Revija za kriminalistiko in kriminologijo / Ljubljana 63 / 2012 / 4, s. 263-280

Spletno in mobilno nadlegovanje v Sloveniji

Aleš Završnik[*], **Anja Sedej**[**]

Kibernetsko nadlegovanje se običajno nanaša na nadlegovanje in ustrahovanje drugih oseb z uporabo novih elektronskih tehnologij, predvsem mobilnih telefonov in interneta. V prispevku so predstavljeni rezultati internetne ankete o kibernetski kriminaliteti in viktimizacijah, izvedene predvsem med študenti na več fakultetah v Sloveniji. 441 odraslih, od tega 246 starih manj kot 24 let, 135 starih od 24 do 35 let in 60 starih več kot 35 let, pri čemer gre za 304 ženske in 137 moških, je bilo anketiranih zaradi proučevanja narave in razsežnosti kibernetskega nadlegovanja v Sloveniji. Tri glavne kategorije nadlegovanja (preko elektronske pošte, spletnih socialnih omrežij in mobilnih telefonov) in sedem podkategorij (ustrahovanje preko SMS-sporočil, e-pošte, spletnih socialnih omrežij od neznanih uporabnikov, preko spletnih socialnih omrežij od anonimnih uporabnikov, objava fotografij na spletnih socialnih omrežjih brez soglasja, označevanje (*tagganje*) obrazov na spletnih socialnih omrežjih, objavljanje spremenjenih fotografij brez soglasja) je bilo proučenih glede na starost in spol, dojet vpliv, samopreventivne ukrepe in iskanje pomoči pri drugih. Ugotovljena je bila velika pojavnost kibernetskega nadlegovanja preko elektronske pošte (65 %), manj preko mobilnih telefonov (44 %) in spletnih socialnih omrežij (22 %). Razlike med spoloma so bile majhne, starostne razlike pa so bile statistično pomembne (71 % anketirancev starih od 24 do 35 let je bilo žrtev nasilja večkrat). Vpliv kibernetskega nadlegovanja je dojet kot zelo negativen za objavo osebnih podatkov in fotografij na internetu brez soglasja. Pogoste žrtve kibernetskega nadlegovanja se obrnejo na policijo redkeje kot uporabniki, ki še niso bili žrtev kibernetskega nadlegovanja.

Ključne besede: kibernetska kriminaliteta, spletno nadlegovanje, mobilni telefoni, internet, zlorabe, preprečevanje kriminalitete, analize, Slovenija

UDK: 004:343.3/.7(497.4)

1 Uvod[1]

1.1 Opredelitev kibernetskega nadlegovanja

Kibernetsko nadlegovanje (angl. *cyberbullying*)[2] obsega ustrahovanje, trpinčenje, tiraniziranje ali šikaniranje po internetu, razumljenem v širšem smislu, na primer po e-pošti, spletnih straneh, blogih, klepetalnicah, forumih, spletnih socialnih omrežjih (na primer Facebook, Tweeter, Google+), straneh za izmenjavo multimedijskih vsebin (na primer Picasa, Youtube). Obsega pa tudi nasilje, ki ni povezano z internetom, temveč s storitvami mobilne telefonije (na primer preko kratkih SMS-sporočil, multimedijskih sporočil MMS, s prekomernimi klici). Temeljni elementi te oblike nasilnosti po uveljavljeni definiciji uporabljeni v medvladnem programu COST (*European Cooperation in Science and Technology*) Akcije IS0801 »*Cyberbullying: coping with negative and enhancing positive uses of new technologies, in relationships in educational settings*«, so naslednji: (1) nadlegovanje drugih z novimi elektronskimi tehnologijami, primarno z mobilnimi telefoni in internetom, (2) agresivno in namerno dejanje, (3) ki ga izvršuje skupina ali posameznik, (4) s pomočjo elektronskih oblik komuniciranja, (5) dalj časa trajajoče ali ponavljajoče, (6) zoper žrtev, ki se ne more zlahka braniti.

Dosedanje raziskave kibernetsko nadlegovanje razvrščajo v več oblik. Prve so ga kategorizirale kot spletno in mobilno. V raziskavi, ki so jo opravili Smith *et al.* (2006), so razlikovali med sedmimi oblikami kibernetskega (vrstniškega) nasilja: (1) nasilje s pošiljanjem kratkih sporočil po mobilnih telefonih (SMS); (2) nasilje s pošiljanjem slik in videov preko mobilnih telefonov (multimedijska sporočila MMS); (3) nasilje s klicanjem preko mobilnih telefonov; (4) nasilje preko e-pošte; (5) nasilje v klepetalnicah; (6) nasilje preko sistemov takojšnjega sporočanja (*Instant Messaging*, kot so *Windows Messenger*, *Yahoo! Messenger*); (7) nasilje preko spletnih strani. A v kasnejši raziskavi Slonje in Smith (2008) ugotavljata, da so bile frekvence za nekatere pojavne oblike tako redke, da bi jih ne bilo več smiselno ponavljati, zato predlagata štiri

[*] Doc. dr. Aleš Završnik, raziskovalec na Inštitutu za kriminologijo pri Pravni fakulteti v Ljubljani.

[**] Anja Sedej, univ. dipl. prav., sodniška pripravnica na Višjem sodišču v Ljubljani.

[1] Za pomoč pri statistični obdelavi podatkov se posebej zahvaljujeva Bogomilu Brvarju.

[2] Pojem je skoval kanadski aktivistični pedagog Bill Belsey, ustanovitelj mreže www.cyberbullying.ca.

kategorije: (1) nasilje s pošiljanjem kratkih sporočil po mobilnih telefonih; (2) nasilje preko e-pošte; (3) nasilje s klicanjem preko mobilnih telefonov; (4) razpečevanje slik in videoposnetkov.

V obsežni evropski raziskavi *EU Kids Online* (Livingstone *et al.*, 2001) so med šestimi tveganji, s katerimi se otroci soočajo na internetu, merili »žaljivo in neprijetno obnašanje na internetu« (poimenovano tudi kot ustrahovanje), v okviru katerega so ločili aktivnosti preko mobilnega telefona ter posebej tveganje v obliki »pošiljanja in prejemanja sporočil s spolno vsebino« (*sexting*).

V raziskavi, katere izsledke predstavljamo v nadaljevanju, smo razlikovali tri temeljne oblike in sedem podoblik kibernetskega nadlegovanja: (1) nadlegovanje po internetu, (2) nadlegovanje po spletnem socialnem omrežju in (3) nadlegovanje po mobilnem telefonu. Tripartitna členitev ima svoje prednosti in pomanjkljivosti. Pojem nadlegovanje je bolj določen kot pojem nasilje, a njegova slabost je, da ne obsega vseh oblik, ki sodijo v *cyberbullying* (na primer relacijskega nasilja v obliki širjenja govoric anketirani zelo verjetno niso uvrstili med »nadlegovanje«). Zato smo poleg teh treh glavnih oblik ločili še bolj specifične oblike: (a) prekomerno pošiljanje SMS/MMS-sporočil; (b) prekomerno pošiljanje e-pošte; (c) vzpostavljanje stikov v spletnih socialnih omrežjih (Facebook, Netlog ipd.) s strani neznancev; (č) vzpostavljanje stikov v spletnih socialnih omrežjih s strani neznancev, ki ne uporabljajo svojega pravega imena; (d) objavljanje fotografij, na katerih je anketirani brez svoje vednosti ali privolitve v spletnem socialnem omrežju; (e) označevanje obraza z imenom na fotografijah drugih uporabnikov spletnega socialnega omrežja; (f) objavljanje spremenjenih/predelanih fotografij posameznika brez njegovega dovoljenja.

1.2 Dosedanje raziskave o kibernetskem nadlegovanju v Sloveniji

Raziskava, osredotočena zgolj na kibernetsko (spletno in mobilno) vrstniško ali siceršnje nadlegovanje v Sloveniji, nam ni znana. Posredno in v drugačnih kontekstih pa so nekatere raziskave obravnavale tudi posamične vidike kibernetskega nadlegovanja pri nas.

V panevropski raziskavi *EU Kids Online* o tveganjih in nevarnostih otrok, starih od 9 do 16 let, na internetu (Livingstone *et al.*, 2001) so ugotovili, da je bil že vsak peti otrok v EU (19 %) v zadnjem letu ustrahovan (skupaj *online* in *offline*). Ustrahovanje s pomočjo IKT je pogostejše v državah, kjer je ustrahovanje nasploh pogostejše; praviloma ni odvisno od penetracije interneta v državi. Za Slovenijo so ugotovili, da je ustrahovanje v živo še vedno trikrat pogostejše kot preko spleta (15 % proti 4 %), delež ustrahovanja preko mobilnega telefona pa je še manjši in znaša 3 %. Delež spletnega ustrahovanja je v primerjavi z evropskim povprečjem v Sloveniji malo nižji (4 % proti 6 %). Vpliv starosti na ustrahovanje ni bil statistično pomemben. Glede *sextinga* so ugotavljali, koliko nasploh si otroci med sabo pošiljajo sporočila s spolno vsebino, kar ni del nadlegovanja.

V raziskavi *Mladi na netu* (Lobe in Muha, 2011), katere namen je bil prav tako ugotoviti spletne navade mladih, starih od 8 do 19 let, so merili tudi tveganja, kot so (1) nezaželeni spolni komentarji, (2) neprijetni in boleči komentarji, (3) sovražno nastrojene in strašljive strani ter (4) pošiljanje in prejemanje golih fotografij; prvi dve tveganji sta lahko razumljeni kot obliki nadlegovanja, tretja ne, ker ni nesorazmerja moči med napadalcem in žrtvijo, četrta pa je lahko tudi povsem konsenzualna in pozitivna izkušnja. Rezultati so pokazali, da polovica (51 %) otrok in mladih, starih od 11 do 19 let, še ni prejela *nezaželenih spolnih komentarjev*. Deklice so nezaželene spolne komentarje prek spletnih socialnih omrežji dobile v večji meri (12 %) kot dečki (6 %). Izkazalo se je, da je tudi skoraj polovica (53 %) otrok in mladih prejela *neprijetne in boleče komentarje*. Bistvenih razlik v spolu niso ugotovili, najbolj pa je takšnemu nadlegovanju izpostavljena starejša skupina.

V raziskavo o poznavanju, razumevanju in dojemanju kibernetskih groženj ter strahu pred kibernetsko kriminaliteto v Sloveniji sta Bernik in Meško (2011) vključila tudi nadlegovanje. Ugotovila sta, da se uporabniki bojijo nadlegovanja pri uporabi kibernetskega prostora (Bernik in Meško, 2011: 248), in zaključila, da je »[o]čitno premoženjska ogroženost še vedno tista, ki posameznike najbolj skrbi oziroma najbolj prizadene, manj pa neprimerno obnašanje in nadlegovanje« (*ibid.*: 249). Z vidika škodljivosti te oblike vrstniškega nadlegovanja pa je bilo sicer na nereprezentativnem vzorcu ugotovljeno (Muršič in Brvar, 2010: 23), da največ neprijetnih čustev v šoli doživljajo učenci, ki trdijo, da so doživeli nadlegovanje po telefonu (38 učencev oziroma skoraj vsak dvanajsti) ali internetu (17 učencev), zatem šele sledi na primer spolno nadlegovanje ali snemanje nasilja s telefonom.

V nadaljevanju prispevek obravnava kibernetsko (spletno in mobilno) nadlegovanje (angl. *cyberbullying*) v Sloveniji in prikaže rezultate empirične študije, ki odgovarja na naslednja vprašanja: ali so bili anketiranci že žrtve kibernetskega nadlegovanja; kakšne so demografske značilnosti žrtev; kakšni uporabniki informacijske tehnologije so žrtve nadlegovanja; kako bi se nanj odzvali ali in kje bi iskali pomoč; kako, če sploh, bi kaznovali storilce kibernetskega nadlegovanja in kakšno je splošno zavedanje ter percepcija te oblike nasilnosti pri nas.

2 Metoda

V letu 2010 smo izvedli spletno anketo o uporabi informacijske tehnologije, kibernetski kriminaliteti in viktimizacijah s pomočjo *online* sistema Google docs. Vsebovala je 38 zaprtih vprašanj (intervalnih vprašanj, vprašanj z eno možno izbiro, tabelaričnih vprašanj z več možnimi odgovori, ocenjevalne tabele). V analizo so vključeni odgovori, prejeti med 1. majem 2010 in 12. avgustom 2010. Anketa je poleg splošnih demografskih podatkov o izpraševancih (n = 441) obsegala tri sklope: prvi se je nanašal na uporabo informacijske tehnologije (na primer kaj, kdaj, koliko, za katere namene, kje anketirani uporabljajo IT-naprave), drugi na kibernetsko kriminaliteto (na primer, ali anketirani uporabljajo P2P, hackajo, pošiljajo neželeno pošto) in tretji na žrtve tovrstnih dejanj (zanimalo nas je, na primer, ali so bili anketirani žrtve kibernetskega kaznivega dejanja, kakšno je njihovo samozaščitno vedenje, na koga bi se obrnili v primeru kibernetskega incidenta, ali poznajo sisteme za zaščito podatkov). V nadaljevanju predstavljamo izsledke analize, ki se nanašajo le na kibernetsko (spletno in mobilno) nadlegovanje.

Udeležence smo k sodelovanju povabili z objavo obvestil na internetu, po fakultetah in preko elektronske pošte. Ciljna populacija so bili študentje (sodelovali so pretežno študentje Pravne fakultete in Fakultete za družbene vede Univerze v Ljubljani ter Fakultete za varnostne vede Univerze v Mariboru), povabilu k izpolnjevanju pa se je odzvalo tudi dovolj starejših posameznikov (neštudentov), da smo opravili še primerjavo med različnimi starostnimi skupinami.

Analiza podatkov je bila opravljena s pomočjo programa SPSS 15. Izdelane so bile dvorazsežne frekvenčne (kontingenčne) tabele, za izračune povezav med spremenljivkami uporabljen Pearsonov test hi-kvadrat (χ^2) in Razmerje verjetij (*Likelihood ratio*). Test χ^2 smo izvajali s stopnjo značilnosti $\alpha = 0{,}05$ (mejno vrednost verjetnosti, pod katero zavrnemo ničelno hipotezo). Ne glede na to, da je pri testiranju neodvisnosti spremenljivk na majhnih vzorcih natančnejši test Razmerje verjetij, pri velikih vzorcih, kot je bil naš, pa Pearsonov χ^2 (Brvar, 2007), sta bila vedno preverjena oba. Če je bil α za Pearsona manjši od 0,05, za test Razmerje verjetij pa večji, smo sprejeli sklep, da spremenljivki nista povezani. Za ugotavljanje srednjih vrednosti so bile izdelane tabele srednje vrednosti in 95 % interval zaupanja. Za ugotavljanje razlik med spoloma in med starostnimi skupinami smo uporabili test Brown-Forsythe.

Tabela 1: Značilnosti zajetega vzorca

Demografske Značilnosti	Σ N = 441	N	%
Spol	moški	137	31,1
	ženski	304	68,9
Starost	manj kot 24 let	246	55,8
	24–35 let	135	30,6
	več kot 35 let	60	13,6
Izobrazba	osnovnošolska/poklicna/dijak	7	1,6
	srednješolska	21	4,8
	študent	297	67,3
	višja/visoka strokovna	24	5,4
	univerzitetna	79	18,0
	podiplomska	13	2,9

3 Rezultati

3.1 Pojavnost in značilnosti žrtev kibernetskega nadlegovanja

Anketirani so odgovarjali na vprašanje, ali so že bili žrtev ene izmed treh oblik kibernetskega nadlegovanja: nadlegovanja po internetu, v spletnem socialnem omrežju in po mobilnem telefonu (tabela 2).

Tabela 2: Število žrtev kibernetskega nadlegovanja

Ali ste že bili žrtev:		Število	%
1. nadlegovanja po internetu (e-pošta, spam)	da, enkrat	26	5,9 %
	da, večkrat	260	59,0 %
	ne	148	33,6 %
	ne vem	7	1,6 %
2. nadlegovanja v spletnem socialnem omrežju (Facebook, Myspace, Netlog ipd.)	da, enkrat	37	8,4 %
	da, večkrat	59	13,4 %
	ne	337	76,4 %
	ne vem	8	1,8 %
3. nadlegovanja po mobilnem telefonu (klici, SMS-i)	da, enkrat	80	18,1 %
	da, večkrat	114	25,9 %
	ne	245	55,6 %
	ne vem	2	0,5 %

Največ izpraševancev je bilo žrtev internetnega nadlegovanja (64,9 %), nato nadlegovanja po mobilnem telefonu (44 %) in najmanj nadlegovanja v spletnem socialnem omrežju (21,8 %).

Demografske značilnosti žrtev treh oblik nadlegovanja so bile preverjene glede na spol (ni statistično pomembnejših razlik, tabela 3), izobrazbo (ni statistično pomembnejših razlik) in starost (obstajajo statistično pomembne razlike, graf 1).

Tabela 3: Kibernetsko nadlegovanje glede na spol

Ali ste že bili žrtev: (vpr. 14)		Spol					
		Moški		Ženski		Skupaj	
		Število	%	Število	%	Število	%
1. nadlegovanja po internetu (e-pošta, spam)	da, enkrat	6	4,4 %	20	6,6 %	26	5,9 %
	da, večkrat	87	63,5 %	173	56,9 %	260	59,0 %
	ne	42	30,7 %	106	34,9 %	148	33,6 %
	ne vem	2	1,5 %	5	1,6 %	7	1,6 %
	skupaj	137	100,0 %	304	100,0 %	441	100,0 %
2. nadlegovanja v spletnem socialnem omrežju (Facebook, Myspace, Netlog ipd.)	da, enkrat	9	6,6 %	28	9,2 %	37	8,4 %
	da, večkrat	14	10,2 %	45	14,8 %	59	13,4 %
	ne	112	81,8 %	225	74,0 %	337	76,4 %
	ne vem	2	1,5 %	6	2,0 %	8	1,8 %
	skupaj	137	100,0 %	304	100,0 %	441	100,0 %
3. nadlegovanja po mobilnem telefonu (klici, SMS-i)	da, enkrat	27	19,7 %	53	17,4 %	80	18,1 %
	da, večkrat	25	18,2 %	89	29,3 %	114	25,9 %
	ne	84	61,3 %	161	53,0 %	245	55,6 %
	ne vem	1	0,7 %	1	0,3 %	2	0,5 %
	skupaj	137	100,0 %	304	100,0 %	441	100,0 %

Iz tabele 3 je razvidno, da je delež moških, ki so bili večkrat nadlegovani po internetu, večji od deleža žensk (M: 63,6 %, Ž: 56,9 %). Rezultat nadlegovanja po spletnem socialnem omrežju in mobitelu pa je obraten. Ne glede na te ugotovitve, razlike med odstotki niso velike, test χ^2 kaže, da med spremenljivkama ni statistično pomembne povezanosti in je nadlegovanje približno enako razporejeno na moške in ženske: nadlegovanje po internetu (χ^2 = 1,991, p = 0,574), nadlegovanje v spletnem socialnem omrežju (χ^2 = 3,146, p = 0,370) in nadlegovanje po mobilnem telefonu (χ^2 = 6,233, p = 0,101) (glej še zbirno tabelo 4).

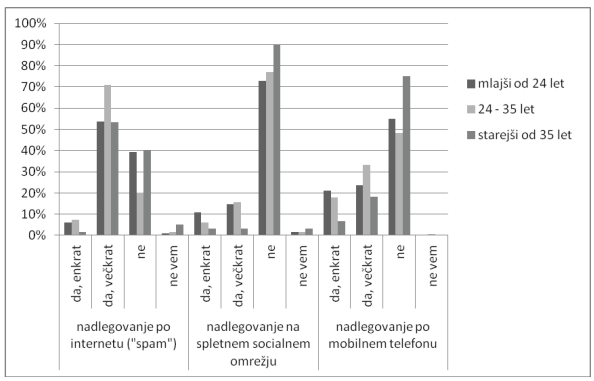
Enako kot za razlike med spolom žrtev velja tudi za razlike med različno izobraženimi,[3] statistično pomembne povezanosti ni: nadlegovanje po internetu (χ^2 = 30,294, p = 0,035, kar sicer kaže na statistično pomembno povezanost, a je premalo podatkov za zanesljivost), nadlegovanje v spletnem socialnem omrežju (χ^2 = 20,403, p = 0,311), nadlegovanje po mobilnem telefonu (χ^2 = 19,060, p = 0,388). Razmerje verjetij za združene vse tri oblike nadlegovanj pri izobrazbi znaša 0,105. Statistično pomembnih razlik tudi ni med različnimi poklicnimi skupinami[4] (nadlegovanje po internetu: χ^2 = 20,763, p = 0,054; nadlegovanje po spletnem socialnem omrežju: χ^2 = 17,383, p = 0,136; nadlegovanje po mobilnem telefonu: χ^2 = 20,927, p = 0,051; razmerje verjetij je za vse tri oblike nadlegovanja 0,024).

Statistično pomembna povezanost pa je med nadlegovanjem in starostjo izpraševancev (graf 1). Po internetu so najbolj nadlegovani stari med 24 in 35 let. Kar 71 % vseh vprašanih te starosti je odgovorilo, da so bili nadlegovani večkrat. Tudi po mobilnem telefonu je v največjem deležu nadlegovana ta starostna skupina (33,3 % jih je bilo nadlego-

[3] Izobrazba: dokončana osnovna, poklicna šola, dijak; dokončana srednja šola; dokončana višja ali visoka strokovna šola; dokončana univerzitetna izobrazba; dokončan magisterij ali doktorat; sem študent.

[4] Poklic ali študij: Pravna fakulteta; Fakulteta za družbene vede; Fakulteta za varnostne vede; učitelj ali profesor; strojni tehnik ali poslovni sekretar; druga fakulteta.

vanih večkrat), medtem ko nadlegovanja po spletnem socialnem omrežju ni izpostavila nobena skupina, očitno pa so tarča tega nadlegovanja v najmanjši meri starejši od 35 let (90 % izpraševancev te starosti ni bilo nadlegovanih). Pearsonov test χ^2 (tabela 4): za nadlegovanje po internetu $\chi^2 = 23{,}242$, $p = 0{,}001$, za nadlegovanje v spletnem socialnem omrežju $\chi^2 = 12{,}838$, $p = 0{,}046$, za nadlegovanjem po mobilnem telefonu $\chi^2 = 16{,}277$, $p = 0{,}012$; razmerje verjetij za združene vse tri oblike nadlegovanj znaša 0,001.



Graf 1: Kibernetsko nadlegovanje glede na starost

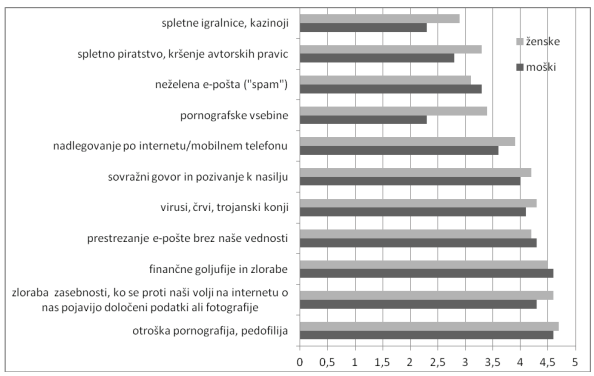
Tabela 4: Pearsonovi testi hi-kvadrat, povezave med žrtvami kibernetskega nadlegovanja in demografskimi značilnostmi anketirancev

Ali ste že bili žrtev: (vpr. 14)		Starost	Izobrazba	Poklic, študij, letnik	Spol
1. nadlegovanja po internetu (e-pošta, spam)	hi-kvadrat	23,242	30,294	20,763	1,991
	s.p.	6	18	12	3
	Sig.	0,001	0,035	0,054	0,574
2. nadlegovanja v spletnem socialnem omrežju (Facebook, Mysapce, Netlog ipd.)	hi-kvadrat	12,838	20,403	17,383	3,146
	s.p.	6	18	12	3
	Sig.	0,046	0,311	0,136	0,370
3. nadlegovanja po mobilnem telefonu (klici, SMS-i)	hi-kvadrat	16,277	19,060	20,927	6,233
	s.p.	6	18	12	3
	Sig.	0,012	0,388	0,051	0,101

3.2 Zaznavanje resnosti kibernetskega nadlegovanja

Zanimalo nas je, kako to novo obliko nadlegovanja anketirani ocenjujejo v primerjavi z drugimi kibernetskimi tveganji in nevarnostmi. Izbrali smo 11 najpogostejših kibernetskih tveganj in nevarnosti ter analizirali statistično pomembne razlike med demografskimi skupinami. Izdelane so bile tabele srednje vrednosti in 95 % interval zaupanja. Za ugotavljanje razlik med spoloma in starostnimi skupinami (mlajši od 24 let, 24–35 let in starejši od 35 let) smo uporabili test Brown-Forsythe. Podoben je F-testu v analizi variance, vendar ne zahteva, da je izpolnjen pogoj enakosti varianc, dopušča pa tudi različne velikosti skupin, v našem primeru 137 moških in 404 žensk. Grafa 2 in 3 prikazujeta razlike v zaznavanju resnosti kibernetskih nevarnosti in tveganj glede na spol in starost (anketno vprašanje 22).

Iz grafa 2 je razvidno, da moški in ženske najbolj različno ocenjujejo pornografske vsebine na internetu ter spletne igralnice in kazinoje. Pornografske vsebine na internetu je kar 37,2 % moških ocenilo kot povsem neproblematične, takšnega mnenja pa je bilo samo 11,5 % žensk. Spletne igralnice in kazinoje je kot povsem neproblematične ocenilo 34,3 % moških in samo 14,8 % žensk. Temu primerne so tudi razlike v grafu prikazanih srednjih vrednosti. Z uporabo testa Brown-Forsythe smo ugotovili statistično značilno razliko tudi med spolom in nadlegovanjem po internetu/mobilnem telefonu, zlorabo zasebnosti, ko se proti naši volji na internetu o nas pojavijo določeni podatki ali fotografije, ter spletnim piratstvom in kršenjem avtorskih pravic; vse naštete nevarnosti se moškim zdijo manj problematične kot ženskam. Statistično značilna razlika med moškimi in ženskami je tudi pri neželeni e-pošti, ki se za razliko od prejšnjih nevarnosti zdi bolj problematična moškim.



Graf 2: Razlike v zaznavanju resnosti kibernetskih nevarnosti *glede na spol*
(1 – sploh ni problematično, 5 – zelo problematično)

Podrobnejša analiza treh izbranih kibernetskih nevarnosti in tveganj kaže naslednje razlike med spoloma (tabela 5 in 6):

Nadlegovanje po internetu/mobilnem telefonu: moškim se zdi ta nevarnost manj problematična kot ženskam. Kot zelo problematično jo je ocenilo 21,2 % moških in 31,3 % žensk. Povprečni oceni se razlikujeta za približno 0,5, pri čemer so ocene moških bolj razpršene kot ocene žensk. Test Brown-Forsythe kaže statistično značilno razliko med moškimi in ženskami. Verjetnost ničelne hipoteze je skoraj 0, da pa razlike niso tako velike kot pri ocenjevanju nevarnosti pornografije, kaže vrednost Brown-Forsythe, ki je nekajkrat manjša.

Zloraba zasebnosti, ko se proti naši volji na internetu o nas pojavijo določeni podatki ali fotografije: moškim se zdi ta nevarnost manj problematična kot ženskam. Kot zelo problematično jo je ocenilo 46,0 % moških in 68,4 % žensk. Povprečni oceni sta pri obeh skupinah nad 4, razliki pa majhni. Test Brown-Forsythe kaže statistično značilno razliko med moškimi in ženskami. Verjetnost ničelne hipoteze je skoraj 0.

Tabela 5: Analiza zaznavanja nevarnosti po spolu: Srednje vrednosti in 95 % interval zaupanja

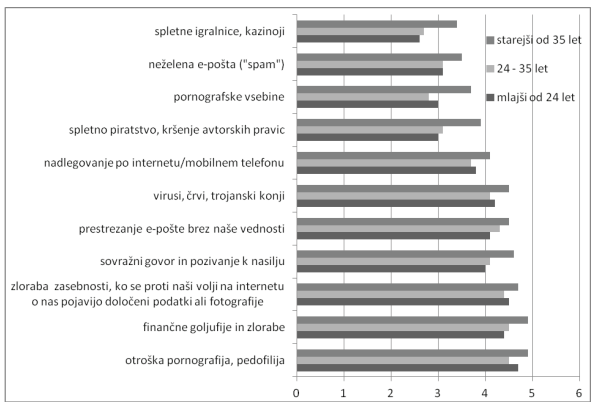
Kako velik problem se vam zdijo naštete nevarnosti, na katere lahko naletimo pri uporabi interneta? (vpr. 22)		N	Sred. vred.	Stand. odklon	95 % interval zaupanja	
					Spod. meja	Zgor. meja
1. nadlegovanje po internetu/mobilnem telefonu	moški	137	3,59	1,019	3,42	3,76
	ženski	304	3,91	0,937	3,81	4,02
	skupaj	441	3,81	0,973	3,72	3,91
2. zloraba zasebnosti, ko se proti naši volji na internetu o nas pojavijo določeni podatki ali fotografije	moški	137	4,27	0,827	4,13	4,41
	ženski	304	4,55	0,761	4,46	4,63
	skupaj	441	4,46	0,791	4,39	4,53
3. neželena e-pošta (spam)	moški	137	3,30	1,080	3,12	3,48
	ženski	304	3,05	1,092	2,92	3,17
	skupaj	441	3,12	1,094	3,02	3,23

Tabela 6: Analiza zaznavanja nevarnosti po spolu: test Brown-Forsythe

Kako velik problem se vam zdijo naštete nevarnosti, na katere lahko naletimo pri uporabi interneta? (vpr. 22)		Statistika	s.p.1	s.p.2	Sig.
1. nadlegovanje po internetu/mobilnem telefonu	Brown-Forsythe	9,990	1	243,503	0,002
2. zloraba zasebnosti, ko se proti naši volji na internetu o nas pojavijo določeni podatki ali fotografije	Brown-Forsythe	11,046	1	243,609	0,001
3. neželena e-pošta (spam)	Brown-Forsythe	5,153	1	264,881	0,024

Neželena e-pošta (spam): ta se zdi nevarnejša moškim. Sicer razlike niso velike: 16,8 % moških je nevarnost ocenilo kot zelo problematično in 13,2 % žensk. Povprečni oceni sta večji od 3 in manjši od 4. Test Brown-Forsythe kaže statistično značilno razliko med moškimi in ženskami. Verjetnost ničelne hipoteze je skoraj 0,02.

Zaznavanje resnosti kibernetskih nevarnosti in tveganj glede na starost za izbrane tri kibernetske nevarnosti in tveganja kaže graf 3.



Graf 3: Razlike v zaznavanju resnosti kibernetskih nevarnosti *glede na starost*
(1 – sploh ni problematično, 5 – zelo problematično)

Med starostnimi skupinami in zaznavanjem resnosti vseh naštetih nevarnosti, razen zlorabe zasebnosti, so statistično pomembne razlike. Iz grafa 3 je razvidno, da se vse nevarnosti zdijo najbolj problematične najstarejši skupini. Največja razlika med starejšimi in drugima dvema starostnima skupinama je pri pornografskih vsebinah (odstotek starejših, ki so jih ocenili kot zelo problematične, je dvakrat večji od odstotkov mlajših skupin) in spletnih igralnicah ter kazinojih, ki se sicer vsem starostnim skupinam zdijo najmanj problematični. Z relativno nizko povprečno oceno so skupine ocenile tudi neželeno e-pošto.

Podrobnejša analiza izbranih kibernetskih nevarnosti in tveganj pa kaže naslednje razlike v zaznavanju resnosti tveganj med starostnimi skupinami (tabela 7 in 8):

Tabela 7: Analiza zaznavanja nevarnosti po starostnih skupinah: Srednje vrednosti in 95 % interval zaupanja

Kako velik problem se vam zdijo naštete nevarnosti, na katere lahko naletimo pri uporabi interneta? (vpr. 22)		N	Sred. vred.	Stand. odklon	95 % interval zaupanja	
					Spod. meja	Zgor. meja
1. nadlegovanje po internetu/mobilnem telefonu	mlajši od 24 let	246	3,79	0,992	3,66	3,91
	24–35 let	135	3,72	0,975	3,55	3,88
	starejši od 35 let	60	4,13	0,833	3,92	4,35
	skupaj	441	3,81	0,973	3,72	3,91
2. zloraba zasebnosti, ko se proti naši volji na internetu o nas pojavijo določeni podatki ali fotografije	mlajši od 24 let	246	4,47	0,775	4,37	4,56
	24–35 let	135	4,36	0,878	4,21	4,51
	starejši od 35 let	60	4,65	0,606	4,49	4,81
	skupaj	441	4,46	0,791	4,39	4,53
3. neželena e-pošta (spam)	Mlajši od 24 let	246	3,05	1,107	2,91	3,19
	24–35 let	135	3,07	1,090	2,89	3,26
	Starejši od 35 let	60	3,53	0,965	3,28	3,78
	skupaj	441	3,12	1,094	3,02	3,23

Tabela 8: Analiza zaznavanja nevarnosti po starostnih skupinah: test Brown-Forsythe

Kako velik problem se vam zdijo naštete nevarnosti, na katere lahko naletimo pri uporabi interneta? (vpr. 22)		Statistika	s.p.1	s.p.2	Sig.
1. nadlegovanje po internetu/mobilnem telefonu	Brown-Forsythe	4,433	2	283,851	0,013
2. zloraba zasebnosti, ko se proti naši volji na internetu o nas pojavijo določeni podatki ali fotografije	Brown-Forsythe	3,089	2	302,709	0,047
3. neželena e-pošta (spam)	Brown-Forsythe	5,359	2	273,388	0,005

Nadlegovanje po internetu/mobilnem telefonu: to nevarnost ocenjuje starejša skupina kot zelo problematično z 38,3 % oziroma z oceno 4 kar 40 %. Edino ta skupina je ocenila nevarnost s povprečno oceno nad 4. Majhni standardni odkloni pa kažejo enako mnenje znotraj skupin. Brown-Forsythova statistika je majhna, znaša 4,433, verjetnost ničelne hipoteze pa je enaka 0,013. Razlike med ocenami nevarnosti nadlegovanja po internetu/mobilnem telefonu so med starostnimi skupinami statistično značilne.

Zloraba zasebnosti, ko se proti naši volji na internetu o nas pojavijo določeni podatki ali fotografije: vse starostne skupine so tovrstno nevarnost ocenile kot problematično. Povprečne ocene nevarnosti 4,36–4,65. Razlike so majhne. To je tudi edino podvprašanje vprašanja 22, pri katerih je verjetnost ničelne domneve 0,047, torej na meji sprejema oziroma zavrnitve. Statistika Brown-Forsythe je majhna – 3,09, zato sklepamo, da med starostnimi skupinami ni statistično pomembne razlike pri oceni nevarnosti zlorabe zasebnosti.

3.3 Stališča do kazenskopravnega sankcioniranja kibernetskega nadlegovanja

V strokovni javnosti[5] se kot eno temeljnih vprašanj pojavlja, ali je treba na kibernetsko nadlegovanje reagirati tudi s kazenskim pravom. Pregledali smo razlike glede na starost, spol, izobrazbo in poklic (tabela 9). Izpraševancem (ženskam sicer bolj kot moškim) velik problem predstavljata dve obliki nadlegovanja: objavljanje fotografij brez posameznikove vednosti ali privolitve v spletnem socialnem omrežju in objavljanje spremenjenih ali predelanih fotografij posameznika. Skoraj ¾ jih meni, da je to nadlegovanje, ki si zasluži inkriminacijo. Nadalje je razvidno, da med tema dvema oblikama nadlegovanja (skupaj z obliko – vzpostavljanje stikov v spletnih socialnih omrežjih s strani neznancev, ki ne uporabljajo svojega pravega imena) in spolom obstajajo statistično značilne razlike (glej tabelo 9).

Tabela 9: Pearsonovi hi-kvadrat testi ocenjevanja nadlegovanja kot vrednega kazenskopravnega reagiranja

Ali menite, da gre v naslednjih primerih za nadlegovanje, vredno kazenskopravnega reagiranja? (vpr. 34)		Starost	Izobrazba	Poklic	Spol
1. Objavljanje vaših fotografij (fotografij, na katerih ste vi) brez vaše vednosti ali privolitve v spletnem socialnem omrežju	Hi-kvadrat	13,449	3,128	6,254	10,524
	s.p.	4	4	4	2
	Sig.	0,009	0,537	0,181	0,005
2. Označevanje vašega obraza z vašim imenom na fotografijah drugih uporabnikov spletnega socialnega omrežja	Hi-kvadrat	57,811	24,576	33,930	5,296
	s.p.	4	4	4	2
	Sig.	0,000	0,000	0,000	0,071

Neželena e-pošta (spam): tudi ta nevarnost je ocenjena z relativno nizko povprečno oceno od 3,05 do 3,53. Statistika Brown-Forsythe je majhna – 5,36, verjetnost ničelne hipoteze pa je enaka 0,005. Razlike med ocenami nevarnosti nezaželene pošte so med starostnimi skupinami statistično značilne.

[5] Glej razprave 4. sestanka COST Akcije *Cyberbullying*, Antwerp, Belgija, 26.5.2010 (COST Action IS0801).

3. Objavljanje spremenjenih/predelanih fotografij, na katerih ste vi	Hi-kvadrat	8,885	1,507	5,738	18,689
	s.p.	4	4	4	2
	Sig.	0,064	0,825	0,220	0,000
4. Prekomerno pošiljanje SMS/MMS-sporočil	Hi-kvadrat	15,817	5,428	9,552	0,642
	s.p.	4	4	4	2
	Sig.	0,003	0,246	0,049	0,726
5. Prekomerno pošiljanje e-pošte	Hi-kvadrat	20,761	19,010	16,771	4,619
	s.p.	4	4	4	2
	Sig.	0,000	0,001	0,002	0,099
6. Vzpostavljanje stikov v spletnih socialnih omrežjih (Facebook, Netlog ipd.) s strani neznancev	Hi-kvadrat	29,967	7,612	27,604	3,795
	s.p.	4	4	4	2
	Sig.	0,000	0,107	0,000	0,150
7. Vzpostavljanje stikov v spletnih socialnih omrežjih (Facebook, Netlog ipd.) s strani neznancev, ki ne uporabljajo svojega pravega imena	Hi-kvadrat	9,800	4,278	13,083	13,830
	s.p.	4	4	4	2
	Sig.	0,044	0,370	0,011	0,001

Pri starostnih skupinah je drugače. Statistično značilne povezave obstajajo med starostjo in vsemi oblikami nadlegovanja (razen objavo spremenjenih/predelanih fotografij, χ^2= 8,885, p = 0,064). Pri vseh oblikah nadlegovanja (razen pri prekomernem pošiljanju SMS/MMS-sporočil) je daleč največ starejših od 35 let tistih, ki menijo, da bi bilo treba kazenskopravno reagirati. Starejši in tisti med 24–35 let se najbolj približajo ravno pri prekomernem pošiljanju SMS/MMS-sporočil in samo tu več mlajših (starih med 24–35 let) kot pa starejših meni, da bi bilo potrebno kazenskopravno reagiranje.

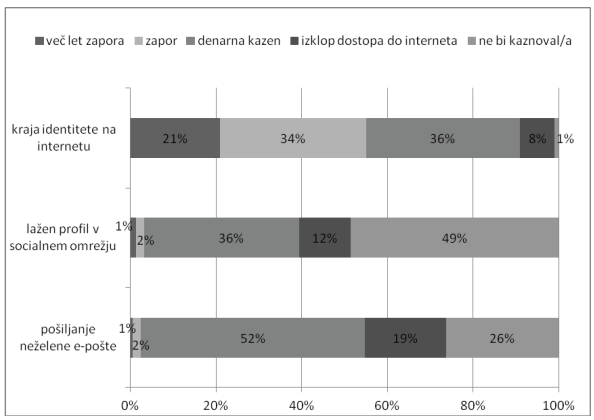
Statistično značilne razlike v mnenju glede potrebnosti kazenskopravnega reagiranja na določene oblike nadlegovanj obstajajo tudi med študenti pravne fakultete in študenti drugih fakultet. Te razlike je test Brown-Forsythe pokazal pri (1) označevanju obraza z imenom na fotografijah drugih uporabnikov spletnega socialnega omrežja, (2) prekomernem pošiljanju e-pošte, vzpostavljanju stikov v spletnih socialnih omrežjih s strani neznancev in (3) s strani neznancev, ki ne uporabljajo svojega pravega imena. Pri vseh oblikah nadlegovanja manj študentov pravne fakultete – glede na študente drugih fakultet – meni, da je potrebno kazenskopravno reagiranje (tabela 10). Očitno so študenti prava ponotranjili enega temeljnih načel kazenskega prava.

Tabela 10: Mnenje študentov o potrebnosti kazenskopravnega reagiranja na določene oblike nadlegovanja

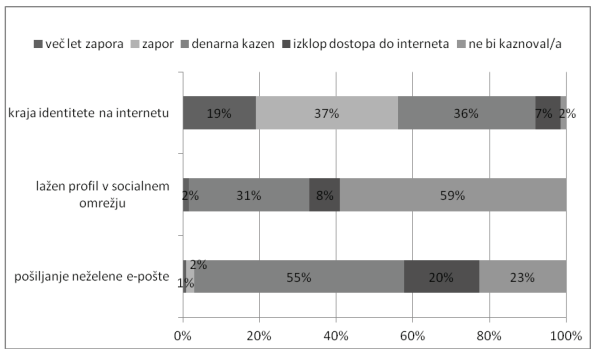
		Število Σ 229	PF UNI LJ	Število Σ 155	Druge fakultete
Označevanje vašega obraza z vašim imenom na fotografijah drugih uporabnikov spletnega socialnega omrežja	da ne ne vem	28 124 23	35,8 % 54,1 % 10 %	67 56 32	43,2 % 36,13 % 20,6 %
Prekomerno pošiljanje e-pošte	da ne ne vem	26 184 19	11,4 % 80,3 % 8,3 %	31 107 17	20 % 69 % 11 %
Vzpostavljanje stikov v spletnih socialnih omrežjih s strani neznancev	da ne ne vem	16 201 12	7 % 87,8 % 5,2 %	19 111 25	12,3 % 71,6 % 16,1 %
Vzpostavljanje stikov v spletnih socialnih omrežjih s strani neznancev, ki ne uporabljajo svojega pravega imena	da ne ne vem	79 129 21	34,5 % 56,3 % 9,2 %	60 64 31	38,7 % 41,3 % 20 %

3.4 Kaznovalna nastrojenost do kibernetskega nadlegovanja

Anketiranci so se na lestvici opredeljevali, kako bi kaznovali tri temeljne oblike kibernetskega nadlegovanja, z opredelitvijo (od najstrožje do ničte) za: več let zapora – zapor – denarno kazen – izklop dostopa do interneta – ne bi kaznoval. Rezultati so razvidni iz grafov od 4 do 6.

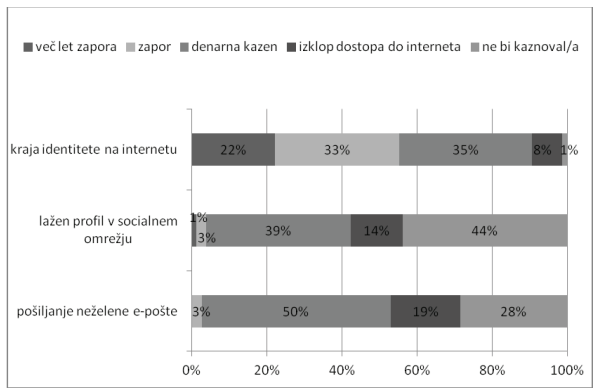


Graf 4: Kako bi kaznovali nadlegovanje?



Graf 5: Kako bi kaznovali nadlegovanje (moški, N = 137)?

Več kot polovica anketiranih bi z zaporno kaznijo kaznovala krajo identitete na internetu (presenetljivo, razlik med M in Ž ni), petina kar z zaporom več let. Strogost kaznovanja preseneča; najbrž so si anketirani predstavljali pod to nevarnostjo v prvi vrsti premoženjske modalitete. Lažen profil v spletnem socialnem omrežju je tudi po mnenju več kot tretjine anketiranih vreden kaznovanja: za to bi se odločilo več kot 30 % moških in več kot 40 % žensk. Natančnejša statistika razlik med spoloma ni bila opravljena, iz navedenega pa je razvidno, da bi moški strožje kaznovali pošiljanje neželene e-pošte in blažje lažen profil v spletnem socialnem omrežju. Nasploh



Graf 6: Kako bi kaznovali nadlegovanje (ženske, N = 304)?

preseneča kaznovalna naravnanost do kraje identitete (več kot 90 % anketiranih bi prisodilo kazenske sankcije) in pošiljanja neželene pošte (več kot 70 % bi jih prisodilo kazenske sankcije), ob majhnih odstotkih pogodbenega »kaznovanja« (izklop dostopa do interneta).

3.5 Preventivno samozaščitno ravnanje žrtev

Pri žrtvah nadlegovanja nas je zanimala korelacija s samozaščitnim vedenjem, na katerega bi lahko sklepali iz treh oblik njihovega vedenja in poznavanja računalniške programske zaščite, spletnih groženj in sistemov za zaščito podatkov.

a) Ali žrtve uporabljajo računalniško programsko zaščito?

Anketirance smo povprašali, ali uporabljajo katero izmed sedmih oblik računalniške programske zaščite, in to primerjali s podatki o žrtvah (vprašanje 12): zanimalo nas je, ali tisti, ki se bolj samozaščitno vedejo, manj pogosto postanejo žrtve nadlegovanja (tabela 11).

Tabela 11: Pearsonov hi-kvadrat test uporabe računalniške programske zaščite žrtev nadlegovanja

Ali uporabljate našteto računalniško programsko zaščito? (vpr. 12)		Ali ste že bili žrtev nadlegovanja po internetu	Ali ste že bili žrtev nadlegovanja v spletnem socialnem omrežju	Ali ste že bili žrtev nadlegovanja po mobilnem telefonu
1. požarni zid	Hi-kvadrat	16,626	14,870	16,395
	s.p.	6	6	6
	Sig.	0,011	0,021	0,012
2. protivirusni program	Hi-kvadrat	8,216	3,759	6,702
	s.p.	6	6	6
	Sig.	0,223	0,709	0,349
3. program, ki blokira pojavna okna (pop-up)	Hi-kvadrat	5,514	11,887	1,016
	s.p.	6	6	6
	Sig.	0,480	0,065	0,985
4. program za starševsko kontrolo	Hi-kvadrat	4,154	5,957	1,505
	s.p.	6	6	6
	Sig.	0,656	0,428	0,959
5. program, ki ščiti pred ribarjenjem (anti-phishing)	Hi-kvadrat	4,036	5,374	10,220
	s.p.	6	6	6
	Sig.	0,672	0,497	0,116
6. program, ki ščiti pred vohunjenjem (anti-spy)	Hi-kvadrat	8,178	9,503	2,843
	s.p.	6	6	6
	Sig.	0,225	0,147	0,828
7. pogosto posodabljate protivirusne programe	Hi-kvadrat	8,887	6,540	7,591
	s.p.	6	6	6
	Sig.	0,180	0,365	0,270

Statistično pomembne povezave ni. Na prvi pogled obstaja povezava med vsemi tremi oblikami nadlegovanja in uporabo požarnih zidov (χ^2 = 16,626; 14,870; 16,395, p = 0,011; 0,021; 0,012), a je premalo podatkov, da bi bil rezultat zanesljiv (Razmerje verjetij ima stopnjo značilnosti 0,170; odstotki se le malo razlikujejo).

b) Ali žrtve razumejo spletne nevarnosti in ogrožanja?

Anketirane smo vprašali (vprašanje 13): Kako dobro razumete delovanje: (1) računalniških virusov in črvov, (2) spletnega ribarjenja (*phishing*), (3) vohunskih programov, (4) požarnih zidov, (5) protivirusnih programov in (6) sisteme spletnih prijav (na primer Safe.si, Spletno okno). Izbirali so lahko na petstopenjski lestvici med: sploh ne razumem – slabo – ne preveč dobro – še kar – zelo dobro razumem. Pri žrtvah *nadlegovanja po internetu* obstaja statistično značilna povezanost le z razumevanjem vohunskih programov (χ^2 = 17,478, p = 0,025; razmerje verjetij = 0,012). Pri žrtvah *nadlegovanja po spletnem socialnem omrežju* in *nadlegovanja po mobilnem telefonu* ni statistično značilne povezanosti z nobeno spremenljivko razumevanja pogostih oblik ogrožanja.

c) Ali žrtve poznajo sisteme za zaščito podatkov?

Podatke o žrtvah smo primerjali še z njihovim poznavanjem sistemov za zaščito podatkov (vprašanje 24): (1) digitalni podpis, (2) digitalno potrdilo, (3) HTTPS – *Secure Http*, (4) AES – *Advanced Encryption Standard*, (5) VPN – *Virtual Private Network*, PGP – *Pretty Good Privacy*. Anketirani so odgovarjali na petstopenjski lestvici med: še nisem slišal – slabo poznam – ne preveč dobro – še kar – zelo dobro.

Žrtve *nadlegovanja po internetu* bolje poznajo digitalni podpis kot tisti, ki niso bili še nikoli žrtve (na primer večkratne žrtve ga v 29 % poznajo zelo dobro – le 25 % nežrtev ga pozna zelo dobro, 42 % večkratnih žrtev in 46 % enkratnih žrtev ga še kar pozna, le 34 % nežrtev ga še kar pozna). Tudi digitalno potrdilo poznajo bolje tisti, ki so že bili žrtve nadlegovanja po internetu (na primer »še kar« ga pozna 54 % enkratnih žrtev, 35 % večkratnih žrtev in 30 % tistih, ki še niso bili viktimizirani na ta način). HTTPS (*secure http*) anketirani ne poznajo dobro, tudi delež tistih, ki so že slišali zanjo, je majhen. Toda delež tistih, ki zelo dobro poznajo zaščito, je največji med anketiranimi, ki so bili večkrat žrtve, prav tako delež tistih, ki so odgovorili »še kar«, in je najmanjši med tistimi, ki so odgovorili »ne preveč dobro«, »slabo poznam« in »še nisem slišal/a«. Kaže, da so žrtve nadlegovanja po internetu boljši poznavalci sistemov za zaščito podatkov od tistih, ki še niso bili viktimizirani na ta način. Čeprav Pearsonov test hi-kvadrat kaže, da statistično značilna povezanost obstaja le s poznavanjem enkripcije (AES) ($\chi^2 = 18{,}402$, $p = 0{,}018$), ob tem, da več kot polovica anketiranih sploh še ni slišala za to obliko zaščite.

Za žrtve nadlegovanja po *spletnem socialnem omrežju* na splošno velja podobno kot za nadlegovanje po internetu: bolje poznajo digitalni podpis in digitalno potrdilo, med boljšimi poznavalci pa so tisti, ki so že bili žrtve. Pearsonov test χ^2 kaže povezanost med nadlegovanjem po socialnem omrežju in poznavanjem digitalnega potrdila, zato so bile izračunane teoretične frekvence (razmerje verjetij = 0,012). Med večkratnimi žrtvami je sicer manj zelo dobrih poznavalcev digitalnega potrdila, kot bi pričakovali (če bi bili spremenljivki neodvisni), a so samo 3, ki »ne preveč dobro« poznajo digitalno potrdilo (če poznavanje ne bi bilo povezano s stopnjo viktimizacije, bi bilo slabih poznavalcev 9 anketirancev); podobno je »še kar« dobrih poznavalcev več med večkratnimi žrtvami, kot bi pričakovali.

Med poznavanjem zaščite in nadlegovanjem po *mobilnem telefonu* pa test χ^2 kaže, da ni statistično značilne povezanosti.

3.6 Ukrepanje žrtev po nadlegovanju

Kako bi se anketirani odzvali na kibernetsko nadlegovanje in kako bi se anketirani, ki so že bili žrtve nadlegovanja, odzvali nanj? Vprašani so bili (vprašanje 18): Na koga bi se obrnili v šestih hipotetičnih primerih (med njimi nadlegovanje na spletnem socialnem omrežju): (1) nepooblaščenega vdora v vaš računalnik, (2) sesutja informacijskega sistema iz neznanega razloga, (3) prevelikega števila neželene e-pošte, (4) nadlegovanja na spletnem socialnem omrežju, (5) če bi na internetu opazili gole podobe otrok.

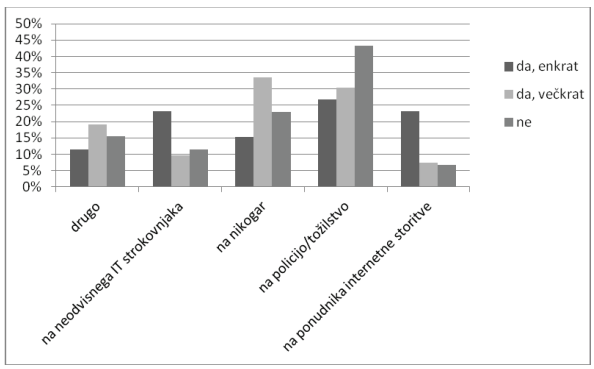
Iz tabele 12 izhaja, da bi se v dveh primerih anketirani večinoma obrnili na neodvisnega IT-strokovnjaka (nepooblaščen vdor v računalnik in sesutje informacijskega sistema iz neznanega razloga), v dveh primerih pa večinoma na organe pregona (nadlegovanje po spletnem socialnem omrežju in golih podobah otrok). Neželeno pošto bi večinoma tolerirali (ali pa se počutili nemočne) in se ne bi obrnili na nikogar.

Tabela 12: Iskanje pomoči žrtev kibernetskega nadlegovanja

Na koga bi se obrnili v primeru: (vpr. 18)		Število	%
1. nepooblaščenega vdora v vaš računalnik	drugo	49	11,1 %
	na neodvisnega IT-strokovnjaka	173	39,2 %
	na nikogar	45	10,2 %
	na policijo/tožilstvo	93	21,1 %
	na ponudnika internetne storitve	81	18,4 %
2. sesutja informacijskega sistema iz neznanega razloga	drugo	58	13,2 %
	na neodvisnega IT-strokovnjaka	210	47,6 %
	na nikogar	59	13,4 %
	na policijo/tožilstvo	5	1,1 %
	na ponudnika internetne storitve	109	24,7 %
3. prevelikega števila neželene e-pošte (spam)	drugo	64	14,5 %
	na neodvisnega IT-strokovnjaka	105	23,8 %
	na nikogar	178	40,4 %
	na policijo/tožilstvo	1	0,2 %
	na ponudnika internetne storitve	93	21,1 %
4. nadlegovanja na spletnem socialnem omrežju	drugo	77	17,5 %
	na neodvisnega IT-strokovnjaka	48	10,9 %
	na nikogar	126	28,6 %
	na policijo/tožilstvo	152	34,5 %
	na ponudnika internetne storitve	38	8,6 %
5. če bi na internetu opazili gole podobe otrok	drugo	40	9,1 %
	na neodvisnega IT-strokovnjaka	5	1,1 %
	na nikogar	59	13,4 %
	na policijo/tožilstvo	324	73,5 %
	na ponudnika internetne storitve	13	2,9 %

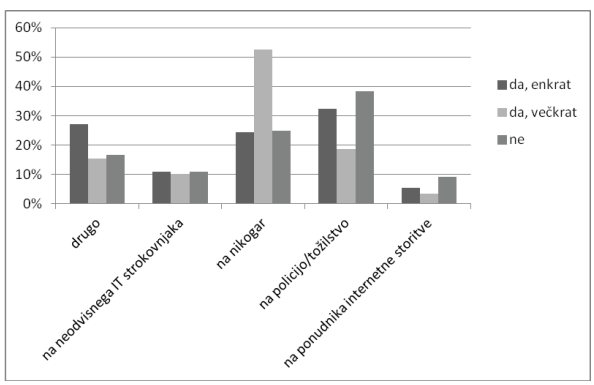
Ko se osredotočimo samo na reagiranje v spletnem socialnem omrežju in preverimo, kako bi se ravnale žrtve (treh oblik nadlegovanja), ugotovimo statistično pomembne razlike pri reagiranju žrtev nadlegovanja po internetu (graf 7) in žrtev nadlegovanja v spletnem socialnem omrežju (graf 8) (ne pa pri žrtvah nadlegovanja po mobilnem telefonu).

Iz primerjave odstotkov v grafu 7 je razvidno, da bi se tisti, ki so bili večkrat žrtev *nadlegovanja po internetu*, v manjšem deležu (30,4 %) obrnili na policijo/tožilstvo kot tisti, ki niso bili nadlegovani (43,2 %). Večkrat nadlegovani se v tem primeru v večji meri (33,5 %) ne bi obrnili na nikogar kot tisti, ki niso bili nadlegovani (23 %). Obstaja statistično značilna povezanost med žrtvami nadlegovanja po internetu in reagiranjem na morebitno nadlegovanje po socialnem omrežju ($\chi^2 = 23{,}281$, $p = 0{,}003$).



Graf 7: Povezava med žrtvami nadlegovanja *po internetu* in na koga bi se obrnili

Večkratne žrtve *nadlegovanja v spletnem socialnem omrežju* se v primeru vnovičnega tovrstnega nadlegovanja še v večji meri ne bi obrnile na nikogar (52,5 %) kot tisti, ki niso bili nadlegovani (25 %) (graf 8). Na organe pregona bi se tudi tu najpogosteje obrnili tisti, ki še nikoli niso bili viktimizirani v spletnem socialnem omrežju (38,3 %), medtem ko bi se večkrat nadlegovani nanje obrnili v manjši meri (18,6 %). Razumljivo je, da obstaja statistično značilna povezanost med nadlegovanjem po socialnem omrežju in reagiranjem na nadlegovanje po socialnem omrežju ($\chi^2 = 23{,}971$, $p = 0{,}002$). Podobni so tudi odstotki reagiranja pri žrtvah *nadlegovanja po mobilnem telefonu*, čeprav statistično značilnih povezav ni.

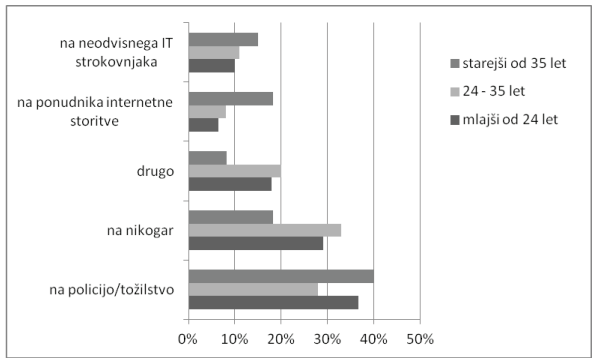


Graf 8: Povezava med žrtvami nadlegovanja *na spletnem socialnem omrežju* in na koga bi se obrnili

Preverili smo tudi, ali se tisti, ki so nadlegovani (na tri osnovne oblike nadlegovanja), odzivajo tudi tako, da uporabljajo računalniško programsko zaščito: požarni zid, protivirusni program, program, ki blokira pojavna okna, program za starševsko kontrolo, program, ki ščiti pred ribarjenjem, program, ki ščiti pred vohunjenjem. Statistično pomembnih povezav med tremi oblikami žrtev nadlegovanja in uporabo tovrstne zaščite ni.

Enako nas je zanimalo, ali se žrtve nadlegovanja odzivajo tudi tako, da ne dajejo svojih podatkov – ali obstaja povezava med žrtvami nadlegovanja in tem, ali bi oddale svoje osebne podatke vključno z e-naslovom za različne namene: za potrebe obveščanja o proizvodih, katalogih; v zameno za dostop do sicer nedostopnih strani na internetu; v zameno za neki brezplačni program; v zameno za popust pri nakupu; v zameno za brezplačni elektronski naslov po želji. Statistična obdelava podatkov tudi tokrat ni pokazala statistično pomembnih povezav.

Statistično pomembne pa so razlike med starostnimi skupinami in tem, na koga bi se obrnile v primeru nadlegovanja v spletnem socialnem omrežju (18. vprašanje) (graf 9). (Med spolom in tem vprašanjem ter med izobrazbo in tem vprašanjem ni statistično značilnih povezav.)



Graf 9: Na koga bi se obrnili v primeru *nadlegovanja v spletnem socialnem omrežju* glede na starost

Zanimivo je, da bi se starejši od 35 let v dvakrat večjem deležu kot vsi mlajši obrnili na ponudnika internetne storitve. Mlajši dve skupini pa se v večjem deležu ne bi obrnili na nikogar kot starejši od 35 let. Iz tega lahko sklepamo, da mlajši takšno nadlegovanje bolj tolerirajo kot starejši, gotovo zato, ker so sami bolj intenzivni uporabniki, morda tudi sami udeleženi kot nadlegovalci.

4 Razprava

Pojem *cyberbullying* je nemogoče pojmovno ustrezno prevesti. Dekleva (2001: 27) v semantični analizi (med)vrstniškega nasilja tako navaja, da so slovenski učenci 2. razreda osnovne šole našli 9 besed za (sicer vrstniško) nasilje, medtem ko so učenci 8. razreda osnovne šole našli kar 29 besed. Avtorji zato pojem slovenijo zelo različno, kot »spletno in mobilno nadlegovanje« (Zoranovič, 2011), »nadlegovanje preko interneta« (Informacijski pooblaščenec, 2009), »spletno ustrahovanje« (Lobe in Muha, 2011), »žaljivo in neprijetno obnašanje na internetu« (Lobe in Muha, 2011), sramotenje ali poniževa-

nje. Ločnice med temi pojavi so zato tudi pogosto zabrisane. Pri projektu SAFE-SI (2012) na primer ločijo od »spletnega ustrahovanja« in »mobilnega ustrahovanja ali mučenja, ko se uporabniki med seboj žalijo, grozijo ali izsiljujejo prek SMS-sporočil in telefonskih klicev«, še *seksting* (pošiljanje/izmenjavanje napol golih ali golih fotografij z vrstniki prek spleta ali mobilnega telefona), kar je lahko le pogojno oblika spletnega ali mobilnega ustrahovanja.

V prispevku smo uporabljali pojem kibernetskega (spletnega in mobilnega) nadlegovanja, ki ga lahko storijo tudi polnoletni. Načelni razlog za uporabo pojma nadlegovanje (in ne nasilje) je, da je pojem nasilja, ki mu danes dodajajo avtorji še relacijsko, psihološko, razredno, strukturno dimenzijo, preširok in ne referira na skoraj nobeno stvarnost več.[6] Takšen pojem ne bi omogočal operacionalizacije za potrebe empirične študije. Pojem nadlegovanje se je tudi bolj uveljavil v vsakodnevni rabi (več o tem na primer Informacijski pooblaščenec, 2009), čeprav bi bila strokovno utemeljena tudi uporaba pojma ustrahovanje (Dekleva, 1996). V kontinentalnih raziskavah je pojem *bullying* rezerviran za vrstniško nasilje. Kljub temu pa smo vključili v pojem tudi polnoletne, saj v anglo-ameriškem govornem območju vanj uvrščajo tudi polnoletne in o tem ni soglasja. Pragmatičen razlog za širše pojmovanje, ki vključuje polnoletne, je ta, da smo z empirično študijo dosegli zgolj polnoletne uporabnike spleta in mobilnih tehnologij. Kibernetsko (med)vrstniško nasilje zato ni predmet te študije.

Dileme, povezane s prevajanjem osrednjega označevalca, so pomembne pri primerjavah s tujimi študijami, zato bi se kazalo pred prihodnjimi raziskavami še bolj sistematično posvetiti temu vidiku. Praviloma (razen angleško govoreči in nekateri Skandinavci) so se morali vsi ukvarjati tudi z dilemo poimenovanja, ker za *bullying* ne poznajo enoznačnega prevoda. Po drugi strani pa krovno poimenovanje ni povsem osrednjega pomena zaradi druge temeljne značilnosti kibernetskega nadlegovanja.

Za to obliko nadlegovanja je namreč značilno, da pomembno narašča ravno med mladimi, ki v uporabi IKT pomembno prekašajo starejše. Natančneje, to je eno redkih področij, na katerem mladi prekašajo starejše (Bauman, 2007). Po podatkih Eurobarometra (Evropska komisija, 2011) namreč 44 % Evropejcev uporablja internet vsak dan (EU27), delež tistih, ki ga uporabljajo vsak dan, pa pada s starostjo uporabnikov: dnevno ga uporablja 74 % starih od 15 do 24 let, 60 % starih med 25 in 39 let, 42 % starih med 40 in 54 let ter 21 % starih nad 55 let. Trend je, da postajajo uporabniki vedno mlajši otroci (Evropska komisija, 2012). To pomeni, da je pri raziskavah nadlegovanja med mlajšo populacijo nujno treba bolj opisno pojasniti, o čem jih spraševalci povprašujejo, in krovna oznaka zato ni osrednjega pomena.

Zelo pomemben element raziskovanja kibernetskega nadlegovanja je zato izbira vzorca. Iz zgornjih raziskav o intenziteti uporabe IKT med različnimi starostnimi skupinami izhaja, da je to težava mladih uporabnikov oziroma težava, s katero se v povečanimi meri srečujejo že otroci. Ti so najbolj ranljiva skupina zato, ker obstaja pri njih velik razkorak med tehnološkimi veščinami in sposobnostjo zrelo se soočati z nadlegovanjem zaradi osebnostne (ne)zrelosti. Slabost pričujoče raziskave je zato v tem oziru ta, da ni zajela otrok kot najranljivejše populacije. V bodoče bo zato treba rešiti še etična vprašanja, povezana z anketiranjem otrok, pridobiti dovoljenja staršev in se lotiti zahtevnega anketiranja v obliki individualnih intervjujev, ki bi lahko edina dala jasno sliko o pojavnosti in značilnostih (vrstniškega) kibernetskega nadlegovanja.

V predstavljeni študiji smo razlikovali tri osnovne oblike kibernetskega nadlegovanja in sedem podoblik. Izbrana taksonomija izvira na eni strani iz študije tujih raziskav (na primer Slonje, Smith, 2008; COST Akcija IS0801) o tem, katere oblike so temeljne, in kar nam omogoča mednarodno primerljivost rezultatov. Po drugi strani pa je tudi odraz trenutnega stanja razvoja IKT in s tega vidika je pričakovati, da bodo določene oblike elektronskega komuniciranja sčasoma zastarele in se bodo pojavile nove (na primer takojšnjega sporočanja – *Instant Messaging* – raziskovalci praviloma ne vključujejo več v raziskave).

Rezultati so na splošno tako kot drugod po svetu (Campbell, 2005; Kowalski *et al.*, 2005; Smith *et al.*, 2006; Bauman, 2007) pokazali, da je to nov problem in da stopnje *cyberbullyinga* niso zanemarljive. To kaže, da gre za problem, ki ga bo treba nadalje proučevati. Največ anketiranih je bilo žrtev internetnega nadlegovanja (64,9 %), nato nadlegovanja po mobilnem telefonu (44 %) in najmanj nadlegovanja v spletnem socialnem omrežju (21,8 %). Vzorec sicer ni bil reprezentativen za celotno slovensko populacijo, saj je bila naša ciljna skupina anketiranih že vnaprej zavestno omejena na študentsko populacijo, ki je bolj izobražena, mlajša in bolj vešča uporabe IKT. Ta izbira je bila pogojena z rezultati že opravljenih raziskav, da je kibernetsko nadlegovanje primarnega pomena za mlajše uporabnike, ki z IKT delajo in preži-

[6] Podobno Kanduč (1998) ugovarja presplošni rabi besede »nasilje«, ker so pojmovanja nasilja odvisna od pripadnosti spolu, posameznim družbenim skupinam ali celo subkulturam, in zato pomembno drugačna: »Poimenovanje (in opredeljevanje) nasilja nikakor ni naravno, ampak družbeno in kulturno »dejstvo«. Dogaja se v simboličnih interakcijah (ideološko pogojenih procesih komuniciranja), kjer ima ključno vlogo »perspektiva« (zorni kot) osebe, ki nekaj opiše kot primer nasilja. Izjavljalne pozicije nasilneža, žrtve, opazovalca ali razlagalca nasilja pa so v praksi pogosto različne.« (Kanduč, 1998: 25).

vljajo tudi prosti čas. Zaradi takšnega vzorca so tudi stopnje kibernetskega nadlegovanja relativno visoke in jih ne moremo posplošiti na celotno slovensko populacijo.

Velik delež internetnega nadlegovanja v primerjavi z drugimi oblikami nadlegovanja je pričakovan, saj več ljudi uporablja internet kot pa spletna socialna omrežja. Po drugi strani je tudi res, da je zastavljeno vprašanje lahko zavajajoče, saj je obsegalo tudi namig na neželeno pošto, kar je lahko sporno; podobno visoke odstotke – v primerjavi z drugimi ogrožanji – nadlegovanja po e-pošti ugotavljata Bernik in Meško (2011: 248). A tudi nadlegovanje po mobilnem telefonu in v spletnem socialnem omrežju ni zanemarljivo.

Moški so bili pogosteje večkrat nadlegovani po internetu kot ženske (63,6 % proti 56,9 %), rezultat nadlegovanja po spletnem socialnem omrežju in mobitelu pa je obraten. To je podobno izsledkom raziskave Smith *et al.* (2006), ki je ugotovila, da so dekleta najpogosteje žrtve nadlegovanja z SMS sporočili in klici, in drugače od Li (2006), ki razlik med spoloma ni ugotovil. Ne glede na te ugotovitve, razlike med odstotki niso velike (po testu χ^2 med spremenljivkama ni statistično pomembne povezanosti). Statistično pomembna povezanost pa je bila ugotovljena med nadlegovanjem in starostjo anketiranih: po internetu so najbolj nadlegovani stari med 24 in 35 let (srednja starostna skupina): 71 % vseh anketiranih te starosti je odgovorilo, da so bili nadlegovani večkrat. Tudi po mobilnem telefonu je v največjem deležu nadlegovana ta starostna skupina (33,3 % večkrat). Ta skupina mladih je najbolj ranljiva tudi sicer, kar kažejo drugi podatki (npr. o majhni zaposljivosti mladih po 23 letu starosti, prekarnosti njihovih zaposlitev, majhnih možnosti, da si uredijo samostojno življenje itn.); to ustvarja napetosti in več medosebne nasilnosti ter se kaže tudi pri kibernetskem nadlegovanju.

Zaznavanje resnosti kibernetskega nadlegovanja dosega visoke povprečne ocene: srednja vrednost znaša 3,8 (1 – ni problematično, 5 – zelo problematični) in je na 7. mestu od 11 tveganj. To je podobno ugotovitvam raziskave Rabe Interneta v Sloveniji (Kozinc *et al.* 2009; leto 2008, n = 2230), ko je bila ta nevarnost ocenjena s povprečno stopnjo problematičnosti 4 in na 4. mestu od 13 tveganj. Visoke stopnje strahu ugotavljata tudi Bernik in Meško (2011: 247), takoj za krekerstvom in hekerstvom si sledijo nadlegovanje po e-pošti, kibernetsko nadlegovanje in razširjanje govoric.

Z uporabo testa Brown-Forsythe smo ugotovili statistično značilno razliko med spolom in nadlegovanjem po internetu/mobilnem telefonu, zlorabo zasebnosti, ko se proti naši volji na internetu o nas pojavijo določeni podatki ali fotografije, ter spletnim piratstvom in kršenjem avtorskih pravic; vse naštete nevarnosti se moškim zdijo manj problematične kot ženskam. Statistično značilna razlika med moškimi in ženskami je tudi pri neželeni e-pošti, ki se za razliko od prejšnjih nevarnosti zdi bolj problematična moškim. Med starostnimi skupinami in zaznavanjem resnosti vseh nevarnosti, vključno z nadlegovanjem po internetu/mobilnem telefonu (razen zlorabe zasebnosti, kjer so vse starostne skupine tovrstno nevarnost ocenile kot problematično in med njimi ni statistično pomembnih razlik), so statistično pomembne razlike: vse nevarnosti se zdijo najbolj problematične najstarejši skupini. Ta razkorak je mogoče interpretirati z večjo previdnostjo starejših uporabnikov, ki IKT uporabljajo bolj za svoje delo kot zabavo. Te generacije so se prvič z IKT bolj verjetno srečale v okviru svojega dela kot mlajše generacije, ki so se z IKT prvič srečale v obliki načina preživljanja prostega časa.

Ali je na nadlegovanje treba reagirati s kazenskim pravom? Anketiranim (ženskam sicer bolj kot moškim) velik problem predstavlja objavljanje fotografij brez posameznikove vednosti ali privolitve v spletnem socialnem omrežju in objavljanje spremenjenih ali predelanih fotografij posameznika: skoraj ¾ anketiranih meni, da je to nadlegovanje, ki si zasluži inkriminacijo. Statistično značilne povezave obstajajo med starostjo in vsemi oblikami nadlegovanja (razen objavo spremenjenih/predelanih fotografij). Pri vseh oblikah nadlegovanja (razen pri prekomernem pošiljanju SMS/MMS-sporočil) je daleč največ starejših od 35 let tistih, ki menijo, da bi bilo treba kazenskopravno reagirati. Statistično značilne razlike v mnenju glede potrebnosti kazenskopravnega reagiranja na določene oblike nadlegovanj obstajajo tudi med študenti pravne fakultete in študenti drugih fakultet. Pri vseh oblikah nadlegovanja manj študentov pravne fakultete meni, da je potrebno kazenskopravno reagiranje. Očitno so bolj ponotranjili načelo *ultima ratio* kot eno temeljnih načel kazenskega prava, o katerem so bili poučeni pri več predmetih iz kazenskega prava.

Kako bi kaznovali nadlegovanje? Več kot polovica anketiranih bi z zaporno kaznijo kaznovala krajo identitete na internetu, petina kar z zaporom več let. Lažen profil v spletnem socialnem omrežju je tudi po mnenju več kot tretjine anketiranih vreden kaznovanja: za to bi se odločilo več kot 30 % moških in več kot 40 % žensk. Preseneča kaznovalna naravnanost do kraje identitete (več kot 90 % anketiranih bi prisodilo kazenske sankcije) in pošiljanja neželene pošte (več kot 70 % bi jih prisodilo kazenske sankcije) ob majhnih odstotkih pogodbenega »kaznovanja« (izklop dostopa do interneta), ki je v kibernetskem prostoru ekvivalent smrtni kazni. Morda je to zadnje bolj kot manjši kaznovalni nastrojenosti pripisati manjši pravni imaginaciji anketiranih ali dejstvu, da je bil izvajalec raziskave kriminolog, s čimer je nehote sporočal anketiranim specifičen referenčni (pravni) okvir odziva na odklonskost. Visoka kaznovalna nastrojenost je morda posledica tega, da v Sloveniji po spremembi Kazenskega zakonika KZ-1B v letu 2011 poznamo tudi posebno kaznivo dejanje, povezano s prevzemom identitete druge osebe (četrti odst. 143. čl. KZ-1).

Preventivno samozaščitno ravnanje žrtev se kaže med drugim tudi v njihovem poznavanju računalniške programske zaščite, spletnih groženj in sistemov za zaščito podatkov. A žrtve nadlegovanja ne odstopajo pri uporabi računalniške programske zaščite, statistično pomembne povezave ni. Njihovo razumevanje spletnih groženj je boljše kot bi pričakovali (če spremenljivki ne bi bili povezani): žrtve *nadlegovanja po internetu* bolje razumejo vohunske programe (χ^2 = 17,478, p = 0,025), drugih statistično pomembnih povezav pa nismo zaznali (na primer glede poznavanja računalniških virusov in črvov, spletnega ribarjenja – *phishing*, požarnih zidov, protivirusnih programov in sistemov spletnih prijav, kot sta Safe.si in Spletno okno). Njihovo poznavanje sistemov za zaščito podatkov je tudi deloma boljše: žrtve *nadlegovanja po internetu* in *spletnem socialnem omrežju* bolje poznajo digitalni podpis in digitalno potrdilo kot tisti, ki še niso nikoli bili žrtve nadlegovanja po internetu, a statistično značilna povezanost obstaja le s poznavanjem enkripcije (AES) (za žrtve nadlegovanja po internetu: χ^2 = 18,402, p = 0,018). Drugih sistemov za zaščito podatkov (HTTPS – *Secure Http*, VPN – *Virtual Private Network*, PGP – *Pretty Good Privacy*) ne poznajo žrtve nič boljše ali slabše kot drugi. Rezultat, da žrtve bolje poznajo določene oblike zaščite, je mogoče razložiti s tem, da so intenzivnejši uporabniki IKT: zato so bolj vešči uporabe, a tudi bolj izpostavljeni tveganjem in nevarnostim.

Na koga bi se anketirani obrnili v šestih hipotetičnih primerih kibernetskih ogrožanj? Če bi bili žrtve nadlegovanja v spletnem socialnem omrežju, večinoma na organe pregona. Tisti, ki so že bili večkrat žrtev *nadlegovanja po internetu, pa* bi se v manjšem deležu (30,4 %) obrnili na policijo/tožilstvo kot tisti, ki niso bili nadlegovani (43,2 %). Večkrat nadlegovani se v tem primeru v večji meri (33,5 %) ne bi obrnili na nikogar kot tisti, ki niso bili nadlegovani (23 %). Večkratne žrtve *nadlegovanja v spletnem socialnem omrežju* se v primeru vnovičnega tovrstnega nadlegovanja še v večji meri ne bi obrnile na nikogar (52,5 %) kot tisti, ki niso bili nadlegovani (25 %).

Podatek je zaskrbljujoč ter kaže na nezaupanje v organe odkrivanja in pregona storilcev kaznivih dejanj. Pri vnovičnih žrtvah je manjše zaupanje mogoče razlagati na dva načina: ti organi so morda nepripravljeni na odzivanje na nove oblike odklonskosti in ne vedo, kako in ali sploh se odzvati, od koder izvira napotek več izobraževanja o novih oblikah nadlegovanja ter njihovih škodljivih posledicah. Lahko pa kaže na to, da ostajajo agenti formalnega družbenega nadzorstva ujetniki lastnih paradigem delovanja. Realno policijsko delo je morda tudi pri nas, tako kot za Veliko Britanijo ugotavlja Manning (2008), še vedno osredotočeno na tradicionalne naloge. Boji za moč med različnimi poklicnimi skupinami znotraj policije, pomanjkanje interesa zaposlenih, slaba opremljenost in poznavanje IKT itn. so lahko dejavniki, ki policijsko delo in naloge ohranjajo v ritmu že preživetih koncepcij policijskega dela.

Statistično pomembne pa so razlike med starostnimi skupinami in tem, na koga bi se obrnile v primeru nadlegovanja v spletnem socialnem omrežju: starejši od 35 let bi se v dvakrat večjem deležu kot vsi mlajši obrnili na ponudnika internetne storitve. Mlajši dve skupini pa se v večjem deležu ne bi obrnili na nikogar; podobno Smith *et al.* (2006), ki so ugotovili, da se 1/3 žrtev ne bi obrnila na nikogar. Ker mlajšim IKT pomeni tudi zabavo in morda celo način življenja, se lahko bojijo, da bodo posledice ali sankcije tudi takšne, da jim bo onemogočena uporaba IKT.

Ključna ugotovitev na koncu je, da izvedena raziskava predstavlja zgolj nov del v mozaiku, na katerega opozarjajo raziskovalci projekta *EU Kids Online*, ki sistematično proučuje uporabo *online* tehnologij med otroci v 21 evropskih državah. Namreč, da je Slovenija med državami z najmanj zbranimi podatki o tem, kaj mladi počno *online*, s kakšnimi specifičnimi tveganji (komercialne, žaljive, pornografske narave) se srečujejo v vlogi prejemnikov, udeležencev in akterjev, kakšna je njihova stopnja in narava osveščenosti o varni rabi *online* tehnologij, katere tehnologije so najbolj izpostavljene.[7] Enako ali še bolj velja za raziskave o tem, kako IKT uporabljajo starejši in s katerimi težavami se tam srečujejo oni.

Literatura

1. Bauman, S. (2007). *Cyberbullying: a Virtual Menace*. Paper presented at the National Coalition Against Bullying National Conference Melbourne, Australia, november 2–4.
2. Bernik, I.; Meško, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto. *Revija za kriminalistiko in kriminologijo*, let. 62, št. 3, s. 242–252.
3. Brvar, B. (2007). *Statistika*. Ljubljana: Fakulteta za varnostne vede.
4. Campbell, M. A. (2005). Cyber-bullying: An old problem in a new guise? *Australian Journal of Guidance and Counseling*, št. 15, s. 68–76.
5. COST (European Cooperation in Science and Technology) Action IS0801: *Cyberbullying: coping with negative and enhancing positive uses of new technologies, in relationships in educational settings*. Po URL: https://sites.google.com/site/costis0801/, dostop 5. 5. 2012.
6. Dekleva, B. (1996). Nasilje med vrstniki v zvezi s šolo – obseg pojava. *Revija za kriminalistiko in kriminologijo*, let. 47, št. 4, s. 355–365.
7. Dekleva, B. (2001): Semantika (med)vrstniškega nasilja. *Revija za kriminalistiko in kriminologijo*, let. 52, št. 1, s. 21–31.
8. Evropska komisija (2011). *Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union. A Report***.** Pridobljeno na: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf, dostop 3. 5. 2012.
9. Evropska komisija (2012). *Digital Agenda: New strategy for safer internet and better internet content for children and teenagers*. Reference: IP/12/445. Pridobljeno na: http://europa.eu/rapid/

[7] Podobno opozarjaju pri projektu Mladi na netu, na URL: http://www.mladinanetu.si/, dostop 16. 7. 2012.

pressReleasesAction.do?reference=IP/12/445&format=HTML&aged=0&language=EN&guiLanguage=en, dostop 2. 5. 2012.
10. Informacijski pooblaščenec (2009). *Smernice glede varstva pred spletnim nadlegovanjem. Verzija 1.0.* Pridobljeno na: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice-glede-varstva-pred-spletnim-nadlegovanjem.pdf, dostop 5. 5. 2012.
11. Kanduč, Z. (1998). Pravo, spolnost in nasilje: kriminološke in viktimološke perspektive. V Kanduč, Z., Korošec, D., Bošnjak, M. (ur.), *Spolnost, nasilje in pravo* (s. 11–138). Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti, Urad RS za žensko politiko.
12. Kowalski, R., Limber, S., Scheck, A., Redfearn, M. Allen, J., Calloway, A. (2005). *Electronic bullying among school-aged children and youth.* Paper presented at the annual conference of the American Psychological Association, 20. avgust 2005.
13. Kozinc, T.; Činkole, T.; Vehovar, V. (2009). Nevarnosti, aktivnosti in spretnosti na internetu. Raba interneta v Sloveniji. Pridobljeno na: http://www.ris.org/db/13/10356/RIS_poročila/Nevarnosti,_aktivnosti_in_spretnosti_na_internetu/?&cat=682&p1=276&p2=285&p3=1318&p4=1327&id=1327, dostop 19. 3. 2012.
14. Livingstone, S., *et al.* (2011). *Risks and safety on the internet: The perspective of European Children.* Pridobljeno na: http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx, dostop 28. 3. 2012.
15. Lobe, B.; Muha, S. (2011). *Internet v vsakdanjem življenju slovenskih otrok in mladostnikov. Prvo poročilo raziskave Mladi na netu*. Ljubljana: Univerza v Ljubljani, Fakulteta za družbene vede, Center za metodologijo in informatiko.
16. Manning, P. (2008). A view of surveillance. V S. Leman-Langlois (ed.), *Technocrime: Technology, crime and social control* (s. 209–242). Cullompton, Devon, Portland: Willan Publishing.
17. Muršič, M.; Brvar, B. (2010). Izbor (s čustvi povezanih) ugotovitev naše raziskave. V M. Muršič (ur.), *Znanje o čustvih za manj nasilja v šoli* (s. 21–26). Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani.
18. SAFE-SI (2012). *Osveščanje o varni rabi interneta in novih tehnologij*. Pridobljeno na: http://www.safe.si/, dostop 16. 5. 2012.
19. Slonje, R.; Smith, P. K. (2008). Cyberbullying: Another main type of bullying?, *Scandinavian Journal of Psychology*, let. 49, št. 2, s. 147–154.
20. Smith, P.; Mahdavi, J.; Carvalho, M.; Tippett, N. (2006). *An Investigation into cyberbullying, its forms, awareness and impact, and the relationship between age and gender in cyberbullying*. Research Brief No. RBX03-06, Unit for School and Family Studies, Goldsmiths College, University of London, London.

Internet and mobile phone bullying

Aleš Završnik, LL.D., Assistant Professor, Institute of Criminology at the Faculty of Law Ljubljana, Slovenia.

Anja Sedej, LL.B., Higher Court in Ljubljana, Slovenia.

Cyberbullying usually refers to bullying and harassment of others by means of new electronic technologies, primarily mobile phones and the Internet. The paper presents the results of an on-line cyberbullying victimization survey conducted mostly among students at several Slovene faculties. 441 adults, of whom 246 were aged less than 24 years, 135 aged 24 to 35 years and 60 aged over 35 years, 304 were women and 137 men, were surveyed to examine the nature and extent of cyberbullying in Slovenia. Three main categories of cyberbullying (by email, social networking sites and mobile phones) and seven subcategories (text message bullying, email bullying, social network bullying from unknown users, social network bullying from anonymous users, posting photos in social networking sites without consent of the user, tagging faces in social networking sites without consent of the user and publishing morphed pictures without consent) were examined in relation to age and gender, perceived impact, self-prevention measures, and turning to others in case of victimisation. There was a significant incidence of cyberbullying by email (65%), less by mobile phones (44%) and in social networking sites (22%). Gender differences were few, age difference were statistically significant (71% of respondents aged from 24 to 35 have been bullied many times). The impact of cyberbullying was perceived as highly negative for posting personal data and photos on the Internet without consent. Frequent cybervictims would turn to police less frequently than users that have never been a victim of cyberbullying.

Keywords: cyber crime, cyberbullying, internet bullying, mobile phones, social networking sites bullying, internet harrasment, interpersonal violence, abusive text messaging, sexting, prevention of crime, Slovenia

UDK: 004:343.3/.7(497.4)