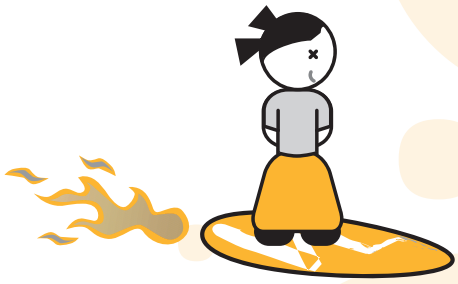


DESKANJE PO VARNIH VODAH

Gradiva za učitelje

DESKANJE PO VARNIH VODAH

Gradiva za učitelje

Avtorji:
dr. Matej Kovačič, mag. Alenka Žavbi
mag. Tomi Dolenc, Gorazd Božič, Tina Zupanič,
Tanja Šterk in Ajda Jerman Kuželički.

Urednica: Tanja Šterk

Izdajatelj: Projekt SAFE-SI
Fakulteta za družbene vede,
Center za metodologijo in informatiko
Kardeljeva pl. 5, 1000 Ljubljana, Slovenija
Fax: +386 (0)1 5805 101, Tel: +386 (0)1 5805 354
Email: info@safe.si

Projekt SAFE-SI je del evropskega omrežja točk osveščanja o varnem internetu (»InSafe«), sofinancirata pa ga Evropska komisija in Ministrstvo za visoko šolstvo znanost in tehnologijo RS.

Tisk: Impress, d.d.

Naklada: 1.000 izvodov

Ljubljana, november 2009

(prenovljena in dopolnjena izdaja)

CIP - Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

004.738.5.056(035)

DESKANJE po varnih vodah : gradiva za učitelje / [avtorji Matej
Kovačič ... [et al.] ; urednica Tanja Šterk]. - Prenovljena in
dopolnjena izd. - Ljubljana : Projekt SAFE-SI, Fakulteta za
družbene vede, Center za metodologijo in informatiko, 2009

- - Deskanje po varnih vodah. CD priročnik za razredne aktivnosti
[Elektronski vir] / avtor Alenka Žavbi

ISBN 978-961-235-381-0 (komplet)
1. Kovačič, Matej, 1974- 2. Šterk, Tanja
248368896

KAZALO

1 Uvod

1.1. Komu je učni komplet namenjen in kako ga uporabljati?

V kompletu, ki je pred vami, so združena obsežna gradiva na temo varne rabe informacijsko komunikacijskih tehnologij ter priročnik za razredne aktivnosti, ki je priložen na CD-ju.

Z gradivi želimo učiteljem in učiteljem multiplikatorjem ponuditi znanja s področij informacijske varnosti in zasebnosti, avtorskih pravic na internetu, škodljivih in nelegalnih vsebin ter napotke za učinkovito in varno rabo interneta in drugih novih tehnologij v šoli in pri pouku. Gradiva temeljijo na vsebinah, ki so nujno potrebne za razumevanje in temeljno uporabo informacijskih tehnologij v izobraževalnem procesu.

Priročnik na CD-ju pa je namenjen učiteljem, učiteljem multiplikatorjem, pedagoškim delavcem s področja vzgoje in izobraževanja, ki želijo v svoje programe vključiti vsebine in metode posredovanja informacij in znanj o varnosti v informacijski družbi. Vsebine in metode se lahko prilagodi tudi za delo z drugimi skupinami, zato lahko priročnik pri svojem delu uporabljajo tudi socialni delavci, mladinski delavci, mentorji interesnih skupin, ipd.

1.2. Predstavitev projekta SAFE-SI

Internet je realen del današnjega sveta: koristen, zabaven, poučen ... Postal je nepogrešljiv pripomoček v službi ter tudi v šoli in doma. Mladi dandanes več časa namenijo brskanju po internetu, kakor pa gledanju televizije ali druženju s prijatelji v realnem svetu. Vendar pa se je potrebno zavedati, da "virtualni" svet vsebuje enake neprijetnosti in nevarnosti kot "realni". Nevarnosti, ki jih nove tehnologije predstavljajo za otroke in mladostnike, niso povezane le z virusi in neželeno elektronsko pošto, temveč tudi s potencialno škodljivimi in nelegalnimi vsebinami, kakršne so npr. otroška pornografija, sovražni govor, nasilne vsebine, zloraba osebnih podatkov in bančnih kartic. Zanemariti ne gre tudi posledic, s katerimi se srečujejo uporabniki interneta (predvsem mladostniki), ki vsak dan na internetu preživijo ure in ure, saj pretirana raba interneta lahko vodi v zasvojenost. Prav tako pa je potrebno mladostnike seznaniti z internetnim bontonom ter jih spodbujati k odgovorni in premišljeni rabi spletnih klepetalnic, forumov ter nenazadnje tudi mobilnih telefonov.

SAFE-SI projekt izvajajo Fakulteta za družbene vede na Univerzi v Ljubljani, ZPS (Zveza potrošnikov Slovenije) in ARNES (Akademsko raziskovalna mreža Slovenije), sofinancirata pa ga Evropska komisija in Ministrstvo za visoko šolstvo znanost in tehnologijo RS.

Projekt sodi v tematski sklop osveščanja javnosti: tako staršev kot učiteljev in otrok. Cilji projekta so povezani z dvigom ravni osveščenosti glede varne rabe interneta (tudi mobilne telefonije) znotraj celotne slovenske družbe. Želimo, da bi dobro seznanjeni uporabniki svoje znanje o varnosti na internetu pričeli tudi uporabljati. Potrebno je izboljšati znanje o varni internetni komunikaciji in zaščiti pred neželenimi vsebinami. Prizadevamo si za uvedbo tematike varnejšega interneta v izobraževanje učiteljev, pa tudi v šolske klopi. Naše vodilo je naslednje: **"Osveščanje naj ne ustvarja strahu pred internetom, temveč spodbuja njegovo uporabo."**

Eden izmed najpomembnejših ciljev SAFE-SI projekta je izobraževanje slovenskih učiteljev o varnih načinih uporabe interneta v šolah. S tem namenom smo v mesecu aprilu 2006 uspešno izvedli prve seminarje za učitelje. Ključnega pomena je vključitev vsebin, ki se navezujejo na vidike varne uporabe IKT tehnologij v šolah, v redni program IKT izobraževanj za učitelje. Nekatere teme so bile s tem namenom v drugi polovici leta 2006 predstavljene na posebnih IKT seminarjih za multiplikatorje, ki jih organizirata Ministrstvo za šolstvo in šport RS ter Zavod za šolstvo RS in se jih udeleži približno 100 učiteljev na seminar.

V okviru projekta deluje tudi svetovalna telefonska linija Nasvet za net, kamor lahko mladi pokličejo vsak delovnik med 16. in 20. uro na brezplačno telefonsko številko 080 80 22.

Za uspeh projekta je pomembna tudi izmenjava naših znanj ter pridobljenih izkušenj z ostalimi evropskimi točkami osveščanja. Nenazadnje je naš cilj zadovoljen in informacijsko dobro izobražen uporabnik interneta, ki se bo zavedal pozitivnih in tudi negativnih vidikov rabe svetovnega spleta.

1.3. Omrežje InSafe

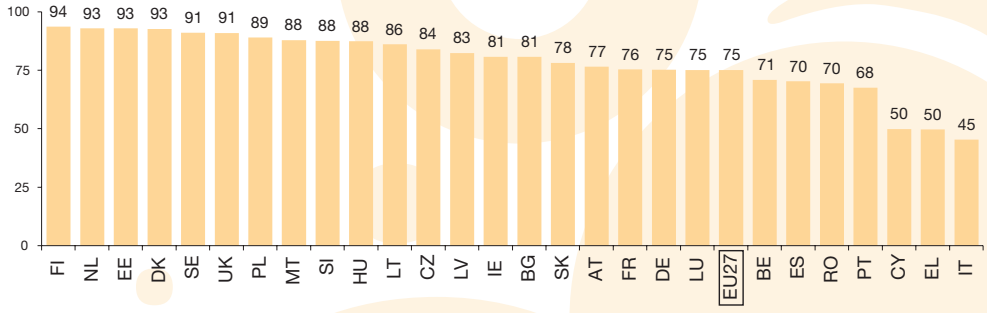
Insafe je evropsko omrežje, ki je zadolženo za koordinacijo aktivnosti s področja osveščanja javnosti glede varne rabe interneta. V omrežje so vključene posamezne nacionalne točke osveščanja (od 1. 3. 2005 tudi Slovenija). Posamezne točke osveščanja v okviru Insafe omrežja medsebojno sodelujejo, izmenjujejo znanja in izkušnje, prav tako pa tudi načrtujejo skupne aktivnosti (npr. priprava aktivnosti ob Dnevu varne rabe interneta).

Dodatne informacije o INSAFE omrežju lahko pridobite na spletni strani: *http://www.saferinternet.org/*.

1.4. Dejstva o rabi IKT tehnologij v Sloveniji

Glede na podatke Statističnega urada republike Slovenije za prvo četrtino leta 2009 je rednih uporabnikov interneta 64 % Slovencev starih med 10 in 74 let. Mladi so pričakovano najbolj pogosti uporabniki interneta, saj ga redno uporablja 98 % otrok med 10 in 15 let. Prav tako so z informacijsko komunikacijskimi tehnologijami bolj opremljena gospodinjstva z otroki - internet jih ima 85 % - kot tista brez otrok – internet jih ima 56 %. Kar 56 % gospodinjstev se na internet povezuje prek širokopasovne povezave, 37 % pa prek mobilnega telefona.

Po podatkih raziskave **Eurobarometer 2008** se Slovenija po uporabi interneta med otroki uvršča na osmo mesto v Evropi (88 %), kar je precej nad evropskim povprečjem (75 %).



Za računalnikom svoj prosti čas preživlja tudi vse več evropskih otrok mlajših od 10 let. V letu 2006 je po podatkih raziskave Eurobarometer internet uporabljalo 34% otrok starih 6-7 let, podatki Eurobarometra iz leta 2008 pa kažejo, da je internet uporabilo že 42% šestletnikov in kar 72% devetletnikov.

Podatki za Slovenijo iz leta 2008 kažejo, da internet v povprečju uporablja 73% otrok v starosti med 6 in 10 let (EU27 pa 60,1%), kar potrjuje, da je Slovenija v tem pogledu nadpovprečna članica EU. Na podlagi danih podatkov lahko tudi ocenimo, da internet v Sloveniji uporablja okoli 70% otrok starih med 5 in 9 let, kar v grobem pomeni okoli 70 tisoč otrok.

Ista raziskava je pokazala tudi sledeče:

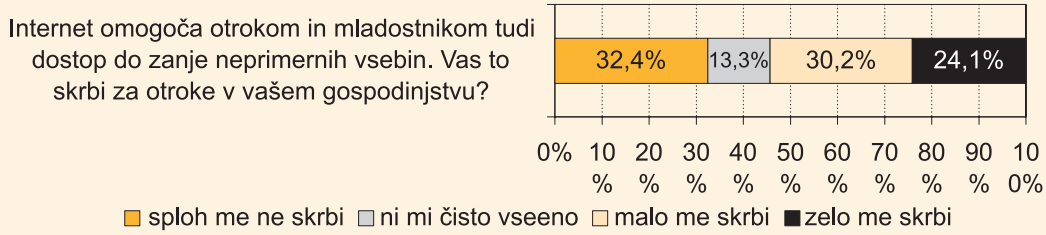
- Slovenske starše (55%) najbolj skrbi, da njihovi otroci na internetu dostopajo do strani s seksualno oz. nasilno vsebino.
- 53% staršev je zaskrbljenih zaradi medvrstniškega spletnega nadlegovanja, medtem ko jih 50% skrbi, da bi njihovi otroci postali žrtve zapeljevanja s strani odraslega z namenom prepričati jih v spolni odnos (t.i. grooming). 40% staršev pa se zaveda tudi možnosti nadlegovanja prek mobilnega telefona.
- 47% staršev se boji, da bodo njihovi otroci postali izolirani zaradi prevelike uporabe interneta.

Slovenski otroci se na svoje starše najraje obrnejo v primeru tehničnih težav (40%), medtem ko se podobno kot njihovi evropski vrstniki na starše najredkeje (6%) obrnejo v primerih, ko jih kontaktirajo tujci, ko naletijo na nasilne oz. strani s seksualno vsebino ali v primerih medvrstniškega spletnega nadlegovanja.

47% slovenskih staršev svojim otrokom ne postavlja nobenih omejitev pri uporabi interneta. Med tistimi, ki omejitve postavljajo, prevladujejo naslednje:

- 93% staršev ne dovoli izdajanja osebnih oz. zasebnih informacij,
- 88% jih ne dovoli spletnega nakupovanja,
- 87% jih postavlja časovne omejitve pri uporabi interneta,
- 80% jih ne dovoli, da bi njihovi otroci na spletu komunicirali z neznanci,

- 44% staršev svojim otrokom ne dovoli obiskovanja določenih spletnih strani,
- 15% pa jih tudi ne dovoli nalaganja glasbe, filmov in igric.



83% slovenskih staršev bi domnevno škodljivo oz. nelegalno vsebino prijavilo policiji. 40% bi tovrstno vsebino prijavilo ustrezni spletni prijavni točki. Slovenski starši (27%) so v primerjavi z evropskimi najslabše seznanjeni z obstojem nacionalne spletne prijavne točke za nelegalne vsebine.

Skoraj 90% slovenskih staršev je prepričanih, da bi se morali njihovi otroci v šoli več učiti o varni rabi interneta. Prav tako visok odstotek staršev je prepričanih, da tudi starši potrebujejo več akcij ozaveščanja.

Kot najpomembnejši vir pridobivanja informacij o varnem internetu starši navajajo družino in prijatelje (76%). Temu sledijo televizija, radio in časopisi s 60% ter različne spletne strani z 52%. Primerjava podatkov po posameznih EU državah kaže, da je iskanje informacij o varni rabi interneta po različnih spletnih straneh med slovenskimi starši zelo priljubljeno, saj znatno presegamo EU-27 povprečje pri 39%. Podatki tudi kažejo, da so organizacije in asociacije, ki se ukvarjajo s problematiko varnega interneta, pri slovenskih starših priljubljen vir informacij, saj se jih je 30% obrnilo na ta vir, s čimer smo v samem vrhu evropskih držav.

NAMIG ZA PRAKTIČNO DELO V RAZREDU: Lotite se aktivnosti iz Priročnika za razredne aktivnosti na CD-ju pod zaporedno številko 6: **»Navade rabe interneta«** in pod zaporedno številko 7: **»Digitalna pismenost«**.

Rezultati **Eurobarometer kvalitativne raziskave 2007 o varnem internetu za otroke** [1], ki je zajela tudi slovenske otroke v starosti 9-10 let ter 12-14 let, pa kažejo naslednje:

- Najpomembnejše spletne aktivnosti otrok po vsej Evropi, vključno s Slovenijo, so spletne igre, brskanje po spletu in komunikacija, medtem ko otroci mobilne telefone uporabljajo predvsem za pošiljanje kratkih SMS sporočil in pogovore s starši in prijatelji.
- V Sloveniji mladi vse manj pošiljajo SMS sporočila in mobilne telefone uporabljajo predvsem za opravljanje klicev, mlajši pa uporabljajo telefon predvsem za obveščanje

[1] Dostopno na: Eurobarometer on Safer Internet for Children: qualitative study 2007 v: *http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/qualitative_study_2007/slovenia.pdf*

staršev in krajše pogovore z njimi.

- Med spletnimi dejavnostmi slovenski mladostniki največ časa posvečajo iskanju vsebin za šolo, mlajši pa pogosto igrajo spletne igrice. Starejši s spleta prav tako nalagajo določene vsebine, predvsem glasbo, filme in igre.
- V Sloveniji starši svojim otrokom ponavadi omejijo uporabo mobilnega telefona s predplačniškim paketom, ki ga uporablja večina vprašanih. Po drugi strani pa gre pri uporabi interneta predvsem za omejevanje časa, ki ga mladi smejo preživeti na internetu, medtem ko je manj omejevanja dostopa do spletnih vsebin.
- Na splošno mladi tako v Sloveniji kot v vsej Evropi poznajo nevarnosti pri uporabi interneta in mobilnih telefonov. Otroci se na splošno dobro zavedajo potencialnih nevarnosti na spletu, kakršne so vprašanja varnosti, virusi, dostop do nezaželenih vsebin, kraje identitete in potencialno nevarni stiki s tujci. Prav tako veliko otrok dobro ve, kako se morajo zavarovati. Čeprav mladi poznajo nevarnosti in vedo, kako se morajo zavarovati, bi večina poskusila rešiti težave sama ali s svojimi prijatelji in bi se le v skrajni sili zatekla po pomoč ali nasvet k svojim staršem.

2 Zasebnost in varnost na internetu

Za začetek je potrebno razumeti razlike med varstvom in zaščito podatkov na internetu. **Varstvo podatkov** se nanaša na varovanje pomembnih podatkov, medtem ko se **zaščita podatkov** nanaša na pravice posameznika in zaščito njegovih osebnih podatkov. Zaščita in varstvo podatkov sta tako med seboj nerazdružljivo povezana. Kajti le, če so podatki primerno varovani, so posledično zaščitene tudi pravice vsakega posameznika.

To je še posebej pomembno na poti v informacijsko družbo, kjer ne smejo biti ovirane pravice posameznika do njemu lastnega, svobodnega razvoja. Zaščita podatkov nam daje možnost, da sami skrbimo za varovanje svojega zasebnega prostora. Zavedati se moramo, da tudi na internetu veljajo zakoni in pravila. Če menite, da so bili na internetu zlorabljeni vaši osebni podatki, o tem poročajte primerni službi (ponudnik internetnih storitev, Urad Informacijskega pooblaščenca, nevladne organizacije za varno uporabo interneta ...).

NAMIG ZA PRAKTIČNO DELO V RAZREDU: Lotite se aktivnosti iz Priročnika za razredne aktivnosti na CD-ju pod zaporedno številko 8: **»Ugani, kdo sem?«**

Zbiralci podatkov so vsepovsod

V času, ko še ni bilo elektronske obdelave podatkov, so bile vse informacije o državljanih napisane na papirju in običajno shranjene v nepreglednih arhivih. Rojstni podatki, spričevala in računi so bili spravljeni na različnih mestih in z njimi so upravljali različni ljudje. Glede na to, da so bili ti podatki napisani na papirju, je bilo praktično nemogoče, da bi med njimi delali (ne nujne) povezave. Medsebojna analiza podatkov je zahtevala ogromno časa in raziskovanja v različnih arhivih. Vsak izmed teh arhivov je imel (kot jih ima še danes) posebna pravila o varnosti osebnih podatkov.

Z naraščanjem uporabe računalnikov se je mnogo stvari spremenilo. O vsakem od nas je v računalniškem sistemu shranjena obilica osebnih podatkov. Če povzamemo in združimo te podatke, lahko dobimo obsežno sliko o posameznikovi osebnosti in njegovih navadah.

- Računi o kreditnih in bančnih karticah povejo, kje in kdaj nakupujemo hrano, v katerih butikih se oblačimo, v katerih restavracijah najraje jemo, kje natočimo bencin in še mnogo več.
- Telefonski računi razkrivajo, s kom in kdaj telefoniramo, posledično sporočajo tudi o intenzivnosti naših stikov z določeno osebo.

Takih primerov je nešteto, izčrpen vir informacij pa lahko postane vse od elektronskih osebnih planerjev do naših elektronskih sporočil. Na različne načine je tako možno dostopati in zbirati podatke o vsakem od nas.

Osebni podatki o državljanih so lahko koristni predvsem za državo, npr. za zasledovanje za potrebe kazenskih pregonov ali finančnih preverjanj, prav tako pa tudi za tajne službe in v znanstvene namene (Ostrež, 2006a: 4-5).

Smo na internetu sploh res lahko anonimni?

Precej trdovratno se je v ljudeh naselil občutek, da lahko internet uporabljamo skriti in izkoriščamo njegovo anonimnost. Gotovo je res, da ne moremo kar brez problemov odkriti identitete našega sogovornika v klepetalnici, na forumu ali kakšni drugi obliki internetne komunikacije. Do te mere je internet še vedno anonimen prostor, vendar pa se moramo zavedati, da ob deskanju na internetu za sabo puščamo sledi.

Po eni strani gre pri tem za tako imenovane datoteke z dnevnikom (oz. ang. »log file«). Vsak priklic posamezne spletne strani se zabeleži in ga je v teh datotekah enostavno prepoznati.

Pri datotekah z dnevnikom sami puščamo sledi za sabo na internetu, medtem ko je pri piškotkih (ang. »cookies«) stvar obratna. Piškotki se na našem računalniku namestijo avtomatično in s tem puščajo sledi, da smo obiskali določeno spletno stran. Tako postanejo javni določeni podatki o posamezniku, za katere ni nujno, da smejo biti javni. Za imenom piškotki se namreč skriva vse kaj prej kot nekaj okusno sladkega, na kar sicer namiguje simpatično ime. Piškotki so krivi za to, da nas določena spletna stran ob vsakem naslednjem obisku avtomatično prepozna. Problematično to postane takrat, ko spletna stran zbira posameznikove osebne podatke in jih spravlja v bazo podatkov. Tako na primer v oglaševalski industriji skušajo s pomočjo piškotkov zbrati informacije o tem, kakšni ljudje obiskujejo posamezne strani. V takih primerih torej gotovo ne moremo več govoriti o anonimnosti na internetu (Ostrež, 2006a: 4-5).

Kaj nam lahko povejo podatki v piškotkih?

Piškotki so informacije, ki se ob obisku posamezne spletne strani shranijo na naš računalnik in so po potrebi ponovno uporabljene. Uporabljajo se za prepoznavanje ponovnega obiskovalca določene spletne strani. V primeru, da uporabljamo isti računalnik, nas lahko spletna stran prepozna tudi mesece in leta po našem zadnjem obisku. Zavedati se moramo, da piškotki pravzaprav prepoznavajo računalnik, ne pa uporabnika računalnika.

Obstajajo različne vrste piškotkov. Razlikujemo jih glede na to, kdaj se jim izteče rok uporabe in ali so dostopni samo obiskanemu strežniku ali tudi kakšnemu zunanjemu strežniku.

Piškotki, ki se po končanem obisku strani sami nemudoma izbrišejo, so popolnoma neškodljivi. V takem primeru nas ob naslednjem obisku spletna stran ne bo prepoznala.

Piškotki so v osnovi uporabna stvar in občasno so nepogrešljivi pri brskanju po internetu. Nevarni postanejo šele, ko se jih tako ali drugače zlorabi. Veliko spletnih trgovin uporablja piškotke. Njihova uporaba je nujna, saj lahko na tak način spletno nakupovalno košarico napolnimo pravemu uporabniku. Vendar imajo prav spletne trgovine tudi velike interese, da svojega obiskovalca ob ponovnem obisku spletne strani prepoznajo.

Na primer, če smo ob zadnjem obisku v spletni trgovini iskali in kupili digitalni fotoaparat, se lahko zgodi, da nas bo naslednjič spletna stran s pomočjo piškotkov prepoznala in nam že na uvodni strani ponudila stvari, ki sodijo v dodatno opremo (bliskavico, spominsko kartico, stativ ipd.). To se lahko zgodi le v primeru, da se po opravljenem nakupu piškotki niso avtomatično zbrisali, temveč so ostali shranjeni na našem računalniku.

V takem primeru lahko to do neke mere še interpretiramo kot skrb za kupca, vendar pa v primeru, da so piškotki shranjeni na vaš računalnik z nekega zunanjega strežnika, vse skupaj postane dvomljivo. Obstajajo velika internetna podjetja, kot na primer DoubleClick, ki postavljajo spletne oglase svojih strank na množici različnih spletnih strani (oglasi se avtomatično odprejo v novem oknu). Piškotki se v tem primeru avtomatično shranijo.

Podjetja lahko na podlagi piškotkov dobijo informacijo, na katerih spletnih straneh je posamezen uporabnik iskal informacije in kakšne informacije je iskal. V primeru, da te podatke združijo, dobijo profil posameznega uporabnika. Glede na uporabnikov profil mu lahko kasneje prikazujejo oglase, ki ga bodo potencialno bolj zanimali (in premamili v nakup). Takšen pristop je potrošniku prilagojeno oglaševanje. K preprečevanju takšnih zlorab lahko pomagajo le skupni pritiski uporabnikov in organizacij, ki se ukvarjajo z varnostjo podatkov na internetu (Ostrež, 2006a: 10-11).

Piškotki: kaj lahko storimo?

Vsak brskalnik nudi različne možnosti za nastavitve, kako ravnati s piškotki. Praviloma ne dovolite, da se shranjujejo piškotki z zunanjih strežnikov. Svoj računalnik lahko nastavite tudi tako, da bo po vsakem zaključenem obisku interneta izbrisal vse piškotke. Piškotke lahko izbrišete tudi ročno, navodila za to najdete v oknu pomoč pri vašem spletnem brskalniku (Ostrež, 2006: 11).

Vsak brskalnik ima svoj način za brisanje piškotkov/cookies. Vsi pa imajo to nastavitev v »nastavitvah/preferences«, ponavadi pod »zasebno/privacy«. Tam imate gumb za izbris vseh piškotkov/cookies.

NAMIG ZA PRAKTIČNO DELO V RAZREDU: Lotite se aktivnosti iz Priročnika za razredne aktivnosti na CD-ju pod zaporedno številko 27: **«Spretni spletni raziskovalci«**.

2.1 Namerne zlorabe vašega računalnika[2]

2.1.1 Najpogosteje uporabljene zlorabe

a) Trojanski konji, virusi in črvi

Trojanski konji

Ena od osnovnih različic škodljive programske kode je trojanski konj. Običajno se predstavlja kot uporaben ali zabaven programček (npr. ohranjevalnik zaslona). Tako kot njegov legendarni soimenjak pa vsebuje tudi destruktivni del: medtem ko je program aktiviran, uničuje datoteke ali ustvari t. i. »back doors«, ki omogočijo tretjim osebam popoln nadzor nad vašim računalnikom in datotekami na njem (npr. kraja gesel).

Trojanski konji samodejno ne »okužijo« drugih računalnikov ali programov, kar je značilno za dve drugi družini škodljivih programskih kod, črvi (»worm«) in virusi.

Več informacij o trojanskih konjih si lahko ogledate v naslednjem dokumentu: *http://www.cert.org/advisories/CA-1999-02.html*.

Virusi

Virus je računalniška koda, ki se pripne na program ali datoteko, tako da se lahko razširi iz enega računalnika v druge in jih tako okuži. Virusi lahko poškodujejo programsko opremo, strojno opremo in datoteke. Virus se lahko razširi zelo hitro, še posebej, če uporabnik tako datoteko/program z uporabo interneta, diskete, CD-ja ali drugega medija prenese na druge uporabnike.

Do nedavnega so bili virusi zmožni okužiti le datoteke programov (tipa .exe, .msi), vendar so se s prihodom raznih skriptnih jezikov – macrojev - v različnih programih (npr. Word, Excel, Outlook ipd) virusi naselili tudi v datoteke dokumentnih tipov (.doc, .xls, .eml, .html ...). S tem se je dokončno zabrisala meja med datotekami, ki lahko vsebujejo virus, in tistimi, ki so na to imune.

Virusi se lahko prenašajo le preko okuženih medijev ali preko računalniških povezav, kot so modemi in računalniške mreže. Najpogosteje viruse prenašajo otroci preko računalniških igric, ker ponavadi ne preverjajo programov. Otrok dobi računalniško igrico od prijatelja, jo spet naprej posodi sošolcu, ki mu v zameno ponudi drugo okuženo igrico in tako se okužba razširi. Največ problemov z virusi, trojanskimi konji in črvi imajo ravno uporabniki, ki si veliko izmenjujejo datoteke preko spleta s pomočjo programov KAZAA, IMESH ipd.

Črvi (»Worms«)

Črvi se prav tako kot virusi razširjajo samodejno, a s to razliko, da ne okužijo obstoječih datotek ali programov. Ostanejo aktivni v delovnem pomnilniku in se skušajo preko omrežja (interneta) ter avtomatiziranih mehanizmov (npr. razpošiljanje e-pošte) operacijskega sis-

[2] Poglavje o namernih zlorabah računalnika je povzeto po spletni strani ARNESA: *http://www.arnes.si/help/zascita_racunalnika.html*.

tema razširiti na čim več računalniških sistemov. Večina tega početja je za uporabnika sprva neopazna, kasneje pa se lahko kaže v večji obremenjenosti - počasnosti sistema (zaradi nekontroliranega razpošiljanja črva na veliko število naslovov). Poleg tega večina črvov vsebuje tudi različne prijeme, ki izkoriščajo varnostne luknje v sistemu in s tem odpirajo t. i. »back doors« (dostop in nadzor nad vašim računalnikom s strani tretjih oseb) in drugo (brisanje datotek, spreminjanje nastavitev ipd.).

b) »Back door« programi in programi, ki omogočajo administriranje na daljavo

Za pridobitev oddaljenega dostopa do računalnikov, ki uporabljajo okolja Windows, napadalci najpogosteje uporabljajo orodja, kot so: BackOrifice, Netbus, Prorat in SubSeven. Ti »back door« programi oziroma programi za oddaljen nadzor, ko so enkrat nameščeni, omogočajo drugim ljudem dostop in kontrolo nad vašim računalnikom.

c) DOS napadi

Naslednja oblika napada se imenuje DOS napad (»Denial-of-service«). Pri tej obliki napada je na žrtev hkrati poslano toliko zahtev za komunikacijo, da ne more več učinkovito komunicirati s poštenimi klienti. V večini primerov bodo najnovejši popravki za vaš operacijski sistem preprečili tak napad. Spodnja dokumenta opisujeta DOS napad bolj podrobno: *http://www.cert.org/advisories/CA-2000-01.html* in *http://www.cert.org/archive/pdf/DoS_trends.pdf*.

Dobro je vedeti tudi, da ste lahko poleg osebne tarče dos napada tudi medij oziroma lahko vaš računalnik napadalci uporabijo kot soudeleženca v dos napadu na drugi računalniški sistem.

d) Sredstvo za napad na drug računalnik

Napadalci bodo pogosto uporabljali ogrožene računalnike kot vzletne plošče za napade na druge sisteme. Poglejmo si to v primeru DOS napada. Napadalec najprej namesti na ogroženi računalnik agenta (pogosto trojanskega konja), ki na računalniku čaka nadaljnja navodila. Ko napadalec pridobi določeno število računalnikov pod svojo kontrolo, vsem skupaj naroči izvedbo DOS napada na nek tretji sistem. Torej končna žrtev DOS napada ni vaš računalnik, temveč računalnik nekoga drugega. Vaš računalnik je le primerno orodje za napad večjih razsežnosti.

e) Nezaščitene datoteke operacijskega sistema Windows

Nezaščitene Windows omrežne datoteke lahko napadalci zlorabljajo tako, da namestijo veliko število orodij na računalnike, na katerih delujejo operacijski sistemi Windows in so priključeni na internet. Ker je varnost računalnikov na internetu medsebojno odvisna, ogroženi računalnik ne povzroča težav le svojemu lastniku, temveč je grožnja tudi ostalim subjektom na internetu. Večjo grožnjo za internetno skupnost potencialno predstavlja veliko število v internet priključenih računalnikov z nezaščitenimi Windows omrežnimi datotekami in z nameščenimi orodji za napade, ki so predstavljena na spletni strani: *http://www.cert.org/incident_notes/IN-2000-01.html*. Druge grožnje predstavljajo škodljive in destruktivne kode, kot so virusi ali internetni črvi, ki nezaščitene Windows datoteke uporabljajo kot bazno postajo za svoje širjenje.

f) Prenosne kode (Java, JavaScript, ActiveX)

Obstajajo poročila o težavah z mobilnimi kodami (Java/JavaScript/ActiveX). To so programski jeziki, ki omogočajo izdelovalcem spletnih strani napisati kodo, ki jo izvede vaš spletni brskalnik. Čeprav je koda splošno uporabna, jo lahko napadalci uporabijo za pridobitev določenih podatkov (npr. katere spletne strani obiskujete) ali za zagon škodljive kode na vašem računalniku. Omenjene kode lahko onemogočite v vašem spletnem brskalniku. Priporočamo, da to storite, če obiskujete spletne strani, ki jih ne poznate oziroma jim ne zaupate.

Bodite pozorni tudi na grožnje, ki vključujejo uporabo mobilnih kod znotraj poštnih programov. Mnogi poštni programi uporabljajo iste kode kot spletni brskalniki za prikaz HTML. Dodatne informacije o škodljivih kodah so na voljo na: *http://www.cert.org/tech_tips/malicious_code_FAQ.html*.

Dodatne informacije o ActiveX varnosti so na voljo na: *http://www.cert.org/archive/pdf/activeX_report.pdf*.

g) Navzkrižno pisanje

Škodljivec lahko na spletni strani pripne škodljivo skripto in ko spletno stran pregledujemo, se škodljiva skripta prenese na vaš računalnik. Svoj spletni brskalnik izpostavljate škodljivim skriptam z:

- odpiranjem povezav na spletnih straneh in v elektronskih sporočilih ne da bi vedeli, kakšna je njihova vsebina,
- uporabo komunikacijskih orodij na straneh, ki jim ne zaupate,
- ogledovanjem forumov, klepetalnic ali drugih dinamično generiranih strani, kjer lahko uporabniki objavljajo tekste s HTML priveski.

Dodatne informacije glede groženj s škodljivimi kodami na spletnih povezavah lahko najdete tukaj: *http://www.cert.org/advisories/CA-2000-02.html*.

h) Prevare z elektronsko pošto

Tarča email spoofing-a postanemo, ko dobimo elektronsko sporočilo od lažnega pošiljatelja. Ta oblika ogrožanja računalnika je poskus prevare uporabnika, s katero napadalci želijo pridobiti pomembne informacije (npr. gesla). Omenjena elektronska sporočila variirajo od neslanih in neškodljivih šal do »social engineering« projektov:

- Elektronsko sporočilo, kjer se pošiljatelj izdaja za sistemskega administratorja in zahteva od uporabnika, da svoje geslo zamenja za tistega, ki mu ga določi on in celo grozi s sankcijami, če uporabnik tega ne stori.
- Elektronsko sporočilo, kjer se pošiljatelj izdaja za osebo z avtoriteto in od uporabnika zahteva, da mu pošlje kopijo datotek z gesli ali drugo pomembno informacijo. Pomembno je vedeti, da nas tudi ISP-ji (Internet service provider oz. ponudnik internetnih storitev) občasno nagovorijo k menjavi gesel, vendar nikoli ne zahtevajo določene oblike oziroma vsebine gesel. Vedeti moramo tudi, da večina legitimnih ISP-jev ne bo nikoli zahtevala od vas, da jim pošljite podatke o vaših geslih preko elektronske pošte. Če sumite, da ste dobili spoofed elektronsko sporočilo, takoj kontaktirajte osebje vašega ISP-ja.

i) Virusi, ki se prenašajo preko elektronske pošte

Virusi in druge oblike škodljivih kod se pogosto prenašajo v priponkah elektronskih sporočil. Preden odprete katerokoli priponko, bodite prepričani o viru in vsebini priponke. To, da je sporočilo prišlo iz elektronskega naslova, ki ga prepoznate, še ni zagotovilo. Virus Melissa se je širil ravno zato, ker je vedno prihajal iz prepoznanih e-mail naslovov. Škodljive kode se lahko prenašajo tudi preko zabavnih in mamljivih programov. Datoteke, ki so pripete k elektronskem sporočilu, so na prvi pogled lahko neškodljive z varnimi končnicami (.txt, .avi, .mpeg ali druge), čeprav so to v resnici datoteke s škodljivimi skriptami (npr. .vbs ali .exe).

k) Programi za klepetalnice

Programi za internetno klepetanje kot npr. IRC (»Internet Relay Chat«), MSN Messenger, Skype, ICQ ... ponujajo mehanizme, s katerimi se informacije prenašajo dvosmerno med računalniki na internetu. »Chat« klienti omogočajo skupinam posameznikom, da si med sabo izmenjujejo dialog, URL povezave in v mnogih primerih tudi datoteke. Ker mnogi »chat« programi omogočajo izmenjavo .exe datotek, predstavljajo podobno grožnjo kot poštni programi. Kot skrbimo za zaščito poštnih programov, bi morali skrbeti tudi za zaščito »chat« programov predvsem z omejevanjem možnosti odpiranja potencialno nevarnih datotek, kot so .vbs in .exe datoteke. Zavedajte se tudi morebitnih neprijetnih posledic izmenjave datotek z neznanimi sogovorniki.

l) Paketno vohunjenje (»packet sniffing«)

»Packet sniffing« je tehnika, ki pregleduje in izloča informacije iz informacijskih paketov, ki potujejo po internetnem omrežju. Izluščene informacije lahko vsebujejo uporabniška imena, gesla in druge pomembne informacije, ki potujejo v omrežju v čisti tekstovni obliki. S pomočjo stotih ali tisočih gesel, ki jih program pridobi, lahko vsiljivec sproži obsežen napad na sisteme. Namestitev omenjenega programa ne zahteva administratorskih pravic na računalniku, kjer program nameščamo. V nasprotju z uporabniki DSL dostopa in klicnih modemov, so uporabniki kabelskega dostopa bolj ranljivi na »packet sniffers« programe, saj je celotna soseska povezana v eno samo LAN omrežje. Program, ki je nameščen na enem samem kabelskem modemu v omrežju, lahko izlušči pomembne podatke iz vseh drugih kabelskih modemov v omrežju.

2.1.2 »Ribarjenje«

Za razliko od tehnik vdorov in prestrezanja pa na internetu obstajajo še nekatere tehnike zlorabe zasebnosti in kiberkriminala. Ena izmed njih je t. i. »ribarjenje«, v angleščini »phishing«; izraz izvira iz angleških besed za geslo (»password«) in ribarjenje (»fishing«). Napadalci postavijo lažno spletno stran oziroma pošljejo prirejeno elektronsko sporočilo, s katerimi poskusijo uporabnika **prepričati, da jim posreduje svoje osebne podatke**. (Kovačič, 2006).

Najpogostejša oblika te prevare je, ko elektronsko pismo ali spletna stran od uporabnika zahteva, da vanjo vnese svoje finančne podatke ali gesla. Tako goljufiva spletna stran kot elektronsko pismo sta lahko na pogled popolnoma enaka spletni strani ali pismu legitimnega podjetja (npr. banke), vendar pa bosta vaše finančne podatke posredovala tretjim osebam, ki se bodo z njimi okoristile.

V svoj elektronski poštni nabiralnik na primer prejmete pismo, ki zatrjuje, da je vaš bančni račun zaklenjen ali pa zahteva potrditev vaše identitete preko spletne strani. Obstaja več različnih scenarijev, ki pa imajo vsi isti cilj - okrasti uporabnika. Prejeta elektronska pisma lahko omogočajo kar direkten vnos podatkov, lahko pa vsebujejo povezave do ponarejenih spletnih strani, kjer uporabnik vnese svoje podatke. Takšna pisma in spletne strani so izredno zavajajoče, saj izvirno podjetje posnemajo tako po izgledu kot tudi po funkcionalnosti. Gre pravzaprav za krajo identitete, katero trenutna zakonodaja v Evropi ne obravnava dovolj ostro.

Kot primer »ribarjenja« oz. phishinga podatkov je bil v Sloveniji odmeven primer ponarejene vstopne strani NLB Klika (dostopno na: *http://www.nlb.si/cgi-bin/nlbweb.exe?doc=16038*), ki pa na srečo ni povzročil večje škode. NLB je uporabnike NLB Klika ob incidentu opozorila, da so ugotovili pojav nove škodljive programske opreme, ki simulira lažni vstopni ekran NLB Klika. Od uporabnika je zahtevala izvoz kvalificiranega digitalnega potrdila ter vnos različnih gesel.

Da boste znali razločiti med pravo in ponarejeno vstopno stranjo v NLB Klik, je NLB za svoje uporabnike pripravil kratke opise in prikaze razlik ter varnostnih opozoril, če tako stran zaznate.

Lastnosti prave vstopne strani:

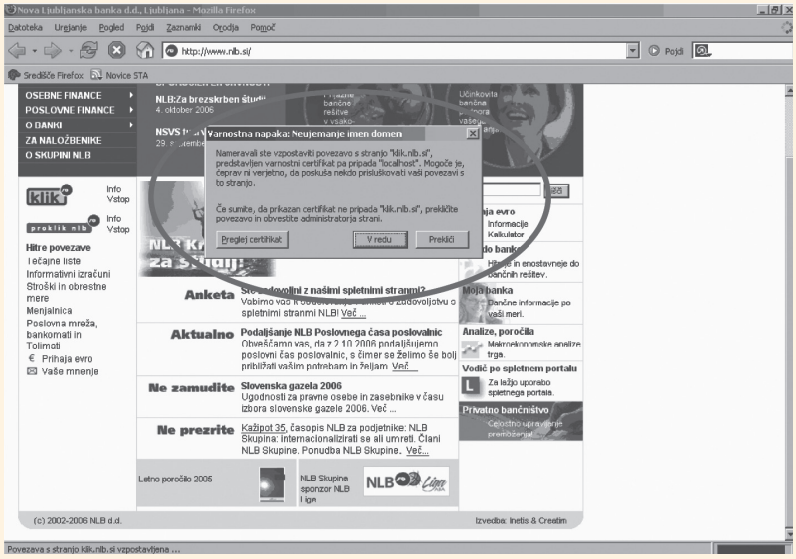
- V naslovni vrstici je naveden naslov ***https://klik.nlb.si***.
- Na ekranu brskalnika je simbol zaklenjene ključavnice.
- Na ekranu brskalnika sta zapisana ime in priimek uporabnika.
- Na ekranu je zgolj polje za vnos vstopnega gesla v NLB Klik.

Lastnosti lažne spletne strani:

- V naslovni vrstici je naveden naslov ***https://klik.nlb.si***, ki **SE NE RAZLIKUJE OD PRAVEGA**.
- Na ekranu brskalnika **NI** simbola zaklenjene ključavnice.
- Na ekranu brskalnika **NISTA** zapisana ime in priimek uporabnika.
- Pojavi se lahko več ekranov, ki omogočajo: brskanje/iskanje kopije shranjene datoteke s kvalificiranim digitalnim potrdilom, povezavo na stran z navodili za izvoz kvalificiranega digitalnega potrdila ali vnos gesla za kvalificirano digitalno potrdilo in gesla za vstop v NLB Klik.

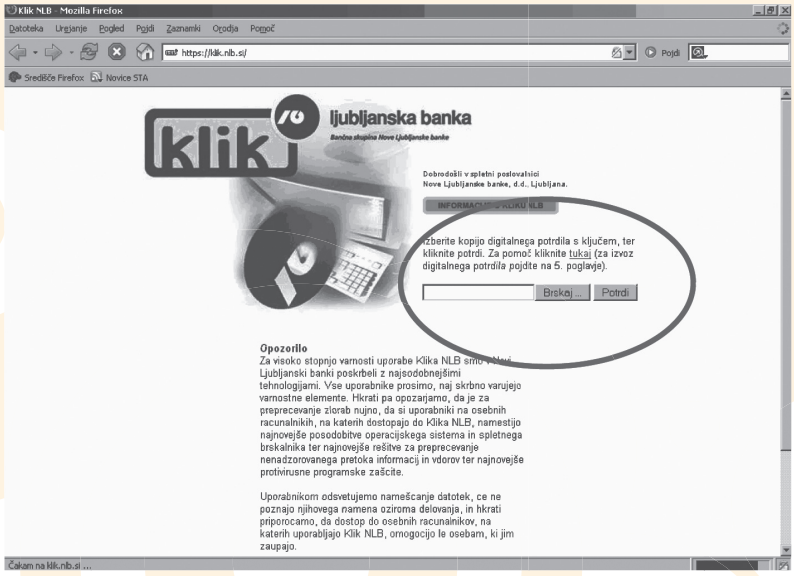
Poleg tega se lahko zavarujete pred ribarjenjem tako, da svojo vstopno stran v NLB Klik personalizirate tako, da si nanjo vpišete svoje osebno sporočilo (npr verz iz najljubše pesmi, priljubljen pregovor, življenjski moto ali kakšno zabavno domislico). To varovalno možnost je NLB ponudil takoj po pojavu lažne spletne strani. Če boste kdaj odprli Klik in ne bo vašega sporočila, boste takoj vedeli, da je s stranjo nekaj narobe.

Primer lažne vstopne strani v NLB Klik:



Lažna spletna stran vas poskuša prepričati, da bi izvozili vaše osebno kvalificirano digitalno potrdilo v datoteko in jo poslali lastniku lažne spletne strani.

Slika 1: Primer lažne vstopne strani, ki od vas zahteva aktivnost izvoza kvalificiranega digitalnega potrdila (vir: NLB).

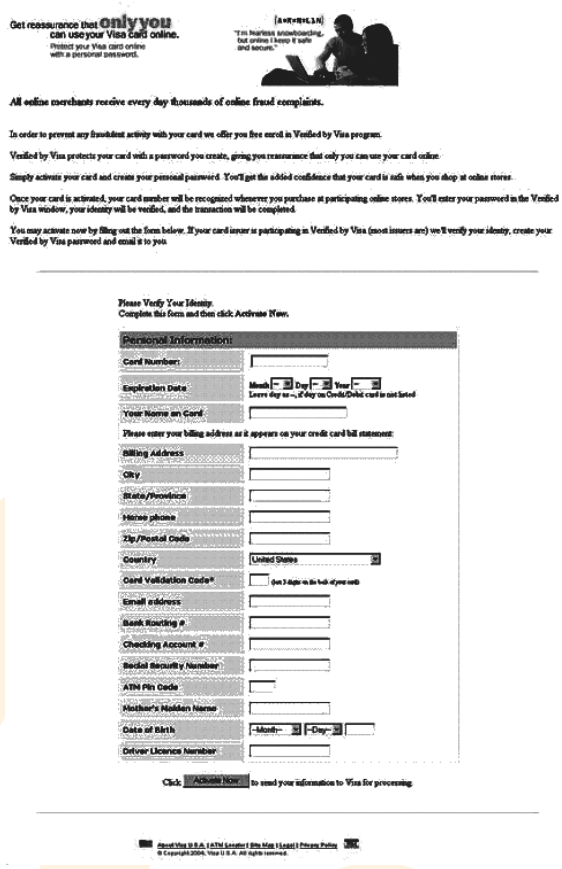


Lažna spletna stran od vas poskuša pridobiti še dva varnostna elementa NLB Klika in sicer: geslo s katerim ste zavarovali datoteko z vašim kvalificiranim digitalnim potrdilom in geslo s katerim vstopate v NLB Klik.

Slika 2: Primer lažne vstopne strani, ki od uporabnika zahteva vnos gesla za kvalificirano digitalno potrdilo in vnos gesla za vstop v NLB Klik (vir: NLB).

Bolj napredne spletne strani, ki vam želijo izprazniti račune, pogosto ponaredijo celo izgled vašega brskalnika. Tako se lahko ponaredi naslovna vrstica, kjer bo na prvi pogled izpisan »pravi« spletni naslov, vključno s predpono »https:« in »varno ključavnico« v statusni vrstici.

V naslednjem primeru elektronsko pismo že vsebuje vnosna polja. Tu preusmeritev na ponarejene spletne strani niti ni potrebna. Vneseni podatki so bili namesto k podjetju »Visa« poslani na poštni predal pri podjetju »halfpricehosting.com«.



Slika 3: Primer zavajajočega elektronskega sporočila »Visa« (vir: Arnes).

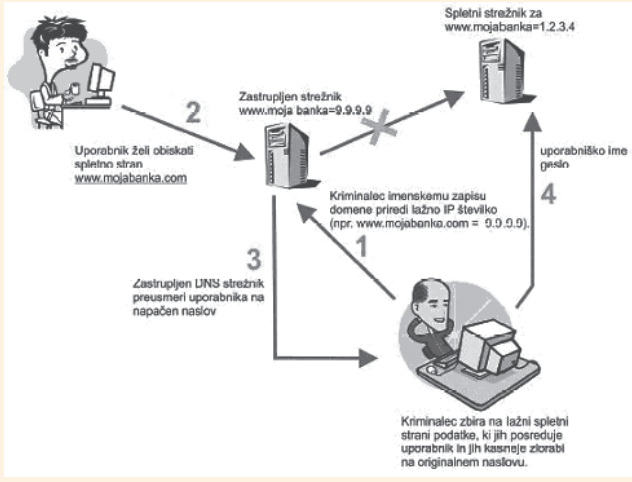
Kako se izogniti prevari »phishing[3]«?

- Nikoli ne odgovarjajte na elektronska pisma, ki od vas zahtevajo osebne in finančne podatke.
- Prav tako ne sledite povezavam do takšnih spletnih strani. Legitimna podjetja vam takšnih zahtev nikoli ne bodo pošiljala po elektronski pošti ali preko spleta.
- Ko se prijavljate na spletne strani, ki imajo karkoli opraviti z denarjem, njihov spletni naslov (url) obvezno vtipkajte direktno v naslovno vrstico.
- Osebnih in finančnih podatkov nikoli ne pošiljajte preko elektronske pošte, ker tovrstno pošiljanje ni varno.
- Redno preverjajte izpiske bančnih računov in kreditnih kartic za kakšne nenavadne odlive z vašega računa, za katere ste prepričani, da jih niste odobrili sami.
- Na računalniku imejte nameščene najnovejše popravke operacijskega sistema (npr. »windows update«) in posodobljen antivirusni program.

[3] Vir: ARNES, dostopno na *http://www.arnes.si/si-cert/obvestila/2004-06.html.*

2.1.3 »Pharming«

Pri tovrstnih napadih so **uporabniki**, ne da bi to sploh vedeli, **preusmerjeni na zlonamerne spletne strani**, četudi v naslovno vrstico brskalnika pravilno vnesejo URL naslov strani, ki bi jo radi obiskali. Ker so lažne strani največkrat popolne kopije originalnih, uporabniki sploh ne opazijo, da so na lažnem spletnem naslovu in da se pravzaprav v ozadju dogaja nekaj škodljivega. Ravno na to »karto nevednosti« igrajo napadalci, saj od uporabnikov, ki so na lažni strani, ni težko izvabiti zaupnih podatkov, med katerimi so še posebej zaželene številke kreditnih kartic s podatki, ki so potrebni za dostop do in uporabo e-bančnih storitev. Pri napadih »pharming« gre za neposredne napade na DNS-strežnike ali na datoteko o gostiteljih (»hosts«), ki je v uporabnikovem računalniku. (Skrt, 2005: 24-25).



Slika 4: Prikaz delovanja napada »pharming« (Skrt, 2005: 24)

2.1.4 Spam

Z izrazom »*spam*« označujemo **nezaželena oziroma nenaročena elektronska sporočila**. Večinoma gre za oglaševanje; pogosto tudi različnih goljufivih ali nezakonitih izdelkov ali storitev. Raziskave kažejo, da količina takšnih sporočil narašča in krni uporabnost elektronske pošte. Zaradi možnosti velikih zaslužkov je spam tudi eden izmed pomembnih dejavnikov za razmah kiberkriminala. Poleg spama povezanega z elektronsko pošto poznamo še spam na konferencah USENET, sistemih za klepet preko interneta (MSN, ICQ, itd), v zadnjem času pa se pojavlja tudi v obliki dopisovanja reklamnih komentarjev na spletne dnevnike oz. bloge (Kovačič, 2006).

V splošnem lahko za spam sporočilo označimo vsako sporočilo, ki je poslano večjemu številu naslovnikov z namenom vsiljevanja vsebine, ki se je naslovniki sami ne bi odločili prejemati. V veliki večini primerov gre za oglaševanje plačljivih storitev ali izdelkov. Ponavadi se s spam pošto oglašujejo izdelki ali storitve dvomljive kvalitete, velikokrat pa gre za goljufije (tipičen primer je nigerijska prevara – *http://www.arnes.si/spam/nigerijska-prevara.txt,* ki prevarantom včasih uspe tudi pri nas*)*.

Pošiljateljev poštni naslov (polje From:) in naslovnikov poštni naslov (polje To:) sta v spam sporočilu skoraj vedno ponarejena. Da bi spam pošta prelisičila programsko opremo, ki

sporočila filtrira, je naslovna vrstica običajno precej nedolžna in osebna (npr. »Info you requested« ali »Did you get my message?«).

Strokovnjaki za varnost v zadnjem času opozarjajo na vrsto spampošte, ki kroži po internetu in zaobide varnostne filtre, ker vsebuje sliko. **Slikovni spam** se je pojavil šele leta 2006, toda naraščal je s tako hitrostjo, da danes predstavlja večino prometa nezaželenih e-poštnih sporočil. Taka sporočila še vedno služijo istim namenom kot standardna nezaželena sporočila, recimo preprodajanju zdravil, kot so Viagra, Xanax ali Valium, ter drugih čudežnih preparatov in naprav (vir: Moj mikro, 2007).

Spamfiltri delujejo tako, da analizirajo vsebino elektronske pošte in iščejo besede ter fraze, ki so običajne za nezaželena sporočila. Če je poslano sporočilo v obliki slike, potem ta tehnologija ne nudi nobene zaščite. Po poročanju spletnega portala RTV SLO (*http://www.rtvslo.si/modload.php?&c_mod=rnews&op=sections&func=read&c_menu=9&c_id=126426)* strokovnjaki za zdaj uporabljajo tehniko blokiranja računov, iz katerih prihajajo slikovni spami. Razvili pa so tudi filter, ki primerja slike v pošti s tistimi, ki so na črni listi v bazi. Ena izmed možnosti za sledenje spamslik je tudi ta, da računalnik prepozna barvo in število pikslov, ki sestavljajo sliko, saj so slike navadno skenirane. Nato se filtri na osnovi teh podatkov odločijo, ali gre za nezaželeno sporočilo ali ne.

Ker ponudniki dostopa do interneta kot zaščitni ukrep pogosto omejujejo dostop do strežnikov za pošiljanje odhodne pošte, so spamerji pričeli vdirati v računalniške sisteme z namenom pošiljanja nezaželene elektronske pošte delno pa tudi postavljanja lažnih spletnih strani, preko katerih prodajajo npr. (otroško) pornografijo ali ponarejena zdravila. Pri tem si pomagajo z računalniškimi virusi in črvi (npr. W32.SoBig.E in F, Fizzer, itd.) (Kovačič,2006a).

Področje neposrednega trženja s pomočjo elektronskih komunikacij (in posledično področje neželenih elektronskih sporočil in nenaročene oglasne pošte) v Sloveniji urejajo štirje zakoni, trije specialni ter sistemski zakon:

- Zakon o elektronskih komunikacijah (ZEKom-UPB1),
- Zakon o varstvu potrošnikov (ZVPot-UPB2),
- Zakon o elektronskem poslovanju na trgu (ZEPT),
- Zakon o varstvu osebnih podatkov (ZVOP-1).

Osnovna načela glede neposrednega trženja, ki so predpisana v naštetih zakonih, so na Uradu informacijskega pooblaščenca[4] povzeli z naslednjimi točkami:

- pošiljatelj mora predhodno pridobiti soglasje vsakega naslovnika,
- naslovnik ima pravico kadarkoli zavrniti nadaljnjo uporabo svojega elektronskega naslova,

[4] *http://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/varstvo-osebnih-podatkov-na-internetu/, 12. 11. 2007*

- pošiljatelj mora pri obdelavi osebnih podatkov upoštevati Zakon o varstvu osebnih podatkov.

NAMIG ZA PRAKTIČNO DELO V RAZREDU: Lotite se aktivnosti iz Priročnika za razredne aktivnosti na CD-ju pod zaporedno številko 9: **»Nenadležno spam sporočilo«.**

2.1.5 Vohunski programi

V zadnjem času vedno bolj pogosta nadloga je parazitno vohunsko programje. Parazitni programi oziroma tako imenovani **»Spyware« ali »Adware**« so različni programi, ki spremljajo brkljanje uporabnika po internetu, odpirajo različna brskalna okna z reklamami in (ne)zanimivo vsebino, včasih pa pred njimi niso varni niti podatki, ki jih tipkamo med delom z računalnikom, npr. številke kreditnih kartic. Obstajajo tudi vohunski programi, ki ugotavljajo, ali je programska oprema na računalniku legalna ali ne.

Izraz »spyware« označuje programe, ki so namenjeni (prikritemu) zbiranju osebnih podatkov. Podobni izrazi so še »adware« za program namenjen prikazovanju oglasov, »browser hijackers«, ki je namenjen preusmerjanju spletnih brskalnikov in »malware« za različne nezakonite dejavnosti. Med slednjimi so najbolj znani t. i. *klicalniki* (ang. »dialer«), ki zamenjajo telefonsko številko ponudnika dostopa do interneta v uporabnikovih nastavitvah omrežja na klic z neko plačljivo telefonsko številko, po možnosti v tujini. Nekateri proizvajalci protivohunskih programov med »spyware« štejejo tudi nekatere spletne piškotke, ker je mogoče s pomočjo njih slediti gibanje uporabnika po spletu in s tem zbirati osebne podatke (Kovačič, 2006).

Pri pregledovanju nekaterih spletnih strani vam lahko neko spletno mesto ponudi namestitev posebnega programa ali pa celo izkoristi ranljivosti v operacijskem sistemu ali spletnem brskalniku in tak program namesti brez opozorila in vednosti uporabnika. Gre za **t. i. »dialer« programe**, ki spadajo v kategorijo *trojanskih konjev*. Najbolj pogosto se takšni programi ponujajo na straneh s pornografskimi vsebinami, in sicer pod pretvezo, da gre za program, ki omogoča pregledovanje slik na teh straneh.

Slika 5: Del spletne strani, ki ponuja dostop do vsebine pod pogojem, da namestite poseben program »Strip Player« (vir: Arnes).

Program se namesti kot »ActiveX« komponenta, če uporabljate Internet Explorer. Avtorji vas celo skušajo prepričati, da gre za varen program in da kliknite potrditev, ko vas bo računalnik vprašal, ali res želite namestiti neznano komponento.

»Dialer« programi (znani tudi pod imenom »autodialers«) po namestitvi na računalniku čakajo, da uporabnik sam vzpostavi zvezo s svojim ponudnikom dostopa do interneta preko telefonske zveze. Po nekaj minutah »dialer« prekine zvezo z domačim ponudnikom in vzpostavi novo, vendar s ponudnikom v tujini. Ta prekinitev traja kratek čas, običajno pa program tudi izključi modemov zvočnik, tako da se ponovno vzpostavljanje povezave v tujino vzpostavi brez piskanja, ki je običajno pri uporabi modema.

Kako preprečiti visoke telefonske račune z omejevanjem odhodnih telefonskih klicev?

- kabel, ki povezuje modem s telefonsko vtičnico vedno iztaknite iz vtičnice, ko ne potrebujete dostopa do interneta ali
- pri Telekomu Slovenije naročite omejitev odhodnih klicev v mednarodnem prometu in na premijske storitve (090).

2.1.6 Zbiranje javno dostopnih podatkov

Za uporabnika lahko predstavljajo problem tudi različni načini zbiranja osebnih podatkov, saj gre v teh primerih pogosto za poseg v informacijsko zasebnost. Osebni podatki se lahko beležijo v različnih datotekah aktivnosti oziroma jih je mogoče najti na javnih mestih. V slednjem primeru se za njihovo zbiranje uporabljajo posebni iskalniki, ki iščejo podatke po vseh javno dostopnih spletnih mestih.

Znani so primeri hekerskih skupin, npr. *L0pht*, ki preiskujejo javne strežnike podjetij in na njih iščejo pomotoma objavljene zaupne dokumente. Iskanje zaupnih informacij in dokumentov je mogoče tudi z uporabo iskalnika Google, gre za t. i. *»Google hacking«, hekanje z Googlom*. Z iskalnikom Google je tako mogoče najti številne občutljive podatke, med drugim tudi gesla in povezave do nadzornih kamer (Kovačič, 2006).

2.2 Tehnični vidiki zaščite

2.2.1 Protivirusni in protismetni programi

Ena pomembnih stvari, na katero opozarjajo strokovnjaki za računalniško varnost, je dobra zaščita pred virusi. Ker pa se novi virusi pojavljajo vsak dan, je pomembno, da uporabnik svoj protivirusni program redno dopolnjuje z novimi protivirusnimi vzorci. Današnji protivirusni programi večinoma omogočajo dopolnjevanje virusnih vzorcev prek interneta s pomočjo tehnologije **t. i. samoposodobitve**, kar uporabniku olajša skrb za redno posodabljanje protivirusnih vzorcev. Dobri protivirusni programi so največkrat plačljivi, posodabljanje virusnih vzorcev pa je brezplačno, vendar strošek zagotovo odtehta tveganje okužbe z virusom, s tem pa zmanjša možnost kraje ali izgube podatkov.

Podobno kot protivirusni programi delujejo tudi protismetni programi, ki odstranjujejo t.i. spyware, a s to razliko, da je kar nekaj protismetnih programov na voljo brezplačno (Kovačič, 2006).

2.2.2 Požarni zid

Požarni zid (ang. »*firewall*«) je poseben vmesnik (program ali strojna oprema), ki omejuje nepooblaščene dostope iz omrežja oz. v omrežje. Omejitve dostopa so mogoče na IP naslov ali na vrata (ang. »*port*«), skozi katera poteka komunikacija. Nekateri programski požarni zidovi s pomočjo digitalnega podpisa tudi preverjajo integriteto in pristnost programov, ki želijo vzpostaviti dovoljeno povezavo. Znani programski požarni zidovi so npr. ZoneAlarm, BitDefender, Kerio Personal Firewall, Personal Tiny Firewall, itd (Kovačič, 2006).

Namestitev požarnega zidu je še posebej pomembna za uporabnike, ki so v internet povezani preko ADSL in Kabla, ki jim zagotavlja neprestano povezavo. Računalnik povezan v internet brez ustrezne zaščite izgleda približno tako, kot če bi odšli od doma in pustili vhodna vrata na široko odprta.

2.2.3 Šifriranje

Ena izmed najbolj znanih zaščitnih tehnik je kriptografija oz. šifriranje. Gre za skupek metod, s katerimi temeljno sporočilo, čistopis (ang. »*cleartext*, *plaintext*«), zašifriramo, oziroma šifropis ali tajnopis (*kriptogram*, »*ciphertext*«) dešifriramo. Pri tem poleg šifrirnega postopka oz. algoritma uporabimo tudi ključ ali geslo. Kriptografske tehnike je mogoče uporabiti tudi za preverjanje integritete podatkov ter izvedbo digitalnega podpisa, za zaščito vsebine sporočil (s čimer zagotovimo tajnost komuniciranja), pa tudi vsebine datotek in celotnih pomnilniških medijev (trdih diskov). Z uporabo šifriranja znotraj računalniškega sistema se lahko izognemo tudi kraji podatkov v primeru nepooblaščenega (fizičnega) dostopa.

Obstajajo številni programi za šifriranje podatkov, med najbolj znanimi pa je PGP, oziroma njegova prosta različica GPG, ki temeljita na asimetrični kriptografiji. Le-ta deluje tako, da imata tako tisti, ki sporočilo pošilja (pošiljatelj), kot tisti, ki sporočilo sprejema (prejemnik), vsak svoj par ključev - *zasebnega*, ki je tajen, in *javnega*, ki je javno dostopen. Ker sta ključa med seboj povezana v posebnem matematičnem razmerju, mora pošiljatelj sporočilo zašifrirati s svojim zasebnim in prejemnikovim javnim ključem, tako šifrirano sporočilo pa potem pošlje prejemniku. Prejemnik pa to sporočilo nato dešifrira s svojim zasebnim in pošiljateljevim javnim ključem (Kovačič, 2006).

2.2.4 Anonimizacija

Eno izmed zaščit predstavljajo tudi sistemi za anonimizacijo, ki jih razvijajo zaradi napovedi obvezne hrambe prometnih podatkov[5] na internetu oziroma poizkusov cenzure na inter-

[5] Po Zakonu o elektronskih komunikacijah RS so podatki o prometu kakršnikoli podatki, ki se obdelujejo zaradi prenosa komunikacij v elektronskem komunikacijskem omrežju ali zaradi njegovega obračunavanja.

netu. Popolna anonimizacija sicer ni mogoča, je pa z uporabo nekaterih programov stopnjo anonimizacije mogoče povečati. Mednje štejemo različne anonimne zastopniške programe (ang. »*anonymous proxy*«), ki predstavljajo vmesnik med uporabnikom in obiskano spletno stranjo oziroma storitvijo.

Med sodobnejše sisteme štejemo anonimizacijsko omrežje Tor, ki pa je trenutno še v razvojni fazi, čeprav testno že deluje. Gre za porazdeljeno omrežje anonimizacijskih strežnikov, med katerimi se preusmerja šifriran promet posameznega uporabnika, dokler ga na enem izmed izhodnih točk omrežja ne zapusti. Uporaba Tor omrežja poteka tako, da si uporabnik v računalnik namesti Tor klienta, ki internetni promet preusmeri v Tor omrežje. Vstopna točka iz uporabnikovega računalnika v Tor omrežje je izbrana naključno, preden pa podatki zapustijo Tor omrežje, potujejo preko več naključno izbranih anonimizacijskih Tor strežnikov. Vse povezave do izhoda iz Tor omrežja (t. i. »*exit node*«) so šifrirane, izhod iz omrežja pa je tudi izbran naključno. Ker povezave od uporabnika do internetnih strežnikov, ki jih uporablja, ne potujejo neposredno, pač pa preko anonimizacijskega omrežja Tor in so poleg tega še šifrirane, je izredno težko ugotoviti, katere storitve interneta uporabnik uporablja in kakšen je pravi IP uporabnika oz. od kod dostopa do storitve.

Ker je Tor omrežje še v razvojni fazi, ne zagotavlja visoke stopnje anonimnosti, poleg tega pa je omrežje razmeroma obremenjeno, saj ga nekateri uporabljajo tudi za anonimni prenos datotek preko P2P.

Na podlagi omrežja Tor so nastale tudi rešitve, ki anonimizacijsko omrežje uporabljajo za nekatere storitve interneta, na primer anonimno surfanje po spletu (»TorPark«) in anonimno komuniciranje preko protokolov za trenutno sporočanje (»Anon-IM«), t. i. »*Internet Messaging*« protokoli, kot npr. MSN Messenger, ICQ itd. Slednji dve rešitvi sta narejeni tako, da ju je mogoče zagnati iz USB ključa in ju ni potrebno namestiti za računalnik, na katerem ju uporabnik uporablja, zato na njem tudi ne puščata sledov uporabe (Kovačič, 2006).

2.2.5 Trajno brisanje podatkov

Ker uporaba računalnika in internetnih storitev na računalniku pušča številne elektronske sledi, ki se zapisujejo v različne začasne datoteke, lokalni medpomnilnik spletnega brskalnika (ang. »*browser cache*«) ter v ostanke v datotečnem sistemu (ang. »*slack space*«), je priporočljivo trde diske izbrisati vsaj pred nadaljnjo prodajo. Priporočljiva je uporaba trajnega brisanja (ang. »*wiping*«), ki vsebino datotek izbriše s prepisovanjem podatkov *čez* stare. Obstajajo različna priporočila glede števila prehodov pri brisanju, za enega najbolj zanesljivih pa velja postopek nepovratnega brisanja podatkov po t. i. *gutmanovi metodi*, ki zahteva 35-kratno prepisovanje podatkov po posebnem postopku. Trajno brisanje sicer ni učinkovito na vseh datotečnih sistemih, saj so nekateri datotečni sistemi zasnovani tako, da je uničene podatke mogoče obnoviti.

Za trajno brisanje podatkov in čiščenje že izbrisanega prostora na diskih so na voljo ustrezne programske rešitve, nekatere so tudi brezplačne. Eden izmed njih je npr. »*Clean Disk Security*«, ki omogoča brisanje vsebine začasnih datotek, brisanje spletnih piškotkov, brisanje začasnega pomnilnika (ang. *»swap file«)* pri zaustavitvi računalnika (Kovačič, 2006).

2.2.6 Filtriranje in blokiranje neprimernih vsebin

Ker otroci pogosto ne vedo čisto dobro, kaj je prav in kaj ne, kaj je na internetu dovoljeno in kaj prepovedano, so starši in učitelji tisti, ki morajo poseči po preventivnih ukrepih. Vendar pa je potrebno že na začetku poudariti, da nobena tehnična zaščita ni 100 % zanesljiva. Vemo tudi, da s starostjo otroci pridobijo spletne veščine, s katerimi lahko tehnično zaščito hitro zaobidejo.

Osnovni korak zaščite je, da že v spletnem brskalniku nastavimo stopnjo prepustnosti za določene vsebine, s čimer otrokom preprečimo dostop do nezaželenih spletnih vsebin (npr. pornografije). Če za brskanje po internetu uporabljamo Internet Explorer, ta postopek izvedemo tako, da v meniju Orodja (»Tools«) izberemo Internetne možnosti (»Internet Options«) in nato jeziček Vsebina (»Content«), kjer lahko v odseku svetovalec o vsebini (Content Advisor) nastavimo prepoved dostopa do nezaželenih spletnih vsebin, kot so npr. pornografske vsebine.

Koristen pripomoček so tudi posebni programi za filtriranje in nadzor nad pregledovanjem vsebin, s katerimi lahko otrokom učinkovito preprečimo dostop do nezaželenih spletnih vsebin. Nekateri programi lahko sledijo otrokovemu deskanju po internetu, drugi lahko snemajo pogovore otrok v klepetalnicah in starše prek elektronske pošte v primeru nevarnosti pravočasno obvestijo, tretji pa denimo lahko zaustavijo elektronsko pošto s sporno vsebino (Skrt, 2004: 50-52).

Morda na tem mestu ni odveč, če omenimo, da imajo otroci pravico do zasebnosti tudi pred lastnimi starši. V tujini je znan primer razsodbe norveškega varuha otrokovih pravic, ki je razsodil, da so starši z nadzorom nad gibanjem svoje hčerke preko GSM telefona, medtem ko je bila s prijatelji na smučanju, kršili njene pravice do zasebnega življenja. Branje otrokove elektronske pošte, sporočil, ki si jih izmenjava preko interneta in v klepetalnicah, je sicer izražanje starševske skrbi, vendar pa tudi grdo posega v otrokovo zasebnost. Preden starši posežejo po takih metodah, je priporočeno, da se z otrokom poskušajo pogovoriti in dosežejo medsebojno zaupanje, kjer tovrstne metode sploh ne bodo več potrebne.

Seznam nekaterih filtrov, ki jih lahko uporabite za zaščito pred potencialno škodljivimi vsebinami, lahko najdete na *www.safe.si*.

2.2.7. Kako se ubraniti pred virusi v elektronski pošti?

Najboljša zaščita pred virusi je pazljivost. Vsa elektronska sporočila, ki vsebujejo priponko, so v osnovi potencialno nevarna, četudi pošiljatelja poznate. Škodljivi programi se v vse večji meri pošiljajo prek okuženih računalnikov in imenika naslovnikov, ki je shranjen na računalniku.

Ne zaganjajte datotek s končnicami ».exe«, ».js«, ».vbs« ».scr«. Le redke izjeme formatov datotek lahko odprete brez skrbi, da bi bile okužene z virusi (npr. datoteke s končnico ».txt«, ».gif«, ».mp3«).

V vašem programu za sprejemanje elektronske pošte aktivirajte vse možne varnostne mehanizme.

Pridobite si program za zaščito pred virusi. Veliko jih lahko brezplačno najdete na internetu ali pa kupite pri specializiranih ponudnikih. Izberite svoj protivirusni program in z njim redno preverjajte datoteke na računalniku ter elektronsko pošto. Ne pozabite ga redno po-

sodabljati (različica programa) – vsaj enkrat na mesec, po potrebi pa tudi pogosteje, virusne baze pa naj se posodabljajo vsak dan. Priporočamo tudi vklop samodejnih posodobitev.

NAMIG ZA PRAKTIČNO DELO V RAZREDU: Lotite se aktivnosti iz Priročnika za razredne aktivnosti na CD-ju pod zaporedno številko 3: **«Kiber spomin«.**

2.3 Kaj storiti v primeru kršitve varnosti in zasebnosti?

V primeru, da menite, da so bili na internetu zlorabljeni vaši osebni podatki oz. kršena vaša zasebnost, o tem poročajte primerni službi. Kršitev lahko prijavite tudi na spletni strani **Informacijskega pooblaščenca** *www.ip-rs.si*.

V skladu s Kazenskim zakonikom RS so kazniva naslednja dejanja:

- 143. člen: Zloraba osebnih podatkov

1) Kdor uporabi osebne podatke, ki se obdelujejo na podlagi zakona, v neskladju z namenom njihovega zbiranja ali brez osebne privolitve osebe, na katero se osebni podatki nanašajo, se kaznuje z denarno kaznijo ali zaporom do enega leta.

(2) Enako se kaznuje, kdor vdre ali nepooblaščeno vstopi v računalniško vodeno zbirko podatkov z namenom, da bi sebi ali komu drugemu pridobil kakšen osebni podatek.

...

(4) Kdor prevzame identiteto druge osebe in pod njenim imenom izkorišča njene pravice, si na njen račun pridobiva premoženjsko korist ali prizadene njeno osebno dostojanstvo, se kaznuje z zaporom od treh mesecev do treh let.

- 221. člen: Neupravičen vstop v informacijski sistem

(1) Kdor vdre v informacijski sistem ali kdor neupravičeno prestreže podatek ob nejavnem prenosu v informacijski sistem ali iz njega, se kaznuje z zaporom do enega leta.

(2) Kdor podatke v informacijskem sistemu neupravičeno uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem neupravičeno vnese kakšen podatek, ovira prenos podatkov ali delovanje informacijskega sistema, se kaznuje za zaporom do dveh let.

(3) Poskus dejanja iz prejšnjega odstavka je kazniv.

(4) Če je z dejanjem iz drugega odstavka tega člena povzročena velika škoda, se storilec kaznuje z zaporom od treh mesecev do petih let.

SI-CERT (Slovenian Computer Emergency Response Team) je center za posredovanje pri internetnih incidentih, ki koordinira obveščanje in reševanje varnostnih problemov v računalniških omrežjih v Sloveniji. Glavna naloga, ki jo SI-CERT opravlja, je sprejem in posredovanje obvestil o zlorabah in vdorih v računalniške sisteme. V primeru vdora ali poskusa letega lahko pošljete sporočilo z opisom incidenta na naslov si-cert@arnes.si.

Če sumite, da je na omrežju prišlo do kaznivega dejanja oz. menite, da je potreben sodni pregon dejanja, vam svetujemo, da se obrnete na **Upravo kriminalistične službe ministrstva za notranje zadeve (UKS MNZ).** Pokličete lahko tudi na telefonsko številko 113 ali 080 1200 (anonimna prijava). Prijavo kaznivega dejanja lahko podate tudi v elektronski obliki na spletni strani policije (*www.policija.si*) oz. na državnem portalu Republike Slovenije e-uprava v rubriki »E-naznanilo kaznivega dejanja policiji«.

Za uresničevanje Zakona o varstvu potrošnikov (ZVpot) skrbi **Tržni inšpektorat**, ki deluje v sklopu Ministrstva za gospodarstvo. Prijave kršitve člena 45.a. Zakona o varstvu potrošnikov lahko pošljete na elektronski naslov inšpektorata tirs.info@gov.si. V skladu z omenjenim členom *lahko podjetje uporablja sistem klicev brez posredovanja človeka, faksimile napravo in elektronsko pošto samo z vnaprejšnjim soglasjem posameznega potrošnika, ki mu je sporočilo namenjeno.*

Kršitve spodaj navedenega 109. člena Zakona o elektronskih komunikacijah (ZEKom) pa naslovite na Agencijo za pošto in elektronske komunikacije (APEK).

- 109. člen ZEKom kot kazniva opredeljuje naslednja dejanja:

(1) Uporaba samodejnih klicnih sistemov za opravljanje klicev na naročnikovo telefonsko številko brez človekovega posredovanja (klicni avtomati), faksimilnih naprav ali elektronske pošte za namene neposrednega trženja je dovoljena samo, če naročnik predhodno soglaša s tem.

(2) Ne glede na določbe prejšnjega odstavka lahko fizična ali pravna oseba, ki od kupca svojih izdelkov ali storitev pridobi njegov elektronski naslov za elektronsko pošto, ta naslov uporablja za neposredno trženje svojih podobnih izdelkov ali storitev, vendar mora kupcu dati možnost, da kadarkoli na brezplačen in enostaven način zavrne takšno uporabo njegovega elektronskega naslova.

(3) Uporaba drugačnih sredstev za neposredno trženje s pomočjo elektronskih komunikacij kot so določena v prejšnjih dveh odstavkih tega člena, je dovoljena le s soglasjem naročnika.

(4) Elektronske pošte za potrebe neposrednega trženja s skrito ali prikrito identiteto pošiljatelja, v imenu katerega se sporočilo pošilja, ali brez veljavnega naslova, na katerega lahko prejemnik pošlje zahtevo za prekinitev takega neposrednega trženja, ni dovoljeno pošiljati.

Pritožbe glede nezaželene pošte lahko naslovite na **ponudnika internetnih storitev**, kjer je pošta svojo pot začela. Pri tem moramo biti pozorni, saj večina nezaželenih sporočil ne izvira iz elektronskega naslova, ki ga vidimo, temveč je pošiljatelj svoj elektronski naslov ponaredil.

NAMIG ZA PRAKTIČNO DELO V RAZREDU: Lotite se aktivnosti iz Priročnika za razredne aktivnosti na CD-ju pod zaporedno številko 10: **»Razkrivanje osebnih podatkov na internetu«.**

2.4 Spletno oglaševanje

Internetne vsebine za otroke postajajo v zadnjih letih vse bolj potrošniško usmerjene. Najpopularnejša podjetja otroške industrije, še posebej pa proizvajalci življenjskih potrebščin, ki so namenjene otrokom, preplavljajo internet s svojimi marketinškimi spletnimi stranmi. V želji, da bi njihove internetne strani pridobile čim več obiskovalcev, se na vsaki

embalaži izdelka nahaja naslov spletne strani (bodisi podjetja ali pa izdelka). Pri televizijskih ali tiskanih oglasih so spletna mesta podjetij pogosto posebej poudarjena.

Magična beseda, ki se skriva za tem pojavom, je medijsko povezovanje, oz. prisotnost v vseh medijih. Vendar pa imajo oglaševani izdelki na internetu veliko težav s privabljanjem potrošnikov (staršev in otrok) k ogledu spletne strani. Vprašljivo je, ali se take spletne strani, zlasti tiste za otroke, podjetjem sploh izplačajo. Zaenkrat so oglaševalski in marketinški gradniki, kot so ciljna skupina, stik s strankami, grajenje ugleda in pospeševanje prodaje, še vedno tako pomembni, da upravičujejo postavitev dragih interaktivnih spletnih strani.

Običajne oblike oglaševanja na otroških straneh

Internetne strani podjetij moramo gledati kot oglase, saj gre pri tem v prvi vrsti za predstavitev podjetja ali produkta.

- **Sponzoriranje**

Ponudnik spletne strani na svojo stran vgradi dodatna besedila, slikovne ali zvokovne elemente nekega drugega podjetja in v ta namen prejeme denar. Sponzorjev namen je, da s tem pridobi želeno ciljno skupino in si pomaga graditi pozitiven ugled.

- **Reklamne pasice (»bannerji«)**

Naslednja, zelo pogosta oblika reklamiranja na otroških straneh so reklamne pasice, ki so vgrajene na spletno stran in se aktivirajo ob kliku nanje. Lahko vodijo na mesta na osnovni spletni strani, ki so namenjena oglaševanju ali pa vodijo na drugo spletno stran, ki ima običajno potrošniško ozadje (npr. spletne trgovine).

- **Pojavna okna (»pop-up«)**

Na otroških straneh so med drugim običajna tudi pojavna okna. Pod tem pojmom razumemo okna, ki se nam nenadoma pojavijo na zaslonu, t. i. prekinitveni oglasi, ki se pojavijo med aktivno internetno povezavo. S klikom lahko pojavna okna zapremo, vendar pa pogosto klik, s katerim mislimo okno zapreti, vodi do druge spletne strani. Slednje je, predvsem za otroke, zelo zavajajoče.

- **Oglaševanje preko elektronske pošte**

Posebej priljubljeni pri spletnih oglaševalcih so oglasi preko elektronske pošte, kar je zelo direktna in interaktivna možnost, s katero lahko nagovorijo otroke. Elektronska sporočila prispejo naravnost v otrokov poštni predal in so opremljena z napotki in povezavami do predstavitvenih strani izdelka, kjer lahko običajno izdelek tudi naročimo. Problem, da otroci pogosto nimajo svojega internetnega naslova, ponudniki enostavno rešijo tako, da otrokom ponudijo brezplačno možnost za registracijo novega elektronskega naslova.

- **Spletne nagradne igre**

Tudi nagradne igre na spletu so priljubljena možnost za nagovarjanje najmlajših uporabni-

kov. Na eni strani predstavljajo uporabniku zabavo, po drugi strani pa so učinkovito oglaševalsko orodje. Otroci se morajo pri igri spoprijemati z izdelki, blagovnimi znamkami ali oglaševalskimi figurami. S tem se podaljša čas, ki ga prebijejo na spletni strani. Pri poteku igre otroci izdajajo svoje osebne podatke in izražajo svojo (ne)naklonjenost do posameznega izdelka. Osebni podatki se tako enostavno zbirajo v bazi potrošniških profilov in pomagajo pri razvoju novih izdelkov. Potrošniki so pogosto nagovorjeni k podajanju svojega mnenja, kar spet izboljšuje komunikacijo s strankami.

Najbolj problematično pri oglasih na otroških straneh je nenehno mešanje vsebine in oglasov. Oglasi postajajo zabavna vsebina in tako jo otroci ne prepoznavajo več kot oglas (Ostrež, 2005: 1-2).

- **Spletne strani izdelkov**

Pri otrocih so zelo priljubljene spletne strani proizvajalcev otroških igrač ali likov, ki se pojavljajo v medijih. Na teh spletnih straneh ponujajo proizvajalci več kot le informacije o izdelku. Otroci lahko pričakujejo samostojne in mamljive dodatne ponudbe pri informacijah o izdelku, kot so npr. nagradne igre in elektronske kartice, ki se seveda nanašajo na izdelke ali proizvajalca.

Na spletni strani priljubljene Barbie lahko otroci iščejo po njeni virtualni garderobni omari in ji (virtualno) nadenejo različna oblačila. Ob tem pa izdajajo svoje in starševe osebne podatke in potrošniške preference, da lahko sodelujejo v nagradni igri. Spletna stran Lego kock ponuja virtualno igranje košarke z Lego figuricami, ipd.

Pripravljene so tudi posebne ponudbe ob predstavitvi najnovejših izdelkov. Proizvajalci poskušajo z vsemi triki vzpodbuditi otrokovo radovednost. Utripajoč napis: »Barbie fotoaparat zate!« na začetni strani zagotovo spodbudi radovednost pri marsikateri deklici. Pritisnemo na ponudbo in ni sledu o fotoaparatu. Namesto tega je predstavljena nova Barbie kolekcija z različnimi oblačili za konec tedna. Čez nekaj sekund se ponovno pojavi utripajoč tekst: »Slikaj s fotoaparatom in se zabavaj. Ob nakupu 'Barbie za konec tedna' ti pripada ta neverjeten fotoaparat!«. Na desni strani, v spodnjem robu okna je še dodatno pojasnilo: »Ponudba velja v sodelujočih trgovinah, dokler bodo fotoaparati na zalogi«. Tako se obljuba »Barbie fotoaparat zate!« izkaže kot dodatna ponudba ob nakupu nove punčke.

Na spletni strani proizvajalca Bibi-Blocksberg pričaka otroka poleg nenehno spreminjajočih se pasic, ki vodijo k različnim spletnim trgovinam ali spletnim stranem otroških časopisov, tudi veliki Bibi-Blocksberg kviz. Za sodelovanje se morajo otroci vpisati z imenom in elektronskim naslovom. Preko elektronskega sporočila dobijo nato skrivno geslo, s katerim se lahko vpišejo na stran s spletnim kvizom. Otrok, ki pravilno odgovori na 100 vprašanj, si lahko na svoj računalnik naloži »nekaj lepega«. Zanka v kvizu se pojavi v tem, da lahko vsak dan odgovorijo le na eno vprašanje, kar pomeni, da morajo priti na stran vsaj 100 krat. Taka obveza zagotavlja ponudniku veliko stalnih obiskovalcev (Ostrež, 2005: 2).

Igre in zabava ali trženje produktov?

Proizvajalci življenjskih potrebščin, ki se obračajo na otroške potrošnike sladkarij, mlečnih proizvodov ali pijač, v svojih spletnih predstavitvah iger in zabavo združujejo z iskanjem cilj-

nih skupin in trženjem. Otroci lahko tako doživijo vesoljsko avanturo z jogurti Fruchtzwerge, postanejo pirati s sokovi Capri-Sonne ali zgradijo drevesno hišo s kakavom Nesquik. Na spletni strani Ferrero ponujajo otrokom prav posebno presenečenje: napetost, igra in zabava so dostopni šele potem, ko vnesejo 10-mestno kodo (»magična koda«), ki jo lahko dobijo le v jajčkih presenečenja (Kinder Surprise). Otrokom sta nato ponujeni dve območji: na eni strani 20-minutna »interaktivna pustolovščina« z oglasnimi figurami njihovih izdelkov in na drugi strani videoigre, ki jih lahko naložijo na svoj računalnik in se na koncu izkažejo kot virtualni objekti za zbiranje Kinder figuric. Vsak, ki želi izkoristiti svojo »magično kodo«, se mora včlaniti v klub in je po tem, ko vnese že svojo peto »magično kodo«, vpisan na listo najboljših in dobi novo presenečenje. Za prijavo v klub morajo otroci izpolniti polja: vzdevek, geslo in skrivno vprašanje. Ostale podatke lahko vnesejo po želji: spol, starost in država. S članstvom v klubu naj bi, kot trdi ponudnik (Ferrero), otroci pridobili varno in njihovim potrebam prilagojeno okolje. Članstvo v klubu gotovo pomeni, da bodo včlanjeni otroci dobili posebno vez s spletno stranjo in jo bodo zvesto obiskovali. V tem primeru pa to pomeni še to, da bodo morali vedno znova kupovati tudi jajčka presenečenja (Ostrež, 2005: 2-3).

Otroški in mladinski časopisi so že dolgo nazaj odkrili internet

Na začetku so internetne izdaje časopisov predstavljale konkurenco klasičnim medijem, danes pa so ti med seboj vse bolj povezani in tako obstajajo klasične in internetne izdaje posamezne revije. Cilj internetnih verzij ni, da bi nadomestili tiskane verzije, ampak želja da bi z dodatno internetno ponudbo spodbudili dodatno povpraševanje, prepoznavanje revije in posledično pridobivanje novih naročnikov (Ostrež, 2005: 3).

Televizija in internet: obojestransko povečanje vpliva

Radijske in televizijske mreže uporabljajo internetne predstavitve kot dopolnilo za boljšo povezanost ciljne skupine poslušalcev ali gledalcev z oddajo.

Nekatere oddaje, ki so javno prepoznavne znamke, v svojem programu opozorijo tudi na svojo spletno stran. Taki nasveti predstavljajo v nepreglednem internetnem svetu, predvsem za otroke, pribežališče v varno okolje, ki ga že poznajo. Tako so pri otrocih priljubljene predvsem spletne strani otroških programov, ki obljubljajo, da naj bi bile brez oglasov, kar pa običajno ni res. Izkaže se, da sicer ne vsebujejo oglasov za druge produkte, ni pa ovir za promocijo lastnih izdelkov, kot so: knjige, računalniške igrice in figure, ki jih lahko kupimo.

Še bolj intenzivno oglaševanje pa imajo komercialne radijske postaje in televizije, ki se morajo preživljati zgolj iz oglasov. Tako imajo mednarodno uveljavljene Disneychannel, Foxkids in Super RTL dobro izdelane sponzorske strategije, ki gradijo njihove spletne predstavitve. Začetna stran oddaje Toggo, ki jo predvaja Super RTL, ponuja majhne interaktivne reklamne površine, ki vodijo do otroških produktov,specifično prilagojenih na spol otroka. Z enostavnim klikom na te površine otroci pridejo do spletnih predstavitev izdelkov, ki ponujajo nagradne igre, elektronske razglednice, računalniška ozadja..., kjer se vse nanaša na predstavitev in trženje izdelka. Nekatere izmed teh strani so ob kliku nanje označene kot oglasna sporočila, druge ne. Tudi vsebina oddaje je pri spletni strani Toggo predstavljena v povezavi s sponzorji npr. »Toggo turnir v nogometu, ki ga predstavlja Kellog's«. Posledica tega je, da je vsa vsebina tako ali drugače povezana z oglasi in tako spletna stran oddaje Toggo predstavlja bolj ali manj oglasno izhodišče (Ostrež, 2005: 3).

Prodaja na internetu

Poleg različnih marketinških strategij je na večini otroških komercialnih spletnih straneh vgrajena tudi spletna trgovina. Za enkrat je še vprašljivo, koliko se ta pri otroških spletnih straneh splača. Do svojega sedmega leta so otroci poslovno nesposobni in tako ne smejo ničesar nakupovati. Med 7. in 18. letom so otroci omejeno poslovno sposobni, kar pomeni, da lahko opravljajo nakupe, ki se gibljejo v okviru vsote iz žepnine. Pri vseh ostalih nakupih morajo biti prisotni in dati soglasje starši ali skrbniki.

Proizvajalci otroških izdelkov na internetu ponujajo svoje produkte, proizvajalci življenjskih potrebščin (pa tudi televizijske oddaje) pa skušajo prodati promocijske izdelke, kot so kape in majice z njihovim logotipom. Direktni nagovori otrok v smislu: »Pridi in vzemi me s sabo!« ali »Privošči si!« so sicer uradno prepovedani, vendar se kljub temu pojavljajo v katalogih in spletnih straneh. Tako je na primer v spletni trgovini napisano povabilo: »Želiš takoj naročiti - klikni na nakupovalni voziček!« Šele ob kliku se nam pojavi tudi opozorilo: »Naročati smejo le osebe starejše od 18 let. Otroci smejo spletni nakup opraviti le skupaj s svojimi starši!«

Pozitivno je potrebno oceniti, da je na mnogih straneh s pomočjo pojavnega okna (pop-up) jasno označeno, kdaj otrok zapušča spletno mesto in bo preusmerjen na spletno trgovino. Skoraj vedno morajo potem otroci ponovno potrditi izbiro in šele potem so preusmerjeni na spletno trgovino.

Vedno pogosteje najdemo na otroških spletnih straneh prodajo melodij, igric in logotipov za mobilne telefone. Ocene ponudnikov mobilne telefonije kažejo, da naj bi Nemčiji za logotipe in melodije mladi porabili približno 107 milijonov evrov letno (Die Welt, 13. 4. 2004). Potrošniške centrale intenzivno opozarjajo o problemu nejasnih in oderuških cen, katerim lahko nedolžni otroci hitro nasedejo (Ostrež, 2005: 3-4).Pomembno je, da odrasli in pedagogi najprej sami izdelajo svojo strategijo soočanja s komercialnimi ponudniki spletnih strani. Pri skupnem obisku spletnih strani skupaj z otroci jim lahko tako predstavite in pokažete svojo strategijo in jim ponudite nasvete. Pri izbiri spletnih strani za svoje otroke bodite pozorni, da so to spletne strani brez oglasov. Pogosto otroci pristanejo na komercialnih ponudnikih spletih strani zaradi slabo predstavljenih alternativ (Ostrež, 2005: 4).

NAMIG ZA PRAKTIČNO DELO V RAZREDU: Lotite se aktivnosti iz Priročnika za razredne aktivnosti na CD-ju pod zaporedno številko 16: **«Ločevati mnenja od dejstev na internetu«.**

3 Avtorsko pravo[6]

3.1 Pravni okvir

Kršitev avtorskih pravic v Sloveniji ne pokriva le ***Zakon o avtorski in sorodnih pravicah,*** pač pa tudi ***Kazenski zakonik.*** 147. člen sankcionira kršitve avtorske pravice. Gre predvsem za sankcioniranje kršitve pravice avtorja do objave, prikaza, izvedbe ali prenosa avtorskega dela, pa tudi do različnih neupravičenih posegov v tuje avtorsko delo. 148. člen sankcionira neupravičeno uporabo avtorskega dela, pri čemer je zagrožena kazen v primeru, da tržna cena neupravičeno uporabljenih del pomeni večjo premoženjsko vrednost, zapor do treh let, v primeru velike premoženjske vrednosti, se storilec kaznuje z zaporom do petih let, če pa je bila pridobljena velika protipravna premoženjska korist, pa je zagrožena zaporna kazen od enega do osmih let.

Za povprečnega uporabnika P2P omrežij (omrežja za izmenjavanje datotek, npr. glasbe, filmov, programske opreme) pa je gotovo najbolj relevanten 149. člen KZ, ki pravi:

(1) Kdor neupravičeno reproducira, da na voljo javnosti, razširja ali da v najem eno ali več izvedb, fonogramov, videogramov, RTV oddaj ali podatkovnih baz, katerih skupna tržna cena pomeni večjo premoženjsko vrednost, se kaznuje z zaporom do treh let.

(2) Kdor neupravičeno reproducira, da na voljo javnosti, razširja ali da v najem eno ali več izvedb, fonogramov, videogramov, RTV oddaj ali podatkovnih baz, katerih skupna tržna cena pomeni veliko premoženjsko vrednost, se kaznuje z zaporom do petih let.

Kaj sta večja ter velika premoženjska vrednost oz. korist, pa je določeno v 99. členu, in sicer pomeni večjo premoženjsko vrednost znesek nad 5000 evrov, veliko pa nad 50.000 evrov.

[6] Celotno poglavje o avtorskem pravu je povzeto po članku dr. Mateja Kovačiča, ki je dostopen na: *http://www.slo-tech.com/clanki/06001/.*

Z drugimi besedami - uporabniki nelegalnih kopij računalniških programov in multimedijskih vsebin ter uporabniki P2P omrežij, ki ta avtorsko zaščitena dela dajejo na voljo javnosti in razširjajo preko interneta, se s svojimi dejanji izpostavljajo kazenskemu pregonu. Treba je namreč tudi poudariti, da 113. člen ZASP avtorju računalniškega programa daje izključno pravico do reprodukcije, priredbe ali kakšne drugačne predelave računalniškega programa ter distribuiranja izvirnika računalniškega programa ali njegovih primerkov v katerikoli obliki, vključno z njegovim dajanjem v najem.

Zaostrovanje na področju boja proti računalniškemu piratstvu pa v Evropski uniji prinaša tudi Direktiva o obvezni hrambi prometnih podatkov, ki je bila sprejeta leta 2005, Slovenija pa jo je implementirala decembra 2006. Direktiva zahteva obvezno hrambo prometnih podatkov telefonskih in internetnih komunikacij (vključno z naslovi elektronske pošte) ter podatkov o lokacijah mobilnih telefonov, kjer čas hrambe znaša od 6 do 24 mesecev, v nekaterih primerih tudi več. Poleg tega pa direktiva ne omejuje, za katera kazniva dejanja je mogoče shranjene podatke uporabiti. Podatki, katerih hrambo predvideva direktiva, bodo tako omogočili naknadno identifikacijo oseb, ki si nelegalno izmenjujejo avtorsko zaščitene datoteke.

- Kazenski zakonik (KZ-1), Uradni list RS, št. 55/2008 (66/2008 popr.)

- Direktiva 2002/58/EC o obdelovanju osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector), sprejeta 12. julija 2002. Official Journal L 201, 31/07/2002 p. 0037 - 0047.
- Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev alijavnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC), sprejeta 14. 12. 2005. Official Journal L 105, 13/04/2006, p. 0054 - 0063.

3.2 Predstavitev avtorskih pravic

T. i. intelektualna lastnina obsega pravice, ki izhajajo iz t. i. intelektualnih aktivnosti. Zaščita intelektualne lastnine temelji na ideji, da je človekov um eno glavnih vodil tehnološkega, kulturnega in družbenega razvoja, zato je potrebno ustvarjalne dosežke zavarovati in avtorju omogočiti primerno nagrado. Pravo, ki ureja področje intelektualne lastnine, tako avtorju podeli začasen monopol nad komercialnim izkoriščanjem njegove ideje oz. dela. S tem naj bi se avtorje spodbujalo k nadaljnjemu ustvarjanju.

Intelektualno lastnino delimo na industrijsko lastnino, ki obsega patente, modele, blagovne in storitvene znamke ter geografske označbe porekla, ter avtorske pravice avtorjev na nji-

hovih delih s področja književnosti, znanosti in umetnosti. Vendar pa je izraz intelektualna lastnina po mnenju nekaterih, npr. ustanovitelja Free Software Foundation Richarda Stallmana, zavajajoč. Po njegovem mnenju so se avtorsko, patentno pravo in pravo blagovnih znamk razvijali ločeno, pokrivajo ločena področja in imajo različne namene. Avtorsko pravo je po njegovem mnenju nastalo zaradi razvijanja pisateljstva in umetnosti, patentno pravo v osnovi promovira publikacijo novih idej v zameno za omejen monopol nad izkoriščanjem teh idej, pravo blagovnih znamk pa je nastalo zaradi zaščite potrošnikov, da vedo, kaj kupujejo in ne zaradi pospeševanja tržnih aktivnosti podjetij.

3.2.1 Avtorska pravica

Slovenski **Zakon o avtorski in sorodnih pravicah** določa, da so avtorske pravice »pravice avtorjev na njihovih delih s področja književnosti, znanosti in umetnosti« (t. i. avtorska pravica) ter »pravice izvajalcev, proizvajalcev fonogramov, filmskih producentov, radijskih ali televizijskih organizacij, založnikov in izdelovalcev podatkovnih baz« (t. i. sorodne pravice).

Zakon določa, da so avtorska dela individualne intelektualne stvaritve s področja književnosti, znanosti in umetnosti. To so zlasti govorjena dela, pisana dela (mednje štejejo tudi računalniški programi), glasbena dela, gledališka, gledališko-glasbena in lutkovna dela, koreografska in pantomimska dela, fotografska dela, avdiovizualna dela (filmi), likovna dela (slike, kipi ...), arhitekturna dela, dela uporabne umetnosti in industrijskega oblikovanja, kartografska dela (zemljevidi ...) ter predstavitve znanstvene, izobraževalne ali tehnične narave (različni načrti, skice, izvedenska mnenja itd.). V Sloveniji pa zakonsko niso varovane: ideje, načela in odkritja, uradna besedila z zakonodajnega, upravnega in sodnega področja ter ljudske književne in umetniške stvaritve.

Avtorska pravica pripada avtorju na podlagi same stvaritve dela. Avtorju ni potrebno kakorkoli označevati, da je delo avtorsko-pravno zaščiteno. Avtorska pravica se deli na moralne avtorske pravice, materialne avtorske pravice (t. i. izključna premoženjska upravičenja) in druga upravičenja avtorja.

3.2.2 Dovoljena in nedovoljena uporaba avtorskega dela

Glede kršitev avtorsko pravne zakonodaje so najbolj relevantne materialne avtorske pravice. Le-te varujejo premoženjske interese avtorja v zvezi z uporabo njegovega dela. To je načeloma dopustno le ob dovoljenju avtorja. Za uporabo se šteje zlasti reproduciranje (torej shranjevanje in kopiranje avtorskega dela), pa tudi javno izvajanje, javno prikazovanje in dajanje na voljo javnosti. Za vse te dejavnosti je potrebno dovoljenje avtorja. To je še posebej pomembno v času P2P omrežij, kjer uporabniki z razdeljevanjem datotek le-te pravno gledano dajejo na voljo javnosti. V primeru, da gre za avtorsko-pravno zaščitena dela, takšno razdeljevanje seveda predstavlja kršitev.

Avtorska pravica ni absolutna in pod nekaterimi pogoji je mogoče avtorsko delo prosto uporabljati. Tako je mogoče avtorsko delo predelati (npr. v parodijo ali karikaturo), uporabiti za citiranje (seveda pa je pri tem potrebno navesti avtorja), uporabiti (predvajati) za izobraževalne namene ipd. Pri računalniškem piratstvu se posamezniki pogosto izgovarjajo, da nezakonite kopije programov in multimedijskih vsebin uporabljajo le v izobraževalne namene in da nimajo pridobitnih namenov. Vendar pa zakonodaja precej natančno določa, kaj so izobra-

ževalni nameni (npr. neposredni pouk), poleg tega pa prosta uporaba ni povsem brez zakonskih omejitev.

Reproduciranje avtorskega dela je v primeru plačila nadomestila načeloma ob nekaterih pogojih in omejitvah mogoče tudi za privatne namene. Zakon določa, da je reproduciranje možno v največ treh izvodih. Gre predvsem za fotokopiranje (vendar samo dela knjige) ter izdelavo t. i. varnostne kopije, ki pa se seveda sme uporabljati le za privatno rabo. Pri računalniških programih so postavljene še nekoliko bolj stroge omejitve. Zakon določa, da upravičeni uporabnik računalniškega programa lahko reproducira največ dva varnostna primerka programa. Prav tako velja, da je javno posojanje računalniških programov in baz podatkov izključna pravica njihovega avtorja. Z drugimi besedami - posojanje računalniških programov brez dovoljenja ni dovoljeno.

Za kršitev avtorske pravice na računalniškem programu se šteje tudi vsako distribuiranje primerka računalniškega programa, za katerega oseba ve ali bi lahko domnevala, da je nedovoljeni primerek, pa tudi posest za gospodarske namene.

Ne glede na vse pa je avtorska pravica časovno omejena, saj je bila osnovna ideja avtorsko pravne zaščite v tem, da se avtorju podeli začasen monopol za komercialno izkoriščanje njegovega dela, po preteku tega monopola pa v zameno za začasen monopol avtorska pravica ugasne in avtorsko delo ni več varovano v nobenem pogledu. Slovenska zakonodaja določa, da avtorska pravica traja do konca avtorjevega življenja in 70 let po njegovi smrti, pri delih z večimi avtorji ta pravica traja 70 let po smrti soavtorja, ki je umrl zadnji, za kolektivna in anonimna dela pa 70 let po njihovi objavi.

Je pa po drugi strani res, da je v svetu opaziti trende povečanja trajanja avtorsko-pravne zaščite. Lessig navaja, da je v ZDA zakonodajna zaščita najprej (od leta 1790) trajala 14 let, z možnostjo podaljšanja za še 14 let (skupaj torej 28 let), vendar pa se večina avtorjev tega podaljšanja ni posluževala (Lessig v Kovačič, dostopno na *http://www.slo-tech.com/clanki/06001/)*.

Leta 1831 so to obdobje zaščite podaljšali na 28 let, s čimer se je celotna zaščita (skupaj z možnostjo podaljšanja) podaljšala na 42 let. Leta 1909 pa so podaljšali še obdobje podaljšanja zaščite in skupna zaščita je sedaj znašala 56 let. A od leta 1962 so v ZDA obdobje zaščite podaljšali kar enajstkrat. Leta 1976 so zaščito vseh del podaljšali za 19 let, leta 1998 pa z zakonom *Copyright Term Extension Act of 1998* še za dodatnih 20 let.

Seveda ni naključje, da je bil zakon *Copyright Term Extension Act of 1998*, znan tudi pod imenom *Sonny Bono Copyright Term Extension Act* oziroma *Mickey Mouse Protection Act*, vložen malo pred tem, ko naj bi nekatera dela, predvsem risanke in izmišljeni junaki nekaterih ameriških korporacij glede na staro zakonodajo izgubili avtorsko pravno zaščito in prešli v javno last.

Hkrati se je v ZDA širil tudi obseg zaščitenih del. Leta 1790 je bilo avtorsko-pravno mogoče zaščititi le zemljevide, grafične prikaze in knjige, ne pa tudi glasbe ali arhitekture. Poleg tega je zaščita obsegala le pravico avtorja do objave del.

Danes je mogoče v ZDA zaščititi tudi glasbo, arhitekturne oblike in računalniške programe, avtor pa nima le pravice do objave, pač pa lahko nadzoruje tudi uporabo kopije posameznega dela ter celo izvedenih del.

3.3 Računalniško piratstvo

Za računalniško piratstvo se šteje vsaka oblika zlorabe avtorsko-pravno zaščitenega dela. Oblike zlorabe sicer določa zakon, vendar pa BSA (Business Software Alliance), organizacija, ki združuje vodilne proizvajalce programske opreme in katere namen je nižanje stopnje piratstva, in slovenska policija računalniško piratstvo delita v pet pojavnih kategorij. Tako ločijo:

- **ponarejanje** (neavtorizirano reproduciranje računalniških programov, pogosto gre za nezakonite kopije, ki se na prvi pogled sploh ne ločijo od originala),
- **nalaganje na disk** (npr. nalaganje nezakonitih kopij programov na novo kupljene računalnike),
- **dajanje računalniških programov v najem oz. posojo,**
- **mehko piratstvo** (gre za nelegalno reproduciranje ene legalno kupljene kopije na več računalnikov, npr. znotraj podjetja),
- **internetno piratstvo,** ki pa ga pri BSA definirajo kot "*neavtorizirana naložitev računalniškega programa na spletno stran (Warez)*" (BSA, 2005), oziroma piratstvo elektronskih oglasnih desk (ang. *Bulletin Board Piracy*), ki ga slovenska policija na svoji spletni strani definira kot "*neavtorizirano naložitev računalniškega programa na elektronsko oglasno desko in obratno (neavtorizirana preložitev računalniškega programa z nje).*"

BSA in policija sta dolgo časa uporabljali zastarele definicije piratstva. Tehnologija in oblike piratstva se hitro spreminjajo in jim policija in celo protipiratske organizacije pogosto ne sledijo. Prodajanje ponaredkov, nalaganje na disk in mehko piratstvo v podjetjih namreč zadnja leta tržna inšpekcija dokaj dosledno preganja, zato teh oblik piratstva pri nas skorajda ni več. Razvoj širokopasovnih povezav do interneta in P2P tehnologij je seveda povzročil tudi premik od organiziranega piratstva (t. i. organizirane ilegalne reprodukcije, ki je imela navadno tudi finančne motive) do neorganiziranega, ki poteka preko interneta in P2P omrežij. Internetno piratstvo se je v zadnjih letih precej razmahnilo, seveda pa ne v obliki nalaganja na spletne strani, pač pa v obliki nezakonite izmenjave datotek preko P2P omrežij. Najbolj znana P2P omrežja so uTorrent, DC++, eMule, Kazaa Lite K++, LimeWire, Edonkey. Poleg P2P pa obstajajo tudi zasebni 0-day strežniki, kjer se nahaja »vroča« in sveža »roba«, kjer si je npr. možno naložiti nove filme, še preden se ti predvajajo v kinematografih.

Ločevanje med t. i. "črnimi uporabniki", ki neupravičeno reproducirana avtorska dela uporabljajo le zase in "pirati" ali "ponarejevalci", ki avtorsko zaščitena dela reproducirajo in razširjajo množično (in imajo pri tem pogosto tudi premoženjsko korist) s pojavom P2P omrežij prav tako izgublja na pomenu. P2P omrežja namreč uporabnikom omogočajo razdeljevanje (ang. »*sharing*«) lastnih datotek. Čeprav uporabnik od tega morda nima neposredne materialne koristi, s takšnim ravnanjem vseeno povzroča materialno škodo. Poleg tega je materialna korist od takšnega početja lahko tudi posredna, saj je dostop do nekaterih P2P omrežij pogojen z ustreznim obsegom oz. količino datotek, ki jih uporabnik nudi ostalim, oziroma je s tem pogojena prioriteta dostopa do datotek, ki jih uporabnik želi prenesti k sebi.

3.3.1 Odzivi na računalniško piratstvo

V začetku 1990-ih računalniško piratstvo ni bilo obravnavano kot resen problem. Prve resnejše akcije segajo v leto 1992, ko je *Software Publishers Association* v ZDA pričela z izobraževalno kampanjo proti piratstvu (z videom "*Don't Copy That Floppy*"), kasneje pa je založniška industrija pričela tudi aktivneje lobirati za sprejem in uveljavljanje ostrejše zakonodaje proti piratstvu.

Eden izmed dejavnikov za razmah računalniškega piratstva je zagotovo razmah širokopasovnega dostopa do interneta, poleg njega pa tudi dostopnost do naprav za digitalno reproduciranje avtorsko zaščitenih del (nizka cena CD in DVD zapisovalnikov in trdih diskov), razvoj tehnologij za razdeljevanje datotek (t. i. P2P) ter neustreznost oz. neučinkovitost tehničnih zaščit, ki naj bi preprečile digitalno reproduciranje. Ne smemo pa pozabiti niti na nepripravljenost ali morda celo nesposobnost založnikov, da se prilagodijo novim tržnim razmeram in ponudijo možnost nakupovanja glasbe in filmov preko interneta po privlačnejši ceni. Da so taki tržni pristopi kljub razširjenemu piratstvu lahko zelo uspešni, je glasbeni in filmski industriji moralo pokazati računalniško podjetje *Apple* s svojo storitvijo *iTunes*. Apple je preko iTunes ponudil poceni nakup glasbe v digitalni obliki in uspel. Razlog za uspeh je bila med drugim ravno nizka cena.

Na togost glasbene in filmske industrije je pokazal tudi primer regijske zaščite DVD-jev. Regijsko zaščitenih DVD-jev zaradi poslovne politike filmske industrije ni bilo mogoče gledati na računalnikih z operacijskim sistemom Linux, zato je leta 1999 norveški programer Jon Lech Johansen razvil program DeCSS, ki je omogočal razbijanje te zaščite. Posledica tega pa ni bila samo ta, da je sedaj možno regijsko zaščitene DVD-je gledati na računalnikih z operacijskim sistemom Linux, pač pa tudi ta, da njegov program omogoča nepooblaščeno kopiranje DVD-jev. Sicer je zelo verjetno, da bi bili podobni programi razviti tudi sicer, vendar ne moremo mimo dejstva, da je razvoj tega programa na nek način spodbudila prav togost filmske industrije in njena nepripravljenost na nove tržne razmere.

Kot odgovor na množične kršitve avtorskih pravic lahko na eni strani opažamo povečevanje zakonodajne represije na tem področju, na drugi strani pa se pojavljajo poskusi izboljšanja tehničnih zaščit pred nepooblaščenim kopiranjem. Povečevanje zakonodajne represije se vpeljuje tako v ZDA kot v Evropi. V ZDA enega takih primerov predstavlja npr. leta 1998 sprejeti *Digital Millennium Copyright Act*, ki sankcionira izdelavo in distribucijo pripomočkov za zaobid tehničnih zaščit avtorsko zaščitenih vsebin (podobne zakonske določbe je leta 2004 v *Zakonu o pogojnem dostopu do zaščitenih elektronskih storitev* sprejela tudi Slovenija). Še bolj daljnosežne posledice pa ima primer *MGM v. Grokster*, ko je Vrhovno sodišče ZDA sprejelo odločitev, da "*kdor distribuira pripomočke, katerih namen je spodbujanje kršitev avtorskih pravic (...), je odgovoren za protipravna ravnanja tretjih oseb, ki tovrstne pripomočke uporabljajo, ne glede na to, da je pripomočke moč uporabljati tudi za pravno dopustne namene.*" Odločitev vsekakor velja za zgodovinsko, saj je Vrhovno sodišče ZDA presodilo, da kršitev predstavlja ne samo kršenje avtorskih pravic, pač pa tudi distribucija pripomočkov, ki se lahko uporabijo za kršitve avtorskih pravic, s čimer distributer tovrstnega pripomočka na nek način odgovarja za nezakonito ravnanje uporabnikov svojega izdelka.

V Evropi pa pomemben korak v boju proti internetnemu piratstvu predstavlja *Konvencija o kibernetski kriminaliteti,* ki jo je leta 2001 sprejel Svet Evrope in ki v 10. členu od držav pogodbenic zahteva sprejem zakonodajnih in drugih ukrepov, ki kot kazniva opredelijo dejanja

kršitve avtorske in sorodnih pravic, če so ta dejanja storjena zavestno, v komercialne namene in s pomočjo računalniškega sistema. Na podlagi te konvencije je Slovenija marca 2004 sprejela novelo *Kazenskega zakonika*, ki je uvedla strožje kriterije za kršilce avtorskih pravic, aprila 2004 pa tudi novelo *Zakona o avtorski in sorodnih pravicah*.

V zvezi z zaostrovanjem zakonodaje na tem področju velja omeniti še *Wassenaarski sporazum* o prepovedi izvoza tehnologije dvojne rabe (ang. »*dual use technology*«) v nekatere nedemokratične države. Med tehnologije dvojne rabe se šteje tudi nekatere kriptografske produkte, ki so namenjeni zaščiti zasebnosti posameznikov. Ti produkti so simetrični algoritmi, ki uporabljajo šifrirne ključe daljše od 56 bitov, rešitve za faktorizacijo celih števil večjih od 512 bitov ter rešitve za izračun nekaterih diskretnih algoritmov. Iz prepovedi pa so izrecno izključeni tisti produkti, ki šifriranje uporabljajo za zaščito avtorskih pravic in t. i. intelektualne lastnine, ter nekateri produkti, ki se uporabljajo v bančništvu (Wassenaar Secretariat, 2003). To kaže na trend, da zakonodaja daje avtorskim pravicam čedalje večjo težo.

Tehnologije DRM in Trusted Computing

Iz stališča pravic posameznikov, predvsem pravice do zasebnosti, pa so zaskrbljujoči predvsem trendi uvedbe tehnologij, ki naj bi onemogočile nepooblaščeno reproduciranje digitalnih vsebin. Zaradi enostavnosti kopiranja digitalnih vsebin, so se lastniki avtorskih pravic odločili uvesti različne tehnične zaščite sicer pravno že avtorsko zaščitenih vsebin. Tehnologija naj bi omogočila predvsem nadzor nad uporabo avtorsko zaščitenih vsebin, vendar pa je mogoče podatke o potrošnji vsebin uporabiti tudi za profiliranje in uvajanje novih tržnih pristopov.

Upravljanje z dostopom do digitalnih vsebin oz. DRM (ang. »*Digital Rights Management*«) je skupek tehnologij, ki naj bi omejile dostop in uporabo računalniških datotek, oziroma digitaliziranih vsebin. To naj bi dosegli z onemogočenjem anonimnega ali vsaj nekontroliranega dostopa do digitalnih vsebin. Sodobne DRM tehnologije so se najprej pojavile v programih za pregledovanje video in zvočnih digitalnih zapisov (npr. *Microsoft Windows Media Player*) ter elektronskih knjig (npr. *Microsoft eBook Reader*), kasneje pa so se nekoliko bolj pričele uporabljati tudi pri zaščiti programske opreme. Prvi večji korak na tem področju predstavlja uvedba obvezne aktivacije operacijskega sistema Windows Xp za domače uporabnike. Aktivacija ob namestitvi operacijskega sistema v del registracijskega ključa vgradi tudi informacijo o strojni opremi (serijska številka procesorja, mrežne kartice, trdega diska itd.). Če uporabnik operacijski sistem prekopira v drug računalnik ali če v svojem računalniku zamenja večji del strojne opreme, ob naslednji uporabi operacijski sistem ne bo več hotel delovati in bo zahteval ponovno aktivacijo. Te podatke bi bilo mogoče povezati tudi z osebnimi podatki posameznega kupca, v končni fazi pa tudi z vsebinami (pravzaprav z natančno določeno digitalno kopijo multimedijske vsebine), ki jih posameznik konzumira. Microsoft je nekaj podobnega že skušal storiti v okviru svojih storitev *Microsoft Passport* in *Microsoft E-Wallet*, ki vsebujeta podrobne osebne in finančne podatke o posameznikih, vendar se njihovi načrti zaradi nasprotovanja javnosti niso uresničili.

Razvoj sodobnih tehnologij DRM kaže na nov trend povezovanja nadzornih tehnologij s področjem zaščite avtorskih pravic. Zbiranje osebnih podatkov se pri tem predstavlja kot nujnost zaradi zaščite avtorskih pravic, na "stranske učinke" profiliranja pa se pogosto "pozablja". Ameriška nevladna organizacija za zaščito elektronske zasebnosti je mnenja, da "*te*

tehnologije označujejo pomemben razvojni mejnik v uporabi avtorskega prava ... avtorske pravice se uporabljajo kot opravičilo tako za zaščito vsebine kot tudi za profiliranje potrošnikov vsebine" (EPIC, 2004). Ideja zaupanja vrednega računalništva (ang. *Trusted Computing*), ki je v bistvu korak naprej pri razvoju DRM tehnologij, te trende dobro ponazarja.

Zaupanja vredno računalništvo je ime za naslednjo generacijo računalniških okolij, v katera naj bi bilo vgrajeno upravljanje z dostopom do digitalnih vsebin. TC tehnologije bodo, če bodo pravilno implementirane, učinkovito preprečile piratstvo, saj bodo uvedle popoln nadzor nad uporabo in dostopom do digitalnih vsebin. To novo računalniško okolje bo imelo tudi zmožnost zaznavanja piratskih ali kako drugače nelegalnih vsebin in tudi njihovega uničevanja (t. i. *traitor tracing*).

Tehnologija TC bo delovala tako, da bo imel v prihodnosti vsak računalnik vgrajen poseben čip poimenovan Fritz čip. Poleg strojnega dela bo TC tehnologija zahtevala še ustrezno programsko podporo, oziroma ustrezno zasnovan operacijski sistem in podporne programe. S pomočjo TC tehnologije bo mogoče ugotoviti digitalni podpis vsakega računalniškega okolja, v katerem se bo nahajala digitalna vsebina. Digitalna vsebina bo šifrirana, njeno dešifriranje pa bo mogoče samo v točno določenem digitalnem okolju - z drugimi besedami, vsebina bo zaklenjena za točno določen računalnik (oz. Fritz čip). Digitalno vsebino bo sicer mogoče prekopirati tudi na druge računalnike, vendar se tam zaradi drugačnega digitalnega okolja ne bo dešifrirala v razumljivo obliko in zato ne bo dostopna. V primeru, da bo tehnologija ustrezno implementirana, predvsem njen kriptografski del, bo v TC okoljih nepooblaščeno kopiranje digitalnih vsebin postalo nemogoče. Nekakšno zgodnjo različico te tehnologije vsebuje *Windows Server 2003*, imenuje pa se *Enterprise Rights Management* in je namenjen uvedbi nadzora nad elektronsko pošto in dokumenti.

Pravni viri:

- Digital Millennium Copyright Act of 1998, 17 U.S.C. (1998)
- Svet Evrope. 2001. Konvencija o kibernetski kriminaliteti (Convention on Cybercrime), sprejel jo je Svet Evrope, 23. novembra 2001. Uradni list RS, Mednarodne pogodbe, št. 17/2004. Konvencijo je Državni zbor Republike Slovenije ratificiral dne 20. 5. 2004. Veljati je začela dne 1. 1. 2005.

3.3.2 Razlogi proti računalniškemu piratstvu

Glede zagotovljene kakovosti legalnih programov, zanesljivosti njihovega delovanja in groženj z virusi je dogajanje ob pojavu nekaterih črvov, ki so izkoriščali varnostne pomanjkljivosti operacijskih sistemov Windows (npr. Slammer, Sobig, Zotob, itd.), posledično skoraj povsem ohromili internet in povzročali veliko poslovno škodo, dovolj zgovorno. Prav tako ni razloga, zakaj bi popolna nelegalna kopija programa delovala kaj drugače, kot legalna kopija programa. Prav tako ni nikakršnega razloga, da se ne bi ilegalno reproducirala tudi dokumentacija, seveda, če se nahaja v digitalni obliki. Prav tako slab je argument o izgubi časa, saj je preko P2P omrežij pogosto mogoče priti do piratske kopije računalniškega programa ali vsebine bistveno prej kot z legalnim nakupom (izjemo pri tem predstavlja le nakup glasbe preko interneta). Podobno slab argument je tudi izguba denarja, seveda v primeru, da uporabnik za svoje nelegalno početje ni kaznovan.

Glede zanesljivosti delovanja pa je dovolj zgovoren tudi naslednji odlomek iz Microsoftove (Microsoft je tudi vidnejši član BSA) licence za uporabo operacijskega sistema *Windows Xp Home Edition* (tim. EULA - *End-User Licence Agreement*), ki v poglavju "*17. Izključitev naključnih, posledičnih in ostalih škod*" (ang. " *17. exclusion of incidental, consequential and certain other damages*") določa da:

"*Microsoft ali njegovi dobavitelji v nobenem primeru niso odgovorni za kakršnokoli posebno, naključno, kazensko neposredno ali posledično škodo ... povezano z uporabo ali nezmožnostjo uporabe programske opreme, nudenjem ali nezmožnostjo nudenja podpore ali drugih storitev, informacij, programske opreme ... celo v primeru napake, delikta (vključno z malomarnostjo), popačenja, izrecne odgovornosti, prekinitve pogodbe, prekinitve jamstva Microsofta ali kateregakoli dobavitelja in to tudi v primeru, če je bil Microsoft ali katerikoli dobavitelj obveščen o možnosti takšne škode*".

Delno bi lahko pritrdili le argumentu tehnične podpore, vendar je za nekatere najbolj razširjene programe brezplačno tehnično podporo mogoče dobiti preko internetnih forumov in IRC kanalov. Takšna pomoč je sicer neuradna, saj jo zagotavlja neformalna skupnost uporabnikov, vendar zato nič manj kvalitetna in zanesljiva kot uradna tehnična pomoč - včasih celo bolj.

Pravzaprav je poleg možnosti sankcij najmočnejši argument proti piratstvu nemoralnost takega početja. Dejstvo je, da gre pravno gledano za krajo, ki povzroča gospodarsko škodo, pa čeprav v primerjavi s klasično krajo oškodovanec ni tako neposredno oškodovan, saj ima še vedno svojo kopijo programa. Poleg tega pa obstaja še en močan razlog proti piratstvu programske opreme. Piratstvo komercialne programske opreme namreč otežuje prodor odprtodkodnih in brezplačnih rešitev, uporabnike pa navaja na komercialne produkte in s tem utrjuje njihov (pogosto monopolni) položaj na trgu.

3.4 Alternative

Obstoječi sistem avtorskega prava se marsikomu zdi neustrezen, na kar pravzaprav kaže tudi stopnja razširjenosti piratstva. Nekateri so zato pričeli poudarjati nujnost prenove sistema t. i. intelektualne lastnine v povezavi z digitalnimi tehnologijami, predvsem avtorskega prava. Kot odgovor na zaprti, lastniški model t. i. intelektualne lastnine so se razvili nekateri alternativni koncepti.

Kot nasprotje pojmu "copyright" se je razvil pojem **"copyleft"** (gre za besedno igro - *right* v angleščini poleg "pravica" pomeni tudi desno, *left* pa levo). Ena izmed najbolj znanih licenc, ki uveljavlja pojem "copylefta" je licenca GPL (GNU General Public Licence), katere končno različico je leta 1989 pripravil Richard Stallman (pod njo je pred tem izdal zgodnje različice svojih programov GNU Emacs, GNU Debugger in GNU Compiler), kasneje pa so pri *Free Software Foundation* pripravili še nekaj različic GPL licence.

GPL licenca uporabniku računalniškega programa daje pravico reprodukcije programa pod nekaterimi pogoji. Glavni pogoj je, da uporabnik skupaj s programom (oziroma na zahtevo) distribuira tudi njegovo programsko kodo, vključno z vsemi lastnimi spremembami in izboljšavami programa. Če torej nek uporabnik predela oz. izboljša program, ki je izdan pod GPL licenco, ga sme reproducirati le v primeru, da reproducirano različico prav tako izda pod GPL licenco (v primeru, da predelani program uporablja za lastno rabo, mu seveda tega ni treba storiti) in s tem programsko kodo odpre javnosti. Ta zahteva je znana pod imenom "co-

pyleft". "Copyleft" tako avtorskopravno zakonodajo izkorišča za širjenje pravic uporabnikov in ne za njihovo ožanje. V primeru, da bi nekdo program, ki je izdan pod GPL licenco redistribuiral v nasprotju z določili licence GPL, ga originalni avtor lahko toži zaradi kršitve avtorskega prava. Dejansko se je to že zgodilo in znane so uspešne tožbe proti kršiteljem GPL licenc (npr. Harald Welte proti podjetju Sitecom v Nemčiji leta 2004 ter leta 2005 proti podjetju Fortinet).

Podobna ideja stoji za projektom **Creative Commons**[7], le da je omenjena licenca namenjena predvsem umetniškim in znanstvenim delom in ne računalniškim programom. Osnovna ideja Creative Commons je, da nekateri ustvarjalci ne želijo uveljaviti vseh pravic, ki jim jih predpisuje zakonodaja o avtorskih pravicah. Namesto načela "vse pravice pridržane" želijo uveljaviti načelo "nekatere pravice pridržane" oziroma celo "nobene pravice pridržane".

Dejstvo je, da v svetu računalništva obstajajo številne odprtokodne in brezplačne alternative zaprtokodnim lastniškim in pogosto tudi razmeroma dragim programom. Nekatere najbolj znane med njimi so odprtokodni pisarniški paket OpenOffice.org, program za obdelavo slik GIMP, programi za delo z internetom (brskalnik Firefox, odjemalec elektronske pošte Thunderbird, odjemalec elektronske pošte in osebni organizator Evolution), različni programi za predvajanje multimedijskih vsebin, npr. Mplayer ter celo programi za obdelavo multimedijskih vsebin (npr. program za obdelavo zvoka Audacity, program za video montažo Cinelerra) in namizno založništvo (Inkscape in Scribus) ter številni drugi. Nekatere alternative se lahko povsem enakovredno kosajo s profesionalnimi izdelki, nekatere pa so sicer manj zmogljive, vendar za povprečnega, domačega uporabnika še vedno povsem zadovoljive.

Med privlačne alternative lahko v zadnjem času štejemo tudi nekatere distribucije odprtokodnega operacijskega sistema Linux, ki so namenjene končnim uporabnikom in so zelo enostavne za namestitev in uporabo. Ena izmed njih je npr. distribucija Linuxa Ubuntu, ki se po enostavnosti namestitve, uporabe in uporabniške prijaznosti lahko primerja z MS Windows sistemi.

Z uporabo tovrstnih alternativ "potreba" po računalniškem piratstvu s strani povprečnih, pa tudi nekoliko zahtevnejših uporabnikov v veliki meri odpade. Na nek način je ravno piratstvo eden izmed dejavnikov, ki zavirajo širitev alternativnih odprtokodnih programov. Če bi bili namreč posamezniki prisiljeni vso programsko opremo, ki jo uporabljajo, tudi kupiti, je verjetno, da bi se pogosteje odločali za enakovredne, a brezplačne alternative.

Center odprte kode Slovenije

Slovenska država se zaveda pomena odprtih standardov in odprte kode, zato spodbuja njihov razvoj in uporabo. Vlada je zato pripravila Strategijo razvoja informacijske družbe v RS[8], ki poudarja pomen interoperabilnosti in odprtih standardov ter podporo razvoju rešitev, temelječih na odprti kodi. Ministrstvo za visoko šolstvo, znanost in tehnologijo RS je na razpisu leta 2007 izbralo konzorcij Center odprte kode Slovenije (COKS) za nacionalnega vzpodbujevalca razvoja, uporabe in znanja o odprtokodnih tehnologijah in rešitvah.

[7] Več o Creative Commons projektu si lahko preberete na spletni strani: *http://creativecommons.si/*.

[8] Dostopna na: *http://www.mvzt.gov.si/fileadmin/mvzt.gov.si/pageuploads/pdf/informacijska_druzba/si2010.pdf*

Center odprte kode Slovenije (COKS) je nacionalni vzpodbujevalec razvoja, uporabe in znanja o odprtokodnih tehnologijah in rešitvah. Razvojno podporni Center odprte kode Slovenije nudi uporabnikom centraliziran sistem storitve pomoči in podpore ter zagotavlja rešitve za potrebe javnega in zasebnega sektorja. Več o samem centru in njegovem poslanstvu si lahko preberete na: *http://www.coks.si/*.

Kaj je odprtokodna programska oprema?

Odprtokodna programska oprema (OKPO) je naziv za programsko opremo, katere izvorna koda je prosto dostopna, da jo je mogoče prosto uporabljati, raziskovati njeno delovanje ter spreminjati in razširjati tako originalne kot dopolnjene in spremenjene kopije tega programja.

A kljub temu, da je na prvi pogled videti, da lahko s takšnimi programi vsak dela vse, kar želi, veljajo tudi za odprtokodne programe pravila "obnašanja", ki so zapisana v različnih licencah.

Vse licence imajo skupne točke:

- Odprtokodno programsko opremo je mogoče svobodno redistribuirati. Lahko jo redistribuira kdorkoli brezplačno ali proti plačilu.
- Izvorna programska koda je dostopna uporabniku. Licenca mora dovoljevati distribucijo v prevedeni kakor tudi v izvorni obliki.
- Licenca mora dovoljevati spremembe osnovne kode in izvedene oblike nove kode.
- Kljub temu, da mora biti izvorna koda dostopna, lahko izvorni avtorji zahtevajo, da se morebitne spremembe jasno ločijo od originalne kode in tako ohranijo ločnico med prvotno in modificirano kodo (npr. v obliki popravkov ali različnih verzij).
- Licenca ne sme omejevati katerekoli osebe ali skupine.
- Licenca ne sme biti omejevalna glede na področje dela, v okviru katerega se programska koda uporablja.
- Distribucija licenc mora biti enakovredna za vse uporabnike, brez dodatnih omejitev.
- Licenca za isto programsko kodo se ne sme razlikovati, če se jo uporablja v kombinaciji z drugo programsko opremo.
- Licenca ne sme omejevati uporabe druge programske opreme.
- Licenca mora biti tehnološko nevtralna.

Dostopno na: *http://www.coks.si/index.php5/Vse_o_Odprti_kodi*

NAMIG ZA PRAKTIČNO DELO V RAZREDU: Lotite se aktivnosti iz Priročnika za razredne aktivnosti na CD-ju pod zaporedno številko 11: «**Peter proti pratom**« ali aktivnosti pod zaporedno številko 12: «**C in CC**« oz. aktivnosti pod zaporedno številko 13: «**Piratska pesem**«.

4 Škodljive in nezakonite spletne vsebine

4.1 Škodljive spletne vsebine

Škodljivost določene spletne vsebine je pogojena s kulturo in vrednotami, ki veljajo v določeni skupnosti oz. državi. Raznolikost v sistemu vrednot vpliva tudi na različnost pogledov na to, kaj je škodljivo in kaj ne. Na splošno lahko rečemo, da so škodljive tiste spletne vsebine, ki prizadenejo čustva določenih oseb oz. družbenih skupin (**npr. spletne strani o nasilju, umorih, spletna mesta za spodbujanje rasizma, anoreksije ali samomorov, ipd.**).

Pogosto sploh ne gre za to, da bi otroci iskali tovrstne teme. Veliko strani, popolnoma nepovezanih z omenjenimi temami, prikazujejo pojavna okna (ang. »pop-up windows«) z vsemi vrstami vsebin, še posebej pornografskimi.

4.1.1 Nasilje na internetu

Nasilje na internetu obsega **nasilne igre, spletno pornografijo, sovražna sporočila, spolne zlorabe** (ang. »cybersexexploitation«) in **nadlegovanje** (Kočevar, 2005: 20).

Veliko nasilja se na internetu dogaja na forumih in klepetalnicah, katerim je skupno, da so namenjeni pogovorom in izražanju mnenj o specifičnih javnih temah. Na forumih in klepetalnicah lahko na žalost najdemo tudi žaljiva sporočila (»flaming«), zalezovanje (»cyberstalking«) in spletno sovraštvo (»cyberhate«) (Kočevar, 2005: 20). Obstajajo sovražno nastrojene skupine, ki preko različnih sredstev obveščanja, npr. knjig, revij, letakov pa tudi časopisov širijo svoje ideje. Z napredkom komunikacijskih tehnologij se je sovražna propaganda preselila tudi na svetovni splet. Tako npr. v klepetalnicah potekajo pogovori različnih ekstremističnih skupin, kot so npr. neonacisti. USENET skupine, ki so zbirka tisočerih javnih diskusij, v katerih posamezniki pišejo, berejo in odgovarjajo na sporočila, vsak dan pritegnejo na tisoče tako aktivnih (tistih, ki pišejo) kot tudi pasivnih posameznikov (tistih, ki samo berejo sporočila in v debatah ne sodelujejo). V teh diskusijah pogosto naletimo tudi na različne sovražne in nasilne vsebine. Ena izmed oblik širjenja nasilne propagande je tudi širjenje preko elektronske pošte. Z ustrezno mailing listo lahko nasilna sporočila dosežejo širok krog posameznikov (Weiss in Espana, 2006).

4.1.2 Računalniške in spletne igre

Igranje računalniških oz. video iger (med slednje spadajo poleg računalniških iger še arkadne in konzolne) sicer ni omejeno na sam računalnik, ampak je to zabavo mogoče izvajati tudi preko arkad in konzol, ki jih na tržišča pošiljajo velika računalniška podjetja. V številnih video igrah, kupljenih na CD-jih ali DVD-jih, je mogoče igrati proti drugim igralcem z uporabo osebnih računalnikov ali igralnih konzol z internetno povezavo. Poleg tega je na voljo veliko spletnih strani, ki nudijo možnost igranja spletnih iger prek interneta, igralec pa jih lahko igra bodisi sam bodisi proti drugim igralcem. To so lahko enostavne arkadne igre, masivne večigralske spletne igre vlog ali MMORPG, ki omogočajo velikemu številu igralcev, da sočasno sodelujejo v eni sami spletni igri.

Kategorije spletnih iger [9]

Slogi in žanri iger se hitro spreminjajo, zato je težko biti natančen, kljub vsemu pa trenutno obstajajo štiri glavne vrste iger, ki se igrajo prek spleta:

- **Miniigre/Browser igre**

Obstajajo spletne različice klasičnih arkadnih, namiznih ali digitalnih iger. Te so ponavadi brezplačne in so pogosto na voljo na spletnih straneh in igralnih portalih, ki se financirajo z oglasi. Te igre so v glavnem namenjene za enega igralca in ne vključujejo virtualnega, pripovednega sveta. Spacewar, PacMan, kakor tudi igre s kartami, kot sta Solitaire in Blackjack, so najpogostejše oblike iger, ki se igrajo prek spleta.

- **Igre z oglasi (advergames)**

Igre z oglasi so oblikovane za namen promocije določenega proizvoda, podjetja ali političnega stališča. Ponavadi vidno predstavljajo proizvod nekega podjetja in se jih igra prek spletne strani tega podjetja ali pa se jih s te strani naloži. Močno so povezane s tržnimi kampanjami, saj je njihov namen čedalje več ljudi seznaniti s proizvodom in podjetjem.

- **Omrežne igre**

Te igre se ponavadi igrajo prek spleta z osebnim računalnikom, vendar čedalje več igralcev uporablja tudi igralne konzole z dostopom do interneta. Njihova priljubljenost se je povečala z dostopom do interneta po pavšalni ceni in lahko dostopno širokopasovno tehnologijo. Zajemajo večino igralnih žanrov, vendar pa je glavni slog igre taktični boj, kot so prvoosebne strelske igre, katerih lastnost je prikaz na zaslonu, ki omogoča gledišče lika iz igre. Igralci lahko tekmujejo eden proti drugemu ali v ekipah. Ena izmed najbolj priljubljenih iger v tej kategoriji je Doom.

- **Strateške igre**

Te igre v resničnem času, pri katerih se uporablja taktično načrtovanje, so rezultat računalniško podprtega razvoja tradicionalnih vojnih iger, omrežne večigralske igre pa so prav tako zelo priljubljene v obliki različnih športnih iger, kot so dirke ali nogomet.

[9] Dostopno na: *http://www.pegionline.eu/sl/index/id/200)*

- **Masivne večigralske igre**

Masivne večigralske igre se od drugih spletnih iger razlikujejo na dva načina: (1) v eni sami igri sodeluje veliko število igralcev sočasno in (2) značilnost iger je neprekinjenost (npr. igra se nadaljuje ne glede na to, ali v njej določen igralec sodeluje ali ne). Te igre nudijo bogat tridimenzionalen svet, ki je poseljen s tisoči igralcev. World of Warcraft podjetja Blizzard Entertainment/Vivendi Game ima več kot 6 milijonov prijavljenih igralcev (1 milijon v Evropi in več kot 1,5 milijona na Kitajskem). Igra Everquest, ki je nekoč veljala za vodilno na tržišču, ima približno 500.000 prijavljenih igralcev, Ultima Online pa 250.000. V tej kategoriji prevladujejo igre vlog, v katerih udeleženci prevzamejo vloge namišljenih likov in skupaj ustvarjajo zgodbe ali jim sledijo. Njihov namen je ustvariti bolj odprt pristop do igranja, znane pa so po družbenih vidikih (omogočena je tudi komunikacija med igralci) in vidikih skupnosti, ki so skozi to storitev postali razpoložljivi. Tako so te igre široko poznane pod nazivom masivne večigralske spletne igre vlog (MMORPG).

Ali lahko nasilne računalniške igrice povzročijo nasilno obnašanje otroka?

Teorije različno odgovarjajo na to vprašanje. Stimulacijske teorije trdijo, da nasilne računalniške igre spodbujajo agresivnost igralcev, inhibicijske teorije pa nasprotno prepričujejo, da nasilne igre vzbujajo strah in s tem zmanjšajo agresivnost pri igralcih. Spet tretje habitualizacijske teorije trdijo, da igre igralce otopijo in se ti nanje tako navadijo, da jim več ne pomenijo ničesar, ne vzbujajo nikakršnih čustev, reakcij, katarzijske teorije pa govorijo o tem, da računalniške igre, tudi nasilne, delujejo sproščujoče in s tem zmanjšujejo agresivnost pri igralcih.

Teorije so si torej nasprotujoče, pa vendar bi se lahko po eni strani strinjali z vsako izmed njih. Dejstvo je, da bodo nasilne računalniške igrice pri nekaterih otrocih verjetno res vzpodbudile strah pred nasiljem in bodo zato manj agresivni, pri drugih pa bodo verjetno vzbudile agresijo, ki je do takrat »počivala« ali pa se je kazala na drug, manj očiten način. Težave povezane z nasilnimi računalniškimi igricami nastanejo takrat, ko igralec mehanizme, ki jih pozna iz računalniških iger, prenese v vsakdanje življenje.

Starši se pogosto sprašujejo, ali naj otrokom prepovejo uporabo računalniških igric ipd. Nekateri strokovnjaki so mnenja, da je treba otrokom sploh prepovedati vse igre, kjer se dogaja kaj akcijskega, na drugi strani pa so proizvajalci iger s pomočjo drugih strokovnjakov dokazovali, da te igre niso škodljive, celo nasprotno, da so zdrave, saj izboljšujejo igralčevo motoriko, sposobnost strateškega razmišljanja, in da niso razlog za to, da tu in tam kak otrok »zaide«. Seveda je realnost nekje vmes, saj v prepiru, kjer so na eni strani starši, ki so občutljivi glede svojih otrok, na drugi pa industrija iger, v kateri se vrtijo milijarde, ne more biti zmagovalca (Banović, 2003: 16-19).

Oznake računalniških igric

Podobno kot filmska industrija so tudi proizvajalci video igric razvili sistem oznak, ki uporabnikom pomaga oceniti primernost določene igrice zanje in za člane njihove družine.

ESRB (»The Entertainment Software Ratings Board«) je staršem ponudil izčrpen spekter oznak primernosti igric za določeno starostno obdobje. Spodnja preglednica prikazuje posamezne oznake in njihov pomen.

OZNAKA	POMEN
	**EC: Zgodnje otroštvo (»Early Childhood«)** Vsebina je primerna za otroke starejše od treh let in ne vsebuje materialov, ki bi jih starši lahko ocenili kot neprimerne.
	**T: Najstniki (»Teen«)** Vsebina je primerna za otroke starejše od trinajst let in lahko vsebuje nasilne vsebine (tudi nekaj krvavih prizorov), namigujoče teme, surov humor, simulirano kockanje in/ali nepogosto uporabo kletvic.
	**AO: Starejši od 18 let (»Adults Only 18+«)** Vsebina je primerna samo za odrasle, saj lahko vsebuje daljše prizore hujšega nasilja in/ ali nazorno spolno vsebino in goloto.
	**E: Vsi (»Everyone«)** Vsebina je primerna za osebe starejše od šestih let in lahko vsebuje tudi nekaj malega nasilja in komične nagajivosti ali občasnega neprimernega govorjenja.
	**M: Zreli (»Mature 17+«)** Vsebina je primerna za osebe starejše od 17 let, saj lahko vsebuje precejšnje nasilje, krvave prizore in surovo, spolno vsebino in/ali kletvice.
	**RP: V ocenjevanju (»Rating Pending«)** Uporablja se le v oglasih, ki napovedujejo prihod nove igre, kar pomeni, da igrica še ni dokončana ali še ni bila uradno ocenjena ali oboje. Pogosto navdušenci nad igricami že veliko prej, preden igrica pride na trg, razpravljajo o njej.

Slika 6: Oznake računalniških iger (vir: Microsoft, dostopno na *http://www.gamesforwindows.com/en-US/Support/Pages/esrb.aspx)*.

Spletni PEGI- zaščita pred neprimernimi vsebinami iger

V zadnjih nekaj letih je Vseevropski informacijski sistem za igre (PEGI) staršem po Evropi posredoval podrobna priporočila v zvezi s primernostjo vsebine iger za mlade. Sistem PEGI nudi zanesljive in razumljive informacije v obliki oznak starostnih ocen in opisov vsebin na embalaži igre, s čimer pripomore k informiranim odločitvam o nakupu.

Spletni PEGI je nov dodatek k sistemu PEGI. Njegov namen je mladim v Evropi omogočiti boljšo zaščito pred neprimernimi vsebinami iger in pomagati staršem, da razumejo tveganja in možnosti škodljivega vpliva v tem okolju. Logotip Spletnega PEGI je prikazan na embalaži igre, ki se prodajala na CD-jih, DVD-jih ali na spletni strani igre. Logotip pomeni, da je igro mogoče igrati prek spleta in tudi, da je določena igra ali spletna stran pod nadzorom operaterja, ki skrbi za zaščito mladih.

Igre, ki se ne igrajo na spletu, temveč s konzolami ali na osebnem računalniku, se še naprej ocenjujejo v okviru veljavnega sistema PEGI ali drugih že veljavnih priznanih evropskih ocenjevalnih sistemov.

Slika 7: Pegi oznake računalniških iger. Za dodatne informacije si oglejte spletno stran: *http://www.pegionline.eu/sl*.

4.1.3 Nadlegovanje preko interneta in mobilnih telefonov[10]

Spletno nadlegovanje je razširjeno na internetu in tudi na mobilnih telefonih. Lahko se odvija preko elektronske pošte, klepetalnic, debatnih skupin, forumov, SMS-ov ali MMS-ov. Oblike nadlegovanja so predvsem naslednje: draženje, norčevanje iz posameznikov, opravljanje, pošiljanje nezaželenih sporočil, pošiljanje prizorov vrstniškega nasilja ipd.

Med različnimi oblikami nadlegovanja na internetu je prisotno tudi spolno nadlegovanje (npr. pošiljanje reklamnih sporočil ponudnikov erotičnih vsebin po elektronski pošti, nagovarjanje h kibernetskemu seksu na IRCu (ali prek spletne kamere), puščanje opolzkih sporočil na osebnih predstavitvenih straneh, ipd.). Na Poljskem se je kar 56% najstnic že znašlo v neželenih pogovorih s seksualno vsebino, kaže evropska raziskava Eu Kids Online.

Po podatkih nekaterih mednarodnih raziskav je eden izmed štirih otrok žrtev nadlegovanja preko mobilnih telefonov oz. preko svetovnega spleta. Kar petina belgijskih otrok, starih med 9 in 12 let, se je na spletu že počutilo ogrožene. Ravno tako petina estonskih otrok poroča o nadlegovanju s strani tujcev. Slaba polovica nemških deklic in tretjina fantov (med 12 in 19 leti) poroča o neprijetnih izkušnjah v spletnih klepetalnicah. V Islandiji pa je 16% otrok že prejelo emaile/sporočila, zaradi katerih so bili prestrašeni ali zaskrbljeni. V Veliki Britaniji je ta pojav sploh dosegel velike razsežnosti in postal opazen družben problem. Okrog 20 mladostnikov si na leto celo vzame življenje med drugim tudi zaradi kibernetskega nadlegovanja.

[10] Povzeto po Becta 2007: *http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_ob_03&rid=9968* in *http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_mob_03*.

Spletno nadlegovanje bi lahko opredelili takole:

> *»Spletno nadlegovanje pomeni uporabo informacijsko-komunikacijskih tehnologij (elektronska pošta, mobilni telefoni, tekstovna sporočila, takojšnje sporočanje, osebne spletne strani in forumi) z namenom podpirati namerno, ponavljajoče se in sovražno obnašanje do posameznikov ali skupin posameznikov* (Becta, 2007a).«

Mobilno nadlegovanje

Mobilni telefoni že dolgo ne služijo več le za opravljanje telefonskih pogovorov, temveč postajajo vse bolj nepogrešljiv pripomoček za zabavo. Pošiljanje sms, nalaganje melodij in izmenjava fotografij so le ene izmed najbolj priljubljenih storitev, ki jih mobilni telefoni omogočajo. Med mladimi sta najbolj priljubljeni storitvi fotografiranje in igranje igric.

Dosegljivost preko mobilnega telefona uporabnikom vzbuja občutek povezanosti, dosegljivosti, varnosti, vključenosti, pa tudi anonimnosti in svobode. Tako ga nekateri uporabljajo tudi za škodljive namene. Mladi lahko po mobilnem telefonu dobivajo grožnje v obliki sms sporočil, zlonamerne klice, klice neznanih klicateljev, fotografije ali videoposnetke, ki jih prizadenejo. Ustrahovanja preko interneta, e-pošte in mobilnih telefonov so poleg učencev vse pogosteje deležni tudi učitelji. Nadlegovanje ali kakršna koli druga oblika nasilja pa seveda ni dopustna.

Mladostnike in otroke je potrebno poučiti, naj:

- Ne odgovarjajo na zlonamerno besedilo oziroma klic – tako le še dodatno vzpodbudijo nadlegovalca.
- Ne odgovarjajo na zgrešene klice neznanega klicatelja. Če ima klicatelj resne namene, bo poklical še enkrat ali pa bo poslal SMS-sporočilo.
- Če prejmejo zlonamerno fotografijo ali SMS sporočilo, le-to pokažejo osebi, ki ji zaupajo. Fotografijo ali sporočilo naj shranijo. To je lahko dokazni material v primeru prijave policiji.
- Številko mobilnega telefona posredujejo le družinskim članom in bližnjim prijateljem.

Na *www.safe.si* najdete informacije, kako lahko pri posameznem mobilnem operaterju prijavite mobilno nadlegovanje in neželene klice in kako vam lahko pomagajo.

Uporaba fotoaparata na mobilnem telefonu je na nekaterih javnih mestih, npr. v kinu, športnih dvoranah, pogosto prepovedana. Prav tako je v nekaterih primerih prepovedano fotografiranje oseb brez njihove privolitve. Posledica javne objave ali razširjanja zasebnih fotografij pa je lahko tudi odškodninska tožba ali kazenski pregon (Becta, 2007b).

Nadlegovanje preko elektronske pošte

Nadlegovanje preko elektronske pošte prav tako predstavlja razmeroma anonimno obliko komunikacije, ki jo t. i. »zalezovalci« uporabljajo za nadlegovanje svojih žrtev.

Starši in učitelji so tisti, ki naj bi otroke naučili, da naj ne odgovarjajo na zlonamerno pošto, ampak naj takšno pošto pokažejo odrasli osebi, ki ji zaupajo. Če otrok prejme elektronsko pošto neznanega pošiljatelja, naj je ne odpre brez prisotnosti starša ali učitelja. Grozilnih sporočil naj otroci ne brišejo, temveč naj jih shranijo kot dokaz za morebitno prijavo policiji.

V primeru, da je bil e-mail poslan direktno z osebnega računa za elektronsko pošto, lahko zlorabo prijavimo pošiljateljevemu ponudniku storitve elektronske pošte, ki bo ukrepal dalje. Številni programi za elektronsko pošto omogočajo tudi blokado nezaželenih e-mail naslovov.

Če se nadlegovanje še kar nadaljuje ali v primeru, da e-mail naslov pošiljatelja ni znan, se lahko za sledenje pošti uporablja posebna programska oprema. Ponudniki internetnih storitev lahko žrtvam nadlegovanja ponudijo pomoč pri nastavitvi programov.

V nekaterih primerih pa je najbolje zamenjati elektronski naslov in ga že vnaprej zaščititi pred možnimi zlorabami (Becta, 2007a).

Nadlegovanje znotraj klepetalnic ter preko takojšnjega sporočanja

Klepetalnice so priljubljen način medsebojne komunikacije v virtualnem svetu, ki jo uporabljajo številni mladi uporabniki interneta. Uporaba klepetalnic je anonimna, zato si mladi v virtualnem svetu dovolijo več, kakor bi si upali v realnem svetu, ko si s sogovorniki gledajo iz oči v oči.

Otroke bi bilo potrebno naučiti, da naj uporabljajo moderirane klepetalnice. Prav tako se morajo naučiti, da med klepetanjem ne smejo izdajati osebnih informacij. Če jih med klepetanjem nekdo nadleguje, naj na takšna sporočila ne odgovarjajo, ampak naj takoj zapustijo klepetalnico in poiščejo pomoč pri odrasli osebi, ki ji zaupajo. Če uporabljajo moderirano klepetalnico, je potrebno o nadlegovanju obvestiti moderatorja, ki potem ukrepa dalje.

Takojšnje sporočanje je oblika klepetalnice, v kateri pa ponavadi sodeluje manj ljudi in je zato bolj zasebna. Sistem deluje na osnovi t. i. seznamov prijateljev (ang. »buddy list«), tako da lahko v klepetanju sodelujejo le ljudje iz seznama. Otroci lahko na seznam dodajajo le ljudi, ki jih poznajo in zavrnejo tiste, ki jih na svojem seznamu nočejo. Tako je mogoče učinkovito zmanjšati nevarnost nadlegovanja, ampak zloraba je vseeno mogoča.

Če otroka nadlegujejo preko takojšnjega sporočanja, je potrebno o tem obvestiti ponudnika internetnih storitev ter mu posredovati vzdevek ali ID, datum, čas in podrobnosti o dogodku. Ponudnik internetnih storitev bo ustrezno ukrepal. Kršitelju lahko izreče le opozorilo ali pa ga tudi odstrani iz sistema. Če je otrok doživel zlorabo preko sistema takojšnjega sporočanja, je najbolje, da se ponovno registrira v sistem z novim ID (Becta 2007a).

NAMIG ZA PRAKTIČNO DELO V RAZREDU: Lotite se aktivnosti iz Priročnika za razredne aktivnosti na CD-ju pod zaporedno številko 22: **»Klepetanje z neznanci na internetu«.**

Nadlegovanje preko spletnih strani

Nadlegovanje preko spletnih strani je manj pogosto, a postaja vse večji problem. Tovrstno nadlegovanje je ponavadi naperjeno proti posameznikom oz. skupinam posameznikov.

Če otrok naleti na spletno stran, ki je žaljiva do njega, naj se takoj obrne na odraslo osebo. Takšno spletno stran je potrebno za dokaz shraniti in sprintati. Prav tako je potrebno takoj obvestiti ponudnika internetnih strani, ki na svojem strežniku gosti sporno spletno stran. Ponudnik potem ukrepa dalje, tako da odkrije avtorja spletne strani in zahteva, da sporno spletno stran umakne s strežnika.

Dandanes vse več spletnih strani in forumov mladim obiskovalcem ponuja možnost glasovanja oz. oblikovanja lastnih komentarjev. Kršitelji pogosto izkoriščajo te dodatne možnosti za poniževanje in nadlegovanje sošolcev ter ljudi, ki jih poznajo.

Kako preprečiti spletno nadlegovanje?

- **Svojih osebnih informacij (imena, naslova, telefonske številke, e-mail naslova) naj otroci nikoli ne posredujejo preko interneta.** Če »zalezovalci« ne bodo imeli dostopa do teh informacij, jih tudi ne bodo mogli zlorabiti.
- **Otroke učite, da ne smejo verjeti vsemu, kar na internetu preberejo.** Ne obstaja nikakršno zagotovilo, da vsi ljudje na internetu govorijo resnico, zato naj otroci ne nasedajo prevaram in lažem.
- **Otroci naj upoštevajo spletni bonton**. V virtualnem svetu naj veljajo ista pravila kot v realnem svetu.
- **Otroci naj ne pošiljajo sporočil, kadar so slabe volje.** Otroke učite, da naj počakajo, da se umirijo in v miru razmislijo, kako pravilno odreagirati. Jezna sporočila bodo kasneje lahko obžalovali, napake pa bodo le stežka popravili, saj se sporočil, ko so enkrat poslana, ponavadi ne da brisati.
- **Otroke naučite, da naj nikoli ne odpirajo sporočil, ki jim jih pošiljajo neznanci.** Otrok naj takšno sporočilo zbriše, prav tako pa naj se posvetuje z odraslo osebo, ki ji zaupa.
- **Če se otroku nekaj ne zdi v redu, potem zagotovo res ni**. Otroke učite, da naj zaupajo svojim občutkom. Vsebine, ki jim povzročajo strah ali nelagodje, naj vedno pokažejo staršem, učiteljem ali drugim odraslim.
- **Otroci naj nikoli ne odgovarjajo na sporočila spletnih nadlegovalcev**. To je natančno tisto, kar nadlegovalci hočejo. Če pa bodo videli, da ni odgovora, bodo prej ali slej odnehali.
- **Otroke naučite uporabljati zaščito (gesla, blokiranje pošiljateljev ...)**.
- **Otroci naj se ne srečujejo z ljudmi, ki so jih spoznali on-line, vsaj ne brez spremstva.**

- **V primeru, da otroke nadlegujejo, naj se le-ti zaupajo staršem ali učiteljem**. Ti jim bodo znali zagotovo prav svetovati (Becta, 2007a).

NAMIG ZA PRAKTIČNO DELO V RAZREDU: Lotite se aktivnosti iz Priročnika za razredne aktivnosti na CD-ju pod zaporedno številko **25**: **»To se pa meni ne more zgoditi!«** in aktivnosti pod zaporedno številko **26**: **»Pomagaj prijatelju«.**

4.1.4 Verodostojnost internetnih virov

Internet ponuja ogromno virov in možnosti za učenje, vendar vsebuje tudi veliko informacij, ki niso ne koristne ne zanesljive. Ker lahko na internetu pripombe ali informacije objavi kdorkoli, **morajo uporabniki razviti kritično mišljenje**, da lahko presojajo točnost spletnih informacij. To še posebej drži za otroke, ki verjamejo v to: »Če je na internetu, je gotovo res.« Tiskani viri so imeli običajno varovalke – kot so uredniki, lektorji in cenzorji –, ki so izločili napake, laži in netočne informacije. Internet pa pogosto nima nobenih varovalk, ko gre za preverjanje verodostojnosti informacij, ki so objavljene v njem. Naučite otroke, kako deluje internet in da lahko spletno stran postavi skoraj vsak, ki ni nujno strokovnjak za področje, o katerem piše. Naučite jih uporabljati širok razpon virov informacij ter da preverijo in podvomijo v to, kar najdejo v internetu[11].

Za vse, ki iščejo raznovrstne informacije preko interneta, navajamo v nadaljevanju nekaj nasvetov (Skrt v Moj mikro, december 2004), ki bodo pripomogli pri iskanju uporabnih in relevantnih informacij:

- **Verodostojnost vira**. Kdo je avtor informacij? Kakšna je njegova strokovnost? So objavljeni njegovi kontaktni podatki oz. kontaktni podatki podjetja, ki je informacije objavilo? Se lahko zanesemo na organizacijo, ki je podatke objavila? Je navedena povezava do druge spletne strani, če so informacije posredovane z drugega vira?
- **Primernost vsebine**. Kako natančno oz. površinsko je vsebina predstavljena? Se vsebina ujema z informacijami, ki ste jih iskali? So predstavljene tako pozitivne kot negativne plati? Lahko ocenite objektivnost?
- **Osveževanje informacij**. Kdaj so bile informacije objavljene? Kako stara je vsebina na spletni strani? Ali je obravnavana tekoča problematika? Preverite rok uporabnosti posredovane informacije?
- **Uporabljate več virov**. Zanesljivost informacij preverite še na kakšni drugi spletni strani. Če več virov poroča o podobni zadevi, je verjetnost, da je informacija prava in ažurna, večja.
- **Bodite sumničavi**, če zasledite, da se spletna stran hvali, da lahko določene informacije dobite samo na njihovi strani (navedbe v stilu »only source«) in nikjer drugje. Verjetnost zanesljivih informacij je manjša, če želi spletna stran diskreditirati drugi vir«

[11] Microsoft: *http://www.microsoft.com/slovenija/doma/varnost/otroci/pomagajte_otrokom.mspx*

NAMIG ZA PRAKTIČNO DELO V RAZREDU: Lotite se aktivnosti iz Priročnika za razredne aktivnosti na CD-ju pod zaporedno številko **16**: **«Ločevati mnenja od dejstev na internetu«** ter pod zaporedno številko 19: **«Komuniciranje v svetu novih tehnologij«.**

4.1.5 Zasvojenost z internetom

Internetno zasvojenost lahko opišemo kot impulzivno kontrolno motnjo, ki je zelo podobna zasvojenosti z igrami na srečo (hazarderstvo), motnjam hranjenja ali alkoholizmu. Posameznik preživi preveč časa pred računalnikom in se tem aktivnostim ne more odpovedati. Poznamo pet podtipov zasvojenosti z internetom: s spletno pornografijo, z virtualnimi odnosi,z igrami na srečo na internetu, z informacijami na internetu, s spletnimi igrami. Večji potencial za zasvojenost ima uporaba interneta, ki je usmerjena v navezovanje stikov ali vzpostavljanje (nadomestnih) odnosov; manjšega pa uporaba interneta za iskanje informacij.

Znaki zasvojenosti:

- **prezaposlenost** z internetom ali mobilnim telefonom
- uporaba interneta oz. mobilnega telefona ali igranje igric **preko vseh časovnih norm** (bedenje dolgo v noč)
- **nervoza, slaba volja, depresija in razdražljivost**, ko je potrebno prekiniti internetno povezavo oz. izklopiti telefon
- **laganje staršem, prijateljem** in ostalim o času, ki ga preživijo »on-line« oz. ob igranju igric
- **poslabšanje šolskega uspeha** zaradi pretirane navezanosti na virtualni svet
- **izguba interesa za druženje** s prijatelji v »resničnem svetu«
- ponavljajoči, **neuspešen trud za nadzor** nad uporabo interneta oz. igranja igric in nezmožnost prenehanja
- uporaba novih tehnologij kot sredstvo **pobega pred problemi** ali za sproščanje različnih negativnih občutkov (občutek nemoči, krivde, strahu ali depresije)
- **fizične težave:** neprespanost, rdeče oči, poslabšanje vida, SMS palec, pomanjkanje gibanja

Dr. Youngova (1998) trdi, da internet lahko zasvoji iz več razlogov. Eden izmed razlogov je ta, da je skupnost resnična in živeča entiteta, ki za zasvojence pomeni drug dom oz. mesto, kjer se vedno čutijo dobrodošle in kamor mislijo, da pripadajo. S pomočjo interneta se zateče v nek fantazijski svet, kjer lahko dobiš prijatelje za pogovor ali igranje iger ob katerokoli uri dneva. Na internetu lahko kadarkoli postaneš kdorkoli. Če si v resničnem življenju sramežljiv, lahko preko omrežja postaneš odprt in komunikativen, če si dolgočasen, lahko takoj postaneš duhovit in če si po naravi previden, lahko to previdnost obrneš v tvegano obnašanje, seveda le v kibernetskem prostoru (Young, 1998). Po besedah dr. Youngove (1998) moške in ženske ne uporabljajo interneta enako in niso zasvojeni z enakimi stvarmi. Moški na splošno raje iščejo moč in dominacijo in se pri uporabi interneta nagibajo k iskanju infor-

macij, obiskovanju strani z erotično vsebino, »cybersexu« in k igranju agresivnih interaktivnih iger. Ženske pa se zatekajo h klepetalnicam, da bi tam našle prijatelje, romanco ali pa da bi samo našle nekoga, ki bi mu lahko potožile o problemih, otrocih, možu. Poleg tega ženskam bolj kot moškim godi, da nihče, ki ga spoznajo preko interneta, ne ve, kako v resnici izgledajo (Young, 1998).

Nekaj meril za določanje zasvojenosti z internetom (več testov najdete tudi na spletni strani *www.safe.si*) je Helena Jeriček v svojem članku Zasvojenost z internetom (2003) povzela vprašalnik, ki ga je pripravila dr. Youngova (1996) in je prirejen po merilih za zasvojenost s hazardiranjem (po Diagnostic and Statistical manual of Mental Disorders- 4th Edition).

Sestavljen je iz naslednjih vprašanj:

1. *Ali se počutiš preobremenjenega z internetom (misliš na prejšnjo aktivnost ali pričakuješ naslednjo)?*
2. *Ali čutiš potrebo, da bi vedno več časa preživel na internetu, da bi doživel zadovoljitev?*
3. *Kako pogosto si neuspešen pri kontroliranju, zmanjšanju ali prekinitvi uporabe interneta?*
4. *Ali si nemiren, nervozen, depresiven ali razdražljiv, ko zmanjšaš ali prenehaš z uporabo interneta?*
5. *Ali ostaneš na mreži dlje, kot prvotno načrtuješ?*
6. *Si tvegal izgubo pomembnejših odnosov, dela ali izobraževalnih priložnosti zaradi interneta?*
7. *Si se kdaj zlagal prijateljem, staršem ali drugim zato, da bi skril svojo navezanost na internet?*
8. *Ali uporabljaš internet kot beg pred problemi ali občutki krivde, nebogljenosti, zaskrbljenosti ali depresije?*

Youngova (1996) meni, da **pet pozitivnih odgovorov že pomeni, da je človek zasvojen z internetom**. Jeričkova (2003) pravi, da se vpliv dolgotrajne in pogoste rabe interneta kaže na treh različnih področjih. Kot prvo na fizičnem področju, ki se odraža v pomanjkanju spanca, saj so zasvojenci pokonci dolgo v noč, posledice pa so preutrujenost, občutljive oči in bolečine v križu. Drugo področje so težave na šolskem in poklicnem področju, saj zasvojenci niso sposobni normalno opravljati službene in šolske obveznosti. Prvi znaki, da z otrokom ni nekaj v redu, se običajno pojavijo ravno pri šolskem uspehu, ki se drastično poslabša. Tretje področje pa je družinsko in socialno življenje. Zasvojenci zaradi pretirane rabe interneta zanemarjajo družinske obveznosti in prijateljske odnose.

Če torej pretirana uporaba interneta vpliva na šolsko in poklicno delo ali slabo vpliva na odnose v družini in s prijatelji, je potrebno ukrepati. V takšnih primerih priporočamo pogovor s strokovnjakom. Jeričkova (2003) priporoča uporabo družinske terapije v primerih, pri katerih je zloraba interneta pretrgala družinske odnose in imela negativen vpliv na družinsko življenje. Pri tem se izpostavlja potreba po izobraževanju družine o tem, kako lahko internet zasvoji, zmanjševanju krivde, izboljšanje poročanja o problemih, ki so bili pred zasvojenostjo in so privedli do tega, da je moral zasvojenec zadovoljevati svoje potrebe na internetu. Prav tako pa je treba družino pripraviti do tega, da zasvojencu pomaga pri iskanju novih konjičk-

ov ter da posluša njegove občutke. Odvisnost od interneta ali pretirana navezanost na mobilni telefon je namreč predvsem simptom in prvo opozorilo, da se z mladim človekom dogaja nekaj pomembnega v čustvenem in socialnem pogledu. Prekomerna raba novih tehnologij je pogosto znak drugih težav, kot so depresija, jeza in nizka samopodoba. Pomemben je vsakodnevni pogovor z otrokom o njegovih težavah, občutkih in potrebah. Računalnik naj ne postane otrokova varuška.

Psihoterapevt Bogdan Žorž svetuje, da se otroke čimbolj zgodaj spodbudi in navadi, da začnejo uporabljati računalnik kot orodje. Za začetek je to lahko zelo preprosta uporaba, še vedno v obliki igre: otrok naj kaj nariše; kasneje naj začne svoje izdelke, svoje igrice urejati v svoji računalniški knjižnici. Večji otroci lahko na računalniku oblikujejo zanimive power point predstavitve o najljubšem športu, zvezdnikih, živalih; lahko se naučijo tudi kaj izračunati v programu Excel itd.

NAMIG ZA PRAKTIČNO DELO V RAZREDU: Lotite se aktivnosti iz Priročnika za razredne aktivnosti na CD-ju pod zaporedno številko 14: **«Zasvojenost z internetom«.**

4.1.6 Zasvojenost z računalniškimi in spletnimi igrami

Vzpostavljanje stikov je tisto, kar zasvoji, tudi pri igranju iger preko spleta, saj igralec sodeluje z drugimi igralci iz vsega sveta in ne more prenehati, ker jih ne želi pustiti na cedilu. Sicer pa igre zasvojijo tudi iz drugih razlogov - že oblikovane so tako, da vlečejo igralca naprej z novimi višjimi stopnjami, izzivi ... Psihoterapevt Bogdan Žorž opozarja še na nekatere elemente, ki v igrah zasvojijo: igre namreč omogočajo razmah občutkov moči, lastne vrednosti in uspešnosti brez pravega napora oziroma tveganja in s tem zadovoljujejo resnične potrebe v navideznem svetu, kar pa pravzaprav pomeni beg iz realnosti, beg od resničnih življenjskih izzivov. K tovrstnim zasvojenostim so bolj nagnjeni dečki kot deklice, ki jih lažje zasvojijo komunikacijske tehnologije, kot so npr. klepetalnice ali mobilni telefoni.

4.1.7 Zasvojenost z mobilnimi telefoni

Mobile phone disorder ali krajše MPD je nova zasvojenost 21. stoletja in je prav tako ena od negativnih posledic pojava mobilne telefonije na trgu ter njene prekomerne uporabe. Dejstvo je, da starost uporabnikov mobilnih telefonov pada. Uporaba predplačniških paketov pa je zelo enostavna, zato ima dandanes večina najstnikov svoj mobilni telefon (na Slovenskem že 95 % mladostnikov). Najstniki za mobilni telefon porabijo veliko časa, saj z njim kličejo, pišejo SMS sporočila, slikajo in pošiljajo slike, dostopajo do interneta, pa tudi kupujejo in izmenjujejo mobilne melodije, ozadja za zaslone ipd. Mnogim je pomembno tudi to, da imajo najnovejši model telefona. Te navade uporabnikom mobilnih telefonov povzročajo dodatne stroške, ki so pravzaprav nepotrebni (Lin, 2004).

Španski psihiatri zatrjujejo, da je zasvojenost z mobilnim telefonom obsesivno-kompulzivna motnja, ki lahko v ekstremnih primerih zasvojence popolnoma izolira, jih ekonomsko uniči ali pa celo spremeni v kriminalce. Večina zasvojencev je najstnikov z nizko samozavestjo, ki podležejo agresivnim marketinškim kampanjam. Mladi zasvojenci porabijo preveč časa za klicanje, prejemanje in pisanje SMS sporočil, povezovanje na internet, zaradi česar izostajajo

od pouka, v ekstremnih primerih pa celo opustijo šolanje. Zasvojenci, ki nimajo sredstev za plačevanje visokih telefonskih računov, lahko zabredejo tudi v kriminal (DPA, 2003).

Vesna Milek (2005) v svojem članku *Ljubezen v času SMS* piše, da mnogi naključno izprašani slovenski mladostniki pravijo, »da si ne znajo predstavljati dneva brez mobilnega telefona«. Kadar ga pozabijo doma, se počutijo goli, nezaželeni, sami. Odmori med šolskimi urami na osnovnih šolah, gimnazijah, v avlah fakultet so videti popolnoma drugače kot še pred desetimi leti. Vse več je tistih, ki odmore med predavanji raje kot za druženja izkoristijo za ukvarjanje s sporočili po telefonu ali za preverjanje e-mailov«. Po besedah psihiatra dr. Mrevljeta[12], ki ga v svojem članku navaja Milekova (2005), so simptomi SMS odvisnosti predvsem: »nenehno pogledovanje na mobitel, vsako minuto, čakanje na SMS, če ga ne dobijo, postanejo tesnobni in jih začnejo kompulzivno pošiljati naokrog, čedalje pogostejše naj bi bile tudi poškodbe palca. Dr. Mrevlje tudi pravi, da se v Sloveniji s to vrsto »odvisnosti« ali pojavom MPD še nismo sistematično srečevali ali ukvarjali. »Tisti, ki delamo z mladostniki, opažamo določeno navezanost na telefone, vendar pretiravanje v tej smeri razumemo kot motnjo le takrat, kadar je posledica drugih mladostniških zapletov ali težav v tem razvojnem obdobju. **Odvisnost ali pretirana navezanost na mobilni telefon je predvsem simptom in prvo opozorilo, da se z mladim človekom dogaja nekaj pomembnega v čustvenem in socialnem pogledu. Gre torej za posledico, ne pa za vzrok**.«

NAMIG ZA PRAKTIČNO DELO V RAZREDU: Lotite se aktivnosti iz Priročnika za razredne aktivnosti na CD-ju pod zaporedno številko 15: **«Pro et. contra: Raba mobilnih telefonov med poukom«.**

4.1.8 Pornografija na internetu

"Seks" je najbolj iskana beseda v spletnih iskalnikih. Na svetovnem spletu je na voljo velikanska količina pornografije. Po nekaterih ocenah naj bi bile kar dve tretjini vsega materiala na internetu pornografskega. **Pornografska industrija je bila ena najmočnejših gonilnih sil razvoja interneta zaradi zahtev uporabnikov pornografije po varnosti in zasebnosti med plačevanjem materiala, je v resoluciji zapisal Evropski parlament.** Internet omogoča uporabniku različne načine prenosa pornografskih vsebin: lahko si jih ogleduje na spletnih straneh, jih prenese v svoj računalnik, jih pošilja po elektronski pošti, se v klepetalnicah druži z enako mislečimi ali si v živo ogleda različne spolne prakse. Pornografsko gradivo pa je dostopno tudi mladoletnim osebam. Pornografska vsebina postaja tudi gonilna sila mobilne telefonije, saj naj bi bilo ogledu »pornografskih vsebin« na mobilnih telefonih namenjenih kar 80 odstotkov vseh zahtevkov (Šribar, Boldin 2007). S pojavom nove generacije mobitelov G3, ki omogočajo prenos slike in videa se poronografija učinkovito širi tudi na mobilne telefone (v Sloveniji lahko omenimo mobilni portal Dajmedol in Planet 9).

V današnji družbi, kjer je pornografija dejansko prisotna na vsakem koraku, se pojavljajo nekateri argumenti, ki govorijo o škodljivosti pornografija za človekov psiho-fizični razvoj in o potre-

[12] Dr. Gorazd V. Mrevlje (1946) je psihiater in psihoterapevt na Centru za mentalno zdravje RS. V okviru kliničnega in pedagoškega dela se že trideset let ukvarja s socialnimi in zdravstvenimi problemi, ki presegajo medicinske in psihiatrične okvire. Deloval je na področju samomorilnosti in odvisnosti mladih, v zadnjem času pa se posveča razpoloženjskim in stresnim motnjam ljudi v urbanem okolju.

bi po njeni zakonski regulaciji. Določena omejitev je osma ***točka 84. člena Zakona o medijih*** (Uradni list RS 110/2006 z dne 26. 10. 2006), ki pravi da mora biti d*ostop do pornografskih vsebin v elektronskih publikacijah s tehničnimi sredstvi oziroma z zaščito omejen tako, da otroci in mladoletniki do njih ne morejo dostopati.* Vendar pa se te omejitve tudi na široko dostopnih portalih in spletnih straneh ne upoštevajo. Pornografske vsebine omejujeta sicer tudi Kazenski zakonik in Oglaševalski kodeks.

Po drugi strani pa trdni dokazi, ki bi potrdili dejansko škodljivost pornografije, ne obstajajo. Po navedbah nekaterih sociologov (v Šribar, Boldin, 2007), ki se s škodljivostjo pornografije strinjajo, se pri osebi, ki je pogosto izpostavljena pornografskim vsebinam, razvije povečana ravnodušnost do spolne neenakosti in spolnega nasilja. Na takšen način se vzpostavljajo družbeno škodljive norme v smislu spolnih razmerij in seksualnega vedenja. Ti sociologi menijo, da je potrebno razlikovati med kratkoročnimi in dolgoročnimi učinki pornografskih vsebin v medijih. Kratkoročni učinki se hitro izgubijo, dolgoročni pa se pojavijo šele čez čas. Šribarjeva in Boldinova (2007) menita, da »gre za medijsko vzpostavljanje kroga asociacij, ki podpira ponižujoč odnos do žensk«. Avtorici članka sta prišli do ugotovitve, da so pogosta ciljna skupina pornografov otroci in mladoletniki, »ki veliko težje zavzamejo do pornografije bolj kompleksen odnos in so tako indoktrinirani z njenimi sporočili in prežeti z učinki«. Vsesplošna prisotnost pornografije po različnih medijih povzroči, da je tovrstno obnašanje za otroke razumljeno kot popolnoma običajno in splošno sprejemljivo. Po navedbah Šribarjeve in Boldinove (2007) tako pri dečkih kakor deklicah velja, »da je povezava med spolnimi izkušnjami in pornografskimi vsebinami posredna; ne gre za enostavno identifikacijo, temveč za posnemanje skozi seksualne scenarije in vrednote. To velja tudi za učinkovanje pornografskih vsebin pri tistih otrocih in mladoletnih, ki teh vsebin ne konzumirajo hote, a so kljub temu njeni posredni porabniki ali porabnice skozi oglaševanje pornografskih vsebin ali vsiljevanje pornografskih podob s strani vrstnikov«.

Manica Ferenc v Družini (2006) navaja Šribarjevo, ki meni, »da imajo pornografske vsebine na mobilcih potencialno precej bolj škodljiv učinek kot internet, saj gre za prenosljiv mali aparat, pri roki v situacijah, ko porno vsebina lahko spodbuja spolno nasilje. In nihče ne more preprečiti, da ne bi teh vsebin starejši, ki imajo dostop do njih, kazali mlajšim. Poleg tega so zaščite na mobitelih prej zavajanje kot kakšna prepreka.«

Dejansko ima veliko mladostnikov izkušnje z listanjem po pornografskih revijah ali z branjem ljubezenskih romanov z vročimi erotičnimi scenami. Prav tako lahko na pornografijo naletijo tudi med brskanjem po internetu. Večina strokovnjakov meni, da je *mehka pornografija* (slike nagih moških in žensk v določenih spolnih položajih) relativno neškodljiva. Tovrstno gradivo, ki lahko pomaga potešiti radovednost, ne bo pospešilo, zavrlo ali kako drugače zmotilo spolnega razvoja mladostnika. Strokovnjaki menijo, da problem nastane, če so te revije oz. spletne strani edini vir informacij o spolnosti. Na tak način lahko mladostnik dobi napačno – stereotipno in konzervativno (včasih celo rasistično) - predstavo o spolnem življenju. V večini primerov je navdušenje nad pornografijo prehodno. Morda je bolje, da starši oz. učitelji pri pouku že vnaprej razložijo otroku, da vsebine v revijah oz. na spletnih straneh ne predstavljajo realnosti.

Trda pornografija (nazorni prikazi in opisi spolnih aktov) lahko veliko bolj negativno vpliva na mladostnikovo mnenje o spolnosti.Trda pornografija poveže spolnost z agresijo, popači žensko-moške spolne odnose (moški vedno nadvladuje žensko in ženska v tem uživa), ignorira intimnost in poda napačno sliko o spolnem vedenju odraslih. Če starši naletijo na revije ali filme s trdo pornografijo pri svojih najstnikih, naj jim tudi podajo argumente, zakaj nameravajo tovrstno »učno« gradivo zapleniti (Kristan, 2007).

Učiteljem in staršem svetujemo, da kadar želijo z mladostnikom govoriti o tako občutljivi temi, kot je spolnost, je dobrodošlo, da vsaj približno vedo, kaj vse najstniku roji po glavi, pa ga je sram povedati. Odprt in odkrit pogovor med otroci in starši oziroma učitelji lahko pomaga mladim, ki so sicer pri teh tematikah prepuščeni komercialnim silam, da najdejo stik s svojo seksualnostjo na bolj naraven način.

4.2 Nezakonite spletne vsebine

Na splošno velja, da so ilegalne naslednje spletne vsebine:

- **otroška pornografija oz. pedofilija** (176. člen Kazenskega zakonika RS),
- **rasistična propaganda in sovražni govor:** »Kdor izziva ali razpihuje narodnostno, rasno ali versko sovraštvo, razdor ali nestrpnost, ali širi ideje o večvrednosti ene rase nad drugo, ali daje kakršnokoli pomoč pri rasistični dejavnosti, ali zanika, zmanjšuje pomen, odobrava ali zagovarja genocid.« (297. člen Kazenskega zakonika RS),
- **propagiranje terorizma.**

Tovrstne nezakonite vsebine so kaznive v skladu z nacionalno zakonodajo (Kazenski zakonik RS) in drugimi ukrepi v notranjem pravu.

4.2.1 Otroška pornografija

Pravni okvir

V novem slovenskem Kazenskem zakoniku (v veljavi od novembra 2008) se otroške pornografije dotika 176. člen. Tako med kazniva dejanja sodijo proizvodnja, razširjanje, prodajanje, uvažanje, izvažanje ali drugačno ponujanje, po novem pa tudi posedovanje otroške pornografije. Dodanih pa je še nekaj drugih sprememb. Po novem se člen glasi takole:

(1) Kdor osebi, mlajši od petnajst let, proda, prikaže ali z javnim razstavljanjem ali kako drugače omogoči, da so ji dostopni spisi, slike, avdiovizualni ali drugi predmeti pornografske vsebine, ali ji pokaže pornografsko ali drugačno seksualno predstavo, se kaznuje z denarno kaznijo ali zaporom do dveh let.

(2) Kdor zlorabi mladoletno osebo za izdelavo slik, avdiovizualnih ali drugih predmetov pornografske ali drugačne seksualne vsebine, jo uporabi za pornografsko ali drugačno seksualno predstavo ali taki predstavi vedoma prisostvuje, se kaznuje z zaporom od šestih mesecev do petih let.

(3) Enako kot v prejšnjem odstavku se kaznuje, kdor proizvede, razširi, proda, uvozi, izvozi ali drugače ponudi pornografsko ali drugačno seksualno gradivo, ki vključuje mladoletne osebe ali njihove realistične podobe, ali kdor poseduje tako gradivo, ali razkriva identiteto mladoletne osebe v takem gradivu.

(4) Če je bilo dejanje iz drugega ali tretjega odstavka tega člena storjeno v hudodelski združbi za izvrševanje takih kaznivih dejanj, se storilec kaznuje z zaporom od enega do osmih let

(5) Pornografsko ali drugačno seksualno gradivo iz drugega, tretjega in četrtega odstavka tega člena se vzame ali njegova uporaba ustrezno onemogoči

Kot vidimo, novi zakonik nekoliko širi območje kaznivega iz samo pornografskih na tudi drugačne seksualne vsebine. Prav tako kriminalizira prisostvovanje pri pornografski predstavi z mladoletnimi osebami. Novi zakonik prepoveduje tudi otroško pornografijo, v kateri so prisotne realistične podobe mladoletnih oseb (npr. pornografsko gradivo, v katerem nastopajo animirani liki) ter razkrivanje identitete mladoletne osebe v otroški pornografiji.

Omenili smo že P2P (»Peer-to-Peer«) programe za prenašanje datotek (Kazaa, BitTorrent, eMule ...). Ti programi ponujajo tudi datoteke z otroško pornografijo, ki se pogosto skrivajo za naslovi filmov, gradiv, glasbe, ki s pornografijo nimajo nikakršne zveze. Če po naključju/nesreči takšne datoteke prenesemo na svoj računalnik, jih je treba takoj odstraniti, saj predstavljajo kršitev - posedovanje otroške pornografije. Vsi uporabniki omenjenih programov morajo, če zasledijo takšne datoteke, le-te nemudoma izbrisati iz računalnika in tako preprečiti njihovo nadaljnje širjenje, sicer se lahko znajdejo v hudih težavah s policijo.

Verjetno ni odveč, če omenimo, da je tudi v namen oglaševanja prepovedana kakršnakoli pornografija, predvsem za skupine, ki so še posebej zaščitene. Prepovedana je tudi golota.

Zakon o medijih (Uradni list RS 110/2006), 49. člen, ki se nanaša na oglaševanje za otroke, pravi: *Oglasi, katerih pretežno ciljno občinstvo so otroci ali v katerih nastopajo otroci, ne smejo vsebovati prizorov nasilja, pornografije in drugih vsebin, ki bi lahko škodovale njihovemu zdravju ter duševnemu in telesnemu razvoju, ali kako drugače negativno vplivale na dovzetnost otrok.*

Izvajanje otroške pornografije preko interneta

Otroška pornografija naj bi v zadnjih letih zelo narasla, predvsem na račun interneta in sodobne tehnologije, kar pa ne pomeni, da ni obstajala že prej. Razvila se je v dobičkonosen posel, saj imajo proizvajalci, razpečevalci in uporabniki otroške pornografije na voljo lahko dostopno tehnologijo, predvsem digitalne kamere in fotoaparate ter internet. Predvsem zaradi širjenja materiala preko interneta je policija postavljena pred zelo težko nalogo. Po besedah policije so pedofili zelo dobro organizirani, zato jim je precej težko stopiti na prste. Umazani posel se ponavadi odvija v »podzemlju«. »Material pedofilov pa je dražji, bolj kot je žrtev, torej otrok, mlajši in bolj kot je dejanje pedofilov sadistično do žrtve.« *(http://www.ecpat.de)*

Po besedah Taylor in Quayle (2003) internet ustvari socialne, individualne in tehnološke okoliščine, ki lahko privedejo do zanimanja za otroško pornografijo:

- **socialne:** na internetu se ustvarjajo virtualne skupnosti za uporabnike otroške pornografije, s pomočjo katerih uporabniki opravičujejo svoja dejanja oz. nagnjenja.
- **individualne:** z uporabo interneta lahko posamezniki dostopajo do gradiva in komunicirajo z ostalimi s pomočjo računalnika. Tako navidezno ustvarijo nekakšno privatno sfero, kjer lahko izražajo svoje spolne fantazije.
- **tehnološke:** digitalna tehnologija in internet sta omogočila uporabnikom otroške pornografije, da lahko postanejo »obsedeni« zbiralci. Internet prav tako omogoča dostop do ekstremnih spolnih fantazij. Takšne fantazije se lahko z otroki »zaigrajo« preko interneta ali pa se preko interneta dogovorijo za fizično srečanje.

Otroška pornografija se preko interneta širi in izmenjuje na več načinov: predvsem s *programi za izmenjavo datotek* (P2P, kot so npr. eMule, BitTorrent, DC++), *FTP*-jem (prenos datotek), *IRC*-em (spletni klepet), *Usenet*-om, ki se odvija v privatnem krogu (svetovno omrežje novičarskih skupin, ki obravnavajo najrazličnejše teme), seveda z *elektronsko pošto* (e-mail), precej tovrstne vsebine pa lahko najdemo tudi na *spletnih straneh* (*www*) (Thornburgh in S.Lin, 2002).

Pedofili ravno s pomočjo interneta medsebojno kontaktirajo, si izmenjavajo izkušnje in material, preprodajajo slike, otroke nagovarjajo k seksualni zlorabi v zameno za plačilo, si posredujejo kontakte in naslove, namige in opozorila pred kazensko-pravnim zasledovanjem. Z medsebojnim sodelovanjem in komuniciranjem ustvarjajo močne mreže proizvodnje in razpečevanja otroške pornografije. Pedofili na internetu ne komunicirajo le s somišljeniki, temveč iščejo tudi kontakte z otroki in mladostniki. Deklice in dečki uporabljajo klepetalnice za spoznavanje novih prijateljev. Otroci imajo te »sobe« za varne, saj sam pogovor poteka javno, predvsem pa se zanašajo na svojo »anonimnost«, saj so prepričani, da jih dejansko nihče ne pozna.

Tudi storilci se lahko med seboj sporazumevajo v klepetalnice. Kar pomeni, da se prijavijo (»logirajo«) z določenim vzdevkom (izmišljenim imenom) v zaprtem krogu klepetalnic. Tako lahko po vsem svetu ob isti uri sedijo doma pred računalnikom in komunicirajo s sebi podobnimi. Z današnjo tehnologijo, kot so digitalne kamere pa lahko slike s seksualnim nasiljem otrok direktno prenesejo tudi na internet. Tako lahko vsi, ki sodelujejo v klepetalnicah, tudi v živo sodelujejo pri spolni zlorabi. Pedofili torej izkoristijo takšne klepetalnice za klepet s potencialno žrtvijo. Seveda se predstavijo, kot da so tudi sami otroci in si s tem pridobijo zaupanje ter poskušajo pregovoriti otroke k srečanju v živo, seveda brez navzočnosti staršev. Pedofil nato želi prepričati otroka s svojim materialom o otroški pornografiji, da so spolni akti, ki si jih želi, povsem normalni. Fotografije tako opravičujejo dejanja, saj otroku kažejo, da to počnejo tudi drugi, njegovi vrstniki. Po mnenju pravnika Jake Repanška mora »upravljavec spletne klepetalnice nedvomno odstraniti očitno nezakonita sporočila, s katerimi pisec na primer širi nestrpnost do posameznikov in skupin na podlagi rasnega ali verskega razlikovanja, prav tako mora odstraniti druga sporočila s protipravno vsebino (otroška pornografija ipd.)« (Kocmur v Nedelu, 21. 8. 2005).

Naj dodamo še zanimivost, da je Microsoft leta 2003 v kar 28-ih državah zaprl svoje brezplačne klepetalnice na internetnem portalu MSN, da bi s tem zaščitili otroke pred morebitno otroško pornografijo. »Po nekaterih raziskavah so namreč ugotovili, da se je vsak četrti uporabnik klepetalnice, star med 9 in 16 let želel dogovoriti za fizično srečanje z osebo, ki jo je spoznal preko interneta. Kar 10 % teh otrok pa je na srečanje tudi dejansko šlo.« (Skrt v Moj mikro, junij 2004). Po nedavno objavljeni raziskavi iz leta 2007 EU Kids Oline sta se npr. na Češkem dobri dve tretjini mladih, starih med 12-17 let že osebno srečali s svojimi online »kontakti«. Na Poljskem je bilo kar 52% mladostnikov povabljenih na offline srečanja z neznanci, kar slaba polovica pa se je takšnih srečanj tudi udeležila.

Med vsemi je UseNet najbolj edinstvena in popularna oblika interneta v obliki javne novičarske skupine, katera ni izpostavljena nikakršni obliki nadzorovanja (redke skupine imajo moderatorje). Pogosto navajajo, da se največ pornografske vsebine pošilja po internetu prav v UseNet skupinah. Novičarske skupine, ki so namenjene izključno seksualnemu razpravljanju in pošiljanju slik, pa vendarle predstavljajo manj kot 1,5 % vseh obstoječih novičarskih skupin (Benschop, II.). Prvo raziskavo analize vsebin UseNet novičarskih skupin na internetu sta izvedla Mehta in Plaza leta 1994. Poleg vseh pornografskih vsebin, ki jih lahko najdemo na internetu, so preučevali tudi teme, ki so po kriminalnem zakonu Kanade nezako-

nite ali veljajo kot tabu. V vzorcu je bilo 15 % takih slik, ki so vključevale otroke, vendar niti ena slika ni nakazovala kakršnekoli spolnosti, večinoma so bile le slike golih otrok (Mehta, 1998). V drugi študiji računalniške pornografije, ki jo je izvedel Rimm leta 1995 med »*bulletin*« *in* »*board services*«, je bil delež pedofilskih vsebin 15,6-odstoten. Mehta je v juliju 1995 in juliju 1996 po sprejetju CDA (»Communications Decency Act«) izvedel novo študijo in ugotovil, da je slik otroške pornografije, ki sodijo v to kategorijo, približno 20 %. PO novi kategorizacijski shemi so bili deleži sledeči: 5,1 % slik golih otrok, 10,6 % slik vizualno mladih ljudi in 4,4 % pedofilskih slik (Mehta, 1998).

Sicer je od leta 1995 število spletnih strani z otroško pornografijo naraslo za 1500 %. Na ravni Evropske unije je napovedan oster boj proti takim vsebinam, nagibajo pa se tudi k temu, da bi kazensko preganjali evropske državljane, ki hodijo v tretje države z namenom spolnega izkoriščanje otrok, iz katerega potem tudi nastane video material, ki se prodaja za visoke vsote. Inicative so tudi v smeri, da se kot kaznivo dejanje opredeli t.i. »grooming«, zapeljevanje otrok v klepetalnicah, na način da se pedofil predstavlja za njihovega vrstnika.

Tip udeležbe	Značilnost	Način zlorabe
Brskalec (Browser)	Uporabnika interneta zapelje spam ali naleti med brskanjem na nezakonito stran, vendar material zavedno shrani na svoj računalnik. Zloraba se kaže v obliki posedovanja materiala, ponavljajoči obiski strani itd.	posredno
Lastna fantazija (Private fantasy)	Zavedno ustvarjanje online teksta ali digitalnih slik za privatno uporabo. Tukaj gre za fantazije o spolnem odnosu z otrokom, ne da bi prišlo do dejanja.	posredno
Aktivni iskalec (Trawler)	Aktivno iskanje otroške pornografije s pomočjo javno dostopnih iskalnikov (najdi.si, google.com ...).	posredno
Zbiralec brez zaščite (Non-secure collector)	Aktivno iskanje materiala iz odprtih virov (brez zaščite – gesla, enkripcije ...) na internetu in v klepetalnicah, pogosto s pomočjo peer-to-peer omrežij (eMule, BitTorrent ...).	posredno
Zbiralec z zaščito (Secure collector)	Aktivno iskanje materiala vendar samo preko zavarovanega omrežja. Zbiralci uporabljajo zaščitne pregrade za dostop in izmenjavo pornografskih zbirk. Poleg enkripcije oz. kodiranja, imajo nekatere skupine vstopne pogoje, ki člane prisilijo k varovanju drug drugega – vsak mora namreč za vstop predložiti slike otroške pornografije, s čimer se tudi sam vplete v kaznivo dejanje in dokaže, da ni »vohun«. Na takšen način je delovala zelo znana skupina uporabnikov otroške pornografije t. i. Čudežna deželica - Woderland Club, ki je kot pogoj za članstvo zahtevala oddajo 10.000 slik otroške pornografije.	posredno
Zapeljevalec (Groomer)	Oseba se trudi vzpostaviti virtualni kontakt z enim ali več otroki z namenom priti do spolne aktivnosti - virtualnega spolnega odnosa (cyber sex) ali fizičnega spolnega odnosa. Storilec pornografski material uporablja za »dvorjenje« in z njim poskuša prepričati žrtev, da je spolni stik nekaj normalnega.	neposredno (direktno)

Oseba, ki fizično zlorablja (Physical abuser)	Gre za zlorabo otroka, ki ga je lahko storilec spoznal preko interneta. Fizična zloraba je posneta za osebno rabo in ni namenjena kasnejši distribuciji. Storilec lahko išče material tudi po katerikoli poti, ki smo jo navedli zgoraj in ga lahko uporabi za nadaljnje zlorabe.	neposredno (direktno)
Producent/ Izdelovalec (Producent)	Izdelovalec posname lastno ali tujo zlorabo otrok ali nagovori otroke, da sami predložijo svoje slike. Producent dobavlja slike zlorab ostalim uporabnikom otroške pornografije.	neposredno (direktno)
Distributer/ Razpečevalec (Distributer)	Distributer otroške pornografije lahko ima ali pa tudi ne spolni interes do otroške pornografije. Distribuira materiale na vseh zgoraj navedenih nivojih.	posredno

Slika 8: Tipologija storilcev otroške pornografije oz. tipologija kako na internetu pride do zlorabe (vir: *http://www.aic.gov.au/publications/ tandi2/tandi279t.html)*.

Posli z otroško pornografijo se vedno bolj odvijajo preko komercialnih (plačanih) internetnih strani, ki so zaščitene z gesli ali z vstopom s kreditno kartico. Večina teh strani se nahaja v ZDA in Rusiji (*http://www.ecpat.de*). »Strokovnjaki ocenjujejo, da je 25 odstotkov spolnih zlorab v komercialne namene, torej gre za otroško pornografijo. Posnetki so namenjeni ljudem, ki zbirajo pornografski material. Med njimi so tudi pedofili, odrasli, ki uživajo v spolnem odnosu s predpubertetniki. Pri tem pa ne gre vedno nujno za klasični spolni odnos. Večina, 75 odstotkov, spolnih zlorab se zgodi doma. Storilec je človek, ki ga otrok pozna. Posneti material pa preda naprej drugim (v zameno za plačilo). »Nekateri moški celo namensko iščejo partnerke z majhnimi otroki,« pravi Tatjana Mušič, kriminalistična inšpektorica na ministrstvu za notranje zadeve.« (Merljak v Delu, 15. 5. 2003).

Jasno je, da ko so fotografije oz. material z otroško pornografijo enkrat na internetu, jih ni mogoče več nadzorovati (umakniti). Žrtev se mora tako za vedno soočiti z zlorabo. Profesor uporabne psihologije Max Taylor iz University College Cork meni, da niso največja skrb število fotografij na internetu, temveč bolj trendi, ki jih je opazil na slikah. Najnovejše slike imajo v ozadju računalnik in so postavljene v domače okolje. S tem se jasno kaže, da so otroško pornografijo ustvarili ljudje, ki so jim otroci zaupali (Taylor in Quayle, 2003).

4.2.2 Sovražni govor

Sovražni govor je izražanje mnenj in idej, ki so po svoji naravi diskriminatorne (ksenofobične, rasistične, homofobične in podobno) in uperjene proti različnim manjšinam (etničnim, narodnim, verskim, kulturnim, spolnim in podobno).

Sovražni govor torej temelji na prepričanju, da so nekateri ljudje manjvredni, ker zaradi posamezne osebne okoliščine pripadajo določeni skupini. Te osebne okoliščine so lahko: narodnost, rasa ali etnično poreklo, versko ali drugo prepričanje, spol, zdravstveno stanje, jezik, spolna usmerjenost, invalidnost, starost, gmotno stanje, izobrazba, družbeni položaj in drugo.

Glavni cilj sovražnega govora je razčlovečiti tiste, proti katerim je usmerjen, ponižati, prestrašiti in spodbuditi nasilje. Izraz zajema govorno, pisno in nebesedno komunikacijo, kot na primer: parade, trakove, simbole in podobno.

Pravni okvir – svoboda izražanja ter omejitve

Svobodo govora zagotavlja vrsta dokumentov, med drugim tudi Evropska konvencija o človekovih pravicah (v nadaljevanju EKČP) v svojem desetem členu. Vsaka pravica je omejena tudi s pravicami drugih in torej implicitno vsebuje tudi dolžnosti in odgovornosti. V drugem odstavku desetega člena EKČP so izrecno navedene predvidene možne omejitve svobode izražanja. Svobodo izražanja lahko države omejujejo, vendar le toliko, kolikor je to nujno potrebno v demokratični družbi zaradi taksativno naštetih razlogov. Omejitve so dopustne zaradi varnosti države in njene ozemeljske celovitosti, zaradi javne varnosti, preprečevanja neredov ali zločinov, za zavarovanje zdravja ali morale, zavarovanje ugleda ali pravic drugih ljudi, za preprečitev razkritja zaupnih informacij in varovanje avtoritete ter nepristranskosti sodstva. Ravno demokratična družba je tista vrednota, zaradi katere je svoboda izražanja zapisana v EKČP, in katero bodo nadzorni organi pri preučevanju nasprotujočih si interesov vedno izbrali kot rešitev. To sta v večini svojih odločitev, ki se nanašajo na sovražni govor, poudarila tudi Evropska komisija za človekove pravice in Evropsko sodišče za človekove pravice. Komisija in sodišče sta v svojih odločitvah večkrat izrazila mnenje, da so bili nameni in cilji tistih, ki so zahtevali zaščito sovražnega govora, v neposrednem nasprotju z demokratičnimi izročili, idejami in ideali, ki so evropske države vodili pri ustvarjanju EKČP (Samaluk, 2005).

Mednarodni dokumenti in standardi glede svobode izražanja:

- Splošna deklaracija človekovih pravic iz leta 1948 (19. člen),
- Evropska konvencija o človekovih pravicah iz leta 1950 (EKČP-10. člen),
- Praksa Evropske Komisije za človekove pravice (od 1954-1998) in Evropskega sodišča za človekove pravice (od leta 1959 – danes)

Ustavno – pravni okvir v Sloveniji

- **Ustava RS (39. člen):**

  »*... vsakdo lahko svobodno zbira, sprejema in širi vesti in mnenja*«.

Zavedajoč se, da je treba tudi znotraj kibernetskega prostora zagotoviti ustrezno ravnotežje med razlogi, zaradi katerih je potrebna zakonska prisila, in spoštovanjem temeljnih človekovih pravic, kot so določene v EKČP in drugih mednarodnih dokumentih, je bila leta 2001 oblikovana Konvencija o kibernetski kriminaliteti (v nadaljevanju Konvencija), kateri je bil kasneje dodan protokol, ki obravnava inkriminacijo rasističnih in ksenofobičnih dejanj storjenih v računalniških sistemih in med drugim zagotavlja tudi ustrezno ravnovesje med svobodo izražanja in učinkovitim bojem proti rasističnim ali ksenofobičnim dejanjem. V Svetu Evrope je bil že pred tem sprejet protokol št. 12 EKČP o splošni prepovedi diskriminacije. Leta 2004 se je z Zakonom o ratifikaciji konvencije o kibernetski kriminaliteti in dodatnega protokola h konvenciji o kibernetski kriminaliteti tudi Slovenija zavezala k zagotavljanju omejevanja sovražnega govora in drugih diskriminatornih praks znotraj kibernetskega prostora. Podpis Slovenije pomeni tudi zavezo za pripravo ustreznih zakonskih podlag, določil in mehanizmov za izvajanje konvencije.

- **Ustava RS (63. člen)**

  Protiustavno je vsakršno spodbujanje k narodni, rasni, verski ali drugi neenakopravnosti ter razpihovanje narodnega, rasnega, verskega ali drugega sovraštva in nestrpnosti. Protiustavno je vsakršno spodbujanje k nasilju in vojni. (Uradni list RS, št. 33/91-I, 42/97, 66/2000, 24/03 in 69/04)

- **Kazenski zakonik (297. člen): Javno spodbujanje sovraštva, nasilja ali nestrpnosti:**

(1) Kdor javno spodbuja ali razpihuje narodnostno, rasno, versko ali drugo sovraštvo, razdor ali nestrpnost, ali spodbuja k drugi neenakopravnosti, se kaznuje z zaporom do dveh let.

(2) Enako se kaznuje, kdor javno širi ideje o večvrednosti ene rase nad drugo ali daje kakršnokoli pomoč pri rasistični dejavnosti ali zanika, zmanjšuje pomen, odobrava, omalovažuje, smeši ali zagovarja genocid, holokavst, hudodelstvo zoper človečnost, vojno hudodelstvo, agresijo ali druga kazniva dejanja zoper človečnost.

(3) Če je dejanje iz prejšnjih odstavkov storjeno z objavo v sredstvih javnega obveščanja se kaznuje tudi urednik oziroma tisti, ki ga je nadomeščal, s kaznijo iz prvega ali drugega odstavka tega člena, razen če je šlo za prenos oddaje v živo in dejanj iz prejšnjih odstavkov ni mogel preprečiti.

Internet in rasizem

S pojavom interneta sta tako rasizem kot nacionalizem dobila nov medij, skozi katerega so se lahko širile njune ideje brez nevarnosti za posameznega rasista ali nacionalista, da bo odkrita njegova identiteta.

Po mnenju Kaloha (2004) internet z velikim veseljem izkoriščajo tudi rasisti vseh možnih organiziranih ekstremističnih skupin in njihovih frakcij, ki jim je ta elektronski medij seveda v veliko pomoč. Skritost identitete akterjev in lahkota širjenja njihovih idej sta vsekakor glavni prednosti internetnega medija. Z eno samo spletno stranjo lahko pisec spletne strani doseže na milijone uporabnikov in potencialnih pristašev (kar je veliko več v primerjavi s shodi). Javno izpostavljanje in proklamiranje rasističnih vsebin se tako vse bolj seli na medmrežje. Internetnih strani, ki propagirajo rasizem in nacionalizem je ogromno; najstarejše med njimi so na medmrežju že skoraj desetletje in izvirajo iz Amerike. Tako sta pionirja spletnih rasistov (Kaloh, 2004) Don Black in Tom Metzger prva ustvarila svoja spletna portala, zdaj med skinheadi že kultna, Stormfront in White Aryan Resistance. Stormfront naj bi bil še vedno eden glavnih portalov za dostop do najrazličnejše rasistične spletne propagande proti Židom, črncem, zavetje pa so med skrajneži našli tudi nasprotniki splava ali tisti, ki zanikajo, da je holokavst sploh kdaj bil. Ameriškim rasističnim spletnim stranem po mnenju Kaloha (2004) nič in nihče ne more do živega, saj so zakoni, ki omejujejo spletno podpihovanje rasnega sovraštva precej ohlapni in v praksi skoraj povsem neuporabni in neučinkoviti. V Ameriki je tako že čez dva tisoč tovrstnih internetnih strani, v Evropi pa jih nekaj sto.

Internet je omogočil lažje širjenje rasističnih idej, prav tako pa se je v spletnem trgovanju pojavilo veliko proizvodov, ki promovirajo rasizem in ksenofobijo. Gregor Cerar v članku Rasizem v vsako vas (Mladina, št. 35, let. 2000, str. 45) piše, da so v Franciji, ki ima sprejete

zakone, ki prepovedujejo oglaševanje in prodajanje vsega, kar bi lahko bilo vzrok rasne nestrpnosti, dve pariški organizaciji, Mednarodna liga proti rasizmu in antisemitizmu in Skupnost židovskih študentov, tožili Yahoo. Na Yahoojevih dražbenih straneh se namreč pojavlja veliko najrazličnejših trgovcev z nacističnimi znamenji. Sodnik je v tem sporu razsodil, da morata ameriški internetni gigant in njegova francoska podružnica uporabiti vse možne ukrepe, da bi preprečila francoskim uporabnikom interneta, da sodelujejo na takšnih dražbah, določil pa je tudi odškodnino, ki jo mora Yahoo plačati tožnikom. Prav takšni strogi evropski zakoni pa naj bi povzročili, da so ameriški strežniki postali pravo gojišče spornih spletnih strani, ki jih ščitijo precej manj omejevalni zakoni. Poleg Francije je pri preganjanju nacističnih spletnih strani najdejavnejša Nemčija. Vendar tudi Nemci lahko urejajo le svoje strežnike, nikakor pa ne morejo preprečiti ljudem, da bi deskali tudi po ameriških ali drugih spletnih straneh. Drugega izhoda, kot je neprestan nadzor spletnih strani, ni. Dosegli so le, da njihove največje spletne knjigarne ne prodajajo več Hitlerjevega dela Mein Kampf.

Cerar (2000) opisuje delo nemške opozicijske CDU, ki se je odločila za drugačen boj proti desničarskim skrajnežem. Sprožila je pobudo Net Against Violence po zgledu klasičnih internetnih filtrov. Njihova spletna stran tudi stalno opozarja vladne tajne službe, ponudnike interneta in razvijalce antinacističnih internetnih filtrov, pod katerimi naslovi se skrivajo spletne strani z nacistično vsebino. Podobno počno tudi nekatere židovske organizacije, na primer Center Simona Wiesenthala. Po njihovih podatkih naj bi bilo spornih okoli 2300 spletnih strani, med katerimi je okoli 500 evropskih, druge pa domujejo na ameriških tleh.Vsaj na stari celini so ponudniki interneta v zadnjih letih začeli z malo bolj represivnimi ukrepi na tem področju in nenehno vršijo kontrolo, kdo vse in s kakšnimi vsebinami gostuje na njihovih strežnikih. Tudi policija je v nekaterih evropskih državah ustanovila tako imenovane kiber enote, ki se borijo proti novodobnim virtualnim poveličevalcem arijske rase. Slovenski skini so po mnenju Kaloha (2004) za eno izmed svojih zadnjih večjih "promocij" poskrbeli leta 2001, ko so temnopoltega Inacia Bintchendeja alias Janeza Belino, najbolj znanega iz oddaje TV Poper, pretepli pred njegovim domom. Nič manj zaskrbljujoča pa je internetna propaganda, ki jo prav tako v zadnjem času širijo na svoji internetni strani Blood & Honour Slovenia.

Stanje sovražnega govora v Sloveniji

Nekdanji slovenski varuh človekovih pravic Matjaž Hanžek je v drugi polovici leta 2005 napovedal boj proti sovražnemu govoru na internetu, ki se je po njegovem mnenju na slovenskih spletnih straneh že preveč razširil, še posebno na strani *http://www.nemejebat.com*, na katero je opozoril. Sporna stran je namenjena izmenjavi mnenj. Je pravzaprav stran z različnimi forumi, na katerih slovenski uporabniki medmrežja komentirajo različne dogodke, predvsem pa manjšine in druge skupine v Sloveniji. Uporabniki, ki se jim v nasprotju z večino drugih internetnih forumov ni treba registrirati, imajo na voljo rubrike, kjer »debatirajo« o homoseksualcih, izbrisanih, Neslovencih, Romih, Židih ... Prav razdelitev na tovrstne teme je »posebnost v našem medmrežnem debatnem prostoru«, saj so sicer internetni forumi razdeljeni na rubrike politika, kultura, zabava, zdravje, računalništvo ... Že sam koncept strani torej napeljuje k sovražnemu govoru, saj se na primer debata na enem izmed forumov, ki so ga poimenovali »Tujci«, začne takole: »Kaj menite, ali je bolje, da je toliko JUŽNJAKOV (čefurjev) v Sloveniji, ali pa bi bilo bolje, da bi jih bilo manj?« Sledijo odgovori, bolj ali manj podobni diskurzu tega odgovora, pod katerega se je podpisala »čistokrvna slovenka«: »Čefurje je treba na šajtergo naložit, pa jih u gnoj kipnat ... FUJ ČEFURJI ... Ka mi gre-

jo na jetre, eni debili ej ...« Podobni odgovori in hate speech sledi tudi v drugih forumih na tej strani (Jakopič, 2005).

Toda tudi pregled mnogih drugih internetnih forumov lahko kaj kmalu razkrije razširjenost nestrpnega govora. Aktualen primer je še ena slovenska stran *http://www.lendava.net*, na kateri se je veliko sovražnega govora zbiralo na njihovih forumih, predvsem v debatah o Romih. Na spletnem forumu Lendava.net se je 11. junija 2004 zvečer v temi Invazija Romov v Lendavo pojavilo sporočilo, ki poziva k pobojem Romov, omenja Hitlerja in širi nestrpnost. Kljub temu, da je takšnih sporočil v slovenskih forumih veliko, pa je bila v zvezi s tem in še nekaj drugimi sporočili podana verjetno ena prvih kazenskih ovadb zaradi zbujanja sovraštva, razdora in nestrpnosti na internetu v Sloveniji. Glede na sporočilo uporabnika foruma Sobotainfo.com naj bi bila zaradi tega proti več kot tridesetim ljudem, ki so sodelovali na spletnem forumu, vložena kazenska ovadba.

Možnosti samoregulacije in filtriranja sovražnega govora na internetu

Kaja Jakopič v članku Boj proti sovraštvu na medmrežju ali boj z mlini na veter (Media Watch, 2005) govori tudi o možnostih samoregulacije in filtriranja sovražnega govora na internetu. V nekaterih primerih internetni servisi sami in prostovoljno preprečijo uporabnikom pošiljanje ali sprejemanje vsebin z rasističnimi in sovražnimi sporočili.

Uporabniki, predvsem starši, lahko v boju proti neustreznim vsebinam na internetu uporabijo posebne računalniške programe-filtre, ki jih nekatere organizacije (na primer Anti-Defamation League) ponujajo brezplačno. Programi onemogočajo dostop na strani, ki promovirajo sovraštvo in nasilje, pa tudi pornografske vsebine. Vendar pa so prav filtri in blokiranje dostopov do določenih strani na internetu po besedah Jakopičeve (2005) prinesli kar nekaj pomislekov, predvsem glede nezanesljivosti in težav s samo računalniško tehnologijo. Samoregulacija je pomemben del v regulaciji sovražnega govora na internetu, vendar po mnenju kritikov posameznim vladam ne odvzema odgovornosti zagotavljanja medmrežja brez sovraštva, ker bi morale nadzor po njihovem mnenju prevzeti demokratične institucije. Vsak dan uporabniki medmrežja zapišejo na različnih forumih, klepetalnicah in blogih nešteto stavkov, ki vsebujejo tudi sovražni govor, prav tako lahko vsakdo za zelo majhen denar zakupi prostor na medmrežju, če je potrebno tudi na tujih strežnikih, kjer se izogne določilom domače zakonodaje. Jakopičeva (2005) meni, da »tudi če bi za boj proti sovražnemu govoru na internetu namenili milijone evrov za posebne moderatorje in tehnično opremo, ki bi preprečevala prepovedane vsebine, ne bi mogli preprečiti posameznikov, ki bi zakupili prostor na tujih strežnikih in tam širili neprimerne vsebine. Države so v svojem boju proti sovraštvu na medmrežju izbrale različne taktike, ZDA s svobodo govora, Nemčija na drugi strani s prepovedjo sovražnega govora, v Singapurju pa so celo prvi v zgodovini aretirali dva blogerja, ki sta na svetovnem spletu širila rasistične ideje. Aretacijo so izvedli na podlagi 57 let starega člena o uporništvu, pod katerega spada tudi širjenje rasističnih idej.«

NAMIG ZA PRAKTIČNO DELO V RAZREDU: Lotite se aktivnosti iz Priročnika za razredne aktivnosti na CD-ju pod zaporedno številko **23**: **»Spletna etika«** ali aktivnosti pod številko **24**: **»Izdelava »proglas« plakata«.**

4.2.3 Otroško pornografijo in sovražni govor nujno prijavite!

www.spletno-oko.si je slovenska spletna prijavna točka, kjer lahko anonimno prijavite otroško pornografijo in sovražni govor na internetu.

Anonimno prijavo lahko poda vsak uporabnik interneta, kadar meni, da je na internetu naletel na otroško pornografijo ali sovražni govor.

Prijavitelj najprej izpolni kratek prijavni obrazec. Ključna informacija v obrazcu je naslov spletne strani, na kateri je domnevno nezakonita vsebina.

Prijavna točka Spletno oko prijavo pregleda in jo, če oceni, da gre za domnevno nezakonito vsebino, posreduje organom pregona (policija in tožilstvo).

Ti ukrepajo v skladu z veljavno slovensko zakonodajo. V primeru, da prijavljena nezakonita vsebina ni v pristojnosti slovenskih organov pregona, torej da je locirane na strežniku v drugi državi, bo Spletno oko podatke o teh vsebinah posredovalo obstoječi prijavni točki v drugi državi. Spletno oko je namreč član organizacije INHOPE (*www.inhope.org*), v okviru katere je združenih več kot 35 prijavnih točk iz 31 držav.

V dveh letih in pol delovanja (Marec 2007 - September 2009) je prijavna točka Spletno oko prejela 1645 prijav domnevno nezakonitih vsebin na internetu, kar pomeni v povprečju 55 prijav na mesec, od tega so bile 802 prijavi domnevne otroške pornografije, 605 prijav domnevnega sovražnega govora in 238 prijav drugih vsebin. Na Policijo je bilo posredovanih 380 prijav domnevne otroške pornografije in 67 primerov sovražnega govora.

5 Fenomen spletnih skupnosti

Poznamo več oblik spletnih skupnosti: forume, klepetalnice, bloge, socialna programja in mreže itd.

Spletni forumi, znani tudi kot Bulletin Board System BBS ali Disscusion Board, so virtualne skupnosti, kjer posamezniki razpravljajo o določeni temi.

Forumi so poimenovani kot mediji potega (»pull media«), saj uporabniki interneta sami poiščejo vsebine, ki jih želijo prebrati in se nanje odzvati. Elektronska pošta pa je primer medijev pritiska (»push medija«), kjer je sporočilo poslano uporabnikom interneta, četudi tega nismo zahtevali oziroma želeli.

Diskusija v forumih navadno poteka množično (čeprav lahko tudi individualno) in asinhrono, saj uporabniki foruma niso nujno istočasno prisotni. Sporočila na forumih so navadno javna, lahko pa so določene teme zasebne, kar pomeni, da imajo do njih dostop le določeni uporabniki. Preden želi uporabnik sodelovati v forumski diskusiji, se mora ponavadi registrirati. V nekaterih forumih zasledimo tudi hierarhijo odnosov, kjer je poleg vzdevka uporabnika zabeleženo, kakšno vlogo ima v forumu glede na število lastnih prispevkov, ipd.

Po podatkih Statističnega urada RS za leto 2008 v forume pošilja sporočila 21 % otrok med 10 in 15 let, ki redno uporabljajo internet, v starostni skupini med 16 in 24 let jih v forumih sodeluje 42%. Za branje forumov so številke še višje, med 10 in 15 letom starosti jih bere 36 % otrok, ki redno uporabljajo internet, med 16 in 24 letom pa dobri dve tretjini (68%).

Primer: USENET (najstarejši in največji forum)

Spletne klepetalnice so virtualne skupnosti, ki omogočajo takojšnjo – sinhrono – komuniciranje med uporabniki priključenimi v omrežje. Klepetalnice so organizirane po različnih kanalih z različnimi temami pogovorov. Uporabniki z uporabo vzdevkov in premišljenim posredovanjem osebnih podatkov lahko ohranjajo relativno anonimnost.

Uporabniki klepetalnic komunicirajo le z močjo besed, svoje razpoloženje pa izražajo tudi s smeškoti. Ker komunikacija poteka hitro, se je v klepetalnicah razvil poseben slog pisanja, ki vsebuje veliko krajšav ter angleških izpeljank.

Spletne klepetalnice so priljubljene med najmlajšimi uporabniki interneta, s starostjo pa aktivnost v klepetalnicah znatno pada.

Po podatkih Statističnega urada RS za leto 2008 spletne klepetalnice uporablja več kot tretjina (34%) otrok med 10 in 15 letom starosti, ki uporabljajo internet. V starostni skupini med 16 in 24 pa jih v klepetalnicah klepeta nekaj manj kot tretjina – 29 %.

Primer: IRC (nekomercialna in brezplačna klepetalnica)

Weblogs oz. blogi so ob prelomu tisočletja postali nov način spletnega komuniciranja. Prvi blog je bil objavljen leta 1991.

Gre za osebni spletni dnevnik, kjer v obliki enostavne spletne strani avtorji bloga objavljajo svoje misli, fotografije, videoposnetke v obratnem kronološkem zaporedju (bolj kot je zapis nedaven, višje v blogu je uvrščen). Brezplačna in uporabniku prijazna programska oprema omogoča enostavno lastno publiciranje.

V primerjavi s forumi ali spletnimi stranmi, kjer so uporabniki le-teh v dokaj enakovrednem položaju, lahko rečemo, da ima avtor bloga popoln nadzor nad celotnim spletnim komuniciranjem. Avtor bloga sicer lahko omogoči tudi komentiranje njegovih prispevkov, vendar tudi te lahko po želji ureja oz. izbriše.

Zakaj ljudje blogajo (Sporiš, 2007) ?

- Blogerstvo predstavlja demokracijo izražanja, ki lahko obide tradicionalne vratarje cenzure.
- Nekateri raziskovalci ga vidijo kot nadaljnji korak v razcvetu narcizma in ekshibicionizma, ki ga spodbujajo resničnostni šovi in drugi moderni mediji.
- Novinarjem predstavlja alternativen vir informacij, spet drugi novinarji pa svoj blog uporabijo za objavo cenzuriranih prispevkov.
- Poslovneži in učitelji blogerstvo vidijo kot obliko izmenjav znanja, t. i. (knowledge)-logs oz. k-blogs.
- Številna podjetja v blogerstvu vidijo nov način marketinga.

Po podatkih Statističnega urada za leto 2008 lasten blog (spletni dnevnik) ureja 6 % otrok med 10 in 15 let, ki redno uporabljajo internet, in 8 % mladih med 16 in 24 let. Medtem ko bere in komentira spletne dnevnike drugih vsak deseti otrok med 10 in 15 letom in vsak peti mladostnik med 16 in 24 letom. Slika celotne populacije pa kaže da 44.500 Slovencev piše lasten spletni dnevnik.

Spletne strani za mreženje (Social Networking Sofware, tudi Social Networking Service)

Družabne mreže so aktualna in zelo priljubljena oblika spletnega druženja in ustvarjanja socialnih skupnosti na internetu. Lastni profil v spletnih socialnih omrežjih je po podatkih Statističnega urada za leto 2009 ustvarjalo ali urejalo 22 % Slovencev. Deleži so še veliko večji, če pogledamo uporabo strani za mreženje med mladimi v starosti od 16–24 let, in sicer ima profil 69 %deklet in 68 % fantov.

Večina družabnih omrežij omogoča registriranim uporabnikom različne načine komuniciranja kot npr. komentiranje, klepetanje, pošiljanje elektronske pošte, sporočil, nalaganje lastnih fotografij, video ali avdio posnetkov, deljenje dokumentov, ustvarjanje lastnega bloga, foruma ipd. Uporabniki socialnega programja postanejo del virtualne skupnosti, kjer se s pomočjo omenjenih orodij komuniciranja spoznavajo, iščejo prijateljstva, zabavajo pa tudi izobražujejo in raziskujejo.

Začetki oblikovanja spletnih strani po načelu socialnega mreženja segajo v zadnje desetletje prejšnjega tisočletja. Classmates.com je bila leta 1995 ena prvih tovrstnih spletnih strani; s pomočjo spletne aplikacije se še danes bivši sošolci iz različnih držav ZDA iščejo in na ta način obujajo svoja šolska prijateljstva. Večina tovrstnih spletnih strani temelji na iskanju osebnih vezi in s tem širjenja lastne socialne mreže preko interneta po načelu zaupanja, prijateljstva oz. priporočil.

Osnovni pogoj za pridružitev v eno izmed mnogih socialnih omrežij na internetu je oblikovanje lastnega profila. Lastni profil navadno vsebuje izbran vzdevek, pogosto tudi kar pravo ime in priimek, nekaj osnovnih podatkov o sebi, sliko ter tudi povezave na »prijatelje«, ki so uporabnika povabili v skupnost (kar deluje kot neke vrste priporočilo). Večina omrežij ima možnost, s katero uporabnik nadzoruje, komu dovoljuje vpogled v njegov profil in kontakt in komu ne. Razvoj družabnega mreženja strmi k širitvi priljubljenih virtualnih skupnosti tudi na mobilne telefone.

Primeri:

***Facebook** – po vsem svetu razširjeno socialno omrežje, ki ga uporabljajo tako najstniki kot starejši, zelo razširjeno tudi v Sloveniji*

***MySpace** - splošna spletna skupnost, odprta za vse, razširjena med mladimi v Sloveniji*

***Netlog** – zelo popularna med mladimi, uporablja jo veliko slovenskih najstnikov*

***Twitter** – skupnost pravzaprav temelji na t.i. mikrobloganju, kar pomeni, da uporabnik pogosto posreduje kratka sporočila (kot SMS) o tem, kaj počne, kje se nahaja, kaj ga trenutno zanima in to deli z ostalimi člani skupnosti, ki lahko odgovarjajo in komentirajo*

***Bebo** – splošna spletna skupnost, odprta za vse, popularna predvsem v Veliki Britaniji, Irskem in Novi Zelandiji*

***LinkedIn** – spletna skupnost, katere registracija uporabnikov temelji na povabilu, mreža temelji predvsem na poklicnih referencah uporabnikov*

***Second Life** (Drugo življenje) je virtualni svet, ki je bil ustvarjen leta 2003. Izdelalo ga je podjetje Linden Resarch Inc. Za sodelovanje je potrebno najprej akt ivirati program Second Life Viewer. Uporabnik s tem postane prebivalec navideznega sveta, kjer lahko sodeluje z ostalimi prebivalci (pogovor, trgovanje ...). Čeprav Second Life včasih ime¬nujemo računalniška igra, je to nekoliko zavajajoče, saj ni točkovanja, ni zmagovalcev, ni poraženčev in ni predpisanega cilja. Je okolje, kjer prebivalci počnejo stvari, ki jih veselijo. Vsak uporabnik najprej ustvari svoje virtualno utelešenje, ki se imenuje ava¬tar in mu določi virtualno starost, spol in videz. Monetarna valuta je lindenški dolar in je konvertibilna v resničnem svetu.*

Podobno kot velja za forume in klepetalnice, se tudi pri uporabi blogov in socialnih mrež uporabniki lahko srečujejo z nevšečnostmi, kot so neželena sporočila, prenos virusov ali kraja identitete. Za vse oblike virtualnih skupnosti velja, da lahko predstavljajo kanale žaljivega komuniciranja, verbalnega nasilja, vcepljanja ekstremističnih ideologij, celo spolnega nadlegovanja ali zlorab.

Družabna omrežja imajo v veliki večini omejeno uporabo na starost nad 13 let. Mlajši otroci tako teh omrežij ne bi smeli uporabljati. Vendar pa otroci pogosto to oviro premagajo tako, da se enostavno zlažejo glede letnice rojstva in tako neovirano vstopijo v svet družabnih omrežij ter vzpostavljajo stike z ostalimi uporabniki, ki tako ne vedo, da so v stiku z otrokom.

NAMIG ZA PRAKTIČNO DELO V RAZREDU: Lotite se aktivnosti iz Priročnika za razredne aktivnosti na CD-ju pod zaporedno številko **20**: **»Slovar za klepetalnice in forume«** oz. aktivnosti pod številko **21**: **»Ustvari si svojega smeška!«**

Nasvet za net: 080 80 20

V Sloveniji imamo telefon, na katerega lahko anonimno pokličejo mladi, ki naletijo na težave pri uporabi interneta. Svetovanje poteka na brezplačni telefonski številki: 080 80 22 vsak delovni dan med 16. in 20. uro. Primarna ciljna skupina so otroci in mladostniki (stari od 10 do 18 let), saj so najbolj izpostavljeni nevarnostim zaradi neprimernih in škodljivih vsebin na internetu. Z nasveti in pomočjo na brezplačni telefonski številki bi radi zagotovili, da bi se otroci pri uporabi interneta počutili varnejše. Še posebej pa si prizadevajo, da bi otroci dobili informacije, kako ravnati, še preden bi naleteli na neprimerne, nezaželene in nevarne vsebine. Pogovor s svetovalci je anonimen in zaupen, odgovarjajo pa tudi na vprašanja po elektronski pošti info@nasvetzanet.si.
Več na spletni strani *www.nasvetzanet.si*.

6 Priporočila za varno rabo interneta v šoli

6.1 Nasveti za varno in uspešno uporabo interneta v šoli[13]

- Ne pozabite, da v vsaki generaciji obstajajo **druge možnosti in tehnike medsebojne komunikacije.** Potrudite se in uporabljajte trenutno najnovejšo in najpopularnejšo tudi pri pouku.
- **Pridobite osnovno znanje uporabe interneta,** saj boste tako lažje ocenili potencialne nevarnosti.
- **V otrokov šolski vsakdan poskušajte dodati internet.**
- Otroke spodbujajte k **upoštevanju t. i. spletne etike oz »Netetiquette«**, ki je zbirka neformalnih navodil oz. bonton, kako se naj bi obnašali na internetu.
- Skupaj z ostalimi učitelji, starši in otroci se **dogovorite o pravilih uporabe interneta.**
- **Pri postavljanju pravil** upoštevajte in spodbujajte vse udeležence naj podajo svoja mnenja in predloge. Pri postavljanju pravil pazite na primernost glede na različne starostne skupine.
- **Otrokom predstavite nevarnosti** in jih opozorite, naj bodo pozorni, kdaj in komu *posredujejo svoje osebne podatke*.
- Pogovarjajte se z otroki o **problemih resničnosti in verodostojnosti vsebin na internetu** in jim predstavite, kako lahko preverimo posamezen vir.
- V primeru, da **uporabljate sisteme za filtriranje vsebin**, to jasno in nazorno predstavite soudeležencem.
- Upoštevajte ukrepe, kako **lahko tehnično zaščitimo svoj računalnik in morebitno šolsko mrežo**. Predstavite tudi svojim učencem, kako lahko zaščitijo svoj računalnik.

[13] Povzeto po *http://www.saferinternet.at/tipps/lehrer.php.*

6.2 Varnost šolskih omrežij

ARNES o varnosti šolskih omrežij *(http://www.arnes.si/dokumenti/filtri/)* piše naslednje: »Popolnoma odprti ali slabo zavarovani računalniški šolski sistemi so lahka tarča napadalcev, ki take sisteme pogosto izkoristijo kot odskočne deske pri vdiranju v druge sisteme. Računalniški sistemi na šolah pri tem niso izjema. Za napadalce so najbolj zanimivi šolski strežniki. To so običajno računalniki z UNIX/Linux in Windows NT operacijskimi sistemi, ki so 24 ur dnevno dosegljivi iz vsega interneta. Izkušnje kažejo, da so najbolj ranljivi in zato tudi pogosto zlorabljeni prav slabo vzdrževani strežniki, za katere skrbijo učenci.

Lokalna omrežja lahko učinkovito zaščitimo s t. i. *požarnim zidom* (angl. *firewall*). Požarni zid nadzoruje ves internetni promet, ki je naslovljen na določen del lokalnega omrežja, kot tudi promet, ki to omrežje zapušča. Požarni zid je običajno poseben računalnik z več omrežnimi priključki in posebno programsko opremo. Tak sistem zahteva stalen nadzor in vzdrževanje, kar je poleg stroškov nakupa in namestitve za marsikatero šolo velika obremenitev.

Okrnjeno (vendar v osnovi podobno) funkcijo kot požarni zid lahko opravlja tudi usmerjevalnik prometa, s katerim se šola povezuje v omrežje ARNES in internet. Usmerjevalnik prometa lahko nadzoruje in filtrira internetni promet na podlagi informacij, ki so kot dopolnilo podatkov shranjene v paketih, ki jih usmerjevalnik prenaša za šolsko omrežje. Usmerjevalnik lahko filtrira na podlagi naslova, od koder promet prihaja, naslova, kamor je promet namenjen, tipa prometa (protokola, internetnega servisa oz. storitve) in še nekaterih drugih podatkov, ne more pa nadzorovati vsebine prometa, količine prenešenih podatkov, trajanja, imena uporabnika ipd. Z usmerjevalnikom, ki ima nameščeno le osnovno programsko opremo, tudi ni mogoče zgraditi virtualnih privatnih omrežij (angl. *VPN*), omogočiti identifikacijo uporabnikov, ki dostopajo do šolskih sistemov, kriptirati (šifrirati) promet itd.

Usmerjevalnik prometa je že del šolskega omrežja in je pod nadzorom in upravljanjem tehničnega osebja ARNES. Zato je to kljub okrnjeni funkcionalnosti v primerjavi z običajnim požarnim zidom, za šolo pogosto cenovno najbolj ugodna in dostopna rešitev.

Nekje vmes med požarnim zidom in filtri na usmerjevalniku so računalniki z več vmesniki za priklop lokalnega omrežja (npr. vmesniki tipa *ethernet*) in z Linux oz. sorodnimi operacijskimi sistemi, za katere je na voljo več programske opreme za nadzor in filtriranje internetnega prometa. Namestitev, konfiguriranje in vzdrževanje takega računalnika in programske opreme zahteva sodelovanje ustrezno izobraženega strokovnjaka.

Do varnostnih incidentov lahko pride tudi znotraj lokalnega omrežja. Ker v tem primeru požarni zid ali filter na usmerjevalniku omrežja ne varuje, moramo poskrbeti za varnost neposredno na računalnikih samih. Požarni zid ali njegov nadomestek namreč filtrira zgolj promet, ki gre "skoznjo" - iz enega segmenta lokalnega omrežja v internet ali v drug segment - na promet znotraj nekega enotnega segmenta lokalnega omrežja pa nima vpliva. Najpomembnejša je zaščita strežnikov, kjer se hranijo pomembni podatki, in računalnikov v administrativnem in vodstvenem delu šolskega omrežja. Na UNIX/Linux in tudi Windows sistemih je na voljo dovolj mehanizmov za učinkovito zaščito pred nepooblaščenim dostopom, le uporabiti jih je treba.«

6.3 Kako oblikovati šolsko spletno stran?

Dolžnost šole je zagotoviti varnost otrok tako v fizičnem kakor tudi virtualnem svetu. Šola mora zagotoviti, da zaradi uporabe šolske spletne strani ne obstaja možnost identifikacije posameznega otroka ali možnost vzpostavitve stika z njim. Šole morajo biti še posebej pozorne na naslednje možne skrite pasti:

- **Fotografije in izdelki učencev**

Pri objavi fotografij učencev na šolski spletni strani je potrebna posebna previdnost. Primernejša je objava skupinskih fotografij, kakor pa objava individualnih, poleg tega pa nikoli ne navajajte imen otrok pod fotografijami. V primeru, da spletna stran prikazuje izdelke učencev priporočamo, da objavite samo ime učenca, ne pa tudi njegovega priimka.

V primeru prikazovanja digitalnih (video) izdelkov je potrebna pazljivost, da otroci v videu niso imenovani z njihovimi pravimi imeni, poleg tega pa tudi ne priporočamo objave podatkov otrok, ki so kakorkoli prispevali k izdelavi izdelka.

Preden objavite slike otrok in njihove izdelke na šolski spletni strani, je potrebno pisno dovoljenje njihovih staršev.

- **Elektronski naslovi**

Nikoli ne objavite osebnih elektronskih naslovov učencev in zaposlenih na šolski spletni strani. Premislite o uporabi anonimnih ali skupinskih elektronskih naslovov npr. razred@guest.arnes.si, ki naj bo kot del šolskega sistema elektronske pošte primerno filtriran.

- **Vsebina in avtorske pravice**

Pred objavo na spletni strani priporočamo pregled besedil učencev. Prepričajte se, da besedilo ne vsebuje celotnega imena učenca ali razkriva kakršne koli osebne informacije, kot je npr. članstvo v obšolskih dejavnostih ali kakšne druge podrobnosti o učencih, na podlagi katerih bi potencialno lahko bili identificirani. Vedno preglejte, da besedila učencev ne vsebujejo izjav, ki bi lahko bile opravljive.

Zagotovite, da šola z objavo kakršnekoli vsebine na spletni strani ne krši avtorskih pravic.

- **Povezave na zunanje spletne strani**

Preden katero koli zunanjo spletno povezavo vključite na šolsko spletno stran, morate preveriti, da je vsebina te povezave primerna tako za šolo kot tudi za ciljno publiko. Vedite, da se lahko vsebina neke spletne strani v zelo kratkem času lahko bistveno spremeni, zato redno preverjajte, ali so spletne strani, na katere imate povezave, še vedno aktivne ter ali njihova vsebina ostaja primerna.

- **Spletni pripomočki**

Bodite previdni, kadar na šolsko spletno stran vključite orodja, kot so spletni iskalniki in spletni števci. Če uporabljate »komercialne« iskalnike, preverite, ali jih lahko oblikujete tako, da iščejo le po vaši spletni strani, da preprečite prikaz kakršne koli neprimerne vsebine. Nekateri iskalniki in števci vsebujejo povezave na oglaševalske strani – premislite ali so takšne povezave primerne za vašo spletno stran oziroma pretehtajte druge možne alternative.

• **Uporaba pripomočkov za povratne informacije in varstvo podatkov**

Bodite previdni, kadar uporabljate pripomočke za povratne informacije, kot je npr. knjiga obiskovalcev. Čeprav je lahko zabavno ter koristno za šolo, da obiskovalci objavljajo svoje komentarje, dobro premislite, do kakšne stopnje ste pripravljeni zbirati in razkriti podatke na vaši strani. Knjige obiskovalcev navadno sprašujejo obiskovalce po njihovem imenu, elektronskem naslovu, od kod stran uporabljajo in kakšen komentar imajo – mnogi mladi neprevidno posredujejo te informacije, čeprav s tem razkrivajo mnoge osebne informacije (Becta, 2007c).

Premislite tudi o varstvu podatkov, ki jih zbirate na svoji spletni strani (področje regulira **Zakon o varstvu osebnih podatkov).**

Pravilnik o zbiranju in varstvu osebnih podatkov na področju osnovnošolskega izobraževanja (UL, št. 80, datum: 23. 7. 2004, stran 9735), v 6. členu opredeljuje, da »*za osebne podatke, za katere se starši učencev s pisno privolitvijo strinjajo, da so javno dostopni, ker po naravi, vsebini ali namenu ne posegajo v zasebnost učencev (npr. razstave izdelkov učencev, skupinski posnetki učencev na fotografijah, videoposnetki, zvočni ali filmski posnetki javnih nastopov učencev na prireditvah, ipd.), šola pridobi pisno soglasje staršev za celo šolsko leto. Iz soglasja mora biti razvidno, za kakšne fotografije, snemanja in intervjuje gre, na kakšen način oziroma za kakšne namene se bodo le-ti uporabljali in koliko časa se bodo shranjevali.*«

Sestavni del dobre šolske spletne strani je tudi »izjava o zasebnosti«. Kot primer navajamo izjavo o zasebnosti, ki jo je na svoji spletni strani objavila OŠ Franceta Prešerna Kranj. »Podatki in slike na spletni strani so izključna last šole, avtorjev in upodobljenih ali imenovanih. Arhiv se izdeluje za potrebe dokumentiranja življenja in dela na osnovni šoli. Slike in druga gradiva se lahko pregleduje, ni pa jih dovoljeno obdelovati, posredovati, kopirati ali objavljati brez soglasja upodobljenih ali imenovanih.«

Dobro je tudi, da šola oblikuje **lastno politiko šolske spletne strani** (dober primer podajamo spodaj), ki vključuje tudi zgornja navodila. Poleg tega je priporočljivo, da šola imenuje osebo, ki bo odgovorna za vso vsebino, ki se pojavi na šolski spletni strani. Ta oseba naj bi tudi skrbela za politiko spletne strani. Šolska spletna stran naj bo tudi mehanizem promocije varne rabe interneta z nasveti, kako varno uporabljati internet, za učence in njihove starše. Pomembno je tudi, da vključite starše v šolski program varne rabe interneta, s čimer proces učenja varne rabe interneta razširite tudi v domače okolje otrok.

Primer politike šolske spletne strani[14]

Dolžnost šole je, da otrok, ki je v njeni oskrbi, ostane varen, kar pomeni tudi, da morajo vsi otroci ostati anonimni, torej da jih obiskovalci šolske spletne strani ne morejo prepoznati. Podobno je tudi z dolžnostjo šole do zaposlenih. Spodnja navodila veljajo za vse osebe, ki sodelujejo pri pripravi materialov za šolsko spletno stran:

- Fotografije objavljene na spletni strani so lahko **samo fotografije razredov**, na katerih so otroci oblečeni, fotografirani od daleč oziroma kako drugače težko razpoznavni. Individualne fotografije otrok ne bodo objavljene.

[14] Povzeto po: *http://www.kelvindaleprimary.org.uk/myweb2/main_frames.htm*

- **Imena oziroma katere koli druge identifikacijske informacije ne smejo biti priložene k fotografijam.**
- Vsebina fotografij objavljenih na šolski spletni strani naj bo primerna, kar pomeni, da **osebe na fotografijah ohranjajo svoje dostojanstvo.**
- Izdelki učencev prikazani na spletni strani so lahko **označeni samo z razredom** – npr. »slika – učenec 2. A razreda«, in naj ne vsebujejo informacij, kot je npr. priimek, s čimer bi lahko nekdo prepoznal učenca in/ali njegove družinske člane. **Lahko so uporabljeni vzdevki, ki direktno ne identificirajo otroka.**
- ***Kakršen koli incident*** v zvezi z vsebino šolske spletne strani glede na smernice politike spletne strani naj učenci, učitelji in straši **prijavijo ravnatelju**. Prijavitelj lahko izbere tudi anonimno prijavo, vendar pa mora podati argumente, zakaj se mu neka stvar v zvezi s spletno stranjo zdi sporna.
- Predstavitvene strani učiteljev ne smejo vsebovati: **njihovega življenjepisa, osebnih kontaktov in sporočil; informacij v zvezi z zaposlitvijo; osebnega mnenja o šolski politiki in povezano sporno tematiko.**
- **Šolska stran naj ne vsebuje osebnih kontaktov članov šolskega odbora.**
- Predstavitvene strani učencev in razredne strani se ponavadi ustvarjajo v učnem procesu, vendar pa jih je potrebno pred objavo natančno pregledati, da **ne bi vsebovale kakršnih koli osebnih informacij o učencih, vključno z elektronskimi naslovi.**
- **Predstavitvene strani učencev in razredov mora pred objavo pregledati učitelj.**
- Predstavitvene strani učencev in razredov **ne smejo vsebovati povezav na osebne predstavitvene strani**, ki vsebujejo kakršne koli kontaktne informacije ali vsebine, ki so v neskladju s temi smernicami.
- **Dogodki in ekskurzije. Objavljene naj bodo le splošne informacije.** Na voljo naj bo spletni naslov za vprašanja staršev, odgovore nanje pa naj v pisni obliki odnesejo domov otroci.

6.4 Uporaba spletnih klepetalnic pri pouku

Spletno klepetanje ima za otroke in mladostnike prav poseben čar in mnoge nepopisno privlači. Vendar pa veliko mladih uporabnikov ni dovolj dobro seznanjenih z nevarnostmi, ki se ob klepetanju lahko pojavljajo, in se tako hitro znajdejo v neprijetnih situacijah. V želji, da bi se izognili neprijetnim izkušnjam, se moramo tudi pri pouku soočiti s takimi temami in otrokom ustrezno predstaviti nevarnosti.

Poleg preventivnega dela na področju spletnih klepetalnic in ozaveščanja mladih o potencialnih nevarnostih lahko klepetalnico uporabno izkoristimo tudi v kontekstu šole. Osnovni, teoretični predstavitvi spletnih klepetalnic bi moral slediti praktični del, v katerem bi imel vsak učenec možnost, da se seznani s tem, kako klepet dejansko deluje. V okviru tega lahko priredimo spletno klepetanje z učenci partnerske šole (doma ali v tujini), debate z znanstveniki, politiki ali pa tudi virtualni pouk oz. razredna srečanja.

Za uvod v tematiko uporabe spletnih klepetalnic pri pouku lahko začnemo z zbiranjem izkušenj, ki jih učenci že imajo s spletnim klepetanjem. Ob tem se že lahko razvije pogovor o pozitivnih in negativnih vidikih spletnega klepetanja, ki jih do konca tematike še poglobljeno obravnavamo. Prav tako pa ob tem, ko učenci poročajo o svojih izkušnjah, učitelj pridobi podatke, katere tematike učence zanimajo in kakšni so motivi za obiskovanje spletnih klepetalnic.

Sledi teoretična obravnava tematike, vendar pa ob tem, kot že omenjeno, ne smemo pozabiti tudi na praktični del, kjer smo omejeni z možnostmi dostopa do računalniške učilnice. Smiselno je, da se učenec na začetku spozna s spletnim klepetanjem v klepetalnici, za katero smo se prej prepričali, da zadostuje pogojem varnega klepetanja. Na koncu je primerno učencem predstaviti še nadalje portale, ki ponujajo varne spletne klepetalnice (Ostrež, 2006b:5).

Na kaj morajo biti učitelji pozorni – konkretni nasveti za pouk:

- Otrokom bi morale biti dostopne le izobraževalne spletne klepetalnice. Uporaba klepetalnic v izobraževalnem kontekstu mora biti vseskozi nadzorovana, učence pa je potrebno poučiti o pomembnosti varnosti pri uporabi spletnih klepetalnic.
- Učitelji se morajo predhodno seznaniti z vsako klepetalnico, ki jo nameravajo uporabiti v učnem procesu, in sicer morajo preveriti, ali klepetalnica resnično ponuja izobraževalne izkušnje, morajo pa se seznaniti tudi z njenim delovanjem.
- Učenci lahko uporabljajo le moderirane klepetalnice. Moderator preverja, kaj se udeleženci klepetalnice pogovarjajo in zagotavlja, da udeleženci spoštujejo pravila uporabe klepetalnice (prepoved prostaškega jezika ali kakršnega koli drugega neprimernega vedenja). V primeru, da tisti uporabniki klepetalnice, ki kršijo njena pravila, niso vrženi iz klepetalnice ali javno opozorjeni, moderator ni on-line ali pa je neučinkovit.
- Učitelj mora preveriti, na kakšen način je klepetalnica moderirana, ali jo moderira učitelj ali kakšna druga primerna odrasla oseba. Nekatere klepetalnice uporabljajo programsko opremo kot dodatek k človeškemu moderiranju, s čimer prikrivajo prihajajoče besedilo. Če je za moderiranje klepetalnice uporabljena programska oprema, preglejte katere so besede, ki se jih prekriva (npr. »kletvice«, »seks«, »skrivnost« itd).
- Dobra klepetalnica mora imeti jasno določene pogoje delovanja ter izjavo o zasebnosti, katere je potrebno tudi uveljavljati, poleg tega pa mora uporabnike tudi opozarjati na nevarnosti in podajati pomembne varnostne nasvete.
- Dobra izobraževalna klepetalnica mora imeti objavljen seznam tem, o katerih se na njej razpravlja. Poleg tega pa mora tudi zagotoviti, da gostitelj nadzoruje klepet ter ga vodi na takšen način, kakor ga vodi učitelj v razredu. V nekaterih primerih gostitelj deluje na takšen način kot moderator.
- Nekatere popularne klepetalnice imajo povezave na oglase ter druge spletne strani, zato je nadvse pomembno, da učitelj preveri pomen uporabe takšne klepetalnice za učni proces. Nekatere klepetalnice imajo tudi arhiv tem, na podlagi česar lahko ocenite primernost uporabe klepetalnice v učnem procesu.

- Da je uporaba klepetalnic v učnem procesu čimbolj učinkovita, morajo imeti učenci v klepetalnicah dejansko priložnost izraziti svoja lastna mnenja, da se učijo eden od drugega ter da načenjajo nove teme.
- Ugotovite, ali lahko vsakdo sodeluje v klepetalnici. Ali obstaja razločevanje glede na starostno skupino? Na kakšen način klepetalnica potrjuje gesla in uporabnike?
- Učence morate poučiti o dogovorjenih načinih pisanja v klepetalnicah. Otroci naj nikoli ne podajajo svojih pravih imen ali kakršnih koli drugih osebnih informacij. Poleg tega pa se morajo zavedati, da njihove izjave predstavljajo tudi šolo.
- Otroke je potrebno poučiti, da se ne smejo nikoli sestati z nekom, ki so ga spoznali v spletni klepetalnici.
- Zgornje smernice za uporabo klepetalnic naj učitelji predstavijo tudi staršem, da jih bodo le-ti uporabljali tudi doma (Becta, 2007d).

6.5 Uporaba blogov pri pouku

Ustvarjanje različnih, za učenca zanimivih situacij je za učitelja v današnjem svetu izredna težka naloga. Številne informacije, različni mediji in tehnologije so mu pri tem ustvarjanju v pomoč. Tako je potrebno v pouk vpeljati sodobne oblike dela, ki zahtevajo tudi učiteljevo znanje uporabe IKT. Z uporabo spletnega dnevnika (bloga) lahko postane pouk aktiven in medpredmetno povezan. Pri tem pa je seveda potrebno upoštevati tudi vidike varnosti in varovanja zasebnosti sodelujočih učencev oz. dijakov.

Strokovna gimnazija Tehniškega šolskega centra v Kranju je za potrebe obveznih izbirnih vsebin Državljanska kultura in Vzgoja za družino, mir in nenasilje le-te izvajala na takšen način, da je bilo pridobivanje znanj podprto z informacijsko-komunikacijsko tehnologijo. Dijaki so tako kot pomoč pri izvedbi petdnevne ekskurzije pripravili poseben spletni portal, za sprotno poročanje pa so uporabili blog, ki je zaradi svoje interaktivnosti in dinamičnosti omogočal ne le rednega poročanja, temveč tudi komunikacijo z dijaki in učitelji, ki so bili na šoli. Šola je uporabila enega izmed brezplačnih javnih blog servisov, ki omogoča enostavno urejanje objav in komentarjev, objavljanje fotografij in prilagoditev oblike z izbiro ustrezne predloge. Link do bloga: *http://magistrala2007.tsckr.si* (Jemec, 2007).

V prvi učeči skupnosti na Univerzi v Ljubljani »Sportfolio« je bilo do aprila 2007 po šestih mesecih delovanja vzpostavljenih 219 blogov. Od tega je registriranih 50 blogov učiteljev, 165 blogov študentov, 3 blogi učiteljev oz. asistentov Fakultete za šport Ljubljana in blog podpore uporabnikom. Od vseh registriranih blogov jih je aktivnih 169 (36 blogov učiteljev – mentorjev, 130 blogov študentov in 3 blogi učiteljev oz. asistentov). 61 študentov bloge uporablja pretežno za objavljanje seminarskih nalog in IKT gradiv; 69 študentov pa na njih piše tudi dnevnik praktičnega pedagoškega usposabljanja in objavlja učne priprave in različne predloge za prakso. 28 učiteljev – mentorjev je na svojih blogih objavilo urnike in druge informacije povezane s praktičnim pedagoškim usposabljanjem študentov; 8 učiteljev pa na njih redno objavlja različne informacije.

Dostopno na: *http://projekt.sportfolio.si/category/blogi/*

6.5.1 Nasveti za varno bloganje

Vloga učiteljev pri seznanjanju mladih z načini etničnega in varnega bloganja je zelo pomembna. V učenje medijske pismenosti je nujno potrebno vključiti tudi osnove bloganja. Učiteljem priporočamo, da se z učenci pogovorijo o nekaterih spornih temah, kakršne so plagiatorstvo, verodostojnost informacij objavljenih na spletu, avtorskih pravicah ter objavi zasebnih ter osebnih informacij.

Priporočamo vam naslednje:

- Otroke učite, da naj svoj **blog vedno zaščitijo s skrivnim geslom**, ki ga poznajo le otroci in njihovi starši.
- Otroke učite, da naj v blog nikoli **ne vpisujejo svojih osebnih podatkov** (imena, naslova, e-mail naslova, telefonske številke itd.), prav tako naj ne navajajo informacij o šoli, ki jo obiskujejo, oz. o mestih, kjer se družijo s prijatelji. Tovrstne informacije namreč iščejo ljudje s slabimi nameni, predvsem pedofili in ostali potencialni nadlegovalci.
- Otroke naučite, naj ne objavljajo **osebnih informacij drugih ljudi (imena, naslova, telefonske številke, e-mail naslova ipd.).**
- Otroke naučite, da naj svoj tekst pred objavo *še enkrat preberejo* ter popravijo podatke, ki bi lahko razkrili njihovo identiteto.
- Blog **ni primerno mesto za objavo osebnih fotografij** prav tako pa tudi ne fotografij prijateljev ali neznancev.
- Otroke naučite, **da ne smejo nikoli puščati spletne strani**, na katero vpisujejo svoje spletne dnevnike, **odprte oz. nezaščitene.** Nekdo drug lahko tako »vdre« v takšen blog in doda žaljiv tekst oz. širi druge lažne informacije.
- Otroke naučite, **da ne smejo širiti govoric oz. obrekovati** svojih sošolcev in prijateljev.
- Otroci naj pri pisanju spletnega **dnevnika upoštevajo pravila bontona** ter naj bodo strpni in prijazni do drugih uporabnikov (iSAFE, 2006).

6.5.2 Problematična področja bloganja

Mladi uporabniki interneta lahko med bloganjem naletijo tudi na potencialno škodljive vsebine. Na svetovnem spletu namreč obstaja cela vrsta blogov, ki pozitivno pišejo o alkoholizmu ter drogah, spodbujajo nezdrave diete, nezdrav način življenja, spodbujajo vse vrste nestrpnosti, samomorilnost ipd.

S pomočjo blogov je mogoče navezati stike z drugimi pisci spletnih dnevnikov, prav tako pa je mogoče izmenjati številne osebne informacije, npr. naslove in fotografije. Osebni dnevnik je tako postavljen na ogled milijonom neznancem, ki se skrivajo za računalniki. Potencialni spletni pedofil oz. nadlegovalec lahko v določenem časovnem obdobju s pomočjo bloga zbere toliko informacij o avtorju, da lahko na podlagi le - teh izdela osebni profil avtorja. Ime šole, imena prijateljev, učiteljev, fizični naslovi, imena ulic, mest, ipd. spadajo med informacije, ki jih pedofili lahko zlorabijo. Najstniki na blogih objavljajo številne podatke, za večino katerih

mislijo, da so le nepomembne podrobnosti. Toda ne zavedajo se dejstva, da z njimi v resnici le rišejo zemljevid do svojega doma. Najstniki živijo v utvari lažne varnosti, ki naj bi jo zagotavljala domnevna anonimnost na internetu.

Domnevna anonimnost povečuje tudi možnosti drugih zlorab, npr. spletnega nadlegovanja in obrekovanja. Najstniški pisci spletnih dnevnikov se v virtualnem svetu obnašajo bolj svobodno in pogosto ne izbirajo besed, ki jih uporabljajo za pisanje. Tako se tudi ne zavedajo posledic uporabe žaljivih besed in obrekovanja, s katerimi lahko prizadenejo osebo, ki jo blatijo v svojem spletnem dnevniku.

Pri bloganju lahko pride tudi do kraje identitete. Če svoje geslo za dostop do bloga zaupamo »prijateljem«, lahko pravzaprav nekdo v našem imenu piše in objavlja stvari, ki jih sami ne bi napisali. Stvar je lahko samo neprijetna in neslana potegavščina, lahko pa postane resen problem, če nekdo v našem imenu napiše kaj nelegalnega. Policiji bo potem namreč težko dopovedati, da to nismo bili mi.

Spletno nadlegovanje preko blogov je prav tako pogost pojav in lahko čustveno prizadene potencialno žrtev. Znani so primeri najstnikov, ki so zaradi spletnega nadlegovanja naredili samomor. Najstniški blogerji se v večini primerov ne zavedajo posledic, ki jih njihovo pisanje lahko povzroči. Internet je pač globalen medij, do katerega ima dostop milijoni uporabnikov, dnevniški zapis pa prav lahko prebere vsakdo, tudi nekdo, kateremu določene besede niso namenjene.

Objavljanje fotografij v blogih lahko postane sporno, še posebej, če se objavijo fotografije ljudi, ki v to objavo niso privolili. Oseba, ki se ne strinja z objavo svoje fotografije, lahko pisca blogov celo toži. Zato previdnost pri objavi fotografij res ni odveč. Seveda pa blogi sprožajo številna pravna vprašanja, predvsem glede cut-and-paste prenašanje informacij iz drugih virov in tudi pravne odgovornosti za zapisane vsebine. Avtorsko pravo je treba upoštevati tudi v blogu. Kar je nekdo zapisal v spletnem dnevniku, je njegova intelektualna lastnina!

Spletni dnevniki so postali vse bolj priljubljeni tudi pri hekerjih, ki prek njih distribuirajo zlonamerno kodo in programsko opremo za sledenje dogajanju na tipkovnici. Hekerji uporabljajo spletne dnevnike, ker jim nudijo brezplačno postavljanje lastnih spletnih strani in veliko prostora brez preverjanja identitete uporabnika. Večina ponudnikov spletnih dnevnikov prav tako nima urejene protivirusne zaščite za objavljene datoteke.

Pomembno se je zavedati vseh potencialnih nevarnosti, ki se pojavljajo ob pisanju blogov. Če pisci spletnih dnevnikov ne želijo, da bi vsakdo vedel vse o njihovem zasebnem življenju, morajo poskrbeti za to, da spletni blogi ostanejo zasebni. Internet je namreč zelo popularen in vedno se bodo na internetu našli ljudje, ki bodo želeli drugim škodovati.

Če pisci blogov niso previdni, se lahko znajdejo v zelo neprijetni in po možnosti tudi nevarni situaciji. Otroke je potrebno naučiti, da vsaka zadeva, ko jo enkrat shranijo na računalnik in objavijo na internetu, pa naj bo to tekst ali slika, tam ostane za vedno in se je ne da zbrisati. Torej naj najstniki ne objavljajo stvari, za katere jim bo mogoče kasneje žal, da so jih postavili na ogled javnosti, saj poti nazaj ni (iSAFE v: *http://www.isafe.org/imgs/pdf/education/Blogging.pdf)*.

NAMIG ZA PRAKTIČNO DELO V RAZREDU: Lotite se aktivnosti iz Priročnika za razredne aktivnosti na CD-ju pod zaporedno številko **18:«Ustvarite razredni blog«**.

6.6 Nasveti za varno mreženje prek spleta

- **Razložite učencem, kateri podatki so osebni.** Podatkov o njih samih, družinskih članih ter prijateljih, kot so npr. polno ime, telefonska številka, domači hišni naslov oz ime šole, naj ne objavljajo javno ter naj jih na spletu ohranijo zasebne.
- **Učencem pokažite, kako naj v spletnih mrežah uporabljajo nastavitve zasebnosti,** s čimer omejijo, kdo vse lahko vidi njihov profil v družabnem omrežju.
- **Učencem svetujte, naj v družabnem omrežju objavljajo le informacije, slike, komentarje, videoposnetke, za katere jim je vseeno, če jih vidijo tudi drugi.** Slike z norih zabav, žaljivi in obrekljivi komentarji ne sodijo na splet, saj so tam na voljo vsem uporabnikom interneta in ko se enkrat objavijo, tam ostanejo za vedno.
- **Učence naučite, da bodo spoštovali tudi zasebnost drugih.** Še posebej naj bodo previdni pri objavljanju osebnih podatkov drugih oseb brez njihovega dovoljenja, vključno s fotografijami. Zavedajo naj se, da je takšno početje lahko tudi kaznivo dejanje.
- **Spregovorite z učenci o spletnem nadlegovanju v družabnih mrežah.** Razložite jim, da imajo lahko besede, ki jih tipkajo, in slike, ki jih objavljajo, posledice v resničnem življenju: prizadenejo tistega, ki jih prejme, in naredijo grd vtis o tistem, ki jih pošilja. Učenci naj zaupajo vam ali staršem, če se zaradi nečesa na spletu počutijo neprijetno. Neprimerne vsebine, kontakte oz. nadlegovanje jim lahko pomagate prijaviti na sami spletni strani družabne mreže, kjer obstajajo mehanizmi za prijavo zlorab.
- **Gesla so skrivnost, zato naj jih ohranijo zase in pogosto menjavajo.** Mladi gesla za dostop do spletnih omrežij, kakor tudi elektronske pošte in programov za takojšnje sporočanje, npr MSN, pogosto zaupajo svojim prijateljem/sošolcem in niti ne pomislijo, da se tudi najboljša prijateljstva lahko razdrejo, kar lahko privede do zlorabe gesel ter medsebojnega obračunavanja tudi tako, da nekdo v njihovem imenu piše neprimerne komentarje ali objavlja neprimerne fotografije oz. videoposnetke.

6.7 Koristne povezave za učitelje

1. Brezplačne izobraževalne delavnice in pomoč pri vzpostavitvi šolskega spletnega mesta:

   http://www.odprtaokna.si/default.aspx

2. Interaktivni scenariji, kvizi, lekcije, nasveti o varni rabi interneta:

   http://www.varenvspletu.si/html/etusivu.htm

3. Vrsta Googlovih orodij za delo v razredu:

   http://www.google.com/educators/index.html

4. Brezplačno spletno učenje za izobraževanje ob delu in na daljavo:

   www.piflar.com

5. Obsežen vir informacij o internetni varnosti in varnosti šolskih omrežij:

   http://www.arnes.si/

6. Spletna stran evropske mreže za varno rabo interneta Insafe z dostopom do različnih informativnih in izobraževalnih gradiv za mlade in učitelje:

   http://www.saferinternet.org/

7. Spletna stran evropskega šolskega omrežja EUN:

   http://www.eun.org/

8. Vodič po tehnologiji za učitelje, načrti lekcij o varni rabi interneta in druge koristne informacije s področja uporabe novih tehnologij pri mladih:

   http://teachtoday.eu/

9. Slovensko izobraževalno omrežje:

   www.sio.si

7 Slovar pojmov

Slovarček najpogostejših IKT izrazov

- A -

ADSL (»Asymmetric Digital Subscriber Line – asimetrična digitalna naročniška linija«). *Glej pod DSL*.

- B -

Bluetooth (»modri zob«) je radijska tehnologija majhnih moči. Omogoča brezžično komunikacijo med računalniki, mobilnimi telefoni, prenosnimi računalniki, dlančniki, tiskalniki, digitalnimi fotoaparati in igralnimi konzolami. Uporablja se za izmenjavo podatkov, kupovanje kart, vpogled na stanje TRR ali brezžično lokalno omrežje (LAN).

Brezžična povezava omogoča povezavo s spletom brez žice (npr. infrardeča, bluetooth, mikrovalovna, satelitska, laserska povezava). Najpogostejša je povezava z internetom preko mobilnega telefona.

Blog: *Glej pod spletni dnevnik*

Brskalnik (angl. browser) je računalniški program, ki omogoča brskanje po spletu in prikazovanje HTML dokumentov in večpredstavnih vsebin (slike, video, glasba). najbolj pogosta sta Internet Explorer in Firefox.

- C -

Cookies (piškotki): so informacije, ki se ob obisku posamezne spletne strani shranijo na naš računalnik in so ob ponovnem obisku iste strani uporabljene za prepoznavanje, sledenje in zbiranje specifičnih informacij o internetnih uporabnikih, kot so na primer preference do določenih strani/vsebin ali nakupovalne navade na spletu.

Creative Commons: ustvarjalcem ponuja vnaprej pripravljene licence, s katerimi jasno določijo dovoljene in nedovoljene uporabe svojih del, tako da lahko dela svobodneje krožijo med uporabniki. Označevanje avtorskih del z licenco Creative Commons (CC) ne pomeni, da se avtor odreka avtorskim pravicam.

- D -

Dlančnik (angl. Handheld computer ali PDA-Personal Digital Assistant ali palmtop computer) je majhen računalnik. Večina jih nima tipkovnice, za vnos podatkov poskrbijo na dotik občutljiv zaslon, virtualna tipkovnica na zaslonu ali razpoznava črk, ki jih ročno napišemo na zaslon. Sicer ni tako zmogljiv kot PC istega cenovnega razreda, omogoča pa uporabo urejevalnika besedil, elektronske pošte, koledarja, imenik, opomnika ...

DSL (Digital Subscriber Line - digitalna naročniška linija) oz. xDSL tehnologija, ki v domove in podjetja prinaša informacije velike pasovne širine preko običajne bakrene telefonske parice. DSL omogoča veliko hitrejši prenos podatkov kot navadna modemska povezava z internetom. Tehnologija DSL zajema več različic, kot so ADSL, HDSL, IDSL, RADSL, SDSL, VDSL in DSL-Lite, hitrost prenosa podatkov pa je odvisna od oddaljenosti doma ali podjetja od centrale telefonskega podjetja, ki nudi storitev DSL. Linija DSL lahko prenaša podatke in glas, del linije s podatki je nenehno povezan.

Domača stran (angl. home page) je vrsta spletne strani, ki je vhodna stran oziroma glavni dokument podjetja, ustanove ali posameznika v svetovnem spletu, prek katere imamo dostop do drugih njegovih spletnih strani in podstrani. *Glej tudi www.*

Domena oz. ime domene umesti organizacijo ali fizično osebo na internetu. Nacionalna vrhnjenivojska domena (ccTLD) - »si« - odraža nacionalno geografsko območje, v katerem se želi oseba nahajati za druge uporabnike. Generična vrhnjenivojska domena (gTLD) pa je ime najvišje domene v internetnem naslovu, ki ga opredeli generično po razredih domen, kot so ".com" (komercialna), ".net" (sprva mišljena za ponudnike internetnih storitev, zdaj pa v rabi za več namenov), ".org" (za neprofitne organizacije, industrijske skupine ...), ".gov" (vladne agencije), ".mil" (za vojsko), ".edu" (za izobraževalne ustanove) in ".int" (za mednarodne pogodbe in baze podatkov).

- E -

EDGE (enhanced data rates for GSM evolution); GSM za hitrejše podatkovne komunikacije. Sistem EDGE predstavlja naslednji korak proti hitrim mobilnim internetnim storitvam (prepustnost do 120 kb/s), predstavlja alternativo (dragemu) sistemu UMTS.

Ekstranet je nadgradnja intraneta, ki dovoljuje zunanjemu uporabniku dostop do nekaterih informacij v podjetju *Glej tudi Intranet*.

Elektronski podpis je poseben postopek, na osnovi katerega lahko enolično ugotovimo podpisnika elektronskega dokumenta.

Elektronsko poslovanje (»electronic business«) se nanaša na izvajanje poslovnih transakcij, na upravljanje odnosov s strankami in na komuniciranje tako znotraj podjetja kot med različnimi podjetji, kupci in državno upravo. Izvaja se lahko preko privatnih ali pa javnih omrežij. Primeri področij elektronskega poslovanja so poslovanje med podjetji (business to business - B2B), poslovanje med podjetji in končnimi kupci (business to consumer - B2C), poslovanje med državo in državljani (G2C – government to citizen) ter poslovanje med državo in podjetji (G2B – government to business).

Elektronsko trgovanje (»e-commerce«) je ožji pojem od elektronskega poslovanja in se nanaša samo na nabavo ali prodajo izdelkov/storitev preko interneta. V praksi pa se ta termin pogostokrat zamenjuje s terminom e-poslovanje. Elektronsko trgovanje se deli na elektronsko nabavo (»e-procurement«) in elektronsko prodajo (»e-commerce«).

E-pošta (angl. e-mail) je elektronski prenos sporočil, besedil, dokumentov z enega računalnika na drugega.

- F -

Faks je vrsta elektronskega sporočila, ki si ga izmenjujejo faksovne naprave, ki po analognem ali digitalnem telefonskem priključku omogočajo prenos digitalizirane slike.

Forum je spletna aplikacija, ki omogoča razpravo, izmenjavo mnenj, komentarjev, nasvetov med uporabniki interneta. Forum je ponavadi razdeljen na forumske mape, ki se tičejo posameznih tematskih sklopov, ki jih lahko oblikujejo uporabniki sami ali pa moderator foruma (tema je lahko karkoli od politike, zabave, šole, dela, potovanja itd.).

- G -

Geslo (angl. password) je skrivno zaporedje znakov, ki se uporablja za preverjanje identitete uporabnika; npr. uporabniško geslo, skrbniško geslo.

Gostitelj je vsak računalniški sistem z naslovom IP, povezan z mrežo. *Glej še IP.*

GPRS (General Packet Radio Service – splošna paketna radijska storitev) je paketna preklopna tehnologija, ki omogoča pošiljanje/prejemanje blokov podatkov z mobilnega telefona ali nanj s hitrostjo 171,2 kbps/28 kbps. Tehnologija GPRS, znana tudi kot 2.5G, omogoča stalno povezavo z internetom, uporabnikom pa se navadno zaračuna cena glede na obseg prenesenih podatkov in ne na čas povezave.

GPS navigacija (Global positioning system) je satelitski sistem za določanje položaja objektov na zemlji. Sateliti, ki iz zemeljske orbite pošiljajo svoj točen položaj in čas oddajanja, so razporejeni tako, da s signalom pokrivajo vsako točko na površini zemlje. Uporablja se tudi za iskanje poti pri vožnji z avtom.

GSM (Global System for Mobile Communication – globalni sistem mobilne telefonije) je glavni sistem za mobilno komunikacijo po svetu. Znan je tudi kot 2G. Ustrezen je za prenos glasu, ne pa za prenos podatkov ali za dostop do interneta.

- H -

HTML (Hyper text Markup Language – jezik za označevanje nadbesedila) je nabor označevalnih simbolov ali šifer, ki so umeščene v datoteko in opisujejo strukturo teksta v dokumentu. Oznake spletnemu brskalniku povedo, kateri deli teksta so naslovi, odstavki, seznami, slike in kako jih je potrebno prikazati uporabniku. *Glej tudi brskalnik, WWW.*

- I -

ID (informacijska družba, angl. IS – Information Society) je izraz, ki ga je sprejela Evropska komisija za označevanje družbe, v kateri je informacija ključna sestavina ekonomskih, političnih, kulturnih in socialnih dejavnosti.

IKT (informacijsko–komunikacijska tehnologija, angl. ICT – Information and Communications Technology) je programska in strojna oprema za komunikacijo s podatki (računalnik, faks, internet, fiksni, mobilni telefon ...).

Internet je svetovno omrežje povezanih računalnikov, ki se povezujejo po standardiziranem protokolu in omogočajo, da si uporabniki na različnih mestih izmenjujejo besedilne, zvočne in slikovne informacije.

Internet café oz. spletna kavarna je lokal, ki ob obisku nudi dostop do interneta.

Internetni strežnik (angl. host) je naprava – največkrat računalnik –, ki v omrežju tipa odjemalec/strežnik po internetnem protokolu omogoča shranjevanje in dostop do datotek odjemnih računalnikov v omrežju.

Intranet je zasebno podatkovno omrežje (za interno uporabo) v organizaciji in uporablja internetni protokol. Namenjen je izmenjavi informacij med uslužbenci.

IP (Internet Protocol – internetni protokol) je zbirka pravil, ki jih je treba upoštevati pri pošiljanju podatkov med dvema računalnikoma po internetu. Vsak računalnik, ki je povezan z internetom (strežnik), ima vsaj en IP-naslov, po katerem se razlikuje od drugih računalnikov na mreži.

IP-telefonija (pogosto tudi VoIP – Voice over Internet Protocol, internetna telefonija) je sistem za glasovno komunikacijo preko računalniškega omrežja in lahko nadomešča klasično telefonijo.

IR je infrardeča povezava (glej pod Brezžična povezava).

IRC (Internet Relay Chat) je namenjen sporazumevanju z drugimi uporabniki interneta. Pogovor poteka v živo v kanalih (channels), z drugimi uporabniki pa se pogovarjate z uporabo tipkovnice, s katero odtipkate svoje sporočilo ali vprašanje, odgovor dobite skoraj takoj, ko ga vtipka vaš sogovornik. Najpogosteje se za IRC uporablja program mIRC, s katerim se povežete s strežnikom, ki se nahaja v enem izmed več omrežij, ter se pridružite uporabnikom v določenem kanalu. Imena kanalov dajo ponavadi vedeti o čem teče beseda v njih. V glavnem se IRC uporablja za skupinsko komunikacijo, vendar omogoča tudi privatno izmenjavo sporočil

ISDN (Integrated Services Digital Network - digitalno omrežje z integriranimi storitvami) je digitalno omrežje, ki omogoča neposredne storitve za vse vrste priključkov. To je tehnologija, ki omogoča hkraten prenos glasu, slike in podatkov do 128 kbit/s.

Iskalnik oz. spletni iskalnik je vmesnik za iskanje informacij na svetovnem spletu. Išče tako spletne strani kot slike, videe in druge oblike dokumentov. Slovenski najbolj uporabljan iskalnik je Najdi.si, v svetovnem merilu pa so to Google, Yahoo ...

ISP (Internet Service Provider – ponudnik internetnih storitev) je dobavitelj internetnih storitev, vključno z dostopom. Sprva so se razlikovali od IAP-ov (Internet Access Provider – ponudnikov internetnega dostopa), ker ponujajo večji del ogrodja povezav med državami in ker se pasovna širina prodaja manjšim IAP-om.

IT (Information Technology – informacijska tehnologija). *Glej IKT.*

- J -

Javna točka za dostop do interneta (angl. Public Internet point) je najširša oznaka za katero koli informacijsko točko, ki omogoča dostop do interneta na javnem mestu. Take točke so na voljo v knjižnicah, mladinskih centrih, šolah, Internet café-jih in hotelih.

- K -

Kabelski modem je naprava, ki je vmesnik med koaksialnima kabelsko televizijo/glasovnim kanalom in domačo računalniško opremo. Ima možnost hitre internetne povezave.

Kartica SIM (SIM-Subscriber Identity Modul in USIM- Universal Subscriber Identity Modul) je kartica z vpisano kodo, ki omogoča priključitev na omrežje in identifikacijo naročnika oz. uporabnika omrežja. Kartica SIM omogoča varovanje naročnika oz. uporabnika z identifikacijsko številko (kodo) PIN (Personal Identification Number).

Klepetalnica je klepet v živo na daljavo med uporabniki interneta (glej tudi IRC)

Konzola je vrsta računalniške opreme za igranje iger; npr. Playstation, xBox, Wii ...

- L -

LAN (Local Area Network – lokalno omrežje) je mreža povezanih računalnikov na manjšem geografskem območju; najpogosteje pokriva območje ene zgradbe, pisarne, domače hiše, šole. Omogoča visoke prenose hitrosti.

- M -

Messenger omogoča spletno komuniciranje in izmenjavo datotek. Gre za tehnologijo takojšnjega sporočanja, ki pomeni predvsem pogovore v dvoje z ljudmi, ki so uporabnikovi znanci (v nasprotju s klepetalnicami, npr. IRC-em, kjer svojih sogovornikov ne poznamo).

MMS (Multimedia Messaging Service – servis za multimedijska (večpredstavnostna) sporočila) je namenski program, ki omogoča pošiljanje/sprejemanje sporočil, ki vsebujejo kombinacijo besedila, zvoka, slik in videa, z mobilnim telefonom ali dlančnikom.

Mobilni operater je ponudniki mobilne telefonije, v Sloveniji npr. Mobitel, Simobil ...

Mobilni telefon je prenosni telefonski aparat, ki ga uporabljamo v celičnem omrežju za mobilno telefonijo GSM. *Glej tudi GSM.*

- N -

Nezaželena pošta (ali tudi e-slama, angl. spam) je nadležno elektronsko sporočilo razposlano na množico elektronskih naslovov z vsiljivo komercialno vsebino, ki si je naslovniki sami ne bi odločili prejemati (pogosto vsebuje tudi viruse, škodljive ali nelegalne vsebine ali je sredstvo spletnih goljufij, prevar).

- O -

Odprtokodna programska oprema (OKPO) je naziv za programsko opremo, katere izvorna koda je prosto dostopna, tako da jo je mogoče prosto uporabljati, raziskovati, spreminjati in razširjati tako originalne kot dopolnjene in spremenjene kopije.

Offline/online sta izraza za osebo, ki je trenutno povezana (online) ali trenutno ni povezana (offline) z internetom.

On-line skupnost je spletna skupnost. V njih se družijo posamezniki s podobnimi interesi; npr. portal za ljubitelje računalništva, astrologije, tržnega komuniciranja, živali.

Optični kabel omogoča optično povezavo nadstropij v eni stavbi ali povezavo med več stavbami. Je veliko dražji od navadne parice oz. žice, toda omogoča veliko hitrejši prenos podatkov – od 600 do 1000 MHz- večpredstavnostnih namenskih programov. Uporablja se v industrijskih omrežjih, v vojaškem in medicinskem okolju. V Sloveniji počasi prodira tudi v širšo uporabo za dostop do interneta, digitalne televizije in internetne telefonije.

- P -

Pametni telefon je mobilni telefon, ki presega zmogljivosti običajnega telefona in nudi podobne funkcionalnosti kot osebni računalnik: brezžično e-pošto, brskanje po spletu in faksiranje, spletno bančništvo, povezanost z LAN-om, lokalni in oddaljen prenos podatkov med telefonom in računalniki ter oddaljen nadzor nad domačimi ali poslovnimi elektronskimi sistemi, računalniki.

Pasovna širina je fizična lastnost telekomunikacijskega sistema, ki določa hitrost, pri kateri se lahko prenašajo informacije. V analognih sistemih se meri v ciklih na sekundo (hertz), v digitalnih sistemih pa v bitih na sekundo (bit/s).

PIN koda (angl. Personal Identification Number) je osebna identifikacijska številka (ponavadi je to 4-mestna številka), ki jo vpišemo, ko vključimo mobilni telefon.

Piškotki *Glej pod Cookies*.

Požarni zid je kombinacija strojne in programske opreme, ki ščiti podatke in računalnik pred škodljivimi vplivi internetnega omrežja.

Protivirusni program (angl. anti-virus program) je računalniški program za odkrivanje in odstranjevanje virusov.

P2P omrežja: (peer to peer omrežja) omogočajo izmenjavo datotek (npr. glasbe, filmov, računalniške opreme) preko interneta.

- R -

Računalniška izmenjava podatkov (RIP) (angl. EDI - Electronic Data Interchange) je elektronska izmenjava poslovnih podatkov, kot so listine, pisma, naročila in podobno, po omrežju med računalniki pri elektronskem poslovanju.

- S -

SMS (Short Message Service – servis za kratka sporočila) je aplikacija za pošiljanje in prejemanje alfanumeričnih sporočil z mobilnim telefonom.

Socialna programja (Social Networking Sofware, tudi Social Networking Service) so zelo aktualna oblika spletnega komuniciranja in ustvarjanja socialnih skupnosti na internetu. Večina socialnega programja omogoča registriranim uporabnikov različne načine komuniciranja kot npr. klepetanje, pošiljanje elektronske pošte, nalaganje lastnih video ali avdio posnetkov, deljenje dokumentov, ustvarjanje lastnega bloga, foruma ipd.

Spam *Glej nezaželena pošta*.

Spletna stran (angl. Web page) je dokument z nadbesedilom (hypertext), kot ga prikazujeta spletni pregledovalnik oz. brskalnik. Na spletni strani so lahko besedilo, nadpovezave (linki oz. Hiperlinki), podobe, video in avdio posnetki.

Spletni dnevnik (blog) je sestavljenka iz besed »web« in »log«, kar v slovenskem jeziku pomeni spletni dnevnik. Preko programskega vmesnika lahko uporabniki na spletno mesto dodajajo besedila, ki so označena z datumom, najnovejši zapis pa se nahaja na vrhu spletne strani.

SSL (»Secure Socket Layer«) je protokol, ki omogoča šifriran prenos podatkov med strežnikom in odjemalcem, s čimer je onemogočeno »prisluškovanje« oz. nepooblaščeno branje informacij.

SSL certifikat je potrdilo, ki ga mora strežniku oz. spletni strani izdati za to pooblaščena organizacija, in obiskovalcu strani zagotavlja, da je komunikacijski kanal med njim in strežnikom zares varen. SSL certifikat naj bi uporabljala vsaka spletna stran, ki od obiskovalca zahteva vnos osebnih podatkov, še posebej pa je to pomembno pri vnosu informacij o kreditnih karticah.

Strežnik je računalniški program, ki omogoča storitve drugim računalniškim programom na istem ali drugem računalniku. Spletni strežnik je računalniški program (nameščen v računalniku), ki dostavlja želene strani HTML ali datoteke (internetne strani). *Glej tudi HTML*.

- Š -

Širokopasovne tehnologije oz. povezave (angl. broadband) omogočajo hiter prenos podatkov (filmi, igre, videokonference) preko omrežja (npr ADSL, kabelska povezava, UMTS, optična povezava). Na splošno so to širokopasovne povezave, ki zmorejo hitrost večjo od 2 Mbit/s. *Glej tudi kabelski modem, UMTS, optični kabel.*

- U -

UMTS (Universal Mobile Telecommunication System – univerzalni mobilni telekomunikacijski sistem je poznan tudi kot 3G (tretja generacija) tehnologija je naslednik GSM-a. UMTS je standardni sistem (IMT-2000) in dosega hitrosti povezave 2 mbps/144 kbps z uporabo širokopasovne CDMA tehnologije. Ta normativ uporabnikom preko brezžične povezave omogoča prenos velikega obsega podatkov, slik, videa in seveda dostop do interneta. *Glej še GSM*.

Uporabnik interneta je po definiciji Statističnega urada RS tista oseba, ki je že kdaj uporabila internet. Uporabljajo se še druge kategorije: mesečni, tedenski uporabnik ...

- V -

VDSL (Voice-over Digital Subscriber Line – govor preko digitalne naročniške linije – DSL) omogoča prenos velikega števila telefonskih pogovorov prek ene fizične telefonske linije. *Glej še DSL*.

- W -

WAP (Wireless Application Protocol – protokol za brezžične aplikacije) je ime za skupino okleščenih protokolov, ki so namenjeni mobilnim napravam (telefonom, ročnim računalnikom, pozivnikom). Omogoča jim dostop do interneta.

WLAN - Brezžično lokalno omrežje (angl. Wireless LAN) je povezava dveh ali več računalnikov brez uporabe kablov. WLAN za komunikacijo med napravami v omejenem področju izkorišča spread-spectrum tehnologijo na podlagi radijskih valov. To omogoča uporabnikom, da so kljub premikanju znotraj območja pokritosti povezave še vedno povezani v omrežje.

WWW (World Wide Web – svetovni splet) je zbirka strani HTML na svetovnem strežniku. V januarju 2005 je bilo ocenjeno, da je na internetu več kot 11,5 milijard javno dostopnih www strani, od takrat se ocene velikosti svetovnega spleta gibljejo med 15 in 30 milijardami spletnih strani. *Glej tudi HTML*.

8 Literatura in viri

8.1 Literatura

1. Banović, Zoran (2003): Ali računalniki ustvarjajo morilce? Moj mikro, 9, str. 16-19.
2. Cerar, Gregor (2000): Rasizem v vsako vas. Mladina, 35, 2000.
3. Direktiva 2002/58/EC o obdelovanju osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector), sprejeta 12. julija 2002. Official Journal L 201, 31/07/2002 p. 0037 - 0047.
4. Ferenc, Manica (2006): Zmaga pornografije? Družina, 28. 5. 2006. Dostopno na:http://www.druzina.net/icd/spletnastran.nsf/all/CB1B64155B63D422C125717900397C64?OpenDocument, 11.7.2007.
5. Jakopič, Kaja (2005): Boj proti sovraštvu na medmrežju ali boj z mlini na veter. Dostopno na: http://mediawatch.mirovni-institut.si/bilten/seznam/24/mwatch/.
6. Jeriček, Helena (2003): Zasvojenost z internetom. Vzgoja, 19, str. 41-43.
7. Kaloh, Dejan (2004): Kibernetski skini brez mej, Večer, 12. 7. 2004. Dostopno na http://www.vecer.si/vecer2006/default.asp?kaj=6&id=2004071200543606.
8. Kocmur, Helena (2005): Spletne klepetalnice: nekaterim pomagajo, drugim lahko zagrenijo življenje. Nedelo, 21. 8. 2005, str. 18.
9. Kočevar, Valentina (2005): Verbalno nasilje v interaktivnih forumih. Diplomsko delo, Univerza v Ljubljani.
10. Mehta, Michael D. (1998): Sex on the Net: Regulation and control of pornography in the new wired world. V L. Pal in C. Aleksander (ur.): Digital Democracy: Politics and Policy in the Wired World, Oxford University Press, Toronto, str. 164-179.
11. Merljak, Sonja (2003a): Otrok storilca večinoma pozna. Delo, 15. 5. 2003, str. 4.
12. Milek, Vesna (2005): Ljubezen v času SMS. Delo-Sobotna priloga, 5. 2. 2005, str. 24-25.
13. Ostrež, Tina prirejeno po Decker, Regina (2005): Werbung und Internet. Ein Netz für Kinder – Surfen ohne Risiko? Bundesministerium für Familie, Senioren, Frauen und Jugend, str. 23-26.

14. Ostrež, Tina, prirejeno po Dax-Romswinkel, Wolfgang (2006a): IT-Sicherheit macht Schule. Arbeitsmaterialien für den Unterricht. Shutz der Privatsphäre in Internet, str. 4-14. Dostopno na: http://www.secure-it.nrw.de/_media/pdf/RZ_Schutz%20der%20Privat_150dpi.pdf.
15. Ostrež, Tina, prirejeno po Platen, Martina (2006b): IT-Sicherheit macht Schule. Sicheres Chatten. Arbeitsmaterialen für den Unterricht, str.5. Dostopno na: http://www.safe.si/uploadi/editor/1140092218sicheres_chatten.pdf.
16. Samaluk, Barbara (2005): Omejevanje sovražnega govora na svetovnem spletu.
17. Skrt, Radoš (2002): Varno internetno nakupovanje v spletnih trgovinah. Moj mikro, 3,str. 72.
18. Skrt, Radoš (2004): Otroci potrebujejo zaščito. Moj mikro, 6, str. 50-52.
19. Skrt, Radoš (2004): Za vsako bolezen raste rož'ca. Moj mikro,12, str 18-25.
20. Skrt, Radoš (2005): Za ribiči gesel še »farmarji«. Moj mikro, 6, str. 24-25.
21. Taylor, Max in Quayle, Ethel (2003): Child pornography: An Internet Crime. Brunner-Routledge, Hove in New York.
22. Young, S. Kimberly (1998): Caught In The Net. New York: John Wiley&Sons, Inc.
23. Uradni list RS, št. 33/91-I, 42/97, 66/2000, 24/03 in 69/04).
24. Uradni list RS, št.63/94, 70/94, 23/99, 40/04.
25. Zakon o medijih (uradno prečiščeno besedilo) /ZMed-UPB1/(Ur.l. RS, št. 110/2006).

8.2 Internetni viri

1. A typology of online child pornography offending (2004): Dostopno na: http://www.aic.gov.au/publications/tandi2/tandi279t.html, 10. 3. 2006.
2. APEK, dostopno na http://www.apek.si/7sec/1sec.html, 10. 3. 2006.
3. Arbeitsgemeinschaft zum Shutz der Kinder vor sexueller Ausbeutung. Dostopno na:http://www.ecpat.de/, 10. 3. 2006.
4. Arnes (2002): Varnost šolskih omrežij. Dostopno na: http://www.arnes.si/dokumenti/filtri/, 10. 3. 2006.
5. Arnes: Zakonodaja RS, ki se nanaša na informacijsko varnost. Dostopno na: http://www.arnes.si/si-cert/kz.html, 10. 3. 2006.
6. Arnes (2004): "Dialler" programi in veliki telefonski računi. Dostopno na http://www.arnes.si/si-cert/obvestila/2004-07.html, 10. 3. 2006.
7. Arnes (2002): Nenaročeno oglaševanje po elektronski pošti (spam). Dostopno na http://www.arnes.si/spam/, 10. 3. 2006.
8. Arnes (2004): »Phishing« - nova oblika spletne prevare (kraje). Dostopno na: http://www.arnes.si/si-cert/obvestila/2004-06.html, 10. 3. 2006.
9. Arnes: Zaščita domačega omrežja. Dostopno na: http://www.arnes.si/help/zascita_racunalnika.html, 10. 3. 2006.
10. Becta (2007a): Online bullying. Dostopno na: http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_ob_03, 16. 11. 2007.
11. Becta (2007b): Mobile technology. Dostopno na: http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_mob_03, 16. 11. 2007.

12. Becta (2007c): School websites. Dostopno na: http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_sw_03, 16. 11. 2007.
13. Becta (2007d): Using chat rooms in the classroom. Dostopno na: http://schools.becta.org.uk/index.php?section=is&&catcode=ss_to_es_pp_com_03&rid=12005, 16. 11. 2007.
14. Benschop, A.: Pornography in Cyberspace – Internet hornification and cyber sexual obsessions. Dostopno na http://www2.fmg.uva.nl/sociosite/websoc/pornography.html, 10. 3. 2006.
15. DPA (2003): Mobile phones becoming a major addiction. Dostopno na: http://www.smh.com.au/articles/2003/12/10/1070732250532.html?from=storyrhs, 10. 7. 2007.
16. Free Expression Policy Project. Dostopno na: http://www.fepproject.org/whitePapers/ntiacomments.html, 10. 3. 2006.
17. http://blog.volja.net, 10. 3. 2006.
18. http://surs.ris.org/, 10. 3. 2006.
19. http://www.adp.fdv.uni-lj.si/kibersub, 10. 3. 2006.
20. http://www.gov.si/srd, 10. 3. 2006.
21. http://www.isuma.net/v02n02/taylor/taylor_e.pdf, 10. 3. 2006.
22. http://www.najdi.si, 14. 11. 2007.
23. http://www.parametica.si, 14. 11. 2007.
24. http://www.pozitivke.net, 10. 3. 2006.
25. http://www.raziskovalec.com, 14. 11. 2007.
26. http://www.ribera.si, 14. 11. 2007.
27. http://www.ris.org/main/novice/readnews.php?sid=312, 10. 3. 2006.
28. http://www.sisplet.org/ris/ris/dynamic/readpublications.php?sid=40, 10. 3. 2006.
29. http://www.skb.si/eban/eban-varno1.html, 10. 3. 2006.
30. http://storitve.siol.net, 14. 11. 2007.
31. http://upctelemach.si/, 14. 11. 2007.
32. http://www.volja.net, 10. 3. 2006.
33. iSafe: The Promise and Perils of blogging. Dostopno na: http://www.isafe.org/imgs/pdf/education/Blogging.pdf, 10. 3. 2006.
34. Jemec, Vlasta (2007): Uporaba IKT pri izvedbi večdnevne strokovne ekskurzije. V: Informacijska družba IS 2007, 10. mednarodna konferenca: Vzgoja in izobraževanje v informacijski družbi, Ljubljana, Slovenija, 12. 10. 2007.
35. Kelvindale Primary School, dostopno na http://www.kelvindaleprimary.org.uk/myweb2/main_frames.htm, 10. 3. 2006.
36. Kovačič, Matej (2006): Kršitve avtorskega prava na internetu. Dostopno na http://www.slo-tech.com/clanki/06001/, 10. 3. 2006.
37. Kovačič, Matej (2006): Zasebnost in varnost na internetu. Dostopno na: http://admin.safe.si/uploadi/editor/1136811791zasebnost_in_varnost_kovacic.pdf), 14. 11. 2007.
38. Kristan, Alma (2007): Mladostnikova razmišljanja o spolnosti. Dostopno na: http://trendi.siol.net/default.aspx?site_id=155&page_id=405&article_id=155405070508105311111&cid=405&pgn=1, 11. 7. 2007.

39. Lin, Sunny (2004): Mobile phones-technology-disadvantages. Dostopno na: http://wiki.media-culture.org.au/index.php/Mobile_Phones_-_Technology_-_Disadvantages, 10. 7.2007.
40. Microsoft (2004): Pomagajte otrokom, da v vsebinah v internetu ločijo zrnje od plev. Dostopno na: http://www.microsoft.com/slovenija/doma/varnost/otroci/pomagajte_otrokom.mspx, 10. 3. 2006.
41. Microsoft. Dostopno na: http://www.microsoft.com/windowsxp/using/games/getstarted/esrbratings.mspx.
42. PEGI Online. Dostopno na http://www.pegionline.eu/sl/index/id/195, 9. 7. 2007
43. RIS raziskave. Dostopno na: http://www.ris.org.
44. SKB: Varni spletni nakupi. Navodila za kupce: spletno naročanje in varno plačevanje s karticami. Dostopno na http://www.skb.si/eban/eban-varno1.html, 10. 3. 2006.
45. Statistični urad Republike Slovenije (2008): Uporaba informacijsko-komunikacijske tehnologije (IKT) v gospodinjstvih in po posameznikih, Slovenija, 2008. Dostopno na: http://www.stat.si/novica_prikazi.aspx?ID=2027, 27.10.2009.
46. Statistični urad Republike Slovenije (2009): Uporaba informacijsko-komunikacijske tehnologije (IKT) v gospodinjstvih in po posameznikih, Slovenija, 1. četrtletje 2009. Dostopno na: http://www.stat.si/novica_prikazi.aspx?id=2670, 27.10.2009.
47. Varstvo osebnih podatkov na internetu. Dostopno na: http://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/varstvo-osebnih-podatkov-na-internetu/,12. 11. 2007.
48. Šribar, Renata in Boldin, Mateja (2007): Porno chic in mobilniki v Sloveniji. Dostopno na: http://www.drustvo-vitaactiva.si/156701/322801.html, 11.7.07.
49. Tipps für Lehrer/Innen. Dostopno na http://www.saferinternet.at/tipps/lehrer.php, 10. 3. 2006.
50. Young, S. Kimberly (1996): Psychology of Computer Use: XL. Addictive Use of the Internet: A case that Breaks the Stereotype, http://www.netaddiction.com/articles/stereotype.htm, 9. 7. 2007.
51. Thornburgh, Dick in Lin, Herbert S. (2002): Youth Pornography and the Internet. Dostopno na http://bob.nap.edu/html/youth_internet/ch2.html.
52. V Sloveniji blogajo predvsem mladi in najbolj internetno pismeni. Dostopno na: http://www.iprom.si/press.html?id=126, 8. 11. 2007.
53. Weiss in Espana: Internet violence. Dostopno na: http://www.uri.edu/personal/mwei84818/RealViolence22.txt, 10. 3. 2006.
54. European parliament, Committee on Women's Rights and Equal Opportunities (2004): Draft report on the consequences of the sex industry in the European Union. Dostopno na: http://action.web.ca/home/catw/attach/ErikssonDraftReportJan2004.pdf.

Gradiva za učitelje je pripravila ekipa projekta SAFE-SI. Projekt SAFE-SI je del evropskega omrežja točk osveščanja o varnem internetu (»InSafe«), sofinanciran pa je s strani Evropske Komisije ter Ministrstva za visoko šolstvo znanost in tehnologijo.

Oblikovanje: Bojan Senjur, Borut Ivanišević, Žiga Valetič

Lektoriranje: Margit Berlič Ferlinc

Tisk: Impress, d.d.

Naklada: 1.000 izvodov

Izdajatelj: Projekt SAFE-SI, november 2009 (prenovljena in dopolnjena izdaja)