Determinants and consequences of social trust. *Sociological Inquiry* 75 (4): 453–473.
62. Zlatolas, N. Lili., Tatjana Welzer, Tanja Heričko in Marko Hölbl. M. 2015. Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behaviour* (45): 158–167.

PRILOGE

Priloga A: Kanali promocije ankete za mlade



Slika A.1: Promocija TOM



Slika A.2: Promocija Safe.si



Slika A.3: Promocija MISSS



Slika A.4: Promocija Deskam varno

Anketa o varni rabi interneta za učence in srednješolce

ponedeljek, 10. 4. 2017

Vabimo vas, da osnovnošolcem (zadnja triada) in srednješolcem posredujete anketo na temo varne rabe interneta mladih in njihovega zavedanja o tveganjih na internetu.

Avtor ankete je študent 4. letnika družboslovne informatike na Fakulteti za družbene vede Univerze v Ljubljani, **Tim Grilc**. V sklopu diplomske naloge se ukvarja z raziskovanjem navad mladih na spletu.

Z rezultati do še boljšega tečaja MOOC-V

Rezultati bodo zbrani in uporabljeni izključno v raziskovalne namene, na Arnesu pa bomo skušali pridobljene rezultate uporabiti za izboljšanje brezplačnega spletnega tečaja o varni rabi interneta in sodobnih tehnologij – **MOOC-V**.

Anketo najdete na naslovu: <https://www.1ka.si/a/123131>

Arnes je pri pripravi ankete nudil strokovno podporo.

[Vabilo k sodelovanju v spletni anketi za učence in učenke.](#)

[Vabilo k posredovanju spletne ankete učencem in učenkam.](#)

[<- Nazaj na stran: Novice](#)

[Naročite se na RSS obvestila](#)



Slika A.5: Promocija Arnes



Kategorije:

[Izobraževanja](#)
[Izpostavljeno](#)
[Podpora](#)
[Projekti](#)

Oznake:

[ankete](#), [arnes](#), [internet](#),
[nevarnosti](#), [varnost](#)

Ocena obiskovalcev:

★★★★★ (5 votes, average:
3,80 out of 5, **rated**)

Deli z ostalimi:



3



Anketa o varni rabi interneta za učence in srednješolce

Vabimo vas, da osnovnošolcem (zadnja triada) in srednješolcem posredujete anketo na temo varne rabe interneta mladih in njihovega zavedanja o tveganjih na internetu.

Avtor ankete je študent 4. letnika družboslovne informatike na Fakulteti za družbene vede Univerze v Ljubljani, **Tim Grilc**. V sklopu diplomske naloge se ukvarja z raziskovanjem navad mladih na spletu.

Z rezultati do še boljšega tečaja MOOC-V

Rezultati bodo zbrani in uporabljeni izključno v raziskovalne namene, na Arnesu pa bomo skušali pridobljene rezultate uporabiti za izboljšanje brezplačnega spletnega tečaja o varni rabi interneta in sodobnih tehnologij – **MOOC-V**.

Anketo najdete na naslovu: <https://www.1ka.si/a/123131>

Arnes je pri pripravi ankete nudil strokovno podporo.

- [Vabilo k sodelovanju v spletni anketi za učence in učenke.](#)
- [Vabilo k posredovanju spletne ankete učencem in učenkam.](#)

Slika A.6: Promocija SIO

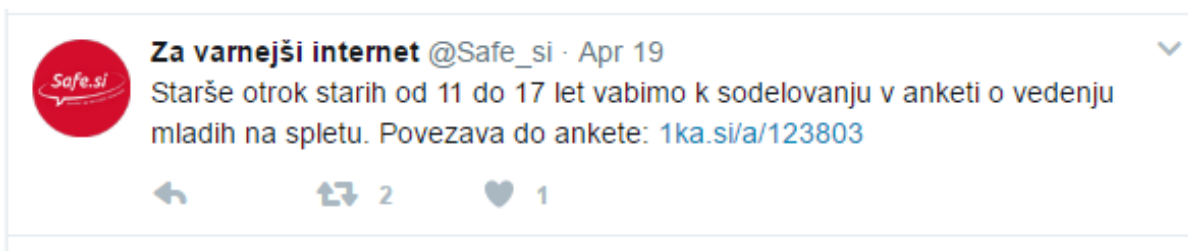
Priloga B: Kanali promocije ankete za starše



Slika B.1: Promocija Za starše



Slika B.2: Promocija Safe.si - starši



Slika B.3: Promocija Safe.si Twitter

Priloga C: Anketni vprašalnik za mlade

Pozdravljeni!

Sem študent 4. letnika Fakultete za družbene vede in v sklopu diplomske naloge raziskujem navade mladih na spletu. Pred vami se nahaja anketa, katere rezultati so zelo pomembni za kakovost moje diplomske naloge. Prosim vas, da na vprašanja odgovarjate po lastnem prepričanju, saj pravih oziroma napačnih odgovorov NI. Pri nekaterih vprašanjih je mogoče vnesti tudi lasten odgovor, in sicer z vpisom v prazen prostor in z označitvijo odgovora »Drugo«.

Podatki, zbrani v anketi, bodo uporabljeni izključno za raziskovalne namene in ne bodo posredovani tretjim osebam. Anketa vam bo vzela največ 10 minut.

Za morebitna vprašanja sem na voljo preko elektronske pošte na naslovu tg2322@student.uni-lj.si.

S klikom na gumb "Naslednja stran" pričnete z izpolnjevanjem ankete.

Zahvaljujem se vam za sodelovanje.

Q1 - V tem sklopu se nahajajo splošna vprašanja o vaših navadah in pogostosti uporabe interneta. Izberite tiste odgovore, ki držijo. Pri nekaterih vprašanjih je možno izbrati tudi več odgovorov.

Q2 - Ali imaš:

	Da	Ne
Svoj računalnik (namizni računalnik, prenosnik ali tablica)	☐	☐
Družinski računalnik (namizni računalnik, prenosnik ali tablica)	☐	☐

	Da	Ne
Pametni telefon, s katerim je mogoče dostopati do interneta	☐	☐
Mobilni telefon, ki nima dostopa do interneta	☐	☐

Q3 - Koliko časa približno preživiš na računalniku v svojem prostem času?

- ☐ V prostem času ne uporabljam računalnika
- ☐ Računalnika ne uporabljam vsak dan
- ☐ Manj kot 2 uri dnevno
- ☐ 3 - 6 ur dnevno
- ☐ Več kot 6 ur dnevno
- ☐ Drugo:

Q4 - Kako pogosto uporabljaš pametni telefon?

Izberi trditev, ki najbolj drži.

- ☐ Ne uporabljam pametnega telefona
- ☐ Na telefon pogledam nekajkrat dnevno
- ☐ Na telefon pogledam samo takrat, ko dobim obvestilo
- ☐ Telefon imam skoraj ves čas pri sebi in sem skoraj ves čas dosegljiv
- ☐ Na telefonu sem dosegljiv kadarkoli, tudi ponoči
- ☐ Drugo:

Q5 - Svoj telefon uporabljaš za:

Možnih je več odgovorov

- ☐ Za telekomunikacijo (SMS-anje, klicanje)
- ☐ Komuniciranje preko aplikacij (Whatsapp, Viber, Skype)
- ☐ Dostop do Facebooka, Snapchata in drugih omrežij
- ☐ Brskanje po spletu
- ☐ Drugo:

Q6 - Ta sklop vprašanj se nanaša na vašo rabo družbenih omrežij. Izberite tiste odgovore, ki držijo. Pri nekaterih vprašanjih je možno izbrati tudi več odgovorov.

Q7 - Ali si uporabnik/ca vsaj enega družbenega omrežja, ki ga dnevno spremljaš?

Primer omrežij: Facebook, Snapchat, Instagram, Twitter itd.

- ☐ Da
- ☐ Ne

Q8 - Na spletu oziroma družbenih omrežjih sem kdaj objavil/a naslednje podatke: V kolikor nisi uporabnik družbenih omrežij, označi, kaj bi objavil, če bi uporabljal družbena omrežja.

Možnih je več odgovorov

- ☐ Svoje slike
- ☐ Slike s prijatelji
- ☐ Datum rojstva
- ☐ E-poštni naslov
- ☐ Svoje pravo ime
- ☐ Ime z vzdevkom - ("nickname")
- ☐ Telefonska številka
- ☐ Nič od naštetega

Q9 - V kakšni meri se strinjaš z naslednjimi trditvami? 1 pomeni "sploh se ne strinjam", 5 pa "zelo se strinjam"

	1 - sploh se ne strinjam	2 - se ne strinjam	3 - niti niti (včasih)	4 - se strinjam	5 - zelo se strinjam
Na spletu lažje komuniciram kot v pogovoru v živo.	☐	☐	☐	☐	☐
Na spletu lažje govorim o osebnih zadevah.	☐	☐	☐	☐	☐
Na spletu se lažje zaupam neki osebi kot v pogovoru.	☐	☐	☐	☐	☐
Svoj prosti čas preživljam na internetu ali v družbi mobilne naprave.	☐	☐	☐	☐	☐
Na internetu ostajam dlje, kot je bilo načrtovano.	☐	☐	☐	☐	☐

Q10 - Ali imaš na svojih družbenih (socialnih) omrežjih prijatelje, ki jih nisi nikoli spoznal/a v »offline« svetu oziroma se z njimi v živo nikoli nisi pogovarjal/a?

- ☐ Da
- ☐ Ne

Q11 - Ali s temi ljudmi, ki jih poznaš le preko spleta, kdaj komuniciraš?

Preko zasebnih sporočil, komentarjev itd.

- ☐ Da
- ☐ Ne

Q12 - Si kdaj "virtualnega" prijatelja spoznal/a v živo? Virtualni prijatelj je oseba, s katero si se npr. prvič pogovarjal po spletu in ne v živo.

- ☐ Da
- ☐ Ne

IF (1) Q7 = [1]

Q13 - Koliko prijateljev oziroma sledilcev imaš na spletu? (Facebook, Twitter, Instagram sledilci oz. prijatelji)

- ☐ Manj kot 100

- ☐ 100 – 300
- ☐ 300 - 600
- ☐ Več kot 600 (koliko?)

IF (1) Q7 = [, 1]

Q14 - Kakšne so nastavitve tvojega prikaza podatkov na družbenih omrežjih?

Omejen (določene podatke vidijo samo moji prijatelji) ali javen (podatki so na voljo vsem).

- ☐ Omejen
- ☐ Javen
- ☐ Ne vem, funkcije ne poznam

Q15 - Kako pogosto objavljaš oziroma deliš informacije na spletu?

Npr. objave na forumu, pisanje bloga, deljenje slike, statusov, povezav in podobno.

- ☐ Informacij nikoli ne delim
- ☐ Manj kot enkrat tedensko
- ☐ Več objav na teden
- ☐ Več objav dnevno

Q31_2 - Ali pametni telefon vzameš s seboj v šolo?

- ☐ Vzamem in ga tudi uporabljam v šoli (tudi med poukom)
- ☐ Vzamem, vendar ga ne uporabljam v šoli (le med odmori)
- ☐ Vzamem, a ga v šoli sploh ne uporabljam
- ☐ Včasih ga vzamem
- ☐ Ne vzamem ga v šolo
- ☐ Nimam pametnega telefona

Q16 - Ali te sošolci, prijatelji ali starši opozarjajo, da preveč časa preživiš na spletu ali pametnem telefonu?

- ☐ Ne
- ☐ Da, starši
- ☐ Da, sošolci oziroma prijatelji
- ☐ Da, starši, sošolci in prijatelji

Q18_2 - Ta sklop se navezuje na vaše dosedanje izkušnje na spletu.

Q17 - Te je kdaj kdo nadlegoval, ustrahoval ali izsiljeval preko spleta? Ustrahovanje pomeni, da ti je kdo pošiljal zlobna sporočila, grozil, od tebe zahteval nekaj kar mu sicer ne bi želel dati in te s tem spravil v neprijeten položaj.

- ☐ Da
- ☐ Ne

Q18 - Morda poznaš koga, ki ga je preko spleta nekdo nadlegoval, ustrahoval oziroma izsiljeval?

- ☐ Da
☐ Ne

Q19 - Ali si povedal staršem ali prijateljem, da te je nekdo nadlegoval, ustrahoval oziroma izsiljeval preko spleta?

- ☐ Da, staršem
☐ Da, prijateljem ali sošolcem
☐ Da, staršem, prijateljem ali sošolcem
☐ Ne
☐ Nihče me ni nikoli nadlegoval, ustrahoval ali izsiljeval preko spleta.

Q20 - Kaj si naredil/a, če te je nekdo nadlegoval, ustrahoval oziroma izsiljeval preko spleta?

Možnih je več odgovorov

- ☐ To osebo sem prosil, da me preneha nadlegovati
☐ Za pomoč sem prosil starše ali pa prijatelje
☐ Osebo sem prijavil ali blokiral na tem spletnem mestu
☐ Naredil nisem ničesar
☐ Nihče me ni nikoli nadlegoval preko spleta
☐ Drugo:

Q21 - Ali ti starši določijo, koliko časa si lahko na spletu?

Npr. največ dve uri dnevno, samo ob vikendih itd.

- ☐ Da
☐ Ne
☐ Drugo:

Q22 - Si bil/a kdaj kaznovan/a tako, da so ti starši vzeli telefon ali računalnik?

- ☐ Da
☐ Ne

Q23 - Ali so ti starši povedali, katere podatke in vsebino lahko objaviš na spletu in katerih ne smeš?

Npr. osebni podatki, telefonska številka, vaše osebne slike in podobno.

- ☐ Da
☐ Ne

Q24 - Ali se ti je že kdaj zgodilo kaj od naštetega?

Možnih je več odgovorov

- ☐ Da te je nekdo žalil preko spleta.
☐ Da ti je nekdo grozil preko spleta.
☐ Da se je nekdo posmehoval ali norčeval iz tvojih objav (iz slik, zapisov) na spletu.
☐ Da ti je nekdo vdrl v e-pošto ali profil na družbenem omrežju

☐ Drugo:

Q25 - Pred tabo je še zadnji sklop vprašanj, povezanih z navadami na spletu.

Q26 - Ali je bilo za učence v sklopu šole organizirano kakšno predavanje o varnosti na spletu?

- ☐ Da
☐ Ne
☐ Ne vem

Q27 - Ali misliš, da na spletu preživiš preveč časa?

- ☐ Da
☐ Ne

Q28 - Ali si morda že kdaj slišal/a za te pojme:

Možnih je več odgovorov

- ☐ Phishing (spletno ribarjenje)
☐ Locky - CryptoLocker (izsiljevalski virus)
☐ Cyberbullying (spletno ustrahovanje)
☐ Zlonamerna koda
☐ Mocking
☐ Spam pošta
☐ Požarni zid

Q34_2 - Če imaš s katero od teh zadev kakršnekoli izkušnje, lahko to napišeš v spodnji okvirček.

IF (2) (Demografija)

Q29 - Za konec pa potrebujem še nekaj splošnih podatkov o tebi.

IF (2) (Demografija)

XSPOL - Označi svoj spol:

- ☐ Moški
☐ Ženski

IF (2) (Demografija)

Q30 - Prosim vnesi letnico tvojega rojstva.

Primer: 2000

IF (2) (Demografija)

XLOKACREGk - Kje prebivaš?

- ☐ V večjem mestu
- ☐ V manjšem mestu z manj kot 10.000 prebivalci
- ☐ Na podeželju/vasi
- ☐ Drugo:

IF (3) Q14 = [3]

Q31 - Več o funkciji omejitve prikaza vsebine si lahko prebereš tukaj:

<https://www.varninainternetu.si/2017/zascitite-svojo-zasebnost-na-spletu/>

Ali pa si ogledaš video tukaj:

<https://www.youtube.com/watch?v=ETdxeas5TaE>

Za dokončanje ankete prosim pritisni gumb "Naslednja stran".

Priloga Č: Anketa za starše

Pozdravljeni!

Sem študent 4. letnika Fakultete za družbene vede in v sklopu diplomske naloge raziskujem spletne navade mladih v Sloveniji. Anketa je primerna za starše, ki imajo otroke stare med 11-17 let. Vaše sodelovanje je zelo pomembno, saj lahko le z dovolj velikim odzivom pridem do konkretnih zaključkov, ki so zelo pomembni za kakovost moje diplomske naloge. Podatki, zbrani v anketi, bodo uporabljeni izključno za raziskovalne namene in ne bodo posredovani tretjim osebam. Anketa vam bo vzela približno 8 minut časa.

Za morebitna vprašanja sem na voljo preko elektronske pošte na naslovu tg2322@student.uni-lj.si. V zadnjem koraku je mogoče vpisati tudi vaš e-poštni naslov, v kolikor bi želeli prejeti rezultate raziskave, ko bo ta zaključena.

S klikom na gumb "Naslednja stran" pričnete z izpolnjevanjem ankete.

Zahvaljujem se vam za sodelovanje.

Q1 - Ali ima vaš otrok:

Označite vrednosti, ki veljajo.

Možnih je več odgovorov

- ☐ Pametni telefon z dostopom do interneta (podatkovni prenos)
- ☐ Pametni telefon brez dostopa do interneta
- ☐ Svoj osebni, prenosni ali tablični računalnik
- ☐ Osebni, prenosni ali tablični računalnik, ki je v skupni rabi
- ☐ Nič od naštetega

Q2 - Ali ste svojega otroka kdaj kaznovali z odvzemom računalnika, interneta ali pametnega telefona?

- ☐ Da
- ☐ Ne

Q3 - Ste svojega otroka seznanili z uporabo računalnika ali pametnega telefona, ga vpisali v kakšen tečaj, ali se je naučil sam?

Možnih je več odgovorov

- ☐ Naučil se je sam
- ☐ Naučil se je s pomočjo delavnic ali v šoli
- ☐ Naučil ga je nekdo znotraj družinskega kroga ali znanec
- ☐ Učenju uporabe nismo posvečali posebnih pozornosti
- ☐ Drugo:

Q4 - Ali svojemu otroku postavljate omejitve glede dostopa do spletnih vsebin oziroma uporabe računalnika?

Označite odgovor, ki drži.

- ☐ Da, postavljena so jasna pravila
- ☐ Da, postavljamo mu omejitve, vendar pravila niso "eksplicitna", ampak prilagodljiva
- ☐ Ne, nima posebnih pravil oz. omejitev
- ☐ Ne, moj otrok je dosti star, da si sam organizira, kako preživlja čas
- ☐ Drugo:

Q5 - Ocenite, koliko časa dnevno mislite, da vaš otrok preživi na računalniku. Tukaj gre za fiksni, prenosni ali tablični računalnik in ne za pametni telefon.

- ☐ Na računalniku preživi skoraj cele dneve
- ☐ Več kot 6 ur dnevno
- ☐ 3 - 6 ur dnevno
- ☐ Manj kot 2 uri dnevno
- ☐ Računalnika ne uporablja vsak dan
- ☐ Drugo:

Q6 - Mislite, da uporaba sodobne tehnologije otrokom olajša učenje in pozitivno vpliva na njihovo iznajdljivost v življenju?

- ☐ Da, ima pozitiven vpliv

- ☐ Ne, ima negativen vpliv
- ☐ Ima tako pozitiven kot negativen vpliv

Q7 - Ali menite, da je vaš otrok prekmalu začel z uporabo sodobne tehnologije?

- ☐ Da
- ☐ Ne
- ☐ Ne vem

Q8 - Se morda spomnite, pri kateri starosti je vaš otrok začel redno uporabljati računalnik ali pametni telefon za dostop do interneta? Ocenite.

- ☐ Ko je bil star 6 let ali manj
- ☐ Ko je bil star 6 - 8 let
- ☐ Ko je bil star 9 - 11 let
- ☐ Ko je bil star 12 - 14 let
- ☐ Ko je bil star 15 let ali več
- ☐ Ne spomnim se
- ☐ Moj otrok še ne uporablja interneta

Q9 - Ali svojega otroka morda nadzirate s pomočjo pametne tehnologije?

Npr. z aplikacijo na pametnem telefonu, poraba na telefonu (SMS sporočila in klici), GPS oddajnik na pametni uri, program za starševski nadzor na spletu ipd.

- ☐ Da
- ☐ Ne

Q10 - Ali...

	Da	Ne
...svojemu otroku omejujete dostop do spletnih vsebin (starševski nadzor) s pomočjo programov?	☐	☐
...ste svojemu otroku morda pomagali pri prijavi na družbeno omrežje ter mu pokazali, kako se ga uporablja? Npr. Facebook, Snapchat, Instagram itd.	☐	☐
...ste morda svojemu otroku postavili omejitve pri uporabi družbenih omrežij in mu npr. prepovedali objavo osebnih družinskih fotografij, domačega naslova, telefonske številke?	☐	☐
...menite, da vaš otrok preveč časa posveča tehnologiji ali pa je celo zasvojen s tehnologijo?	☐	☐
...menite, da pretirana raba računalnika ali pametnega telefona na splošno vodi v	☐	☐

	Da	Ne
slabše rezultate v šoli?		

IF (1) Q9 = [1] (Da)

Q11 - S pomočjo katerih naprav ali storitev nadzorujete svojega otroka?

Možnih je več odgovorov

- ☐ Aplikacija na pametnem telefonu ali tablici (NetNanny, SecureTeen, Family Time, Screen Time, Kids Place, Family Locator itd.)
- ☐ GPS oddajnik na pametni uri ali zapestnici
- ☐ Nadzor otrokovih SMS sporočil in klicev (spremljanje porabe)
- ☐ Starševski nadzor na spletu (F-Secure, Norton Family, Kaspersky itd.)
- ☐ Imam gesla za dostop do otrokove e-pošte in/ali družbenih omrežij
- ☐ Svojega otroka ne nadziram z ničimer od zgoraj napisanega
- ☐ Drugo:

Q12 - Kako pogosto vas...Ocenite pogostost na lestvici od 1 (nikoli) do 5 (zelo pogosto).

	1 - nikoli	2 - zelo redko	3 - včasih	4 - pogosto	5 - zelo pogosto
...zanimam, kaj vaš otrok počne na spletu?	☐	☐	☐	☐	☐
...skrbim, da je vaš otrok žrtev medvrstniškega spletnega nadlegovanja?	☐	☐	☐	☐	☐
...skrbim, da bi vaš otrok zapadel v slabo družbo?	☐	☐	☐	☐	☐
...skrbim, da bi vaš otrok začel uživati droge, kaditi, ali prekmalu uživati alkohol?	☐	☐	☐	☐	☐

Q13 - Označite stvari, ki jih svojemu otroku dovolite.

Možnih je več odgovorov

- ☐ Uporabo družbenih omrežij (Facebook, Instagram, Snapchat, Twitter)
- ☐ Igranje spletnih iger
- ☐ Druženja s prijatelji v večernih urah zunaj hiše
- ☐ Da si sam organizira čas na spletu
- ☐ Da uporablja računalnik pozno v noč
- ☐ Nič od naštetega

Q14 - Ali se je vaš otrok že znašel v kakšni neprijetni situaciji, ki se je zgodila na spletu?

Če je odgovor "da", lahko v okvirček na kratko opišete situacijo.

Npr. spletno izsiljevanje, norčevanje, posmehovanje ali celo kaj hujšega?

- ☐ Ne
- ☐ Da

Q15 - Za konec samo še nekaj demografskih vprašanj

XSPOL - Prosim izberite vaš spol:

- ☐ Moški
- ☐ Ženski

XDS2a4 - Kakšen je vaš trenutni status?

- ☐ Šolajoči
- ☐ Aktivni - zaposleni
- ☐ Neaktivni (porodniški dopust ipd.)
- ☐ Brezposelni

XZST1surs4 - Kakšen je vaš zakonski stan?

- ☐ Samski
- ☐ Poročeni
- ☐ V zvezi
- ☐ Razvezani/ločeni
- ☐ Ovdoveli

XIZ1a2 - Kakšna je vaša najvišje dokončana formalna izobrazba?

- ☐ Osnovna šola (II. stopnja)
- ☐ Srednja šola (III. - V. stopnja)
- ☐ Visokošolska / univerzitetna izobrazba VI. - VII. stopnja)
- ☐ Višja specializacija (VIII. stopnja)

Q16 - Vnesite še letnico rojstva vašega otroka.

email - V kolikor želite prejeti analizirane rezultate ankete, prosim vnesite svoj e-poštni naslov. Podatki, izpolnjeni v anketi, so ločeni od tega sklopa in so anonimni.

Če analiziranih rezultatov ankete ne želite prejeti, pritisnite na gumb "Zadnja stran".

Rezultati bodo poslani najkasneje do konca septembra 2017.

(npr. janez.novak@gmail.com)

Priloga D: Vabilo za mlade

Ljubljana, 13. april 2017

Dragi učenci in učenke!

Zadeva: Vabilo k sodelovanju v spletni anketi

Sem študent 4. letnika Fakultete za družbene vede in v sklopu diplomske naloge raziskujem navade mladih na spletu.

Zelo bi vam bil hvaležen, če bi si vzeli 10 minut časa za izpolnitev ankete o vaših navadah na spletu. Vprašalnik je anonimen in podatki bodo uporabljeni izključno v raziskovalne namene. Vaši odgovori so zelo pomembni, saj bom le z vašo pomočjo lahko uspešno končal svoje raziskovanje. Morda pa boste iz vprašalnika tudi sami izvedeli kaj novega in koristnega.



Anketa se nahaja na tem naslovu: <https://www.1ka.si/a/123131>

Do ankete pa lahko dostopate tudi s pomočjo telefona, v kolikor imate nameščen bralnik QR kod.

Zahvaljujem se vam za sodelovanje in vam želim varno uporabo interneta,

Tim Grilc

Priloga E: Tabele povezanosti pri anketi za starše

Tabela E.1: Povezanost med kaznovanjem in spolom

		Ali ste svojega otroka kdaj kaznovali z odvzemom računalnika, interneta ali pametnega telefona?		Total
		Da	Ne	
Prosim izberite vaš	1	87	7	94
spol:	2	151	22	173
Total		238	29	267

Tabela E.2: Povezanost med kaznovanjem in spolom - hi-kvadrat

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	1,747 ^a	1	,186	,220	,131
Continuity Correction ^b	1,245	1	,264		
Likelihood Ratio	1,844	1	,175		
Fisher's Exact Test					
Linear-by-Linear Association	1,741	1	,187		
N of Valid Cases	267				

Tabela E.3: Povezanost med omejitvami in spolom

		Ali svojemu otroku postavljate omejitve glede dostopa do spletnih vsebin oziroma uporabe računalnika? Oznacite odgovor, ki drži.					Total
		Da, postavljena so jasna pravila	Da, postavljamo mu omejitve, vendar pravila niso "eksplicitna", ampak prilagodljiva	Ne, nima posebnih pravil oz. omejitev	Ne, moj otrok je dosti star, da si sam organizira, kako preživlja čas	Drugo	
Prosim izberite	1	11	73	6	1	3	94
vaš spol:	2	58	99	10	4	2	173
Total		69	172	16	5	5	267

Tabela E.4: Povezanost med omejitvami in spolom - hi-kvadrat

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	17,064 ^a	4	,002
Likelihood Ratio	18,469	4	,001
Linear-by-Linear Association	7,468	1	,006
N of Valid Cases	267		

Tabela E.5: Povezanost med omejitvami in spolom - Cramer

		Value	Asymp. Std. Error ^a	Approx. T ^b	Approx. Sig.
Nominal by	Phi	,253			,002
Nominal	Cramer's V	,253			,002
Interval by Interval	Pearson's R	-,168	,058	-2,767	,006 ^c
Ordinal by Ordinal	Spearman Correlation	-,204	,055	-3,386	,001 ^c
N of Valid Cases		267			

Tabela E.6: Povezanost med uporabo sodobne tehnologije in spolom - Cramer

		Mislite, da uporaba sodobne tehnologije otrokom olajša učenje in pozitivno vpliva na njihovo iznajdljivost v življenju?			Total
		1	2	3	
Prosim izberite vaš	1	6	62	26	94
spol:	2	14	62	97	173
Total		20	124	123	267

Tabela E.7: Povezanost med omejitvami in spolom - hi-kvadrat

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	22,806 ^a	2	,000
Likelihood Ratio	23,195	2	,000
Linear-by-Linear Association	11,185	1	,001
N of Valid Cases	267		

Tabela E.8: Povezanost med uporabo sodobne tehnologije in spolom - Cramer

		Value	Asymp. Std. Error ^a	Approx. T ^b	Approx. Sig.
Nominal by	Phi	,292			,000
Nominal	Cramer's V	,292			,000
Interval by Interval	Pearson's R	,205	,058	3,411	,001 ^c
Ordinal by Ordinal	Spearman Correlation	,234	,058	3,924	,000 ^c
N of Valid Cases		267			

Tabela E.9: Povezanost med zgodnjo uporabo sodobne tehnologije in spolom

		Ali menite, da je vaš otrok prekmalu začel z uporabo sodobne tehnologije?			Total
		1	2	3	
Prosim izberite vaš	1	67	23	4	94
spol:	2	89	62	22	173
Total		156	85	26	267

Tabela E.10: Povezanost med zgodnjo uporabo tehnologije in spolom - hi-kvadrat

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	11,051 ^a	2	,004
Likelihood Ratio	11,685	2	,003
Linear-by-Linear Association	10,925	1	,001
N of Valid Cases	267		

Tabela E.11: Povezanost med zgodnjo uporabo sodobne tehnologije in spolom - Cramer

		Value	Asymp. Std. Error ^a	Approx. T ^b	Approx. Sig.
Nominal by	Phi	,203			,004
Nominal	Cramer's V	,203			,004
Interval by Interval	Pearson's R	,203	,054	3,369	,001 ^c
Ordinal by Ordinal	Spearman Correlation	,202	,057	3,362	,001 ^c
N of Valid Cases		267			

Priloga F: Tabela korelacij med spremenljivkami pri anketi za starše

Tabela F.1: Tabela korelacij med spremenljivkami pri anketi za starše

		Sum of Squares	df	Mean Square	F	Sig.
Kako pogosto vas zanima, kaj vaš otrok počne na spletu?	Between Groups	1,534	1	1,534	1,920	,167
	Within Groups	211,799	265	,799		
	Total	213,333	266			
Kako pogosto vas skrbi, da je vaš otrok žrtev medvrstniškega spletnega nadlegovanja?	Between Groups	67,488	1	67,488	43,201	,000
	Within Groups	410,852	263	1,562		
	Total	478,340	264			
Kako pogosto vas skrbi, da bi vaš otrok zapadel v slabo družbo?	Between Groups	35,667	1	35,667	38,091	,000
	Within Groups	245,329	262	,936		
	Total	280,996	263			
Kako pogosto vas skrbi, da bi vaš otrok začel uživati droge, kaditi, ali prekmalu uživati alkohol?	Between Groups	1,687	1	1,687	1,430	,233
	Within Groups	309,007	262	1,179		
	Total	310,693	263			

Priloga G: Tabele povezanosti pri anketi za mlade

Tabela G.1: Povezanost med uporabo družbenega omrežja in spolom

		Ali si uporabnik/ca vsaj enega družbenega omrežja, ki ga dnevno spremljaš? Primer omrežij: Facebook, Snapchat, Instagram, Twitter itd.		Total
		Da	Ne	
Označi svoj spol:	Moški	235	20	255
	Ženski	300	19	319
Total		535	39	574

Tabela G.2: Povezanost med uporabo družbenega omrežja in spolom - hi-kvadrat

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	,797 ^a	1	,372	,406	,233
Continuity Correction ^b	,527	1	,468		
Likelihood Ratio	,792	1	,374		
Fisher's Exact Test					
Linear-by-Linear Association	,795	1	,372		
N of Valid Cases	574				

Tabela G.3: Povezanost med neznanimi virtualnimi prijatelji in spolom

		Ali imaš na svojih družbenih (socialnih) omrežjih prijatelje, ki jih nisi nikoli spoznal/a v »offline« svetu oziroma se z njimi v živo nikoli nisi pogovarjal/a?		Total
		Da	Ne	
Označi svoj spol:	Moški	174	81	255
	Ženski	191	131	322
Total		365	212	577

Tabela G.4: Povezanost med neznanimi virtualnimi prijatelji in spolom - hi-kvadrat

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	4,870 ^a	1	,027	,030	,017
Continuity Correction ^b	4,494	1	,034		
Likelihood Ratio	4,899	1	,027		
Fisher's Exact Test					
Linear-by-Linear Association	4,862	1	,027		
N of Valid Cases	577				

Tabela G.5: Povezanost med neznanimi virtualnimi prijatelji in spolom - Cramer

		Value	Approx. Sig.
Nominal by Nominal	Phi	,092	,027
	Cramer's V	,092	,027
N of Valid Cases		577	

Tabela G.6: Povezanost med spoznavanjem virtualnih prijateljev v živo in spolom

		Si kdaj "virtualnega" prijatelja spoznal/a v živo?		Total
		Da	Ne	
Označi svoj spol:	Moški	123	131	254
	Ženski	143	179	322
Total		266	310	576

Tabela G.7: Povezanost med spoznavanjem virtualnih prijateljev in spolom – hi-kvadrat

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	,921 ^a	1	,337	,355	,191
Continuity Correction ^b	,767	1	,381		
Likelihood Ratio	,921	1	,337		
Fisher's Exact Test					
Linear-by-Linear Association	,919	1	,338		
N of Valid Cases	576				

a. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 117,30.

b. Computed only for a 2x2 table

Tabela G.8: Povezanost med spletnim nadlegovajem in spolom

		Te je kdaj kdo nadlegoval, ustrahoval ali izsiljeval preko spleta?		Total
		Da	Ne	
Označi svoj spol:	Moški	33	221	254
	Ženski	67	253	320
Total		100	474	574

Tabela G.9: Povezanost med spletnim nadlegovajem in spolom - hi-kvadrat

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2- sided)	Exact Sig. (1-sided)
Pearson Chi-Square	6,214 ^a	1	,013	,015	,008
Continuity Correction ^b	5,674	1	,017		
Likelihood Ratio	6,350	1	,012		
Fisher's Exact Test					
Linear-by-Linear Association	6,203	1	,013		
N of Valid Cases	574				

Tabela G.10: Povezanost med spletnim nadlegovajem in spolom - Cramer

		Value	Approx. Sig.
Nominal by	Phi	-,104	,013
Nominal	Cramer's V	,104	,013
N of Valid Cases		574	

Priloga H: Tabela korelacij med spremenljivkami pri anketi za mlade

Tabela H.1: Tabela korelacij med spremenljivkami pri anketi za mlade

		Sum of Squares	df	Mean Square	F	Sig.
V kakšni meri se strinjaš z : Na spletu lažje komuniciram kot v pogovoru v živo.	Between Groups	,009	1	,009	,007	,935
	Within Groups	810,694	575	1,410		
	Total	810,704	576			
V kakšni meri se strinjaš z : Na spletu lažje govorim o osebnih zadevah.	Between Groups	,282	1	,282	,195	,659
	Within Groups	831,273	574	1,448		
	Total	831,556	575			
V kakšni meri se strinjaš z : Na spletu se lažje zaupam neki osebi kot v pogovoru.	Between Groups	4,852	1	4,852	4,077	,044
	Within Groups	679,654	571	1,190		
	Total	684,506	572			
V kakšni meri se strinjaš z : Svoj prosti čas preživljam na internetu ali v družbi mobilne naprave.	Between Groups	,003	1	,003	,002	,961
	Within Groups	623,100	572	1,089		
	Total	623,103	573			
V kakšni meri se strinjaš z : Na internetu ostajam dlje, kot je bilo načrtovano.	Between Groups	9,639	1	9,639	7,421	,007
	Within Groups	742,976	572	1,299		
	Total	752,615	573			