Zbornik znanstvenih razprav
Letnik 73 (2013) / Volume 73 (2013)
Oktober / October 2013

Spletna stran Zbornika: / Journal website:
http://zbornik.pf.uni-lj.si
http://journal.pf.uni-lj.si

9

UDK 343:004.738.5, 343:621.395.721.5

*Dr. Aleš Završnik**

Spletno in mobilno nadlegovanje: pojem, oblike, posledice in soočanje s kazenskim pravom

1. Uvod

Z razvojem naprav, ki združujejo storitve telefonije, televizije, predvajalnikov glasbe in filmov ter dostopa do interneta (npr. e-pošte, spletnih socialnih omrežij in drugih storitev interneta 2.0)[1] v »pametne« telefone, tablične računalnike in »pametne« ure, povrhu opremljene še s kamerami in mikrofoni, so se pojavile nove priložnosti za nadlegovanje uporabnikov in kršitev njihove zasebnosti. Kakšne so primeroma najhujše oblike kibernetskega nadlegovanja, ki zahtevajo tudi kazenskopravno odzivanje?

Luis Mijangos iz južne Kalifornije je bil heker na invalidskem vozičku, ki je z zlonamerno kodo na oddaljen način »ugrabil« spletne kamere žrtvinih računalnikov, priklopljenih na internet, ali pametnih telefonov ter jim prisluškoval in jih neupravičeno snemal. Ko je prek ugrabljenih spletnih kamer žrtve dodobra spoznal, je dekleta izsiljeval za različna spolna dejanja pred spletno kamero, jim grozil z objavo zaupnih podatkov in tega, kar je videl in posnel.[2] Poznal je

* Višji znanstveni sodelavec na Inštitutu za kriminologijo pri Pravni fakulteti v Ljubljani in docent za kriminologijo pri Pravni fakulteti Univerze v Ljubljani; ales.zavrsnik@pf.uni-lj.si.

1 Pri storitvah spleta 2.0 oziroma socialnih medijev (angl. *Web 2.0*, *social media*) uporabniki sami (so)oblikujejo vsebine in niso le enosmerni uporabniki vsebin. Splet 2.0 obsega sodelovalne projekte (npr. *Wikipedia*), spletne dnevnike (bloge), strani za izmenjavo multimedijskih vsebin (npr. *YouTube*, *Picasa*), spletna socialna omrežja (npr. *Facebook*), virtualne socialne svetove (npr. *Second Life*) in virtualne igričarske svetove (npr. *World of Warcraft*).

2 Wired, URL: http://www.wired.co.uk/news/archive/2012-07/20/sextortion (9. 11. 2012). Izsiljevanje s spolnim gradivom (angl. *sextortion*) je izsiljevanje z grožnjami o razkritju spolnega gradiva žrtve, ki se začne, ko storilec nezakonito ali naključno pride do gradiva s takšnimi

podrobnosti njihovih prebivališč in številne druge osebne podatke, fotografije, gesla za uporabo spletnih računov. Svojo dejavnost je kasneje razširil in ogledovanje tujih prostorov prek spletnih kamer, ki jih je upravljal brez vednosti žrtev, odplačno ponujal drugim uporabnikom interneta. Na primer za 150 dolarjev je ponujal okužbo računalnika: naročniku je potem poslal internetno povezavo, prek katere je ta lahko sam vohunil za svojo tarčo. Policija je v sklepni fazi preiskave pri njem našla prek 15.000 *webcam*-video posnetkov, 900 zvočnih posnetkov in 13.000 zajemov zaslonske slike. Skupno je ogrozil več kot 230 žrtev, vključno z mladoletniki in žrtvami z drugih celin. V ZDA je bil obsojen na šestletno zaporno kazen.

Najodmevnejši primeri kibernetskega nadlegovanja so se končali s samomori žrtev (*bullicide*).[3] Prvi takšen svetovno znan je primer kibernetskega nadlegovanja Megan Meier, ki je sprožil izjemno zakonodajno aktivnost ameriških zveznih držav.[4] Primer je bil zapleten z vidika pravne kvalifikacije očitanega dejanja. V njem je 47-letna Lori Drew s hčerjo Sarah Drew leta 2006 na spletnem socialnem omrežju MySpace ustvarila lažen profil 16-letnega Josha Evansa, da bi zavajala 13-letno Megan Meier, sicer hčerino prijateljico, za katero je vedela, da se zdravi zaradi depresije.[5] Ko je Josh Evans po krajši romantični navezi grobo prekinil razmerje, je Megan storila samomor. Lori Drew je bila obtožena računalniških kaznivih dejanj po Zakonu o računalniških goljufijah in zlorabi računalnikov in grozilo ji je do 20 let zaporne kazni. A ker je kršila »zgolj« splošne pogoje uporabe spletnega socialnega omrežja, ki prepoveduje prijavo z lažnimi osebnimi podatki, jo je sodišče oprostilo kaznivih dejanj, povezanih z računalniki.[6] Zapisalo je, da karkoli že pomeni kaznivo dejanje »nepooblaščenega dostopa« do informacijskega sistema, temu samo kršitev splošnih pogojev uporabe spletnega socialnega omrežja ne zadosti. Takšno stališče je z odobravanjem sprejela tudi

---

podatki (npr. z vdorom v računalnik na daljavo, prek izgubljenega mobilnega telefona ali USB-ključka).

3 Hinduja, Patchin, Bullying, Cyberbullying, and suicidal ideation, v: Archives of Suicide Research 14 (2010), str. 210.

4 Federalni zakon The Megan Meier Cyberbullying Prevention Act je bil predstavljen 2. 4. 2009, a ni bil sprejet. Do januarja 2013 je 16 zveznih držav vključilo v zakonodajo zoper nadlegovanje kibernetsko različico nadlegovanja in 12 držav tudi kazenske sankcije zanj. Megan Meier Cyberbullying Prevention Act (2009), URL: http://www.govtrack.us/congress/bills/111/hr1966 (15.4.2013). Pregled zakonodaje po zveznih državah ZDA v: Hinduja, Patchin, State Cyberbullying Laws: Brief Review of State Cyberbullying Laws and Policies (2013), URL: http://www.cyberbullying.us/Bullying_and_Cyberbullying_Laws.pdf.

5 Maag, A Hoax Turned Fatal Draws Anger But No Charges, v: New York Times (28. 11. 2007), str. A23.

6 Sodba *United States v. Lori Drew* (259 F.R.D. 449 (C.D. Cal. 2009)), URL: http://www.volokh.com/files/LoriDrew.pdf (23. 1. 2013).

teorija. Grossman je menil,[7] da bi v nasprotnem primeru »manj pomembne« pogodbe postale »zelo pomembne« kazenske prepovedi,[8] Kerr[9] pa, da bi vsakršna drugačna odločitev vladi dala skoraj neomejene možnosti za kazenski pregon internetnih uporabnikov, državljanom pa ne bi dala zadostnih možnosti, da se seznanijo z območjem prepovedanega pri uporabi interneta.[10]

Primer vohunjenja in posegov v zasebnost 18-letnega študenta Tylerja Clementija se je končal podobno tragično. Obtoženi 20-letni Dharun Ravi je kot sostanovalec Tylerja Clementija na Univerzi Rutgers (ZDA) v njegovi sobi namestil spletno kamero, da bi vohunil za njim v intimnih trenutkih, kar je istospolno usmerjenega Clementija naposled pognalo v samomor. Ravi je o tem, kar je videl, prek omrežja Twitter sporočal svojim prijateljem in jih vabil, naj se mu pridružijo pri *on-line* voajerskem početju. Obtožen je bil 36 kaznivih dejanj[11] in bil na koncu spoznan za krivega po 24 točkah obtožnice.[12] Slovenski primer izsiljevanja, povezan z novimi tehnologijami, pa se je menda zgodil v Ljubljani na začetku leta 2012, ko je policija ovadila 18 osumljencev, večinoma gimnazijcev, ker naj bi izsiljevali profesorico in razpošiljali njene gole fotografije.[13]

Opisani primeri so skrajne oblike poniževanja, nadlegovanja, ustrahovanja, smešenja in razgaljevanja zasebnosti žrtve, ki pred razvojem vsenavzočih komunikacijskih naprav in spleta 2.0 niso obstajale. Kažejo tudi na izjemno raznolike vsebine pojma kibernetskega nadlegovanja (angl. *cyberbullying*)[14] tako glede ravnanja in starosti storilca in/ali žrtve, vloge tehnologije pri izvrševanju spornih ravnanj, zavarovane pravne dobrine kot tudi glede pravnih kvalifikacij dejanj, ko pride do kazenskega pregona domnevnih storilcev. Zato je pomembno poudariti, da je že pri opredeljevanju pojma kibernetskega nadlegovanja (in s tem pri

---

7 Grossman, The MySpace Suicide: A Case Study in Overcriminalization, v: Legal Memorandum, 32 (2008), str. 6.

8 Grossman, prav tam, str. 8.

9 Kerr, The Volokh Conspiracy blog (2009), URL: http://www.volokh.com/posts/1251601962.shtml.

10 Sodnik v sodbi *United States v. Lori Drew* na več mestih citira Kerr, Cybercrime's Scope: Interpreting »Access« and »Authorization« in Computer Misuse Statutes, v: New York University Law Review, 1596 (2003), na primer str. 15.

11 Hu, Legal Debate Swirls Over Charges in a Student's Suicide, v: The New York Times (1. 10. 2010), URL: http://www.nytimes.com/2010/10/02/nyregion/02suicide.html.

12 Cheng, Rutgers »cyberbully« found guilty of privacy invasion, hate crimes, v: ArsTechnica (13. 3. 2012), URL: http://arstechnica.com/tech-policy/2012/03/rutgers-cyberbully-found-guilty-of-privacy-invasion-hate-crimes/.

13 Lovšin, 18 ovadenih zaradi izsiljevanja in razpošiljanja fotografij gole profesorice, URL: http://www.dnevnik.si/kronika/1042503121.

14 Termin je skoval kanadski aktivistični pedagog Bill Belsey, ustanovitelj mreže www.cyberbullying.ca.

preučevanju in soočanju z njim) veliko nejasnosti in še vedno veliko neskladje med psihologi, pedagogi in drugimi preučevalci te nove oblike nasilnosti na eni strani ter pravno stroko, od katere se zaradi hudih posledic nekaterih takšnih dejanj za žrtve pogosto zahteva hiter in učinkovit odziv, na drugi strani.

Namen prispevka je zato predstaviti *pojem* in *oblike* kibernetskega (internetnega in mobilnega) nadlegovanja, ki ga uvodoma definiramo kot prikrito psihološko nasilje, ki se izvaja prek elektronskih medijev,[15] oziroma kot ponavljajoče se in sovražno vedenje posameznika ali skupine, ki vključuje uporabo informacijsko-komunikacijske tehnologije (IKT), s ciljem škodovati drugemu, ne glede na starost storilca in/ali žrtve.[16] Namen prispevka je tudi predstaviti *posledice* dejanj kibernetskega nadlegovanja in *načine spoprijemanja* z njim, pri čemer se razprava zoži na kazenskopravno odzivanje.[17] Pri prikazu pojma in oblik se razprava omeji na osnovne pojavne oblike, s ciljem prikazati mnogoterost možnega oškodovanja, šikaniranja in ustrahovanja, v katere so vpleteni storilci in žrtve različnih starosti. Ker se v literaturi o psihološki škodi teh dejanj[18] in v medijih ob primerih hudih posledic za žrtve pojavljajo pozivi k odločnemu kaznovanju storilcev, velja že uvodoma opozoriti, da večina dejanj, ki so razvojnopsihološko opredeljena kot kibernetsko nadlegovanje, ne vstopa (in ne bi smela vstopiti) na območje kaznivega, čeprav sprožajo potrebo po specifičnih preventivnih in intervencijskih ukrepih (npr. digitalno opismenjevanje uporabnikov IKT). Pri prikazu posledic se prispevek osredotoči na prikaz razvojnopsiholoških raziskav, ki kažejo dimenzije psihološke škode teh dejanj; v velikem delu se te raziskave nanašajo na mladoletnike, ker so ti pogosteje žrtve kot polnoletni, a ugotovitve niso nepomembne niti za polnoletne žrtve. Pri načinih soočanja pa prispevek prikaže zemljevid mnogoterih metod in načinov spoprijemanja s kibernetskim nadlegovanjem, ki lahko le skupno vodijo v manjše stopnje kibernetskega nadlegovanja in učinkovitejše odpravljanje njegovih posledic. Ob pregledu kazenskopravnega odzivanja razprava odgovarja na vprašanje, kako naj kazensko pravo *de lege ferenda* zagotovi dovolj gosto mrežo inkriminacij in s tem ustrezneje in še vedno sorazmerno odgovori na posebnosti novih viktimizacij.

---

15 Shariff, Gouin, Cyber-dilemmas: Gendered Hierarchies, Free Expression and Cyber-Safety in Schools (2005), URL: www.oii.ox.ac.uk/cybersafety.

16 Belsey, Cyberbullying: An emerging threat to the »always on« generation (2005), URL: http://www.cyberbullying.ca/pdf/Cyberbullying_Article_by_Bill_Belsey.pdf.

17 Več o pojavnosti v Sloveniji glej Završnik, Sedej, Spletno in mobilno nadlegovanje v Sloveniji, v: Revija za kriminalistiko in kriminologijo, 63 (2012) 4, str. 263–280.

18 Glej na primer program medvladnega programa znanstvenega sodelovanja 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*, URL: https://sites.google.com/site/costis0801/ (15. 4. 2013).

2. Pojem kibernetskega nadlegovanja

Normativna operacionalizacija kibernetskega nadlegovanja zahteva primarno definiranje osrednjega označevalca. Pregled raziskav o definiciji in nujnih elementih kibernetskega nadlegovanja kaže veliko pojmovno raznolikost.

Pojem nadlegovanje (angl. *bullying*) se v kontinentalni Evropi uporablja na področju nasilja v šoli in med mladoletniki. V Veliki Britaniji in drugih anglosaških državah pa ga ne uporabljajo zgolj za označevanje nasilja med vrstniki (mladoletniki), temveč tudi v družini, partnerskih odnosih, na delovnem mestu,[19] med otroki, mladostniki in polnoletnimi.[20] Še več, *bullying*, pojmovan kot sistematična zloraba moči,[21] postaja vse širša krovna oznaka ne glede na (1) starost (*bullying* med predšolskimi otroci in tudi med starostniki), (2) družbene odnose (tj. med vrstniki, v družini, med zakonci oziroma partnerji, na delu med zaposlenimi in med nadrejenimi in podrejenimi) in (3) družbene kontekste (na primer v predšolskem, šolskem, družinskem, zmenkarskem, zaporskem in zaposlitvenem kontekstu).[22] Psihologi[23] kot glavni razlog za tako široko pojmovanje nadlegovanja (in s tem implicitno tudi za spoprijemanje z njim) navajajo, da so ločene obravnave (in poimenovanja, kot so zloraba starostnikov, vrstniško nasilje, *mobbing* na delovnem mestu) zelo podobnih pojavov vodile v nesorazmerno poznavanje posamičnih oblik *bullyinga* in ločenost ekspertiz, ki bi združene lahko vodile do celovitejšega razumevanja in s tem kakovostnejše prevencije in intervencije.

V nobenem jeziku, razen v angleškem in nekaterih skandinavskih, tudi ni ustreznega izraza, ki bi pomenil isto ali podobno kot angleški *bullying*.[24] Zato ni nenavadno, da avtorji navajajo različne definicije nadlegovanja, na primer, da to nasilje označuje številne modalitete, kot so ustrahovanje, trpinčenje, nasilje, zafrkavanje, zlorabljanje, grožnje, maltretiranje, šikaniranje in mučenje (nanašajoč se na dejanja med mladoletniki).[25] Po najširše sprejeti opredelitvi je *bullying*

---

[19] Za nasilje na delovnem mestu se je v kontinentalni Evropi kot *terminus technicus* uveljavil *mobbing*.

[20] Lines, The Bullies (2008), str. 127 (*bullying* v družini), str. 171 (*bullying* na delovnem mestu). V iniciativi StopCyberbullying (2012) nasprotno menijo, da je ta pojav možen le med otroki in mladostniki; ko so vpleteni polnoletni, gre za *cyber-harassment* ali *cyberstalking*.

[21] Smith, Sharp, School Bullying (1994), str. 2.

[22] Po Monks, Coyne, A history of research into bullying, v: Bullying in Different Contexts (2011), str. 8.

[23] Monks, Coyne, prav tam, str. 8.

[24] Več Nocentini *et al.*, Cyberbullying, v: Australian Journal of Guidance & Counselling, 20 (2010) 2.

[25] Ostrman, Medvrstniško nasilje (2002), str. 138.

agresivno, namerno dejanje ali vedenje, ki ga posameznik ali skupina dlje časa izvaja zoper žrtev, ki se ne more uspešno braniti.[26] Nekateri avtorji[27] kot posebne oblike opredeljujejo *rasistični bullying* (usmerjen zoper žrtev zaradi njene rasne pripadnosti), *spolni bullying* (s seksistično motivacijo nadlegovalca) in tudi *kibernetski bullying*, ki ga povzročitelj izvaja prek spleta, mobilne ali druge informacijske tehnologije.

Glede posebne *kibernetske* oblike nadlegovanja je pojmovnih nejasnosti še več. Pojem *cyberbullying* se je v anglo-ameriškem okolju, kjer je nastal, spreminjal tudi tako, da se je najprej nanašal na odraslo populacijo, ki je sprva imela dostop do računalnikov in druge nove komunikacijske tehnologije. Kasneje, konec devetdesetih let, ko so starši opremili z računalniki in mobilnimi telefoni tudi otroke, pa je postala tema povezana z otroki (mladoletniki) ali nasploh mladimi.[28]

V literaturi danes prevladuje definicija, po kateri so temeljni elementi kibernetskega nadlegovanja:[29]

1. agresivno in namerno dejanje,
2. dejanje, ki ga izvršuje skupina ali posameznik,
3. dejanje, storjeno s pomočjo elektronskih oblik komuniciranja, predvsem prek interneta in z mobilnimi telefoni,
4. dalj časa trajajoče ali ponavljajoče se dejanje,
5. dejanje zoper žrtev, ki se ne more zlahka braniti, tj. nesorazmerje moči.

Ta oblika nadlegovanja se razlikuje od klasičnega nadlegovanja v dodatnih kriterijih – naklepu, ponavljanju in nesorazmerju moči dodajajo avtorji kriterij anonimnosti in publicitete dejanja.[30] Kljub temu ta definicija zaradi premalo določnih pojmov za potrebe kazenskega prava ni primerna. Kar ni usodno, saj samostojnega kaznivega dejanja (kibernetsko nadlegovanje) države ne poznajo: med pregledanimi kazenskimi zakoni ga izrecno ne omenjajo niti kanadski,[31]

---

[26] Whitney, Smith, A survey of the nature and extent of bullying, v: Educational Research, 35 (1993) 1, str. 7; Smith, Sharp, School Bullying (1994), str. 2; Lines, The Bullies (2008), str. 18; Rigby, New Perspectives on Bullying (2002), str. 27.

[27] Rigby, New Perspectives on Bullying (2002), str. 180–182.

[28] Rivers, Chesney, Coyne, Cyberbullying, v: Bullying in Different Contexts (2011), str. 212.

[29] Po akciji COST (*European Cooperation in Science and Technology*) IS0801 *Cyberbullying: coping with negative and enhancing positive uses of new technologies, in relationships in educational settings*, URL: https://sites.google.com/site/costis0801/ (15. 4. 2013).

[30] Nocentini *et al.*, Cyberbullying, v: Australian Journal of Guidance & Counselling, 20 (2010) 2, *passim*.

[31] Stanton, Beran, A review of legislation and bylaws relevant to cyberbullying, v: McGill Journal of Education, 44 (2009) 2, str. 245–260.

britanski[32] in avstralski kazenski zakonik[33] niti zakoniki Brazilije, Finske, Grčije, Litve, Nemčije in Španije.

Slovenjenje pojma *cyberbullying* je različno, uporabljajo se izrazi spletno in mobilno nadlegovanje,[34] nadlegovanje prek interneta,[35] spletno ustrahovanje,[36] žaljivo in neprijetno obnašanje na internetu.[37] Tudi klasifikacije so različne, o čemer več v nadaljevanju. Na splošno pa pojem *bullying* za potrebe tega prispevka prevajamo kot nadlegovanje, ki ga ločimo od kibernetskega (spletnega in mobilnega) nadlegovanja (angl. *cyberbullying*), ne glede na starost vpletenih (tj. nadlegovalcev, žrtev ali opazovalcev).

3. Oblike kibernetskega nadlegovanja

Oblike kibernetskega nadlegovanja sledijo razvoju novih storitev informacijske družbe, kar otežuje longitudinalne primerjave in medkulturne študije pojavnosti.[38] Na splošno kibernetsko nadlegovanje razvrščamo na odkrite ali prikrite oblike nadlegovanja,[39] oblike prek računalnika, mobilnika[40] ali štiridelno[41] kot

[32] Marczak, Coyne, Cyberbullying at school, v: Australian Journal of Guidance and Counselling, 20 (2009) 2, str. 182–193.

[33] Campbell, Butler, Kift, A school's duty to provide a safe learning environment, v: Australian and New Zealand Journal of Law and Education, 13 (2008) 2, str. 21–32.

[34] Zoranovič, Medvrstniško spletno in mobilno nadlegovanje (2011), str. *passim*.

[35] Informacijski pooblaščenec, Smernice glede varstva pred spletnim nadlegovanjem, URL: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice-glede-varstva-pred-spletnim-nadlegovanjem.pdf (15. 10. 2012).

[36] Lobe, Muha, Tveganja in varnost otrok na internetu, URL: www.eukidsonline.net (25. 4. 2013).

[37] Lobe, Muha, prav tam.

[38] Primerjaj taksonomije v: Smith, Mahdavi, Carvalho, Tippett, An Investigation into cyberbullying, its forms, awareness and impact, and the relationship between age and gender in cyberbullying (2006); Gillespie, Cyber-bullying and harassment of teenagers: The legal response, v: Journal of Social Welfare & Family Law 28 (2006) 2, str. 123–136; Bauman, Del Rio, Preservice teachers's responses to bully scenarios, v: Journal of Educational Psychology, 98 (2006) 1, str. 219–231; Slonje, Smith, Cyberbullying, v: Scandinavian Journal of Psychology, 49 (2008) 2, str. 147–154; Dooley, Cross, Hearen, Treyvaud, Review of Existing Australian and International Cyber-Safety Research (2009); Wunmi Grigg, Cyber-Aggression, v: Australian Journal of Guidance & Counselling 20 (2009) 2, str. 143–156.

[39] Spears, Slee, Owens, Johnson, Behind the scenes and screens, v: Zeitschrift für Psychologie/ Journal of Psychology, 217 (2009) 4, str. 189–196.

[40] Smith, Mahdavi, Carvalho, Fisher, Russell, Tippett, Cyberbullying: Its nature and impact in secondary school pupils, v: Journal of Child Psychology and Psychiatry, 49 (2008) 4, str. 376–385.

[41] Nocentini, Calmaestra, Schultze-Krumbholz, Scheithauer, Ortega, Menesini, Cyberbullying: Labels, Behaviours and Definition in Three European Countries, v: Australian Journal of Guidance & Counselling, 20 (2010) 2, str. 129–142.

(a) nadlegovanje prek besedil in izrečenih besed,[42] (b) prek vizualnih vsebin (na primer objavljanje, pošiljanje ali deljenje kompromitirajočih slik in filmov prek mobilnih telefonov ali interneta),[43] (c) z izključevanjem (na primer iz skupine v spletnem socialnem omrežju) in (č) z lažnim predstavljanjem za nekoga tretjega (kraja ali razkrivanje osebnih podatkov, uporaba imena drugega ali njegovega uporabniškega računa).[44]

Eno prvih raziskav o kibernetskem nadlegovanju sta opravila Noret in Rivers,[45] ki sta anketirala 11.227 britanskih učencev, starih od 11 do 15 let, in jih spraševala, ali so v zadnjem letu prejeli kakšno gnusno ali grozilno tekstovno sporočilo na mobilnik ali prek e-pošte. V raziskavi, ki so jo opravili Smith in drugi,[46] so razlikovali med sedmimi oblikami kibernetskega (vrstniškega) nasilja: (1) nasilje s pošiljanjem kratkih sporočil po mobilnih telefonih (SMS), (2) nasilje

---

[42] Na primer s prekomernimi telefonskimi klici ali esemesi kot *nadlegovanje prek mobilnega telefona,* katerega cilj je motiti naslovnika ali zmanjšati zmogljivosti njegove komunikacijske naprave; kot *nadlegovanje v spletnem socialnem omrežju*, ki obsega nadlegovanje prek besedil ali večpredstavnostnih oblik.

[43] Na primer *veselo klofutanje* (angl. *happy slapping*) in *sekstanje* (angl. *sexting*). Prvo je objavljanje posnetkov nasilja, ki obsega dve povezani dejanji: dejanje nasilnega vedenja do žrtve (sprva so bile to klofute, v praksi pa so prerasle v grobo fizično nasilje in samostojna kazniva dejanja, kot sta posilstvo in umor), ki ga opazovalci posnamejo s telefonom, posnetek pa žrtvi v posmeh objavijo (drugo dejanje) na spletnih straneh za izmenjavo multimedijskih vsebin (na primer *Youtube*). *Sekstanje* (angl. *sexting*) pa je pošiljanje spolno eksplicitnih vsebin (v obliki slik, filmov ali besedil). Značilen je primer, ko oseba fotografira lastno telo ali njegov del in posnetke pošilja naslovniku v obliki multimedijskega MMS-sporočila. V širšem smislu pojem obsega pošiljanje spolnih vsebin nasploh, tj. bodisi osebam, ki se s tem strinjajo, bodisi tistim, ki se s prejemanjem ne strinjajo, in ne glede na starost, tj. med mladoletniki ali med polnoletnimi ali med mladoletnimi in polnoletnimi udeleženci. V ožjem smislu pa seksting obsega zgolj pošiljanje spolno eksplicitnih vsebin osebi, ki v to ni vnaprej privolila. Pomembna razlika je tudi med primarnim in sekundarnim *sekstingom*: pri prvem pošiljatelj pošilja gradivo, ki ga je ustvaril sam in ga deli prostovoljno, pri drugem pa nastane takrat, ko je pošiljatelj zgolj prejemnik takšnega gradiva, ki ga posreduje naprej tretji osebi, kar običajno stori brez vednosti ali soglasja izdelovalca gradiva. Glej še Schmitz, Siry, Teenage folly or child abuse?, v: Policy & Internet, 3 (2011) 2, str. 19; Calvert, Sex, Cell Phones, Privacy and the First Amendment, Comm Law Conspectus, 18 (2009), str. 30.

[44] Nekatere oblike nadlegovanja lahko spadajo v eno ali drugo skupino, na primer *pošiljanje »ekstremnih« vsebin*, ki šokirajo (na primer nasilje, posneto v živo); *smetenje* (angl. *spamming*) drugače od neželenih vsebin cilja na zasipavanje prejemnika z nenaročeno elektronsko pošto poljubne vsebine; *poplavljanje* (angl. *flooding*) je podobno smetenju v tem, da je namenjeno povzročanju nevšečnosti s kopičenjem elektronskih sporočil v poštnem nabiralniku, zmanjševanju zmogljivosti IKT-naprave in/ali povečevanju stroškov prenosa podatkov, a se od razlikuje v tem, da gre pri poplavljanju za večkratno pošiljanje enakega sporočila.

[45] Noret, Rivers, The prevalence of bullying by text message or email (2006), cit. po Slonje, Smith: Cyberbullying, v: Scandinavian Journal of Psychology, 49 (2008) 2, str. 147.

[46] Smith *et al.*, An Investigation into Cyberbullying, its Forms, Awareness and Impact ... (2006), *passim*.

s pošiljanjem slik in video posnetkov prek mobilnih telefonov (multimedijska sporočila – MMS), (3) nasilje s (čezmernim) klicanjem po mobilnih telefonih, (4) nasilje prek e-pošte, (5) nasilje v klepetalnicah, (6) nasilje prek sistemov takojšnjega sporočanja in (7) nasilje z objavami na spletnih straneh.

Ker so z razvojem IKT ločnice med terminalnimi napravami in storitvami informacijske družbe postale zabrisane (na primer med mobilnimi in stacionarnimi napravami, telefonskimi in video napravami, računalniki in telefoni, televizijo in internetom), je danes težko ohranjati prvotne členitve. Z razvojem pametnih telefonov je spletno nadlegovanje lahko tudi mobilno, naprave se združujejo (na primer internet in telefon v »pametni« telefon, televizija in internet v »pametno TV«). Vsaka taksonomija kibernetskega nadlegovanja je zato odraz razvitosti IKT v izbranem času in prostoru (npr. modnosti Facebooka v izbrani starostni skupini v izbrani državi). Tako sta na primer Slonje in Smith[47] ugotovila, da so bile v kasnejši raziskavi frekvence nekaterih pojavnih oblik tako redke (npr. sistemi takojšnjega sporočanja so postali *démodé*), da sta predlagala le štiri kategorije: (1) nasilje s pošiljanjem kratkih sporočil po mobilnih telefonih, (2) nasilje prek e-pošte, (3) nasilje s klicanjem po mobilnih telefonih in (4) nasilje, povezano z razširjanjem slik in video posnetkov.

Druge raziskave so ločevale oblike kibernetskega ustrahovanja po vsebini, ne po mediju ali vrsti storitve informacijske družbe. Willard[48] je navedel sedem kategorij: podžiganje (*flaming*),[49] nadlegovanje, zaničevanje, lažno predstavljanje, zavajanje, izključevanje in (kibernetsko) zalezovanje. V slovenski raziskavi[50] so bile raziskane tri temeljne oblike in sedem podoblik. Med prvimi je bilo: (1) nadlegovanje po internetu, (2) nadlegovanje po spletnem socialnem omrežju in (3) nadlegovanje po mobilnem telefonu, med drugimi pa: (a) prekomerno

---

47 V Slonje, Smith, Cyberbullying, v: Scandinavian Journal of Psychology 49 (2008) 2, *passim*.

48 Willard, Cyberbullying and Cyberthreats (2006), *passim*.

49 *Podžiganje* (angl. *flaming*) je v internetnem žargonu objava na spletnem forumu, v klepetalnici, blogu, spletnem socialnem omrežju ali na drugi platformi, kjer uporabniki sami prispevajo vsebine, ki napadajo drugo osebo ali skupino z odprtim izražanjem jeze in besa. Včasih se kot sinonim uporablja *trolanje*, ki označuje nasploh objavljanje žaljivih, sovražnih, hujskaških sporočil v spletnih skupnostih, na primer po spletnih forumih, klepetalnicah, blogih ali po spletnih socialnih omrežjih, katerih namen je spodbuditi emocionalne reakcije udeležencev ali drugače motiti normalno diskusijo o določeni temi ali vzbuditi pozornost (angl. *troll* je oseba, ki izvršuje takšno dejanje, po skandinavskih mitičnih gozdnih bitjih). Obstaja več metod »trolanja«, na primer »skrbeči trol« nastopa pod pretvezo, da deli prepričanja spletne skupine, z namenom ustvariti zmedo v skupini in v njej zasejati dvom in strah, »dominacijsko trolanje« itn. Več v Rivers, Chesney, Coyne, Cyberbullying, v: Bullying in Different Contexts (2011), str. 212.

50 Završnik, Sedej, Spletno in mobilno nadlegovanje v Sloveniji, v: Revija za kriminalistiko in kriminologijo, 63 (2012) 4, *passim.*

pošiljanje SMS/MMS-sporočil, (b) prekomerno pošiljanje e-pošte, (c) vzpostavljanje stikov v spletnih socialnih omrežjih s strani neznancev, (č) vzpostavljanje stikov v spletnih socialnih omrežjih s strani neznancev, ki ne uporabljajo svojega pravega imena, (d) objavljanje fotografij v spletnem socialnem omrežju brez uporabnikove vednosti ali privolitve, (e) označevanje obraza z imenom na fotografijah drugih uporabnikov spletnega socialnega omrežja (angl. *tagging*) in (f) objavljanje spremenjenih/predelanih fotografij posameznika brez njegovega dovoljenja (angl. *morphing*). V drugi slovenski raziskavi SAFE-SI[51] so razlikovali med spletnim ustrahovanjem, »mobilnim ustrahovanjem ali mučenjem, ko se uporabniki med seboj žalijo, grozijo ali izsiljujejo prek SMS-sporočil in telefonskih klicev«, in sekstingom, ki so ga opredelili kot pošiljanje in prejemanje sporočil s spolno vsebino. V vseevropski raziskavi *EU Kids Online*, ki je zajela tudi Slovenijo in merila tveganja in varnost od 9 do 16 let starih otrok na internetu, so med tveganji in negativnimi posledicami (6 oblik) merili tudi žaljivo in neprijetno obnašanje na internetu (*bullying online*) in posebej seksting.[52]

4. Posledice kibernetskega nadlegovanja

4.1. Primerjava škodljivosti kibernetskega in tradicionalnega nadlegovanja

Škodljivost kibernetskega nadlegovanja sega, kot kažejo predstavljeni primeri in oblike, od nevšečnosti do hudih posegov v osebnostne in premoženjske pravice, ki izpolnjujejo znake samostojnih kaznivih dejanj. Avtorji, ki preučujejo škodljive posledice, ugotavljajo, da so te pri kibernetskem nadlegovanju lahko tudi *hujše* kot pri tradicionalnem.[53] Storilčeva anonimnost – zamaskiranost z anonimnimi uporabniškimi računi, ki jih je težko ali nemogoče izslediti (npr. zaradi uporabe anonimizacijskih orodij, kot je omrežje Tor) – povečuje strah žrtve. Ko grožnje prihajajo iz neznanega vira, žrtev ne more pravilno oceniti

[51] SAFE-SI, Osveščanje o varni rabi interneta in novih tehnologij (2012), URL: http://www.safe.si/c/1482/Soocenje_z_ustrahovanjem_na_internetu/?preid=978.

[52] Lobe, Muha, Tveganja in varnost otrok na internetu, URL: www.eukidsonline.net.

[53] Campbell, Cyberbullying, v: Australian Journal of Guidance and Counselling, 15 (2005) 1, str. 69; Smith *et al.*, An Investigation into Cyberbullying, its Forms, Awareness and Impact... (2006), *passim*; Patchin, Hinduja, Bullies move beyond the schoolyard, v: Youth Violence and Juvenile Justice, 4 (2006) 2, *passim*; Ottenweller, Cyberbullying, v: Valparaiso University Law Review, 41 (2007) 3, *passim*.

resnosti grožnje in njene izvedljivosti, niti oceniti, kdo ali koliko ljudi grožnje pošilja.[54]

Kibernetska različica je permanentnejša zaradi trajnejše povezanosti žrtev v splet, ko ni mogoče preprosto »izklopiti« naprave. Posebej mladi prejemajo socialne potrditve pri druženju po različnih internetnih storitvah in so prek njih povezani in vključeni v socialno življenje vrstnikov. Večji del svojega delovnega in prostega časa preživljajo povezani na internet in tam pridobivajo svoj družbeni status, kar je za posameznikov identitetni razvoj posebej pomembno. Pred kibernetskim nadlegovalcem se zato ni mogoče skriti, žrtev je dostopna kjerkoli in od koderkoli.[55]

Nadlegovalci lahko dosežejo tudi veliko večjo množico naslovnikov kot kadarkoli doslej. Hammack zato slikovito meni:[56] »Posamezniki niso omejeni z glasnostjo svojega glasu.« Javna narava interneta in preprosta distribucija informacij sta v prid nadlegovalcem.[57]

Manko neverbalnih elementov komunikacije in nevidnost žrtvine takojšnje neposredne reakcije povzročita, da je nadlegovalec zapeljan v stopnjevanje pritiska, medtem ko bi ob žrtvini vidni reakciji prej prenehal z dejanji. Dezinhibicijski učinek interneta, tj. (navidezna ali resnična) anonimnost in posrednost komunikacije, lahko povzroči, da se storilec nečesa hipoma domisli in to s klikom miške brez presojanja posledic tudi izvede. Tudi manjši trud za izvajanje nadlegovanja pospeši kibernetsko nadlegovanje. Kot meni Harlin Goodno,[58] je internetno nadlegovanje v primerjavi s klasičnim telefonskim nadlegovanjem preprostejše: če je klic po telefonu še zahteval nadlegovalčevo dejavnost in njegov čas, nadlegovanje z e-pošto zahteva oblikovanje zgolj enega sporočila, ki ga računalnik samodejno pošilja žrtvi.

Pomanjkanje nadzora nad objavljenimi osebnimi podatki in javna narava spletnega okolja sta nadaljnja dejavnika, zaradi katerih so kibernetske oblike nadlegovanja lahko hujše od tradicionalnega.[59] Žaljive in drugače kompromitira-

[54] Hammack, The Internet Loophole, v: Columbia Journal of Law and Social Problems, 36 (2002) 65, str. 81.

[55] Harlin Goodno, Cyberstalking, a New Crime, v: Missouri Law Review, 72 (2007), str. 129.

[56] Hammack, The Internet Loophole, v: Columbia Journal of Law and Social Problems, 36 (2002) 65, str. 81.

[57] Ruedy, Repercussions of a MySpace Teen Suicide: Should Anti-bullying Laws be Created?, v: North Carolina Journal of Law & Technology, 9 (2008) (2), str. 328.

[58] Harlin Goodno, Cyberstalking, a New Crime, v: Missouri Law Review, 72 (2007), str. 128–132.

[59] Walrave, Michel; Demoulin, Marie; Heirman, Wannes; Van der Perre, Aurélie: Onderzoeksrapport Cyberpesten (2009), URL: http://www.internetobservatory.be/internet_observatory/pdf/brochures/Boek_cyberpesten_nl.pdf, v: Lievens, Bullying and sexting in social networks from a legal perspective, URL: http://ssrn.com/abstract=2088166, str. 3.

joče vsebine je težko in pogosto nemogoče izbrisati, kot kažejo primeri neuspešnih izvršitev sodb zaradi kršitev osebnostnih pravic. Sporno gradivo se množi in prenaša po različnih spletnih straneh in gostuje na strežnikih po svetu. Škoda je kljub uspešnemu kazenskemu pregonu ali civilnopravnim sodbam v korist žrtev dejansko *konstantna*. Žaljive, kompromitirajoče ali nadlegovalne vsebine je včasih nemogoče zbrisati in to gradivo lahko spodbuja bralce k nasilju, čeprav je nadlegovalec svoja stališča že spremenil.[60]

Bocij[61] večjo nevarnost kibernetske različice utemeljuje tudi s posebnostjo, da ni nujno, da storilec kibernetskega nadlegovanja žrtev tudi osebno »pozna«. To po eni strani sproža dezinhibicijske učinke, po drugi strani pa resnosti ali nevarnosti dejanja ne zmanjšuje sicer pomembna okoliščina tradicionalnega nadlegovanja, namreč da mora biti storilec fizično blizu žrtve, temveč lahko prebiva tudi v drugi državi ali na drugem koncu sveta. Grožnje kljub fizični oddaljenosti niso nič manj kredibilne, nadlegovalska dejanja nič manj škodljiva.

Vse navedeno kaže, da ni mogoče enoznačno *in abstracto* trditi, da je kibernetska oblika nadlegovanja blažja (ali težja). Gre za novosti, ki ne bi obstajale, če ne bi bilo interneta, mobilne telefonije in drugih informacijsko-komunikacijskih tehnologij, njihovi učinki pa so v primerjavi s tradicionalnimi oblikami nadlegovanja na splošno manj raziskani. Ne glede na dileme o hujši ali blažji naravi kibernetske različice nadlegovanja v nadaljevanju podajam pregled raziskav o *psiholoških* posledicah kibernetskega nadlegovanja, ki se nanašajo na vse uporabnike, kadar veljajo posebej za mladoletnike, pa na to posebej opozorim.

4.2. Psihološka škoda zaradi kibernetskega nadlegovanja

Žrtve kibernetskega nadlegovanja se počutijo *jezne* (50 odstotkov moških – M, 56 odstotkov žensk – Ž), *frustrirane* (46 odstotkov M, 56 odstotkov Ž), *žalostne* (44 odstotkov M, 49 odstotkov Ž), *osramočene* (41 odstotkov M, 36 odstotkov Ž), nekaterih pa se dejanja ne dotaknejo (54 odstotkov M, 52 odstotkov Ž).[62] Osramočenost je večja v primerih, ko si uporabniki zaupajo gesla za dostop do e-pošte ali profila v spletnem socialnem omrežju (zaradi tega so sicer trikrat pogosteje žrtve spletnega nadlegovanja) ali ko lahkomiselno privolijo v

[60] Hammack, The Internet Loophole, v: Columbia Journal of Law and Social Problems, 36 (2002) 65, str. 82.

[61] Bocij, Cyberstalking (2004), str. 107.

[62] Po Hinduja, Patchin, Bullies move beyond the schoolyard, v: Youth Violence and Juvenile Justice, 4 (2006) 2, str. 158 in nasl.

lokacijsko sledenje po spletnih socialnih omrežjih in aplikacijah (na primer v spletnem družabnem omrežju Facebook ali storitvi Google Latitude).[63] Viktimizacija vpliva na *samopodobo*, ki je na lestvici (od 1 – slaba do 4 – dobra) pri žrtvah 2,76, pri tistih, ki še niso bili žrtve, pa 3,01.[64] V slovenski raziskavi o čustvenem opismenjevanju je bilo za šolajočo se mladino tudi ugotovljeno, da največ neprijetnih čustev doživljajo učenci, ki trdijo, da so doživeli nadlegovanje po telefonu, kar je za avtorje pomemben kazalnik, da gre za posebej ogrožene in ranljive učence oziroma za zelo problematične oblike viktimiziranosti s hujšimi čustvenimi posledicami.[65]

Škodljivost kibernetskega nadlegovanja se kaže nadalje v tem, da je dejavnik tveganja pri razvoju simptomov *depresije*.[66, 67] Takšne so ugotovitve za mladoletnike, ki izjavljajo, da jih boli fizično in psihično, da se počutijo ničvredne, da gredo strahoma v šolo ali da jim je tam nerodno.[68] Adolescenti imajo *psihosomatske* simptome, kot so glavoboli, nespečnost in prebavne težave, najhujše psihiatrične in psihosomatske simptome pa imajo tisti, ki so udeleženi v kibernetskem nadlegovanju v vlogi žrtev in storilcev.[69]

Kibernetsko nadlegovanje je po definiciji dalj časa trajajoče dejanje, kar pa ne pomeni, da posamično dejanje ni škodljivo. Tudi enkratna agresivna grožnja lahko povzroči čustveno škodo in skrb glede prihodnosti.[70] V zvezi z oceno resnosti grožnje je pomembna tudi ugotovitev, da posamezniki, ki imajo več znanja o IKT in so bolj tehnološko vešči, ob izkušnji kibernetskega zalezovanja občutijo manjši stres.[71]

Dodatno so bile dokazane statistično pomembne povezave med kibernetskim nadlegovanjem in težavami v družini, šolskim uspehom in odklonskim

---

63 Hinduja in Patchin, prav tam.

64 Hinduja, Patchin, Bullying Beyond the Schoolyard (2008), *passim*.

65 Muršič, Brvar, Izbor (s čustvi povezanih) ugotovitev naše raziskave, v: Znanje o čustvih za manj nasilja v šoli (2010), str. 23.

66 Hinduja, Patchin, Bullying Beyond the Schoolyard (2008), *passim*.

67 Perren, Dooley, Shaw, Cross, Bully/Victim Problems in Schools and in Cyberspace, v: Child and Adolescent Psychiatry and Mental Health 4 (2010) 28, URL: http://www.capmh.com/content/4/1/28 (13. 2. 2013); Gradinger, Strohmeier, Spiel, Traditional Bullying and Cyberbullying, v: Zeitschrift fur Psychologie/Journal of Psychology, 217 (2009) 4, *passim*.

68 Hinduja, Patchin, Bullying Beyond the Schoolyard (2008), str. 85.

69 Sourander, Brunstein Klomek, Ikonen, Lindroos, Luntamo, Koskelainen, Ristkari, Helenius, Psychology Risk Factors Associated with Cyberbullying among Adolescents, v: Archives of General Psychiatry, 67 (2010) 7, str. 724 in nasl.

70 Dzuka, Dalbert, Aggression at School, v: Studia Psychologica, 49 (2007) 4, str. 315.

71 Bocij, Cyberstalking (2004), str. 107.

vedenjem.[72] Raziskovanje vzročnosti je sicer dalo nasprotujoče si rezultate o povezanosti med slabim šolskim uspehom in kibernetskim nadlegovanjem: učenci so lahko manj uspešni v šoli zaradi kibernetskega nadlegovanja, velja pa tudi nasprotno, da so žrtve nadlegovanja zato, ker so slabi učenci. Simptomi so predhodniki in posledice kibernetskega nadlegovanja.[73]

Glede dolgotrajnosti posledic je dejstvo, da je kibernetsko nadlegovanje vedno verbalno in v osnovi psihološko nasilje, manj pomembno. Posledice so lahko posebej pri mladoletnikih tudi dolgotrajnejše,[74] negativni učinki besednega nadlegovanja lahko učinkujejo na razvoj pozitivne samopodobe, zastavljanje ciljev in emocionalni razvoj.[75] Relacijske viktimizacije imajo lahko bolj škodljive učinke na šolski uspeh kot neposredno fizično nadlegovanje, ker so bolj boleče na dolgi rok ali pa so osredotočene na razred, kar moti otrokovo zbranost pri šolskih nalogah.[76] Glede storilcev pa je bila ugotovljena močna povezava med gledanjem nasilnih vsebin in resno nasilnim vedenjem.[77]

Na navedene škodljive posledice se je mogoče odzvati prilagojeno potrebam specifičnih skupin uporabnikov (npr. mlajšim od 14 let, starejšim polnoletnim, mlajšim polnoletnim) in z upoštevanjem različnih faz: v prevencijski fazi z zmanjševanjem tveganj za nastanek primera, nato z opolnomočenjem uporabnikov pri konfrontaciji oziroma odzivanju na potekajoče primere nadlegovanja, v fazi reakcije pa se obravnavajo že izvršeni primeri. Zadnja faza obsega pravne možnosti, na primer povrnitev škode in možnost kazenskega pregona storilcev za najhujše oblike nadlegovanja in disciplinske ukrepe po šolski zakonodaji, ter programe pomoči za odboj negativnih učinkov nadlegovanja in izboljšanje počutja žrtve.

---

72 Mitchell, Ybarra, Finkelhor, The Relative Importance of Online Victimization in Understanding Depression, Delinquency, and Substance Abuse, v: Child Maltreatmant, 12 (2007) 4, str. 321.

73 Kift, Campbell, Butler, Cyberbullying in social networking sites and blogs, v: Journal of Law, Information and Science, 20 (2010) 2, str. 66-68.

74 Reid, Monsen, Rivers, Psychology's contribution to understanding and managing bullying within schools, v: Educational Psychology in Practice, 20 (2004) 3, str. 244.

75 Kift, Campbell, Butler, Cyberbullying in social networking sites and blogs, v: Journal of Law, Information and Science, 20 (2010) 2, str. 66-67.

76 Kift, Campbell, Butler, prav tam, str. 67.

77 Ybarra, Diener-West, Markow, Leaf, Hamburger, Boxer, Linkages between internet violence and serioulsy violent behaviour, v: Pediatrics, 122 (2008) 5, *passim*.

5. Soočanje s kibernetskim nadlegovanjem

5.1. Tridelna shema soočanja

Soočanje s kibernetskim nadlegovanjem obsega tri domene: zmanjševanje tveganja za nastop primera kibernetskega nadlegovanja, boj zoper potekajoči primer in odboj negativnih posledic izvršenega dejanja. Tridelna shema soočanja je pomembna za vse uporabnike IKT ne glede na starost. Ker pa so bile škodljive posledice kibernetskega nadlegovanja v doslejšnjih raziskavah ugotovljene večinoma pri mladoletnikih, se raziskave o strategijah in načinih soočanja pogosto nanašajo tudi na to populacijo. Tako Perren in drugi (2012) v metaštudiji 225 raziskav o kibernetskem nadlegovanju v navedenih domenah prepoznavajo naslednje načine soočanja: (1) zmanjševanje tveganj za nastanek primera obsega strategije za zmanjšanje tradicionalnega nadlegovanja (kot so izboljševanje šolskega ozračja, treningi socialnih veščin) na eni strani in specifične strategije (kot so zmanjševanje tvegane uporabe interneta s programi ozaveščanja otrok in staršev, treningi empatije z uporabo zgodb) na drugi strani, pri čemer se za najuspešnejše izkazujejo strategije, ki vključujejo šole in družine ter krepijo moč otrok; (2) boj zoper konkretno kibernetsko nadlegovanje obsega bodisi problemsko soočanje (če oseba verjame, da lahko z lastnimi viri odpravi problem) bodisi čustveno odzivanje (če oseba ne verjame, da lahko sama bistveno spremeni stresno situacijo). V prvo skupino spadajo tehnični ukrepi (npr. brisanje sporočil ali blokiranje pošiljatelja), iskanje podpore pri starših, učiteljih in vrstnikih (tj. ali se mladi obrnejo na druge osebe in na katere), v drugo pa izogibajoče in emocionalno osredotočene strategije (npr. ignoriranje, izogibanje, občutki krivde); (3) v domeni odboja negativnih učinkov in izboljšanja počutja žrtve so ukrepi emocionalne podpore in odpravljanja občutkov krivde žrtev.

Celovita večdimenzionalna nacionalna strategija soočanja s kibernetskim nadlegovanjem bi morala upoštevati vse omenjene ravni: izobraževalno raven, emocionalno opismenjevanje, tehnično raven in tehnične veščine ter pravne odzive. Vse te ravni bi morale biti prilagojene specifičnim skupinam uporabnikov. Takšna strategija bi zahtevala tudi vključitev vseh akterjev, ki že sodelujejo ali bi utegnili sodelovati pri soočanju na eni ali vseh treh ravneh. Konkretno v Sloveniji to obsega mrežo deležnikov, ki se neposredno ukvarjajo z opolnomočenjem uporabnikov, zagotavljanjem informacij in drugim oblikami prevencijske in reaktivne dejavnosti, povezane s kibernetskim nadlegovanjem, sestavljajo pa jo vladne,[78]

[78] Od *državnih organov* so to v Sloveniji Agencija za pošto in elektronske komunikacije, Informacijski pooblaščenec RS, Varuh človekovih pravic RS, ministrstvo, pristojno za tehnologijo

nevladne[79] in hibridne institucije,[80] akademske organizacije,[81] stanovska združenja ter gospodarski subjekti in njihove kolektivne organizacije in društva.[82]

Če je za klasično kriminaliteto značilno, da se žrtve najprej in najpogosteje obrnejo prav na organe odkrivanja in pregona kaznivih dejanj, pri kibernetski kriminaliteti za nadzor skrbi mreža akterjev,[83] v kateri so organi odkrivanja in pregona kaznivih dejanj pogosto manj središčni akter,[84] na katerega se žrtve niti ne želijo obrniti.[85] Celovita nacionalna strategija bi zato morala vključiti deležnike, ki delujejo na vseh treh ravneh soočanja (preventivna dejavnost, boj zoper konkretne primere nadlegovanja in odboj negativnih posledic) in prilagojeno potrebam specifičnih skupin uporabnikov.

(Direktorat za informacijsko družbo objavlja vsebine s področja nevarnosti na internetu na URL: http://www.informacijskadruzba.si/eucenje/, 25. 4. 2013), Varuh medijskih pravic in Tržni inšpektorat RS. Aktivnosti na področju preprečevanja spletnega zmenkarskega nadlegovanja je izvajal tudi Urad za enake možnosti, glej Robnik, Sonja, Nasilje med zmenkanjem (2009), URL: www.uem.gov.si (25. 4. 2013).

79 *Nevladne organizacije,* kot ta Zveza potrošnikov Slovenije, ki je vodila projekt Nasvetzanet, ali Zveza prijateljev mladine Slovenije, ki vodi projekt TOM – telefon pomoči.

80 *SI-CERT* (*Slovenian Computer Emergency Response Team*), osrednja institucija za varstvo računalniških omrežij v Sloveniji, ki posreduje pri internetnih incidentih za vsa računalniška omrežja v Sloveniji in izvaja projekt Varni na internetu. URL: https://www.varninainternetu.si/ (25. 4. 2013).

81 Na primer *Center za varnejši internet SAFE-SI*, ki je nacionalna točka evropskega programa Varnejši internet 2009–2013. Financirata ga Generalni direktorat za informacijsko družbo pri Evropski komisiji in Ministrstvo za Visoko šolstvo, znanost in tehnologijo, URL: http://ec.europa.eu/information_society/activities/sip/policy/programme/index_en.htm (28. 12. 2012).

82 *Gospodarska zbornica Slovenije* na primer skrbi za samoregulacijo ponudnikov, ki ponujajo storitve informacijske družbe, z mehanizmi, **kot je Kodeks ravnanja izvajalcev javnih elektronskih** komunikacijskih storitev za zaščito uporabnikov (2013), URL: http://www.arnes.si/obvestila/obvestilo/article/na-dan-varne-rabe-interneta-slovenski-mobilni-operaterji-in-internetni-ponudniki-podpisali-kodeks-za.html (12. 4. 2013).

83 Wall, Cybercrime (2007), str. 157.

84 Izsledki raziskave o kibernetskem nadlegovanju v Sloveniji to neposredno dokazujejo. Vnovične žrtve nadlegovanja po internetu in nadlegovanja v spletnem socialnem omrežju bi se namreč v manjši meri obrnile na policijo kot tisti uporabniki spleta, ki še niso bili žrtve tovrstnega nadlegovanja. Po Završnik, Sedej, Spletno in mobilno nadlegovanje v Sloveniji, v: Revija za kriminalistiko in kriminologijo, 63 (2012) 4, str. 274–276.

85 Težavo zanikanja viktimizacij v kibernetskem prostoru obravnava predlog Direktive Evropskega parlamenta in Sveta o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij v Uniji (COM(2013) 48 final, 7. 2. 2013), ki določa obveznost, da podjetja kritične internetne infrastrukture, podjetja iz bančnega in borznega sektorja, energetska, prometna in druga infrastrukturna podjetja prijavijo kibernetske incidente pristojni nacionalni inštituciji. Česa podobnega pri tradicionalnih oblikah kriminalitete ne poznamo.

5.2. Odzivanje s kazenskim pravom

5.2.1. Umestitev v ustavnopravni okvir

Inkriminiranje kibernetskega nadlegovanja zaradi simbolno posredovane narave trči ob pomembno ustavnopravno materijo: pravno relevantna analiza inkriminiranja se začenja pri možnostih *omejitev pravice do svobode govora*.[86] Pravico do svobode govora[87] je kot relativno pravico mogoče omejiti,[88] med razlogi za omejevanje pa so tudi ugled in pravice drugih, kakršna je pravica do zasebnosti.[89] V primeru *K.U. proti Finski* (2008) je tako Evropsko sodišče za človekove pravice odločilo, da je bila mladoletnikova zasebnost (8. člen EKČP) kršena v obliki lažnega oglaševanja spolnih storitev, ki je bilo oblika kibernetskega nadlegovanja. Vrhovno sodišče ZDA in ameriška ustavnopravna teorija sta si pri tem postavila vprašanje, ali bi morebitna zakonodaja, ki bi prepovedovala kibernetsko nadlegovanje, zadostila standardom zaščitenega govora po prvem amandmaju ameriške ustave. V ZDA sta relevantna vodilna primera[90] *Watts proti U.S.*,[91] v katerem je sodišče odločilo, da »resnične grožnje« (angl. *true threat*) niso ustavno zaščiteni govor, in *Brandenburg proti Ohio*,[92] v katerem je sodišče odločalo o spodbujanju ali hujskaštvu drugih k nezakonitemu početju (angl. *inciting speech*). Inkriminacija bi zato morala upoštevati obsežno doktrino svobode govora in njenih dopustnih omejitev.

Drugo načelno vprašanje pri inkriminaciji je vprašanje umestitve posameznih oblik kibernetskega nadlegovanja. *Seksting* je bil vključen v inkriminacije, povezane s posedovanjem, razpečevanjem in drugimi prepovedanimi ravnanji, povezanimi z otroško pornografijo, kar je nesorazmerno omejilo pravico do svobode izražanja. Konvencija Sveta Evrope o kibernetski kriminaliteti[93] je otroško pornografijo opredelila kot gradivo, na katerem je upodobljena oseba, ki *je videti* kot mladoletnik (tj. čeprav je stara nad 18 let), in tudi gradivo *fiktivne* otroške pornografije (tj. računalniško ustvarjena »virtualna« pornografija, ki ne

---

86 Jameson, Cyberharassment, v: Commlaw Conspectus, 17 (2008) 1, str. 231–236.

87 Glej na primer 10. člen Konvencije Sveta Evrope o človekovih pravicah (EKČP), Ur. l. RS, MP, št. 7-41/1994.

88 Drugi odstavek 10. člena EKČP.

89 Člen 8 EKČP.

90 Po Ruedy, Repercussions of a MySpace Teen Suicide, v: North Carolina Journal of Law & Technology, 9 (2008) 2, str. 323–346; King, Constitutionality of Cyberbullying Laws, v: Vanderbilt Law Review, 63 (2010) 3, str. 845–884

91 394 U.S. 705 (1969).

92 395 U.S. 444 (1969).

93 Konvencija Sveta Evrope o kibernetski kriminaliteti, Ur. l. RS, MP, št. 17/2004.

upodablja resničnih oseb) (9. člen navedene konvencije). S tem je zajela še seksting in kriminalizirala tudi prostovoljna dejanja mladoletnikov in vrstnikov.[94]

Kasnejša Konvencija Sveta Evrope o zaščiti otrok pred spolnim izkoriščanjem in spolnim zlorabljanjem[95] in Direktiva Evropskega parlamenta in Sveta o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji[96] sta za seksting določili izjemo. Po direktivi produkcija in posest nista kaznivi, če sta posledica konsenzualnega in prostovoljnega dejanja otrok, ki lahko pravno veljavno privolijo v spolnost (8. člen), Lanzarotska konvencija pa državam podpisnicam dovoljuje (20. člen), da ne inkriminirajo proizvodnje in posesti otroškega pornografskega gradiva, če so osebe na gradivu dosegle starost, ko lahko pravno veljavno privolijo v spolnost, in če so podobe proizvedene in v posesti s soglasjem upodobljenih oseb in samo za njihovo zasebno rabo.[97] Izločitev teh dejanj s področja, ki ureja prepovedi, povezane z otroško pornografijo, je bila zato v teoriji večinsko označena kot primerna.[98]

5.2.2. Inkriminiranje – pro et contra

Nekatere oblike kibernetskih dejanj izpolnjujejo znake *samostojnih kaznivih dejanj*.[99] Večina drugih oblik si po svoji nevarnosti v skladu z načelom *ultima ratio* ne zasluži kazenskopravne intervencije. Nevšečnosti in nečednosti še niso (in naj ne bodo) kazniva dejanja. Danes ima pojem nasilja poleg fizične še psihično, relacijsko, razredno, strukturno dimenzijo, kar je privedlo do tega, da je postala

---

94 Lievens, Bullying and sexting in social networks from a legal perspective (2012), *passim.*

95 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (t. i. Lanzarotska konvencija, velja od 1. 7. 2010, Slovenija jo je podpisala, a še ne ratificirala).

96 Direktiva 2011/92/EU Evropskega parlamenta in Sveta z dne 13. decembra 2011 o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji in nadomestitvi Okvirnega sklepa Sveta 2004/68/PNZ.

97 Točka 3 20. člena Lanzarotske konvencije.

98 Po Lievens, prav tam.

99 Npr. grožnja (135. člen KZ-1), mučenje (135.a člen), neupravičeno prisluškovanje in zvočno snemanje (137. člen), neupravičeno slikovno snemanje (138. člen), kršitev tajnosti občil (139. člen), nedovoljena objava zasebnih pisanj (140. člen), zloraba osebnih podatkov (143. člen), kazniva dejanja zoper čast in dobro ime, spolno nasilje (171. člen), spolni napad na osebo, mlajšo od petnajst let (173. člen), prikazovanje, izdelava, posest in posredovanje pornografskega gradiva (176. člen), šikaniranje na delovnem mestu (197. člen), izsiljevanje (213. člen), napad na informacijski sistem (221. člen), uporaba ponarejenega negotovinskega plačilnega sredstva (247. člen), izdaja tajnih podatkov (260. člen), javno spodbujanje sovraštva, nasilja ali nestrpnosti (297. člen), izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje (306. člen).

beseda nasilje označevalec, ki ne označuje skoraj nobene stvarnosti več.[100] Kazenskopravna zaščita pred različnimi pojavnimi oblikami nasilnosti zato ne bi smela slediti kulturnemu vzorcu, ki želi družbo »očistiti« vseh konfliktnih situacij.

Vmes pa so tudi dejanja, ki kažejo, da zaradi nekaterih značilnosti obstoječa mreža inkriminacij ne zadostuje. Vrednotenje nevarnosti in škodljivosti teh namreč kaže, da inkriminacije ne zajamejo nove kriminalne količine, hkrati pa interpretativno širjenje pomena obstoječih norm lahko privede do kršitev načela enakosti in načela *lex certa*.

Uvodno omenjeni primer Lori Drew, obtožene za nadlegovanje v spletnem socialnem omrežju MySpace, namreč potrjuje, da lahko tudi odsotnost specifičnih inkriminacij vodi v širjenje območja kriminalnega, ne le njihovo dodajanje. Prav odsotnost inkriminacije je tožilstvo vodila v pretirano ekstenzivne razlage primera, ko je poskušalo doseči obsodbo s *prima facie* krivičnimi obtožbami Lori Drew, kot so na primer očitki o storitvi kibernetskih kaznivih dejanjih in zarote, čeprav je obtoženka kršila »zgolj« splošne pogoje uporabe spletnega socialnega omrežja. Prav odsotnost specifičnih inkriminacij je privedla do širjenja območja kriminalnega, zato so nove konkretnejše inkriminacije bolj prilagojene sodobnemu tehnološkemu razvoju, nastopajo kot ščit, ne kot nov meč (sicer razširjenega) kazenskega pregona.

Razlogi za kazenskopravni odziv na kibernetsko nadlegovanje v prvi vrsti izhajajo iz škodljivih *posledic in družbene nevarnosti* kibernetskega nadlegovanja, ki so bile predstavljene v prejšnjem poglavju.

Raziskave o načinih in učinkovitosti odzivanja na kibernetsko nadlegovanje tudi kažejo, da je tridelna shema soočanja, ki obsega tudi kaznovanje najhujših primerov, najbolj učinkovita.[101] Po mnenju strokovnjakov in trenerjev, ki za starše, šolsko osebje in mladostnike pripravljajo izobraževanja o kibernetskem nadlegovanju, so dejavniki, ki pospešujejo pojavnost nadlegovanja, močno odvisni tudi od tega, da v zakonih ni jasne meje med dovoljenim in nedovoljenim ravnanjem.[102] Ti strokovnjaki so menili, da bi jasnejša pravila, mehanizmi monitoringa in sankcije pomembno prispevali k soočanju s tem problemom.[103]

Kazensko pravo je sredstvo zastraševanja in s tem deluje preventivno, odslikava družbene norme neke družbe, z določanjem novih meja nesprejemljivega

---

100 Kanduč, Pravo, spolnost in nasilje, v: Spolnost, nasilje in pravo (1998), str. 25.

101 Glej na primer Perren *et al.*, Tackling Cyberbullying (2012), *passim*.

102 Jäger, Amado, Matos, Pessoa, Analysis of experts' and trainers' views on cyberbullying, v: Australian Journal of Guidance and Counselling, 20 (2010) 2, str. 169–181.

103 Jäger, Amado, Matos, Pessoa, prav tam.

vedenja pa te iste družbene norme lahko tudi spreminja.[104] Jasna prepoved ima lahko progresivne učinke za družbene spremembe.

Soočanje v okviru izobraževalnega sistema je vsaj za specifično mladoletniško populacijo lahko učinkovito. A tudi tu drugače kot pri tradicionalnem vrstniškem nadlegovanju pri kibernetskem nadlegovanju meje med šolskim in domačim (zunajšolskim) okoljem niso jasne. Režim šolske zakonodaje je zato za sankcioniranje dejanj, storjenih »zunaj« šolskega okolja, neuporaben. Kibernetsko nadlegovanje se tudi pri mladoletnikih praviloma seli ven iz šole in stran od šolskih dvorišč, za odzivanje nanj pa se pogosto zahteva hitro sodelovanje in posredovanje ponudnikov storitve informacijske družbe, ki lahko ukrepajo na podlagi odredbe sodišč in izvedb policije, da se preneha s kršitvami pravic in identificira storilec. Izobraževalni ukrepi ne vsebujejo strožjega odvračalnega učinka, ki ga vsebujejo zakoni, ki prepovedujejo in kaznujejo.[105]

Starši, učitelji in širša skupnost tudi vse bolj pričakujejo, da bo kazensko pravo zagotovilo primeren pravni odgovor na kibernetsko nadlegovanje.[106] To je lahko posledica »moralne panike« v zvezi s kibernetskim svetom, v katerem so bolj vešči ravno mladi, ki kot digitalni domorodci bolj razumejo digitalno okolje. Zahteve javnosti po normativni aktivnosti so pogoste vezane na posamične odmevne primere, ki sprožajo obsežne normativne aktivnosti, kar je neupravičeno, saj so tragični dogodki statistično še vedno izjemno redki. Pri zahtevah javnosti je zato potrebna previdnost.

Za vrstniške oblike nasilja velja, da potekajo pred publiko, pred katero se storilec dokazuje in (vsaj z lastnega zornega kota ali zornega kota skupine) krepi svoj statusni položaj. Pri kibernetski različici pa je na internetu publika lahko izjemno obsežna, sega prek nacionalnih, jezikovnih meja in nasploh presega publiko, zbrano »na dvorišču« (npr. posnetek *happy slapping* ne potrebuje pojasnil in prevodov in se hitro razmnoži po medmrežju, kjer lahko postane viralen). Izjemna publiciteta in število opazovalcev sta pomembni novi dimenziji kibernetskega nadlegovanja in ustrahovanja, ki se ne nanašata samo na mladoletnike.

Digitalne tehnologije omogočajo beleženje, zbiranje, shranjevanje in distribuiranje velike količine osebnih podatkov po javnih telekomunikacijskih mrežah. Ti podatki, do nedavnega shranjeni razpršeno in med seboj nepovezano, so danes prosto dostopni in lažje dosegljivi kot v preteklosti, lažje jih je posredovati

---

[104] Evan, Law as an instrument of social change, v: Applied Sociology: Opportunities and Problems (1965), str. *passim*.

[105] Po King, Constitutionality of Cyberbullying Laws, v: Vanderbilt Law Review, 63 (2010) 3, str. 883.

[106] Kift *et al.*, Cyberbullying in social networking sites and blogs, v: Journal of Law, Information and Science, 20 (2010) 2, str. 62.

tretjim osebam, objaviti in drugače razpečevati tretjim osebam in javno objavljati. V takih primerih nevarnost kibernetskega nadlegovanja, kot je kibernetsko zalezovanje, preseže zgolj nevšečnost, ki je omejena na določen kraj in čas. *De lege ferenda* bi morala vstopiti v območje kaznivega zaradi te izjemne zmogljivosti digitalnih tehnologij za opazovanje in zbiranje osebnih podatkov.

Anonimnost storilca dejanja je v kibernetskem prostoru dodaten dejavnik, ki govori v prid posebnim kazenskopravnim določbam. Storilčeva moč je »okrepljena« tudi s tem, da lahko žrtve doseže kjerkoli in od koderkoli, dejanje pa lahko traja dalj časa (ali neomejeno).

5.2.3. Predlogi sprememb kazenske materialne zakonodaje

Spremembe so mogoče vsaj v treh pogledih.[107] Pogosto bo zadostovala nova interpretacija veljavnih pravil. Na primer kaznivo dejanje spolnega nasilja bi kazalo v prihodnosti tolmačiti tako, da bi vključevalo tudi spolna dejanja, storjena prek interneta in druge komunikacijske tehnologije. Na primer prisiljenje žrtve, da izvršuje spolna dejanja prek komunikacijskega kanala (na primer pred spletno kamero) ali da pod grožnjo trpi spolna dejanja storilca (na primer prek video pogovora v živo), enako posega v posameznikovo integriteto.

Obstoječim kaznivim dejanjem bi kazalo dodati kvalifikatorne oblike za primere množičnega kršenja pravic. Gre za primere popolnega razkritja vseh (najintimnejših in najobčutljivejših) osebnih podatkov tarče, ki so naenkrat na razpolago za zlorabo neomejenemu številu tretjih oseb (tako imenovani *doxing*).[108] Takšne oblike kršitev so že ustrezno zajete na primer pri kaznivih dejanjih zoper čast in dobro ime, ki kot kvalificirano obliko kaznivega dejanja določajo »javno objavo kršitev« (to pomeni s tiskom, po radiu, televiziji ali z drugim sredstvom javnega obveščanja in – težko razumljivo, zakaj – le na »spletnih straneh«, ki so samo ena od možnosti objave na internetu, poleg na primer priljubljenih spletnih socialnih omrežij); podobno tudi kaznivo dejanje zlorabe osebnih podatkov (peti odstavek 143. člena KZ-1). Poleg »javne objave« pa gre pri tem tudi za primere, ko javna objava kršitev doseže nepredstavljivo veliko množico. Javna objava na internetu pomeni druge časovne in krajevne parametre. Takšen primer

[107] Podpoglavje povzemam po Završnik: Spletno in mobilno nadlegovanje, v: Zbornik 2012, 5. konferenca kazenskega prava in kriminologije (2012), str. 98.

[108] *Doxing* (iz angl. *documents* ali *.docx*) je zbiranje informacij o tarči iz prosto dostopnih informacij na internetu. Temelji na zalezovalčevi sposobnosti, da najde in prepozna koristne informacije o tarči, ki jih potem uporabi zoper njo. Zasebnost žrtve je razgaljena, vsi njeni podatki (prava imena, naslovi, telefonske številke, slike iz šole, službe ali z zabav, uporabniška imena in gesla na drugih računih, številke kreditnih kartic ipd.) so na voljo vsem uporabnikom.

je pogost pri elektronskem zmenkarskem nadlegovanju, katerega posebnost je, da ga storijo žrtvi znane osebe, ki so z njo (bile) bolj povezane in so si (bile vsaj na neki ravni) všeč.[109] Gre za primere, ko (bivši) partner izkoristi zaupanje in objavi zasebne fotografije ali video posnetke žrtve na internetu ali jih razpošlje. Posnetke je tako rekoč (kljub morebitnim sodbam zaradi kršenja osebnostnih pravic v korist žrtve) nemogoče izbrisati. Časovno viktimizacija traja v nedogled. Gradivo se pojavlja na vedno novih platformah, shranjuje po različnih strežnikih po svetu, razmnožuje po različnih spletnih straneh ali pa celo ostaja med zadetki internetnih iskalnikov v obliki začasno shranjenih strani. Krajevno pa »javna objava« sega čez nacionalne meje, saj je sporno gradivo mogoče razpečevati brez stroškov, hitreje in učinkoviteje. Javna objava ima več modalitet, lahko je tudi prostorsko globalna in trajna.

Za nekatere nove oblike ravnanj bi bilo mogoče oblikovati povsem nove inkriminacije. Kaznivo dejanje *zalezovanja* (angl. *stalking*) so že inkriminirale nekatere države anglo-ameriškega pravnega kroga, vendar s sodobno informacijsko-komunikacijsko tehnologijo to ravnanje doseže nepredstavljive razsežnosti. Kibernetsko zalezovanje (angl. *cyber-stalking*) je posebno kaznivo dejanje v številnih anglo-ameriških pravnih sistemih, na primer od devetdesetih let naprej v Avstraliji. Zakonodajalec je tam pri inkriminaciji upošteval dejstvo, da so storilčeva dejanja posamično sicer nepomembna, *na agregatni ravni* pa vodijo v pomembno ogrožanje.[110] Kibernetsko zalezovanje ima pogosto dodatno *javno dimenzijo* in drugače kot siceršnje zalezovanje ni zasebno in skrito pred očmi javnosti. Inkriminacija torej upošteva celoto številnih ravnanj, na primer pošiljanje neželene pošte, pošiljanje sovražne ali obscene e-pošte, pošiljanje zlonamerne računalniške programske opreme (virusov, črvov in vohunskih programov),

[109] *Elektronsko zmenkarsko nadlegovanje* obsega nadlegovanje prek storitev spletnih zmenkarij. Sodobne zmenkarske platforme združujejo več storitev, na primer razpravljalnice (angl. *message board*), možnost nalaganja in izmenjave fotografij in filmov, tematske forume, pogovore v realnem času (*chat*) in storitve spletnega oddajanja (*webcast*). Na primer najbolj priljubljena svetovna e-zmenkarska platforma *match.com* je pritegnila 3 milijone uporabnikov, za ujemanje med partnerjema pa skrbi poseben program, ki odloča na podlagi vnesenih osebnih podatkov uporabnika in njegovih preferenc. Množičnost uporabe teh strani (na primer slovenska mreža *ona-on.com* je pritegnila 120.000 uporabnikov, med katerimi naj bi bilo 50.000 aktivnih) kaže, da internet postaja eden najbolj priljubljenih načinov spoznavanja. Takšna množičnost pa prinaša tudi odklonske in moteče vsebine, vključno z nadlegovanjem ali ustrahovanjem. Hinduja, Cyberbullying and Electronic Dating Violence, URL: http://cyberbullying.us/blog/cyberbullying-and-electronic-dating-violence.html; Hinduja, Electronic Dating Violence and Teens – our 2010 research findings, URL: http://cyberbullying.us/blog/electronic-dating-violence-and-teens-our-2010-research-findings.html; Kholos Wysocki, Childers, 'Let My Fingers Do the Talking': Sexting and Infidelity in Cyberspace, v: Sexuality & Culture, 15 (2011) 3, str. 235.

[110] Goode, Stalking, v: Criminal Law Journal, 19 (1995) 1, str. 24.

telefoniranje in druge poskuse navezati stik z osebo na način, za katerega lahko *razumno pričakujemo*, da bo vzbudil *strah, občutke ogroženosti in kršitve zasebnosti* ali *razumno utemeljene* občutke strahu.[111] Vsa ta dejanja sama zase ne konstituirajo kibernetskega zalezovanja, ampak le, če *se ponavljajo* in so poslana na način in z *namenom ustrahovanja*. Storilčev namen je v nekaterih avstralskih zveznih državah določen tako, da mora obsegati naklep povzročiti žrtvi (ne kakršenkoli, temveč) *resen* strah ali občutke ogroženosti. Pogosto je element kaznivega dejanja zalezovanja tudi izvrševanje na *specifičnem* (omejenem) prostoru, kot je nadzorovanje ali sledenje na območju, kjer žrtev prebiva ali dela. Prostor lahko zakonodaja opredeljuje z generalno klavzulo kot »vsak prostor, ki ga oseba pogosto obiskuje za katerekoli družbene namene ali prostočasno dejavnost«, v ta okvir pa spadajo tudi kibernetski prostor oziroma posamične storitve informacijske družbe, kamor žrtev razširi svoje socialno življenje (na primer obiskovanje izbranega spletnega socialnega omrežja ali druge skupnosti).

6. Sklep

Kibernetsko nadlegovanje je nov problem, na katerega se pravu še ni uspelo ustrezno odzvati. Predstavitev oblik kibernetskega nadlegovanja, njegovih posledic in kazenskopravnih odzivov nanj je pokazala, da največja dilema ostaja izredno širok osrednji označevalec (angl. *cyber-bullying*). Prvič, v državah na angleškem govornem območju že pojem nadlegovanje uporabljajo široko (na primer za *bullying* v družini, v partnerskih odnosih, na delovnem mestu in med vrstniki), v kontinentalni Evropi pa se termin uporablja za nasilje v šoli in med mladimi. V vseh drugih jezikih (razen angleškega in nekaterih skandinavskih) tudi ni ustreznega izraza, ki bi pomenil isto ali podobno kot angleški *bullying*. Kibernetska različica ta pojav z vidika inkriminiranja *de lege ferenda* še dodatno zaplete, saj se IKT hitro spreminja in uporaba posamičnih »kibernetskih« storitev informacijske družbe izrazito niha v prostoru in času. Drugič, definicija, ki se je uveljavila med pedagogi in psihologi (tj. agresivno in namerno dejanje, ki ga izvršuje skupina ali posameznik s pomočjo elektronskih oblik komuniciranja, primarno interneta in z mobilnimi telefoni, dalj časa ali ponavljajoče se, zoper žrtev, ki se ne more zlahka braniti), je za potrebe kazenskega prava preohlapna. Zato ni nenavadno, da posebnega kaznivega dejanja kibernetskega nadlegovanja *per se* ne poznajo v nobeni pregledani državi (tj. v Kanadi, Veliki Britaniji, Avstraliji, Braziliji, Finski, Nemčiji, Grčiji, Litvi ali Španiji).

[111] Povzemam po Ogilvie, Stalking (2000), str. 54.

Kljub temu iz raziskav, ki so merile učinkovitost soočanja s kibernetskim nadlegovanjem, izhaja, da naj kazensko pravo nastopi kot zadnja (*ultima ratio*) možnost v odzivanju na novo obliko odklonskih ravnanj. Razlogi so številni in so v članku posebej predstavljeni. Veljavna kazenska zakonodaja ponuja številne možnosti kazenskega pregona domnevnih storilcev in v večini primerov ne bo dvomov. Vendar pa bi zaradi nekaterih predstavljenih specifičnosti kibernetskega nadlegovanja kazalo posodobiti kazenske materialne razlage in kazenski zakonik: (1) z novimi interpretacijami kaznivih dejanj, predvsem spolnih kaznivih dejanj, pri katerih je do zdaj v teoriji prevladovalo stališče, da jih je mogoče storiti le s fizičnim kontaktom; (2) z novimi kvalifikatornimi oblikami kaznivih dejanj za primere razgaljanja žrtev v obsegu, ki si ga pred pojavom interneta ni bilo mogoče zamisliti niti glede na globino posega v pravice niti glede na trajanje negativnih posledic, in (3) z inkriminacijo kibernetskega zalezovanja, saj smo zaradi izjemne dostopnosti IKT in eksponentnih računskih in spominskih zmogljivosti IKT priča vse bolj intenzivnim posegom v pravice drugih, ki so jih v preteklosti lahko izvršile le posebej usposobljene skupine strokovnjakov: rudarjenje po javno dostopnih podatkih in obveščevalna dejavnost iz javnih virov (angl. *open source intelligence*) sta posamično lahko zakonita, na agregatni ravni storjena z namenom ustrahovanja pa lahko vodita do močnih občutkov ogroženosti in strahu.

Nazadnje je pomembno poudariti, da se je z raznolikimi oblikami kibernetskega nadlegovanja mogoče učinkovito spoprijeti le celovito: (1) prilagojeno potrebam specifičnih skupin uporabnikov, (2) s tridelno shemo v prevencijski fazi, z opolnomočenjem tarč za konfrontacijo s storilci in z odbojem negativnih posledic dejanja in (3) z vključitvijo večdeležniške mreže akterjev. Vsaj za najbolj ranljivo skupino uporabnikov zato velja, da spoprijemanje z novimi oblikami nadlegovanja ni najučinkovitejše v sodni dvorani (*ultima ratio*), temveč v učilnici (kot »*prima ratio*«).

Literatura

Bauman, Sheri; Del Rio, Adrienne: Preservice teachers's responses to bully scenarios: Comparing physical, verbal, and relational bullying, v: Journal of Educational Psychology, 98 (2006) 1, str. 219–231.

Belsey, Bill (2005): Cyberbullying: An emerging threat to the »always on« generation, URL: http://www.cyberbullying.ca/pdf/Cyberbullying_Article_by_Bill_Belsey.pdf (14. 1. 2013).

Bocij, Paul: Cyberstalking: Harrassment in the Internet Age and How to Protect your Family, Praeger Publishers, Westport 2004.

Calvert, Clay: Sex, Cell Phones, Privacy and the First Amendment: When Children Become Child Pornographers and the Lolita Effect Undermines the Law, v: CommLaw Conspectus, 18 (2009) 1, str. 1–65.

Campbell, Marilyn A.: Cyber bullying: an old problem in a new guise?, v: Australian Journal of Guidance and Counselling, 15 (2005) 1, str. 68–76.

Campbell, Marilyn A.; Butler, Desmond A.; Kift, Sally M.: A school's duty to provide a safe learning environment: Does this include cyberbullying?, v: Australian and New Zealand Journal of Law and Education, 13 (2008) 2, str. 21–32.

Cheng, Jacqui: Rutgers »cyberbully« found guilty of privacy invasion, hate crimes, v: ArsTechnica, 13. 3. 2012, URL: http://arstechnica.com/tech-policy/2012/03/rutgers-cyberbully-found-guilty-of-privacy-invasion-hate-crimes/ (14. 2. 2013).

Dekleva, Bojan: Semantika (med)vrstniškega nasilja, v: Revija za kriminalistiko in kriminologijo, 52 (2001) 1, str. 21–31.

Dooley, Julian J.; Cross, Donna; Hearen, Lydia; Treyvaud, Robyn: Review of Existing Australian and International Cyber-Safety Research, Child Health Promotion Research Centre, Edith Cowan University, Perth 2009, URL: http://www.dbcde.gov.au/__data/assets/pdf_file/0004/119416/ECU_Review_of_existing_Australian_and_international_cyber-safety_research.pdf (15. 4. 2013).

Dzuka, Jozef; Dalbert, Claudia: Aggression at School: Belief in a Personal Just World and Well-Being of Victims and Aggressors, v: Studia Psychologica, 49 (2007) 4, str. 313–320.

Evan, William M.: Law as an instrument of social change, v: Applied Sociology: Opportunities and Problems (ur. A. W. Gouldner, S. M. Miller), Free Press, New York 1965, str. 285–293.

Evropska komisija: Eurobarometer 2008. Towards a Safer Use of the Internet for Children in the EU – a Parents' Perspective. Analytical Report, URL:

http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/analyticalreport_2008.pdf (7. 5. 2012).

Gillespie, Alisdair A.: Cyber-bullying and harassment of teenagers: The legal response, v: Journal of Social Welfare & Family Law, 28 (2006) 2, str. 123–136.

Goode, Matthew: Stalking: Crime of the Nineties?, Eighteenth International Symposium on Victimology, World Society of Victimology, 1994, v: Criminal Law Journal, 19 (1995) 1, str. 21–31.

Gradinger, Petra; Strohmeier, Dagmar; Spiel, Christiane: Traditional Bullying and Cyberbullying: Identification of Risk Groups for Adjustment Problems, v: Zeitschrift fur Psychologie/Journal of Psychology, 217 (2009) 4, str. 205–213.

Grigg, Dorothy: Cyber-Aggression: Definition and Concept of Cyberbullying, v: Australian Journal of Guidance & Counselling, 20 (2010) 2, str. 143–156.

Grossman, Andrew M.: The MySpace Suicide: A Case Study in Overcriminalization, v: Legal Memorandum, (2008) 32, str. 1–11.

Harlin Goodno, Naomi: Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws, v: Missouri Law Review, 72 (2007), str. 125–157.

Hinduja, Sameer: Cyberbullying and Electronic Dating Violence, URL: http://cyberbullying.us/blog/cyberbullying-and-electronic-dating-violence.html (6. 9. 2010).

Hinduja, Sameer: Electronic Dating Violence and Teens – our 2010 research findings, URL: http://cyberbullying.us/blog/electronic-dating-violence-and-teens-our-2010-research-findings.html (26. 10. 2010).

Hinduja, Sameer; Patchin, Justin W.: Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying, Corwin Press, Thousand Oaks California 2008.

Hu, Winnie: Legal Debate Swirls Over Charges in a Student's Suicide, v: The New York Times, 1. 10. 2010, URL: http://www.nytimes.com/2010/10/02/nyregion/02suicide.html (14. 2. 2013).

Informacijski pooblaščenec: Smernice glede varstva pred spletnim nadlegovanjem. Verzija 1.0 (2009), URL: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice-glede-varstva-pred-spletnim-nadlegovanjem.pdf (15. 10. 2012).

Jäger, Thomas; Amado, João, Matos, Armanda; Pessoa, Teresa: Analysis of experts' and trainers' views on cyberbullying, v: Australian Journal of Guidance and Counselling, 20 (2010) 2, str. 169–181.

Jameson, Sarah: Cyberharassment: Striking a Balance Between Free Speech and Privacy, v: Commlaw Conspectus, 17 (2008) 1, str. 231–236.

Kanduč, Zoran: Pravo, spolnost in nasilje: kriminološke in viktimološke perspektive, v: Spolnost, nasilje in pravo (ur. Z. Kanduč, D. Korošec, M. Bošnjak),

Inštitut za kriminologijo pri Pravni fakulteti/Urad RS za žensko politiko, Ljubljana 1998, str. 11–138.

Kerr, Orin S.: Cybercrime's Scope: Interpreting »Access« and »Authorization« in Computer Misuse Statutes, v: New York University Law Review, 78 (2003) 5, str. 1596–1668.

Kerr, Orin S.: The Volokh Conspiracy blog (29. 8. 2009), URL: http://www.volokh.com/posts/1251601962.shtml (23. 1. 2013).

Kholos Wysocki, Diane; Childers, Cheryl D.: »Let My Fingers Do the Talking«: Sexting and Infidelity in Cyberspace, v: Sexuality & Culture, 15 (2011) 3, str. 217–239.

Kift, Sally M.; Campbell, Marilyn A.; Butler, Desmond A.: Cyberbullying in social networking sites and blogs: legal issues for young people and schools, v: Journal of Law, Information and Science 20 (2010) 2, str. 60–97.

King, Alison Virginia: Constitutionality of Cyberbullying Laws: Keeping the Online Playground Safe for Both Teens and Free Speech, v: Vanderbilt Law Review, 63 (2010) 3, str. 845–884.

Lievens, Eva: Bullying and sexting in social networks from a legal perspective: between enforcement and empowerment, ICRI Working Paper 7/2012, Interdisciplinary Centre for Law and ICT, KU Leuven, URL: http://ssrn.com/abstract=2088166 (22. 1. 2013).

Lines, Dennis: The Bullies. Understanding Bullies and Bullying, Jessica Kingsley Publishers, London 2008.

Lobe, Bojana; Muha, Sandra: Tveganja in varnost otrok na internetu: Slovensko poročilo. Ugotovitve raziskave EU Kids Online o 9–16 let starih otrocih in njihovih starših (2010), URL: www.eukidsonline.net (5. 5. 2012).

Lovšin, Peter: 18 ovadenih zaradi izsiljevanja in razpošiljanja fotografij gole profesorice, v: Dnevnik online, 18. 1. 2012, URL: http://www.dnevnik.si/kronika/1042503121 (12. 5. 2013).

Maag, Christopher: A Hoax Turned Fatal Draws Anger But No Charges, v: New York Times, 28. 11. 2007, str. A23.

Marczak, Magdalena; Coyne, Iain: Cyberbullying at school: Good practice and legal aspects in the United Kingdom, v: Australian Journal of Guidance and Counselling, 20 (2010) 2, str. 182–193.

McCarthy, Paul: The Bullying Syndrom: Complicity and Responsibility, v: Bullying: From Backyard to Boardroom (ur. P. McCarthy, J. Rylance, R. Bennett, H. Zimmermann), The Federation Press, Sydney 2001, str. 86–99.

Meloy, J. Reid; Gothard, Shayna: A Demographic and Clinical Comparison of Obsessional Followers and Offenders with Mental Disorders, v: American Journal of Psychiatry, 152 (1995) 2, str. 258–263.

Mitchell, Kimberly J.; Ybarra, Michele; Finkelhor, David: The Relative Importance of Online Victimization in Understanding Depression, Delinquency, and Substance Abuse, v: Child Maltreatment, 12 (2007) 4, str. 314–324.

Muršič, Mitja; Brvar, Bogomil: Izbor (s čustvi povezanih) ugotovitev naše raziskave, v: Znanje o čustvih za manj nasilja v šoli (ur. M. Muršič), Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani, Ljubljana 2010, str. 21–26.

Nocentini, Annalaura; Calmaestra, Juan; Schultze-Krumbholz, Anja; Scheithauer, Herbert; Ortega, Rosario; Menesini, Ersilia: Cyberbullying: Labels, Behaviours and Definition in Three European Countries, v: Australian Journal of Guidance & Counselling, 20 (2010) 2, str. 129–142.

Ogilvie, Emma: Stalking: Legislative, Policing and Prosecution Patterns in Australia, Research and Public Policy Series, No. 34, Australian Institute of Criminology (2000), URL: http://www.aic.gov.au/documents/3/D/D/%7B3DDEC8F8-7ECC-4DC3-9E92-CCD62DA463EE%7DRPP34.pdf (20. 4. 2013).

Ostrman, Anka: Medvrstniško nasilje, v: Socializacija agresije (ur. A. Kristančič), Združenje svetovalnih delavcev Slovenije, Zveza prijateljev mladine Slovenije, AA Inserco, Ljubljana 2002, str. 137–162.

Ottenweller, Cara J.: Cyberbullying: The Interactive Playground Cries for a Clarification of the Communications Decency Act, v: Valparaiso University Law Review, 41 (2007) 3, str. 1285–1334.

Patchin, Justin W.; Hinduja, Sameer: Bullies move beyond the schoolyard: A preliminary look at cyberbullying, v: Youth Violence and Juvenile Justice, 4 (2006) 2, str. 148–169.

Perren, Sonja; Dooley, Julian; Shaw, Thérèse; Cross, Donna: Bully/Victim Problems in Schools and in Cyberspace: Associations with Depressive Symptoms in Swiss and Australian Adolescents, v: Child and Adolescent Psychiatry and Mental Health, 4 (2010) 28, URL: http://www.capmh.com/content/4/1/28 (22. 4. 2013).

Perren, Sonja; Corcoran, Lucie; Cowie, Helen; Dehue, Francine; Garcia, D'Jamila; McGuckin, Conor; Sevcikova, Anna; Tsatsou, Panayiota; Völlink, Trijntje: Tackling Cyberbullying: Review of Empirical Evidence Regarding Successful Responses by Students, Parents, and Schools, v: International Journal of Conflict and Violence, 6 (2012) 2, str. 283–293.

Prensky, Marc: Digital natives, digital immigrants, v: On the Horizon, 9 (2001) 5, str. 1–6.

Reid, Philippa; Monsen, Jeremy; Rivers, Ian: Psychology's contribution to understanding and managing bullying within schools, v: Educational Psychology in Practice, 20 (2004) 3, str. 241–258.

Rigby, Ken: New Perspectives on Bullying, Jessica Kingsley Publishers, London 2002.

Rivers, Ian; Chesney, Thomas; Coyne, Iain: Cyberbullying, v: Bullying in Different Contexts (ur. C. P. Monks, I. Coyne), Cambridge University Press, Cambridge 2011, str. 211–230.

Ruedy, Matthew C.: Repercussions of a MySpace Teen Suicide: Should Anti-bullying Laws be Created?, v: North Carolina Journal of Law & Technology, 9 (2008) 2, str. 323–346.

SAFE-SI: Osveščanje o varni rabi interneta in novih tehnologij, URL: http://www.safe.si/c/1482/Soocenje_z_ustrahovanjem_na_internetu/?preid=978 (16. 5. 2012).

Schmitz, Sandra; Siry, Lawrence: Teenage folly or child abuse? State responses to »sexting« by minors in the U.S. and Germany, v: Policy & Internet, 3 (2011) 2, str. 25–50.

Schwartz, Bernard: Holmes Versus Hand: Clear and Present Danger or Advocacy of Unlawful Action?, v: The Supreme Court Review, 1994 (1995), str. 209–245.

Scott Hammack: Note, The Internet Loophole: Why Threatening Speech On-Line Requires a Modification of the Courts' Approach to True Threats and Incitement, v: Columbia Journal of Law and Social Problems, 36 (2002) 65, str. 81–83.

Shariff, Shaheen; Gouin, Rachel: Cyber-dilemmas: Gendered Hierarchies, Free Expression and Cyber-Safety in Schools, Oxford Internet Institute, Oxford University (2005), URL: http://www.oii.ox.ac.uk/microsites/cybersafety/?view=papers (23. 10. 2012).

Slonje, Robert; Smith, Peter K.: Cyberbullying: Another main type of bullying?, v: Scandinavian Journal of Psychology, 49 (2008) 2, str. 147–154.

Smith, Peter; Mahdavi, Jess; Carvalho, Manuel; Tippett, Neil: An Investigation into Cyberbullying, its Forms, Awareness and Impact, and the Relationship Between Age and Gender in Cyberbullying (Research Brief No. RBX03-06), Goldsmiths College, University of London, London 2006.

Smith, Peter K.; Mahdavi, Jess; Carvalho, Manuel; Fisher, Sonja; Russell, Shanette; Tippett, Neil: Cyberbullying: Its nature and impact in secondary school pupils, v: Journal of Child Psychology and Psychiatry, 49 (2008) 4, str. 376–385.

Smith, Peter K.; Sharp, Sonia: School Bullying: Insights and Perspectives, Routledge, London 1994.

Sourander, Andre; Brunstein Klomek, Ana; Ikonen, Maria; Lindroos, Jarna; Luntamo, Terhi; Koskelainen, Merja; Ristkari, Terja; Helenius, Hans: Psychology Risk Factors Associated with Cyberbullying among Adolescents, v: Archives of General Psychiatry, 67 (2010) 7, str. 720–728.

Spears, Barbara; Slee, Philip; Owens, Laurence; Johnson, Bruce: Behind the scenes and screens: insights into the human dimension of covert and cyberbullying, v: Zeitschrift für Psychologie/Journal of Psychology, 217 (2009) 4, str. 189–196.

Stanton, Lauren; Beran, Tanya: A review of legislation and bylaws relevant to cyberbullying. McGill Journal of Education, 44 (2009) 2, str. 245–260.

Vehovar, Vasja; Šterk, Tanja; Pestotnik, Andreja; Šmid Božičevič, Urša: Za varen internet: predstavitev projektov za zaščito otrok pri uporabi interneta, v: Mednarodna konferenca o otrokovih pravicah in zaščiti pred nasiljem, Državni zbor, 6. in 7. oktober 2009, Ljubljana, URL: http://www.varuh-rs.si/fileadmin/user_upload/word/Otrokove_pravice_in_nasilje___SE_09/Prispevki/Vasja_Vehovar.doc (30. 1. 2013).

Wall, David S.: Cybercrime, Polity Press, Cambridge 2007.

Whitney, Irene; Smith, Peter K.: A survey of the nature and extent of bullying in junior/middle and secondary schools, v: Educational Research, 35 (1993) 1, str. 3–25.

Willard, Nancy E.: Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Cruelty, Threats, and Distress, Center for Safe and Responsible Internet Use, Champaign, Illinois 2006.

Wilson, Sandra Jo; Lipsey, Mark W.: School-based interventions for aggressive and disruptive behavior. Update of a meta-analysis, v: American Journal of Preventive Medicine, 33 (2007) 2, Supplement, str. S130–S143.

Wunmi Grigg, D.: Cyber-Aggression: Definition and Concept of Cyberbullying, v: Australian Journal of Guidance & Counselling, 20 (2010) 2, str. 143–156.

Ybarra, Michele L.; Diener-West, Marie; Markow, Dana; Leaf, Philip J.; Hamburger, Merle; Boxer, Paul: Linkages between internet violence and seriously violent behaviour: findings from the Growing Up with the Media national survey, v: Pediatrics, 122 (2008) 5, str. 929–937.

Završnik, Aleš: Spletno in mobilno nadlegovanje: nova oblika nasilja za novo inkriminacijo?, v: Zbornik 5. konference kazenskega prava in kriminologije, GV Založba, Ljubljana 2012, str. 92–100.

Završnik Aleš; Sedej, Anja: Spletno in mobilno nadlegovanje v Sloveniji, v: Revija za kriminalistiko in kriminologijo, 63 (2012) 4, str. 263–280.

Zoranovič, Marko: Medvrstniško spletno in mobilno nadlegovanje (diplomska naloga), Pravna fakulteta Univerze v Ljubljani, Ljubljana 2011.

Cyberbullying: Concept, Types, Consequences and Criminal Law Response

Summary

The development of new information-communications technology (ICT), primarily Internet and mobile phones, triggered new opportunities for bullying. The article analyses new *types and forms* of cyberbullying, its *consequences and harms* and *interventions* against cyberbullying. The article begins by presenting general definitions and taxonomies of cyberbullying. It analyses specific types of cyberbullying, including mobile phone bullying, bullying on social networking sites, bullying through unsolicited »extreme content«, flooding, »photoshopping«, sexting, Happy Slapping, »trolling«, »flaming«, Bluetooth bullying, bullying over rating sites, electronic dating violence, »doxing« and cyber-stalking. The increasing number of forms of cyberbullying shows how cyberbullying can be defined with regard to the method and technology being used, the bully's age and also the object of legal protection (e.g. honour, reputation, public morals). The article claims that an all-encompassing definition of cyberbullying for the purposes of criminal law seems at this stage impossible and also not reasonable.

The criminal cases against cyberbullies presented in the article nevertheless show how criminal law is struggling to keep up with the technological progress that has brought bullying from the schoolyard into cyberspace. The devastating consequences of cyberbullying (e.g. suicides of victims, leading to the coinage of a new word, »bullicide«), evidence of psychological damage caused by cyberbullying and public calls for more decisive action against it manifest a pressing need to address cyberbullying in a more comprehensive way that would include preventive and repressive means.

Before offering a possible intervention scheme against cyberbullying in Slovenia the article presents in more detail the results of studies revealing the harmful and damaging consequences of cyberbullying. It shows why cyberbullying can be more harmful than traditional bullying in the long term, since it is subtler and thus detrimental for the psychological development of children. The anonymity of Internet users increases victims' fears as victims since they are often unable to see who is actually bullying them, how many bullies there are and where the threat is coming from. The intense personal investment of adolescents in digital space, »hanging-out« and socialising by using services such as social networking sites, increase their vulnerability. Additionally, the technology itself enables threats to spread more easily and can cause massive victimisations.

The inability of bullies to fully observe the reactions of victims due to the electronically mediated form of communication, limited to a written word, gives additional spin to this type of violence. The so called »cockpit« and disinhibition effect can mislead bullies to continue activities that might otherwise – if they saw directly their victims' reactions – stop. In comparison to traditional bullying the effort needed to commit cyberbullying is also smaller as it can be automated by the use of computer software. The control that the perpetrators have over published material is in most cases even smaller or even nonexistent. For instance, offensive material can be easily copied without a cyberbully's consent onto different internet sites within different jurisdictions.

Research projects into the personal and psychological consequences of cyberbullying have shown furthermore how victims of cyberbullying often feel angry, frustrated, sad and humiliated. Cyberbullying victimisations influence not only self-esteem and emotional development, but aggravate depressive and psychosomatic symptoms, such as headaches, insomnia and digestive disorders. The article shows findings that statistically significant correlations exist between cyberbullying and family problems, school performance and delinquency.

Divergent types of cyberbullying and the myriad consequences of cyberbullying call for, continues the article, a comprehensive intervention strategy. Such a strategy should be designed (1) for special user groups (i.e. separately for children, adolescents, younger adults, parents and teachers), (2) adjusted to three stages of intervention, i.e. prevention, the fight against ongoing cases of cyberbullying and buffering negative impacts of cyberbullying (a »three-fold intervention strategy«) and (3) designed in a way to ensure participation of all stakeholders included in the provision of safety on the Internet, e.g. internet service providers and content providers and their respective associations in charge of industry self-regulation, NGOs established for victim support, contact points for reporting network security incidents – CERTs, etc. (the so called »multi-stakeholder network«). A comprehensive multi-dimensional national strategy against cyberbullying would thus have to encompass a specific approach adjusted for different users, three intervention stages and include various stakeholders.

The first finding of the article is that preventive and educational measures combined with technological measures are proven to be the most efficient approach in tackling cyberbullying. In designing an intervention strategy the article analyses different approaches taken by the European countries and shows that measures against cyberbullying are to a certain extent similar to measures against traditional bullying (e.g. empathy trainings), but to a certain extent demand specific action (e.g. raising digital literacy).

In order to be more specific, the article analyses in more depth measures within the educational setting in Slovenia. It shows the regime of rights and duties in elementary schools and particularly within a selected elementary school. According to the Elementary School Act the implementation of the goals and values of primary education, of educational procedures and educational measures have become responsibilities of each individual elementary school. The article shows how educational measures and educational admonitions set either in the legislation or in »school plans« offer a range of tools for intervening against cyberbullying. Slovenian (elementary) schools directly tackle the problems of students' communication on the Internet and via other electronic means in the school premises. They regulate the use of computers and mobile phones very strictly, probably in order to avoid eventual reparation claims from potential victims of cyberbullying.

The article then concludes that educational measures designed for schools may sometimes fail to prevent cyberbullying. A cyberbullying case may raise questions of a bully's criminal responsibility. The article claims that a new criminal offence designated as »cyberbullying« is not needed. In fact a special criminal offence *per se* does not exist in Canada, United Kingdom, Australia, Brazil, Finland, Germany, Greece, Lithuania or Spain. The existing definitions of cyberbullying are focused on psychological aspects and are too broad for purposes of criminal law. Having said that, the existing incriminations in the Criminal Code of Slovenia show that the criminal code as it stands cannot fully legislate for the harmful dimensions of cyberbullying in their entirety. The article claims that a lack of specific modalities within current definitions of criminal offences can even lead to a disproportionate narrowing of the scope of freedom. Legislation adapted to advances in new technologies can perform also as a »shield« and not only a »sword« for criminal prosecution.

The detrimental consequences of cyberbullying presented in the article raise the need for the criminal law to adjust. According to empirical research on experts' and trainers' views on cyberbullying, one factor that facilitates cyberbullying is the very fact of the non-existence of clear boundaries between permitted and prohibited conduct in cyberspace. According to their views criminal law should be used as a deterrent from cyberbullying. It reflects the social norms of a given society and can redefine previously accepted behaviour as being unacceptable.

In contrast to traditional »school-yard« bullying, cyberbullying does not have spatial boundaries. It often transcends national and cultural borders. Educational legislation and schools thus can not be regarded as the only actors responsible for preventing and responding to cyberbullying. Educational legislation

also fails to address cases demanding swift collaboration by Internet service providers according to a judicial order executed by the police. Digital technologies enable perpetrators to accumulate, preserve and organise data and create sensitive personal data databases much more easily than before. The dangers of cyerbullying can thus become more than just a nuisance limited to a specific place and time. All these factors increase the need to adapt provisions of the criminal code.

The first challenge in drafting substantive criminal law changes lies in the important constitutional territory of freedom of speech. The limitations of sexting set in the Council of Europe's Convention on Cybercrime have disproportionally limited the range of freedom of speech, as the article explains in more detail. The proposed changes to the Criminal Code are as follows: (1) inclusion of sex-related offences committed with the use of ICT in the traditional sex offences repertoire; (2) inclusion of aggravated types of offences for cases of massive victimisations and global or »viral« dissemination of offensive material for enduring violations; and (3) inclusion of a new incrimination of stalking and cyber-stalking. The reasons for new incriminations are presented in the article in more detail. They include the fact that a perpetrator may commit many acts that are not individually very harmful but may be extremely harmful at an aggregate level; the public dimension of cyberbullying; the increasing capacities of ICT and ability of perpetrators to acquire, combine and cross-reference personal data from formerly separate sources, substantively increasing their power to commit offences. The article offers several safeguards that should be put in place in order to prevent disproportionate prosecution, such as an element of »reasonable expectation« that offensive conduct will raise fear, intimidation or breach of privacy; along with an element accounting for repeated misconduct and the clear intent of the perpetrator to cause distress.