UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Vesna Štimac

Nadzor in razkrivanje osebnih podatkov na internetu

Diplomsko delo

Ljubljana, 2011

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Vesna Štimac

Mentor: doc. dr. Gregor Petrič
Somentor: asist. dr. Matej Kovačič

Nadzor in razkrivanje osebnih podatkov na internetu

Diplomsko delo

Ljubljana, 2011

Nadzor in razkrivanje osebnih podatkov na internetu

Uporabniki interneta za seboj puščajo digitalne sledi, te sledi pa vsebujejo najrazličnejše podatke, ki v kombinaciji še z drugimi viri podatkov omogočajo profiliranje. Profili uporabnikov so postali pomembna valuta v digitalnem svetu, saj jih marketinške in trženjske organizacije uporabljajo za ugotavljanje uporabnikovih želja in interesov. Z množičnim članstvom v različnih spletnih socialnih omrežjih so lažje dostopni postali tudi različni osebni podatki, ki jih uporabniki razkrivajo, misleč da gre za zasebno izmenjavo in da imajo nadzor nad razkrivanjem teh podatkov v svojih rokah. Skoraj nobena aktivnost na internetu pa ni več zasebna, spremlja in nadzoruje nas neko nevidno občinstvo, pa naj si bodo to le radovedni souporabniki spletnih socialnih omrežij, marketinške organizacije, vlada ali škodoželjni hekerji. Za izboljšanje informacijske zasebnosti imamo na voljo najrazličnejšo tehnologijo, ravno tako pa je na voljo veliko tehnologije, ki vdira v našo zasebnost, zbira naše podatke in nas nadzoruje. V diplomskem delu sem proučevala, ali se z večjim poznavanjem tehnologije za zaščito zasebnosti ter večjim zavedanjem nadzora na internetu količina javno razkritih osebnih podatkov manjša ali ostaja nespremenjena. V ta namen sem opravila raziskavo med študenti Fakultete za družbene vede.
Ključne besede: tehnologija za izboljšanje informacijske zasebnosti, tehnologija nadzora na internetu, zavedanje nadzora, informacijska zasebnost.

Surveillance and disclosure of personal data on the Internet

The users of the Internet leave digital traces which contain various data that in combination with other sources of data enable profiling. Users profiles have became an important currency in the digital world as marketing organizations use them to determine user's wishes and interest. By mass membership in different social networks all kinds of personal data became easily accessible, as the users reveal them presuming that the exchange is private and that they have a control over the disclosure of data. However, almost none of the activities on the Internet is private anymore, we are monitored and controlled by some kind of invisible public, this be only inquisitive joint users of social networks on the Internet, marketing organization, government or malicious hackers. To upgrade the information privacy, various technologies are available, as are available numerous technologies for invading our privacy, collecting our data and surveilling us. I wanted to study whether better knowledge on technologies for protection of privacy and better understanding of the surveillance on the Internet is diminishing the quantity of publicly revealed personal data or does it stay the same. With this purpose I did a research among the students of the Faculty of Social Sciences.
Key words: technology for improvement of the information privacy, online surveillance technology, awareness of the surveillance, information privacy**.**

KAZALO

KAZALO SLIK

KAZALO TABEL

1 UVOD

V diplomskem delu raziskujem vprašanje, kakšen pomen ima stopnja uporabnikove osveščenosti o zasebnosti na internetu pri razkrivanju osebnih podatkov. S pojmom osveščenost natančneje obravnavam poznavanje tehnologije za zaščito informacijske zasebnosti in zavedanje nadzora na internetu. Zanima me torej, ali se z večanjem stopnje uporabnikove osveščenosti količina javno razkritih osebnih podatkov manjša ali ostaja nespremenjena. Pri reševanju raziskovalnega vprašanja sem si pomagala s pregledom relevantne literature in z že opravljenimi raziskavami. Ker me zanima predvsem slovensko področje, bolj izpostavim raziskavi »Slovenski uporabniki interneta in zasebnost«, ki jo je leta 1999 opravil Matej Kovačič, ter »Pomen zasebnosti med slovenskimi uporabniki interneta«, ki jo je leta 2006 opravila Darja Praprotnik. Opravila sem tudi lastno raziskavo, in sicer sem raziskovala populacijo študentov Fakultete za družbene vede (v nadaljevanju FDV). Pridobljene podatke sem nato s pomočjo programa SPSS analizirala z različnimi statističnimi metodami.

Meja med zasebnim in javnim je nejasna, saj na internetu dobimo lažen občutek zasebnosti. S tem, ko brskamo po internetu, se nam zdi, da gre za zasebno izmenjavo podatkov, vendar ko je zasebna informacija razkrita na internetu, postane dostopna za branje širši javnosti. Nad tem, kdo bere naše navidezno zasebne podatke, pa imamo malo kontrole (Barnes 2006). Z razvojem informacijsko-komunikacijske tehnologije je postala bolj dostopna tudi tehnologija za zbiranje, procesiranje, klasificiranje in povezovanje podatkov, zato je v informacijski družbi najbolj ogrožena informacijska zasebnost, ključnega pomena pa je njena zaščita s kontrolo pretoka in posredovanja osebnih podatkov (Kovačič 2000, 1024).

Lahko bi rekli, da na internetu obstajata dve vrsti nadzora oziroma vdora v informacijsko zasebnost. Prvi je nadzor, ki ga nad nezaščitenimi uporabniškimi profili v spletnih socialnih omrežjih izvajajo drugi uporabniki spletnih socialnih omrežij. Drugi pa je nadzor, kjer zaščitenost ali nezaščitenost profila nima nobenega pomena, torej nadzor, ki ga predvsem v marketinške namene izvajajo različne korporacije.

Uporabniki so obremenjeni predvsem s prvo vrsto nadzora, saj jih skrbi, da bi njihove profile videli uporabniki, pred katerimi imajo neke vrste strahospoštovanje. Zgodilo se je že, da je kdo zaradi neprimernih objav na Facebooku dobil odpoved v službi ali pa so študenta, ki je imel na svojem profilu objavljene neprimerne fotografije, izpisali z univerze. Zato uporabniki spletnih socialnih omrežij pogosto zaščitijo vidnost svojih profilov in kontrolirajo, katere vsebine bodo vidne komu. S takimi dejanji mogoče res dobijo občutek, da imajo nadzor nad svojo zasebnostjo in da so se mogoče rešili nezaželenega nadzora, vendar se še vedno niso znebili druge vrste nadzora. Še vedno se o njih zbirajo informacije nekje drugje, ne glede na vse možne zaščite vidnosti njihovega profila. Če uporabniki nimajo tehnologije za izboljšanje zasebnosti, potem ne uidejo takšnemu nadzoru. V diplomskem delu se osredotočam na nadzor, ki ga nad nami izvajajo različne institucije in korporacije, saj gre tu za nadzor večjih razsežnosti in se pred njim težje ubranimo. Kljub temu ne morem mimo nadzora, ki se izvaja med uporabniki v socialnih omrežjih, saj je ta problem še vedno zelo aktualen.

Iz navedenih ugotovitev izhaja moja teza, ki se glasi: »*Uporabnikova osveščenost o nadzoru na internetu in splošno poznavanje tehnologije za izboljšanje zasebnosti pripomoreta k večji informacijski zasebnosti uporabnikov na internetu.«*

1.1 Opredelitev relevantnosti izbrane teme

Organizacija za elektronsko zasebnost meni, da bomo za komuniciranje v prihodnje uporabljali predvsem elektronska sredstva, ta pa je s pomočjo kriptografije lahko neopazno in v veliki meri nadzorovati, zato je po njihovem mnenju kriptografija sredstvo, ki zagotavlja zasebnost (Kovačič 2000, 1031). Res je, da obstajajo različna sredstva, ki lahko izboljšajo naše varovanje zasebnosti, toda problem se pojavi v osveščenosti uporabnikov interneta, saj povprečni uporabnik niti dobro ne ve, kaj je na primer kriptografija, kaj šele, da bi jo uporabljal. Po drugi strani pa se uporabniki ne zavedajo nadzora in nevarnosti, ki jim preti na internetu, zato niti ne čutijo potrebe, da bi zaščitili svojo zasebnost s kakršnokoli tehnologijo. Zato je pomembno ljudi osveščati in izobraževati o grožnjah

zasebnosti, ki se pojavljajo na internetu, ter jim predstaviti sredstva, s katerimi svojo zasebnost lahko zaščitijo.

Številna podjetja, vključno s ponudniki internetnih storitev, kontrolirajo uporabnike interneta, zbirajo informacije o tem, katere spletne strani obiskujejo, čas in dolžino teh obiskov, katere iskalne izraze vpisujejo, spremljajo njihove nakupe ali pa celo preverjajo njihovo odzivnost na oglasne pasice. Vse to lahko primerjamo s tem, da nam nekdo sledi, ko gremo po nakupih, pregleda vsako stran vsake revije, ki smo jo prebrskali, vsak par čevljev, ki smo ga pogledali, in vsak meni, ki smo ga prebrali v restavraciji. Ko so te informacije zbrane v kombinaciji z demografskimi podatki, ustvarjajo zelo natančen profil internetnih uporabnikov. Ti profili so postali pomembna valuta v elektronskem poslovanju, saj jih oglaševalci in tržniki uporabljajo za napovedi uporabnikovega obnašanja, kakšni so njegovi interesi in potrebe ter možni nakupi v prihodnosti (Laurant 2003).

2 JAVNOST IN ZASEBNOST NA INTERNETU

Problem zasebnosti ni več samo tehnični, ampak je tudi družbeni problem. Uporabniki interneta bi se morali bolj zavedati nevarnosti različnih zlorab, in tudi kako se proti njim zavarovati, saj je s samozaščitnim ravnanjem varnost mogoče precej povečati (Kovačič 2003, 62).

Uporabniki interneta se na splošno ne zavedajo, da vsak prispevek, ki ga pošljejo na kakšen forum, vsak delček elektronske pošte, ki jo pošiljajo, vsako spletno stran, ki jo obiščejo, ter vsako stvar, ki jo kupijo v spletnih trgovinah, lahko opazuje tretja oseba, ki je ne vidimo. Vpliv na zasebnost je zelo velik, saj obstajajo baze podatkov, ki dajejo ali prodajajo zbirke osebnih informacij, ta praksa pa postaja vedno bolj pogosta z rastjo povpraševanja po informacijah. Grožnje zasebnosti na internetu lahko razdelimo na dva dela. Kot prvo so naše aktivnosti na internetu opazovane s strani neavtoriziranih oseb, kot drugo pa se informacije shranjujejo in so dostopne še mnogo let (Goldberg 2000, 2–5).

Pomemben del zaščite informacijske zasebnosti je nadzor pretoka in posredovanja podatkov, ki se nanašajo na nekega posameznika. Mellors ugotavlja, da najboljša zaščita ni

ta, da oni vedo manj o nas, ampak da mi vemo več o njih, s tem da vemo, kaj oni vedo o nas in kako te informacije uporabljajo (Mellors v Raab v Kovačič 2003, 37).

2.1 Zasebnost

Na zasebnost lahko gledamo iz različnih perspektiv, ki vključujejo pravice državljanov ter varovanje potrošnikov. Zasebnost je pravica ljudi, da nadzorujejo to, katere informacije o njihovem življenju ostanejo pri njih doma ter katere gredo lahko v javnost (Barnes 2006). Zasebnost je želja, da preprečimo drugim dostop do naših osebnih informacij (Flaherty v O'Neil 2001, 18).

Kovačič (2006, 12) pravi, da je zasebnost pomembna zato, ker ščiti svobodo posameznika, kar pomeni, da omogoča svobodno odločanje, torej odločanje brez vmešavanja in prisile drugih. Prisila ni nujno samo neposredna in fizična, ampak gre lahko tudi za manipulacijo in pritiske, internet pa je te probleme zasebnosti prenesel tudi v virtualni prostor.

Čebulj (v Kovačič 2000, 1021) navaja tri elemente zasebnosti:

- zasebnost prostora (možnost posameznika, da je sam),
- zasebnost osebnosti (svoboda izražanja),
- informacijska zasebnost (možnost posameznika, da ima nadzor nad svojimi osebnimi informacijami).

V informacijski družbi je najbolj ogrožena informacijska zasebnost, kamor sodi tudi varstvo osebnih podatkov, ostala dva elementa pa sodita med temeljne človekove pravice.

Poročilo *Privacy and Human Rights 2003* pa zasebnost loči v štiri kategorije (Laurant 2003):

- *informacijska zasebnost*, ki zajema pravila o zbiranju in obdelavi osebnih podatkov, kot so informacije o plačilnih karticah, zdravstvene in vladne informacije ter druge;
- *zasebnost telesa*, ki ščiti človeška telesa pred invazivnimi posegi, kot so genetsko testiranje, testiranje drog in drugo;

- *zasebnost komunikacije*, ki vključuje varovanje in zasebnost elektronske pošte, navadne pošte, telefonskih številk in ostalih načinov komuniciranja; ter
- *prostorska zasebnost*, ki določa mejo vdora v domače, delovno in javno okolje in kamor sodi tudi videonadzor.

En vidik razumevanja zasebnosti je pravica biti puščen pri miru, kar je tudi vzrok za razumevanje problema nezaželene elektronske pošte ali »spama« in neposrednega trženja kot nečesa, kar vdira v zasebnost posameznikov, čeprav pri teh vdorih v zasebnost ne gre za odtekanje informacij (Kovačič 2006, 43).

Solove (v Marwick in drugi 2010, 6–7) pravi, da je pojmovanja informacijske zasebnosti na splošno možno razdeliti v šest skupin:

- pravica biti puščen pri miru,
- omejen dostop do osebnih informacij ali možnost, da se zaščitimo pred nezaželenimi posegi drugih,
- tajnost ali prikrivanje nekaterih zadev pred drugimi,
- sposobnost nadzora nad lastnimi osebnimi informacijami,
- zaščita posameznikove osebnosti, individualnosti in dostojanstva,
- intimnost, omejen dostop do intimnih vidikov življenja.

Katz in Rice (v Barnes 2006) opisujeta internet kot panoptikon. Idejo panoptikona vidijo v neprestanem nadzoru nad posamezniki s parasocialnimi mehanizmi, ki vplivajo na vedenje posameznikov samo zaradi možnosti, da nas nekdo opazuje. Internet je lahko uporabljen kot parasocialni mehanizem za opazovanje spletnih interakcij.

Trije glavni trendi, ki pripomorejo k vdoru v zasebnost (Banisar 1999):

- *globalizacija* - odpravlja geografske omejitve pretoka podatkov. Internet je najbolj znan primer globalne tehnologije;
- *konvergenca* - vodi v odpravo tehnoloških ovir med sistemi. Moderni informacijski sistemi vedno bolj sodelujejo z drugimi sistemi, medsebojno si lahko izmenjujejo in obdelujejo različne oblike podatkov;

- *multimediji* - informacije, zbrane v določeni obliki, se lahko hitro pretvorijo v drugačne oblike.

2.1.1 Osebni podatki

Cilj informacijske zasebnosti je kontrola nad lastnimi osebnimi podatki, zato je potrebno natančno definirati pojem osebni podatek.

Opredelitev pojma osebni podatek Evropske direktive o varstvu podatkov (95/46/ES) se glasi:
»Osebni podatek pomeni katerokoli informacijo, ki se nanaša na določeno ali določljivo fizično osebo (posameznik, na katerega se nanašajo osebni podatki); določljiva oseba je tista, ki se lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali socialno identiteto« (Delovna skupina za varstvo podatkov 2007).

Posredovanje osebnih podatkov je na zasebnost vezano na dva načina. Prvič, osebni podatki, navedeni v enem kontekstu, se lahko prenesejo v druge kontekste. Osebne profile na spletnih socialnih omrežjih lahko izkopavajo in uporabljajo za marketinške informacije (Nissenbaum v Marwick in drugi 2010, 23). Drugič, objavljeni osebni podatki na spletu postanejo javni, to pa pomeni, da so lahko iskani in vztrajni (Read in Giffen v Marwick in drugi 2010, 23).

2.1.1.1 Varstvo osebnih podatkov in zaščita zasebnosti

Leta 1995 je Evropska unija sprejela Direktivo o varovanju podatkov, da bi s tem uskladila zakonodajo držav članic pri zagotavljanju zaščite državljanov in prostega pretoka osebnih podatkov znotraj Evropske unije. Direktiva se nanaša na obdelavo osebnih podatkov v elektronskih, kot tudi v fizičnih datotekah in določa skupno izhodiščno raven zasebnosti, ki

ne krepi zgolj sedanje zakonodaje o varovanju podatkov, temveč tudi določa vrsto novih pravic (Laurant 2003).

Osnovna načela, ki jih vsebuje Direktiva, so: pravica vedeti, od kje podatki izvirajo, pravica do zahteve, da popravijo netočne podatke, pravica do povračila v primeru nezakonite obdelave in pravica do odvzema dovoljenja za uporabo podatkov v določenih okoliščinah. Direktiva vsebuje okrepljeno zaščito v primeru uporabe občutljivih osebnih podatkov, kot so informacije o zdravju, spolnem življenju ter verskem ali filozofskem prepričanju. Za komercialno ali vladno uporabo takšnih informacij je na splošno zahtevana eksplicitna in nedvoumna privolitev posameznika (Laurant 2003).

Evropska direktiva o varovanju podatkov določa, da morajo imeti vse države članice neodvisen organ pregona. V Sloveniji je to Urad informacijskega pooblaščenca. V skladu z Direktivo je tem organom dana znatna moč, saj se mora vlada pri oblikovanju zakonodaje, ki se nanaša na obdelavo osebnih podatkov, posvetovati s tem organom. Organi imajo pristojnost za vodenje preiskav in pravico do dostopa do informacij, pomembnih za njihove preiskave. Lahko izvajajo tudi ukrepe, kot so uničenje podatkov ali prepoved obdelave, kršitelje lahko sodno preganjajo, razrešujejo pritožbe in izdajajo poročila. Prav tako je organ odgovoren za javno izobraževanje in mednarodno povezovanje na področju varovanja in prenosa podatkov. Slovenija je leta 2001 dopolnila svoj Zakon o zaščiti podatkov, da bi lahko vzpostavila neodvisen nadzorni organ in si s tem zagotovila skladnost z Evropsko direktivo o varovanju podatkov, ki je bilo pred tem v pristojnosti Ministrstva za pravosodje (Laurant 2003).

Obstajajo štirje glavni modeli za zaščito zasebnosti. V večini držav jih uporabljajo več hkrati. V državah, ki zasebnost ščitijo najučinkoviteje, pa se hkrati uporabljajo vsi modeli (Laurant 2003):

- *nadzorni zakoni* – v večini držav po svetu obstaja splošni zakon o zbiranju, uporabi in obdelavi osebnih podatkov v zasebnem in javnem sektorju, nadzorno telo pa

nadzira njegovo izvajanje. Ta model je priporočljiv za vse države, ki sprejemajo zakon o zaščiti podatkov in je bil sprejet tudi v Evropski uniji;

- *sektorski zakoni* - nekatere države, kot recimo ZDA, so se izognile vpeljavi enotnega zakona o zaščiti podatkov, vendar so sprejele zakone, ki se nanašajo na posamezne sektorje, kot so finančni sektor in sektor IT. Slabost tega modela je, da je treba za vsako novo tehnologijo vpeljati nov zakon, zato dejanska zaščita zasebnosti velikokrat zaostaja. V večini držav so sektorski zakoni sprejeti le kot dopolnilo nadzornemu zakonu, saj vključujejo podrobnejše informacije glede določene kategorije informacij;

- *samoregulacija* - teoretično je lahko zaščita zasebnosti dosežena z vrsto samoregulativ. Z njihovo pomočjo komercialni in javni sektorji sprejmejo pravila, s katerimi se samonadzorujejo. Takšen model žal ni preveč uspešen, saj obstaja le malo dokazov o tem, da so podjetja res sposobna slediti samoregulacijskim zakonom;

- *tehnologija za zaščito zasebnosti* - tehnologija za zaščito zasebnosti je postala dostopna širši javnosti, s tem pa je bila posameznikom dana možnost, da lahko sami zaščitijo svojo zasebnost. Uporabniki interneta imajo na voljo vrsto programov in sistemov, ki do neke stopnje zagotavljajo zasebnost in varno komunikacijo. Sem sodijo šifriranje, anonimni strežniki, strežniki Proxy in drugi.

2.2 Javnost na internetu

Spletna socialna omrežja so najnovejša generacija »posredne javnosti«. To so okolja, kjer se ljudje zberejo javno s posredovano tehnologijo. V nekem smislu je posredna javnost enaka neposredni javnosti, ki jo najdemo v parkih, gostinskih lokalih, nakupovalnih centrih itd. Najstniki pridejo na internet, da se povežejo s svojimi prijatelji, najverjetneje so zraven

prisotni tudi drugi ljudje, ki sledijo pogovoru dveh prijateljev, če sta zanimiva, v nasprotnem primeru pa ju ignorirajo (Boyd 2007, 2–3).

Med tem, ko obe vrsti javnosti, posredna in neposredna, igrata podobni vlogi v življenju ljudi, pa ima posredna javnost štiri lastnosti, ki so značilne samo zanjo. To so (Boyd 2007, 2–3):

- vztrajnost (kar rečeš ostane, kar rečeš danes, bo še vedno tam čez 10 let),
- iskanost (danes lahko na internetu najdemo, kje je bil nekdo včeraj),
- kopiranje (pogovor iz enega kraja lahko skopiraš na drugi kraj),
- nevidno občinstvo (nekaj vsakdanjega je, da srečujemo v javnem življenju tujce, toda z vidom si lahko pomagamo, ali nam slučajno kdo prisluškuje). Ne samo, da so v posredni javnosti lurkerji nevidni, ampak tudi vztrajnost, iskanost in kopiranje predstavljajo naše izraze občinstvu, ki ni bilo nikoli prisotno, ko so ti izrazi nastajali.

2.2.1 Spletna socialna omrežja

Spletna socialna omrežja so spletne strani, ki uporabnikom omogočajo, da si ustvarijo svoj profil. To je neke vrste njihova osebna predstavitvena stran, s pomočjo katere si nato lahko ustvarjajo svoje socialno omrežje. Sem uvrščamo spletne strani, kot so Facebook, Hi5, Myspace, Netlog itd. Profili uporabnikov ponujajo vpogled v njihove osebne podatke, od datuma rojstva, spola, verskega prepričanja, kraja bivanja, pa vse do najljubših filmov, knjig in glasbe. Uporabniki lahko poleg informacij, ki jih puščajo na voljo, kreirajo tudi izgled svojega profila, nalagajo slike, filmčke ter glasbene datoteke. Uporabniki pridobijo omrežje stikov, ki so nato predstavljeni kot njihovi prijatelji. Pomen prijateljstva v spletnih socialni omrežjih je precej drugačen od prijateljstva, ki ga poznamo v tradicionalni obliki v resničnem svetu. V spletnih socialnih omrežjih ni treba, da neko osebo sploh poznaš, da jo šteješ kot svojega prijatelja, medtem ko za resnično življenje tega ne moremo trditi (Ofcom 2008).

Slika 2.1: Spletno socialno omrežje - Facebook

Vir: Facebook.com (2011).

Raziskava Ofcom[1] je prišla do ugotovitve, da se uporabniki spletnih socialnih omrežij med seboj razlikujejo po svojem obnašanju, kot tudi po namenu uporabe spletnih socialnih omrežij. Prioritete uporabnikov so različne, zato uporabnike razvrščamo v pet različnih skupin glede na namen uporabe spletnih socialnih omrežij (Ofcom 2008):

- *alfa uporabniki za druženje* – to so ljudje, ki uporabljajo spletne skupnosti predvsem za zabavo, spogledovanje in spoznavanje novih ljudi;
- *iskalci pozornosti* – ljudje, ki iščejo pozornost in od drugih uporabnikov pričakujejo, da bodo komentirali njihov profil ter objavljene fotografije;
- *pripadniki* – ljudje, ki si ustvarijo profil za to, da so na tekočem z dogajanjem svojih prijateljev;
- *zvesti* – ljudje, ki uporabljajo spletna socialna omrežja za to, da obnovijo stike s starimi prijatelji, pogosto s sošolci;

[1] Offcom Social Networking research je kvalitativna raziskava, ki je bila izvedena leta 2007 z namenom proučevanja obnašanja ter odnosa uporabnikov in neuporabnikov do spletnih socialnih omrežij. V njej je sodelovalo 39 uporabnikov in 13 neuporabnikov spletnih socialnih omrežij.

- *funkcionalni* – ljudje, ki so osredotočeni na to, da uporabljajo spletna socialna omrežja v točno določen namen.

Ravno tako lahko v različne skupine razdelimo tudi neuporabnike spletnih socialnih omrežij, saj so tudi razlogi za njihovo nečlanstvo med seboj različni (Ofcom 2008):

- *zaskrbljeni za varnost* – ljudje, ki so zaskrbljeni zaradi varnosti na internetu, še posebej jih skrbi dejstvo, da lahko postanejo njihovi osebni podatki javno dostopni;
- *tehnično neizkušeni* – ljudje, ki se ne čutijo dovolj sposobne za uporabo interneta ali računalnika;
- *intelektualni zavrnitelji* – ljudje, ki nimajo niti najmanjšega interesa za članstvo v spletnih skupnostih in se jim zdijo potrata časa.

2.2.2 Nadzor zasebnosti v spletnih socialnih omrežjih

Kot sem že omenila, obstaja nadzor v socialnih omrežjih, za katerega ni potrebno imeti posebne tehnologije, sam nadzor pa se izvaja le zaradi tega, ker se lahko, torej ker nadzorovani uporabnik iz različnih razlogov v svojem profilu ni uredil nastavitev za zaščito zasebnosti.

Spletna socialna omrežja ponujajo nove možnosti za interakcijo in komunikacijo z drugimi, hkrati pa povzročajo zaskrbljenost glede zasebnosti. Med spletnimi socialnimi omrežji po množičnem članstvu ter po podatkih, ki so edinstveni in identificirajo osebe, izstopa Facebook. Večina članov je precej selektivna glede tega, katere osebne podatke bo razkrila, večina razkrije datum rojstva, toda ne razkrije številke mobilnega telefona. Če je določen tip informacije sploh razkrit, potem obstaja večja verjetnost, da je ta podatek točen in zanesljiv, v nasprotnem primeru pa osebne informacije raje ostanejo skrite (Acquisti in Gross 2006, 13). Facebook svojim uporabnikom ponuja precejšnjo kontrolo nad tem, komu in katere osebne podatke bodo člani razkrili. Uporabniki lahko izberejo vidnost svojega profila (kdo lahko vidi njihov profil), kot tudi iskanje profila (kdo lahko najde njihov profil

s pomočjo iskalnika glede na tip uporabnika), žal pa veliko članov ne ve, da take opcije sploh obstajajo[2] (Acquisti in Gross 2006, 16).

Za boljše razumevanje, kako uporabniki Facebooka (zlasti mlajši od 30 let) razumejo zasebnost, je Raynes–Goldie v januarju 2008 opravila leto dni dolgo etnografsko raziskavo. Eden od njenih ciljev je bil razkriti uporabniški odnos do zasebnosti. Raynes–Goldijeva je ugotovila, da uporabnike skrbi njihova zasebnost, predvsem pa so bolj zaskrbljeni za tako imenovano socialno zasebnost[3] kot pa za institucionalno[4].
Skrb za socialno zasebnost bi lahko opredelili s tem, da je uporabnike bolj skrbelo to, da lahko v svojih profilih nadzorujejo dostop do svojih podatkov, kot pa to, da bodo podjetja, ki stojijo za Facebookom, v vsakem primeru uporabila te podatke.
Uporabnike predvsem skrbi to, kako bi najbolje zaščitili svoje profile pred »prijatelji«, kot so njihovi šefi ali učitelji, ter kako bi zaščitili profile, da jih ljudje, ki jim niso všeč, sploh ne bi našli in zato ne bi mogli poslati prošenj za »prijateljstvo«.
Uporabniki svojo socialno zasebnost večajo s tem, da namesto pravih imen uporabljajo vzdevke, čeprav je to v nasprotju s pogoji uporabe Facebooka, saj ta vztraja, da morajo uporabniki, ko uporabljajo njihovo stran, uporabljati prava imena in identitete, v nasprotnem primeru je njihov profil lahko izbrisan. Druga metoda večanja socialne zasebnosti pa je brisanje objav z zidu in brisanje oznak na slikah, ki jih lahko identificirajo (Raynes–Goldie 2010).

Kako zelo so pomembne nastavitve zasebnosti v spletnih socialnih omrežjih, pa nam ponazori naslednji primer: Facebook je decembra 2009 prosil uporabnike, da ponovno razmislijo o svojih nastavitvah zasebnosti. Uporabniki naj bi razmislili o različnih vrstah vsebin in nato izbrali, ali naj bi bile te vsebine vidne vsem ali pa bi ohranili svoje stare nastavitve. Privzeta nova nastavitev je bila izbira »vsi«. Mnogi uporabniki so se med prijavljanjem na Facebook srečali s »pop-up« okencem in ga samo zaprli, ker so želeli priti do samega Facebooka, pri tem pa so ti uporabniki spremenili vse svoje nastavitve v javne in

[2] Ugotovitev izhaja iz raziskave, kjer je skupno sodelovalo 294 posameznikov, od tega je 209 sodelujočih imelo Facebook profil, 78 sodelujočih profila ni imelo nikoli, 7 sodelujočih pa je nekoč imelo profil, vendar so ga deaktivirali.
[3] Urejanje vidnosti uporabniških profilov, onemogočanje dostopa do podatkov izbranim uporabnikom.
[4] Onemogočanje dostopa do podatkov različnim korporacijam, ki zbirajo podatke v marketinške namene.

mnogi se tega niti niso zavedali. Če so nekateri mnenja, da nikogar ne skrbi za zasebnost, potem bi zlahka lahko verjeli, da so uporabniki Facebooka svoje vsebine prostovoljno spremenili v javne. Da to ni tako, lahko pokažemo z resničnim primerom, ki se je zgodil v Ameriki. Nasilni oče neke najstnice je bil izpuščen iz zapora. Ob spoznanju, da prepoved približevanja ne bo zadosten ukrep, ki bi lahko zagotavljal varnost, sta se najstnica in njena mati preselili tisoče kilometrov stran od očeta. Ko je najstnica pričela pridobivati krog prijateljev v novi šoli, je prosila mamo za Facebook račun. Njena mati je prošnji ugodila, zato sta mati in hči previdno delali na tem, da bi bil Facebook profil zaseben, kolikor je to mogoče, saj se nobena od njiju ni želela soočiti s posledicami, če bi bili najdeni. Ko je Facebook v decembru spremenil nastavitve zasebnosti, najstnica in njena mati nista vedeli, kaj te spremenjene nastavitve zasebnosti sploh pomenijo, dokler ju na to ni opozoril nekdo drug (Boyd 2010).

Raziskava Ofcom je razkrila, katera so potencialno najbolj tvegana in nevarna ravnanja uporabnikov spletnih skupnosti:

- nespreminjanje varnostnih nastavitev, uporabniki puščajo varnostne nastavitve takšne, kot so jih dobili ob pričetku uporabe spletne skupnosti, s tem pa dopuščajo, da je njihov profil odprt in viden vsem uporabnikom;
- objavljanje občutljivih osebnih informacij in fotografij;
- objavljanje vsebin, posebno fotografij, ki lahko škodujejo njihovemu ugledu;
- kontakt z ljudmi, ki jih ne poznajo, uporabniki pogosto sprejemajo povabila za prijateljstvo od ljudi, ki jih sploh ne poznajo ali pa jih ne poznajo dovolj dobro.

Da do takšnega potencialno nevarnega obnašanja uporabnikov v spletnih skupnostih sploh prihaja, pa so krivi naslednji razlogi: pomanjkanje ozaveščenosti o problematiki zasebnosti na internetu, prepričanje, da so za varnost in zasebnost na internetu poskrbele že spletne strani same, nizka raven samozavesti med uporabniki, da lahko sami spreminjajo varnostne nastavitve, težko najdljive informacije o varnosti in zasebnosti na internetu, občutek med mlajšimi uporabniki, da so nepremagljivi, miselnost, da so spletne strani s socialnimi omrežji manj škodljive kot pa na primer internetno bančništvo (Ofcom 2008).

3 TEHNOLOGIJA ZA IZBOLJŠANJE INFORMACIJSKE ZASEBNOSTI

Tehnologija za izboljšanje zasebnosti (PET[5]) je bila razvita z namenom pomagati posameznim uporabnikom pri nadzoru nad količino osebnih podatkov, ki se razkrijejo v »on-line« interakciji. Ta tehnologija obljublja, da bodo uporabniki interneta imeli nadzor nad tem, kako se zbirajo njihovi podatki. Cilj je ponovno vzpostaviti ravnovesje moči med posamezniki, ki si želijo ohraniti zasebnost, in številnimi akterji v spletnem okolju, ki želijo zbirati osebne podatke (Stalder 2002).

Tehnologije za izboljšanje zasebnosti lahko razdelimo v tri kategorije (Stalder 2002):

- zasebnost prek strežnika Proxy[6],
- zasebnost prek zavestne privolitve,
- zasebnost prek neizsledljivosti.

Goldberg je orodja za izboljšanje zasebnosti na internetu razdelil v štiri široke kategorije (Goldberg 2002, 7):

- za osebno rabo: to so produkti, kot so »spam filtri«, upravljavci piškotkov, orodja, ki blokirajo oglase, podjetniški sistemi za upravljanje na področju zasebnosti. Te produkte lahko uporabnik osebno namesti na računalnik, saj so neodvisni od zunanjih partnerjev in drugih uporabnikov sistema;
- centralni vmesnik: ta tehnologija deluje kot vmesniška storitev. Vmesnik vzdržuje strežnik, ki združuje uporabnikove zahteve. Vzdrževanje takšnega strežnika je relativno lahko, toda če ga odstranimo, uporabniki izgubijo zaščito zasebnosti. V to kategorijo spada Anonymizer[7];

[5] PET je okrajšava za Privacy-Enhancing Technologies.
[6] Proxy strežnik je strežniški program, ki ima vlogo posrednika med računalnikom in internetom v lokalnem omrežju, omogoča anonimno brskanje po internetu, saj navidezno zakrije IP računalnika.
[7] Anonymizer je anonimni strežnik, ki poskuša aktivnosti na internetu narediti neizsledljive, ščiti osebne podatke s tem, da skriva identifikabilne podatke o računalniku.

- distribuiran vmesnik: tehnologija v tej kategoriji deluje na principu sodelovanja več različnih vmesnikov. Ta tehnologija je v primerjavi s posamičnimi vmesniki bolj zanesljiva, toda tudi dražja. Sem sodijo Remailer, Crowds[8] in Freedom Network[9];
- zahtevana podpora strežnika: ta kategorija vsebuje tehnologijo, ki potrebuje sodelovanje ne samo vmesnikov, ampak tudi vseh strežnikov, s katerimi želi uporabnik opraviti zasebno transakcijo. Primer te tehnologije je e-cash[10].

Simone Fischer-Hübner pa je tehnologijo za izboljšanje zasebnosti, imenovano tudi PET, razdelila v tri skupine (Fischer-Hübner 2003):

- PET za zaščito uporabnikove identitete:
  - zaščita na komunikacijski ravni: DC nets[11], MIX nets[12], MIX net aplikacije, kot so Anonymous Remailers, Onion Routing[13], Freedom network, Crowds;
  - zaščita na sistemski ravni: anonimni sistemski dostop s kontrolo, ki temelji na elektronskem certifikatu;
  - zaščita na aplikacijski ravni: slepi digitalni podpis, E-cash, anonimni plačilni protokoli;
  - zaščita uporabnikove identitete in nadzornih sledi: psevdonimno nadzorovanje.
- PET za zaščito uporabnika, ki so mu podatki posredovani: inferenčna kontrola za sisteme statističnih baz podatkov, podatkovno rudarjenje za ohranjanje zasebnosti.
- PET za zaščito osebnih podatkov: P3P[14], formalni model zasebnosti za nadzor dostopa, poslovna zasebnostna politika, steganografija.

[8] Ime Crowds izhaja iz ideje »zliti se z množico«. Deluje tako, da uporabnike grupira v velike in geografsko raznolike skupine (crowds), ki skupaj razrešujejo zahtevke v imenu svojih članov. Spletni strežniki ne morejo ugotoviti, od kje točno zahtevek prihaja, saj lahko izhaja od kateregakoli člana skupine.

[9] Freedom Network je prekrivno omrežje, ki deluje na principu enkripcije. S tem omogoča svojim uporabnikom, da lahko opravljajo vrsto psevdonimnih aktivnosti na internetu, saj pred prisluškovalci skriva resnični IP računalnika, e-mail naslov ter druge identifikabilne podatke.

[10] E-cash je bil posebej izdelan za potrošnike in spletno poslovanje, za varno spletno nakupovanje in posredovanje informacij.

[11] Okrajšava za Dining-Cryptographer networks. DC nets obravnavajo problem analize prometa na internetu, zagotavljajo, da tudi opazovalec, ki ujame vsak paket, ne more določiti njegovega izvora.

[12] MIX nets zagotavljajo težko sledljivo komunikacijo, saj uporabljajo verigo strežnikov Proxy, vsako sporočilo je za vsak Proxy šifrirano, pri tem je uporabljen javni ključ.

[13] Onion Routing je tehnika anonimnega sporočanja prek računalniškega omrežja. Sporočila so večkrat šifrirana in nato poslana skozi več omrežnih vozlišč, imenovanih Onion routers. Vsak Onion router odstrani plast šifriranja in pošlje sporočilo do naslednjega usmerjevalnika, kjer se to ponovi.

Kot vidimo, so različni avtorji orodja za zaščito zasebnosti različno klasificirali, Darja Praprotnik pa je klasifikacijo poenostavila ter poznane mehanizme in tehnologijo za zaščito zasebnosti razdelila v tri sklope, zato bom tudi v nadaljevanju uporabljala njeno klasifikacijo (Praprotnik 2006, 42):

- mehanizmi za zaščito podatkov (kriptografija, steganografija),
- zaščita z zagotovitvijo anonimnosti in psevdonimnosti (zaščitnik identitete, zaupni centri, anonimni strežnik, ponovni pošiljatelj, Freenet, Crowds),
- zaščita zasebnosti s privolitvijo (P3P, upravitelj piškotkov).

V nadaljevanju diplomskega dela bom iz vsake skupine orodij za zaščito zasebnosti opisala nekaj orodij, ki so med uporabniki najbolj poznana in razširjena.

3.1 Mehanizmi za zaščito podatkov

3.1.1 Kriptografija

Bolj znan in učinkovit način zaščite zasebnosti omogoča kriptografija. Kriptografija je veda o šifriranju, zakrivanju sporočil in razkrivanju šifriranih podatkov. Na ta način prisluškovalcu, ki sporočilo prestreže, preprečimo dostop do vsebine.

Sporočilo, ki ga hoče pošiljatelj poslati, najprej s pomočjo šifrirne metode zašifrira ter nato zašifriranega pošlje. Četudi kdo sporočilo prestreže, mu to ne pove nič, saj ga ne more dešifrirati. Prejemnik pa po prejemu šifriranega sporočila z dešifrirno metodo sporočilo dešifrira ter ga prebere (Praprotnik 2006, 43).

Poznamo več vrst kriptografije, simetrično in asimetrično šifriranje ter zgostitvene algoritme. Šifriranje se ne uporablja samo za skrivanje vsebine elektronskih sporočil, ampak tudi za datoteke in disketne pogone. Pri uporabi šifriranja je zelo pomembno, katero kriptografsko metodo uporabljamo. Velikokrat določene metode v tajnosti razvijejo neznana podjetja, zato jim ni ravno mogoče zaupati (Kovačič 2003, 64).

[14] P3P ali Platform for Privacy Preferences Project je protokol, ki internetnim stranem daje možnost, da lahko razglasijo, za kakšne namene zbirajo podatke o uporabnikih, medtem ko ti brskajo po internetu.

3.2 Zaščita z zagotovitvijo anonimnosti in psevdonimnosti

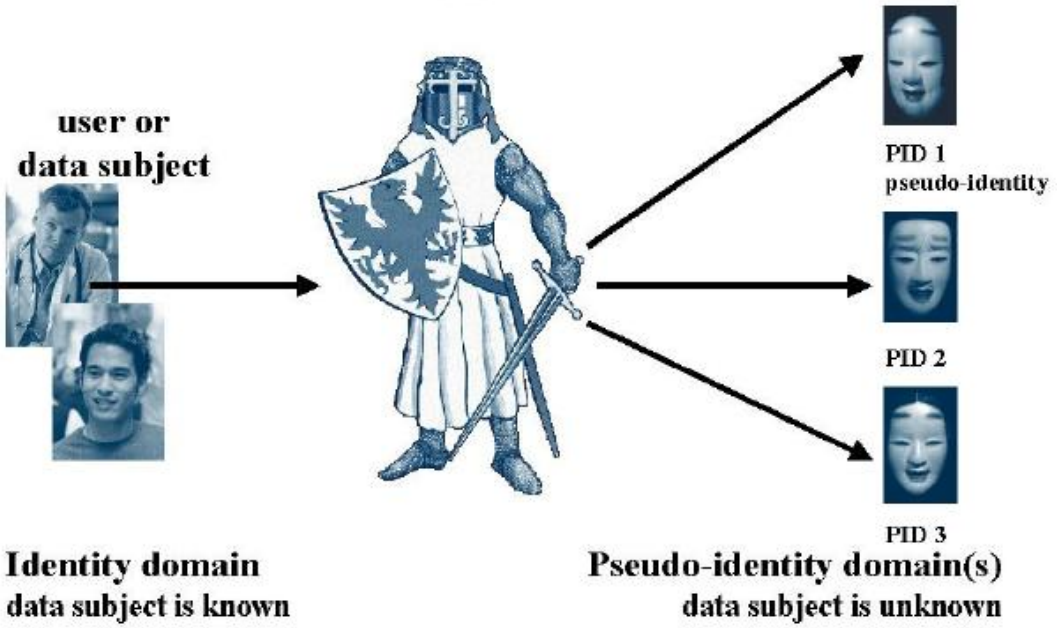
Ena od zaščit zasebnosti na internetu je anonimizacija. Popolna anonimizacija ni mogoča, saj mora uporabnik že na začetku, ko zaprosi za dostop do interneta, s ponudnikom skleniti pogodbeno razmerje, kjer pa anonimnost ni mogoča. Zato anonimizacija pride bolj v poštev pri obiskovanju spletnih strani kot pa za anonimno uporabo interneta (Kovačič 2003, 62).

Pri anonimizaciji si lahko pomagamo z različnimi orodji. Pri pošiljanju elektronske pošte uporabljamo posebne strežnike, ki izbrišejo podatke o izvoru elektronskega sporočila (ponovni pošiljatelj ali re-mailer), pri anonimnem obiskovanju spletnih strani pa lahko uporabljamo zastopniški program (anonymous proxy), ki je neke vrste vmesnik med računalnikom in internetom. Zastopniški program na internetu uporablja svoj IP naslov, zato lahko skrije identiteto pravega uporabnika, vendar pa identiteta ostane skrita samo obiskanemu spletnemu strežniku, medtem ko ponudnik interneta ali pa prisluškovalec še vedno lahko spremljata promet uporabnika (Kovačič 2003, 62).

3.2.1 Zaščitnik identitete (Identity Protector)

Zaščitnik identitete je v informacijskem sistemu uporabljen, da spremeni identiteto vpletenega subjekta (oseba, katere podatki se procesirajo) v eno ali več psevdoidentitet.
Namestitev zaščitnika identitete priskrbi vsaj dve različni domeni v okviru informacijskega sistema. Na eni izmed domen je identiteta uporabnika znana ali dostopna (identitetna domena), na vsaj eni izmed domen pa to ni tako (psevdoidentitetna domena). Cilj psevdoidentitetne domene je zaščititi uporabnika pred identifikacijo na osnovi predhodno pridobljenih osebnih podatkov in obratno, zagotoviti, da se osebni podatki ne morejo zbirati na osnovi pridobljene identitete (Blarkom in drugi 2003, 34).

Slika 3.1: Zaščitnik identitete



Vir: Blarkom in drugi (2003, 37).

Zaščitnik identitete ponuja naslednje možnosti (Blarkom in drugi 2003, 34):

- generira psevdoidentitete,
- pretvarja psevdoidentitete v prave identitete uporabnika in obratno,
- pretvarja psevdoidentitete v druge psevdoidentitete,
- daje poročila in kontrolira primere, ko je identiteta odkrita,
- bori se proti prevaram in zlorabam.

3.2.1.1 Anonimni strežnik

Anonimni strežniki omogočajo uporabnikom, da vzpostavijo svoje anonimne spletne poštne predale. Vsakemu anonimnemu računu je dodeljena unikatna identifikacijska številka. Tako se uporabniki lahko odzivajo na anonimna elektronska sporočila. Takšni strežniki omogočajo poleg vzpostavitve elektronskega poštnega predala tudi nekatere druge aktivnosti, kot so novičarske skupine (Usenet) ter aktivnosti, vezane na brskanje po spletu (Macaulay 2002, 9).

Slika 3.2: Primer ponudnika anonimnega strežnika

Vir: Anonymizer.com (2011).

Princip anonimnih strežnikov je preprost: pri ponudniku internetnih storitev, ki mu zaupamo, odpremo uporabniški račun. Uporabniku je zagotovljeno, da njegovih osebnih podatkov ne bodo posredovali drugim strankam ali jih uporabljali za marketinške namene. Tako lahko uporabnik anonimno in brez strahu brska po internetu. Anonimni strežnik spada v skupino orodji za zaščito zasebnosti , ki se imenuje »Anonymizer«. Sem lahko prištejemo še strežnike proxy in požarne zidove (firewall), ki prav tako predstavljajo pregrado med računalnikom in internetom. Komunikacijo dovoljujejo le pod določenimi pogoji, nekatere vrste komunikacije pa lahko popolnoma blokirajo, na primer požarni zid ščiti omrežje pred neavtoriziranim dostopom, strežnik proxy pa je lahko nastavljen za blokiranje elektronskih piškotkov in neželene pošte (junk mail) (Seničar in drugi 2003, 154).

3.2.2 Ponovni pošiljatelj (re-mailer)

Ponovni pošiljatelj ali re-mailer je program, ki sprejme elektronsko pošto, očisti informacije, ki bi lahko identificirale izvor sporočila, ter sporočilo posreduje naprej določenemu prejemniku. Stopnja zasebnosti je odvisna od zanesljivosti ponudnika, saj kdor

re-mailer nadzoruje, ima dostop do identitet pošiljateljev in prejemnikov (Seničar in drugi 2003, 154).

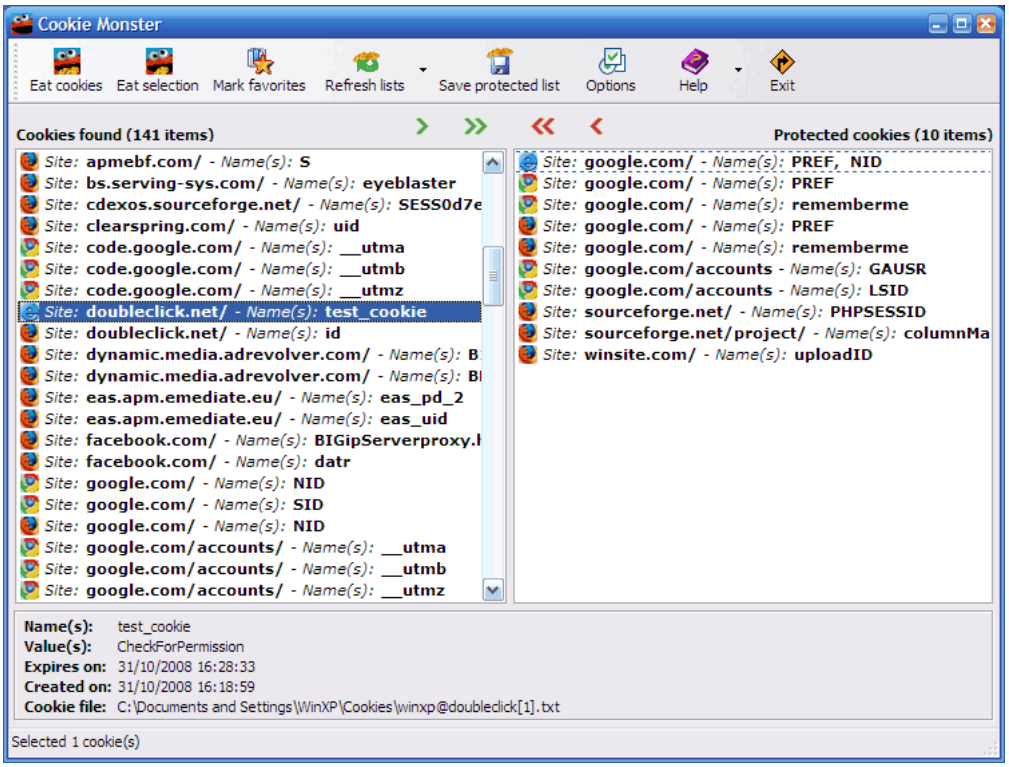
3.3 Zaščita zasebnosti s privolitvijo

3.3.1 Upravitelj piškotkov (cookie management)

Piškotki so podatkovne datoteke HTML. Shranjene so na računalniku, tja pa jih namesti oddaljeni spletni strežnik, ki ga je uporabnik obiskal z uporabo spletnega brskalnika. Piškotki so lahko uporabljeni na načine, ki predstavljajo zlorabo osebnih informacij. Pogosto so v piškotkih shranjene informacije občutljive narave, kot so razna gesla in podatki o kreditni kartici, ki prosto prehajajo po internetu. Eden izmed načinov nadzora nad piškotki je Cookie management. Ta orodja omogočajo (Seničar in drugi 2003, 153–154):

- onemogočanje elektronskih piškotkov - piškotkom preprečujejo, da bi se shranili na računalnik;
- selektivno sprejemanje elektronskih piškotkov - uporabniku omogoča izbiro, od koga bodo prejeli piškotke;
- pregled datotek elektronskih piškotkov - uporabniku omogoča, da lahko preišče vsebino piškotka.

Slika 3.3: Orodje za upravljanje s piškotki - Cookie Monster



Vir: Ampsoft.net (2011).

4 NADZOR NA INTERNETU

Če želimo uravnavati in načrtovati življenja ljudi, potem moramo o njih imeti ustrezne informacije, zato veliko organizacij zbira podatke o ljudeh in njihovih aktivnostih, te informacije pa organizacijam služijo kot feedback (Kovačič 2000, 1020). Nadzor je tesno povezan predvsem z informacijsko tehnologijo, ki je namenjena zbiranju in obdelavi različnih podatkov, ter s komunikacijsko tehnologijo, ki je po mnenju Thomasa zajela vse vidike človeške komunikacije, saj naj bi posredovala skoraj vsako obliko človeških odnosov (Thomas v Kovačič 2006, 28).

Lahko bi rekli, da sta ugodne pogoje za nadzor in razkrivanje osebnih podatkov na internetu ustvarila Googlova tehnologija in infrastruktura Web 2.0. Infrastruktura Web 2.0 je vzpodbujala posameznike, da uporabljajo nove tehnologije interneta, si z njimi organizirajo in izmenjujejo informacije, komunicirajo znotraj skupnosti ter se na ta način

izražajo. Obljubljala je ustvarjalnost, demokratizacijo medijske produkcije in vzpodbujala izražanje individualnosti s sodelovanjem v socialnih omrežjih (Zimmer 2008b). Googlov cilj pa je bil organizirati svetovne informacije, jih narediti univerzalno dostopne in uporabne ter ustvariti popoln brskalnik, ki bo zagotavljal samointuitivne, poosebljene in ustrezne rezultate. Neizogibna kombinacija Googlovih produktov za iskanje informacij in infrastrukture Web 2.0 je zajela le najboljše iz obeh tehničnih sistemov. Z zajemanjem pretoka informacij prek Web 2.0 lahko iskalniki bolje predvidevajo potrebe uporabnikov in zagotovijo ustreznejše ter bolj smiselne rezultate. Da bi dobili popoln iskalnik, je moral iskalnik pridobiti popoln priklic posameznega iskalca. Za popoln priklic pa je moral spletni iskalnik razumeti intelektualne želje in potrebe iskalca, medtem ko ta išče informacije na spletu. Primarno sredstvo za iskalnike, da obdržijo popoln priklic, je spremljanje in sledenje uporabnikovim iskalnim navadam in zgodovini. Večina spletnih iskalnikov na strežniku vodi natančno evidenco ogledanih spletnih strani, iskalnih nizov, ki so bili posredovani iskalniku, ter klikov na najdene rezultate. Uporabnike Web 2.0 vzpodbuja, da na spletu, kolikor je to mogoče, objavijo čim več iz svojega življenja (Zimmer 2008a). Web 2.0 s tem prinaša tudi cel kup nepredvidenih posledic, kot so povečan pretok osebnih informacij po omrežjih, pojav močnih orodij za nadzor nad uporabniki, izkoriščanje osebnih informacij za komercialno korist ter strah pred povečanim sodelovanjem korporacij v spletnih socialnih omrežjih (Zimmer 2008b). Velik del prostega pretoka podatkov med spletnimi stranmi Web 2.0 in storitvami vsebuje osebne podatke, ki, ko jih zajamejo spletni brskalniki, predstavljajo grožnjo informacijski zasebnosti na spletu (Petersen v Zimmer 2008b).

Spletna socialna omrežja dovoljujejo visoko stopnjo nadzora. Ustvarjajo skladišče, kjer se shranjujejo osebne informacije. To skladišče je vztrajno ter se kopiči. Namesto da bi se stare informacije zamenjale z novejšimi, se spletni dnevniki le arhivirajo ter omogočajo pregledovanje vnosov (Barnes 2006).

Organizacija Privacy Rights Clearinghouse ugotavlja, da ne obstaja nobena spletna aktivnost, ki bi omogočila popolno zasebnost. Qiang Alex Zhao navaja nekatere elemente, ki ogrožajo zasebnost posameznikov, in to so: sledenje (kje se nekdo nahaja), prisluškovanje (prestrezanje komunikacij), snemanje brez dovoljenja, identificiranje posameznikov in njihovih aktivnosti ter zaznavanje podrobnosti delovanja. Vsi ti načini

ogrožanja zasebnosti obstajajo tudi na internetu, in sicer z obstojem razpršenih arhivov ter informacij o posameznikih, ki jih je mogoče povezovati, s puščanjem elektronskih sledi, prestrezanjem elektronskih komunikacij ter vdiranjem v računalniške sisteme (Kovačič in Vehovar 2000).

Uporabniki interneta se ne zavedajo, da zasebnost na internetu ni več ogrožena samo neposredno z vdori v računalniške sisteme, vendar gre čedalje bolj za nadzor nad osebnimi podatki in izdelavo uporabniških profilov. Gre torej za bolj prefinjeno in posredno ogrožanje zasebnosti, ki pa ima velik tržni potencial in ki bo zaradi svoje množičnosti v prihodnosti postajalo bolj nevarno (Kovačič in Vehovar 2000).
Povprečni uporabniki pa prav tako niso seznanjeni z obstojem datotek aktivnosti ali »log files«, kjer se avtomatsko vpisujejo aktivnosti uporabnikov interneta (Kovačič 2000, 1026).
James Rule ugotavlja, da za sodobne sisteme nadzora predstavljajo omejitev le štirje dejavniki. To so velikost datotek, ki jih sistem lahko shranjuje, stopnja, do katere so lahko ti sistemi centralizirani, hitrost pretoka podatkov in informacij ter število stičnih točk med sistemom in subjektom (Lyon v Kovačič 2006, 29).

Interes za zbiranje in shranjevanje informacij imajo različni subjekti, država uporablja nadzor za zagotavljanje zunanje in notranje varnosti, kapitalistične korporacije pa skušajo čim bolj ugotoviti potrošnikove želje ter jim prilagoditi ponudbo. Zato se nadzor pojavlja v obliki »nadzorovanja ljudi«, ki ga v glavnem uporablja država, ter v obliki »zbiranja podatkov« v namene potrošniškega nadzorovanja (Lyon v Kovačič 2003, 23). V interesu države je, da varuje svoje meje in interese, zato načrtno zbira informacije o vsem, kar bi lahko ogrožalo njene meje in interese. Vendar pa povečan nadzor lahko hitro vodi v totalitarizem, zato mora demokratična država doseči pravo razmerje med nadzorom in zasebnostjo posameznika (Raab v Kovačič 2000, 1020).

Nissenbaum deli zaskrbljenost zaradi novih tehnologij v tri kategorije:

- nadzorovanje in sledenje,
- razširjanje in objavljanje,
- združevanje in analiziranje.

Prva kategorija vključuje zaskrbljenost razširjene nadzorne tehnologije, kot so elektronsko cestninjenje, sistemi za prepoznavanje obraza, spletni piškotki in vedenjsko oglaševanje. Za drugo kategorijo lahko rečemo, da je širjenje komunikacijskih omrežij in digitalnih informacij ustvarilo okolje, v katerem so osebni podatki dostopni z večjo lahkoto kot kdajkoli prej. Ko informacije postanejo digitalizirane, so praktično nepopravljive in se lahko prestrezajo ali kupujejo za komercialne, vladne ali tržne namene. Tretja kategorija vključuje velike podatkovne baze, ki dajejo možnost, da se v zasebnost posameznika lahko posega na obsežnejše in novejše načine (Nissenbaum v Marwick in drugi 2010, 7–8).

4.1 Datoteke aktivnosti (log files)

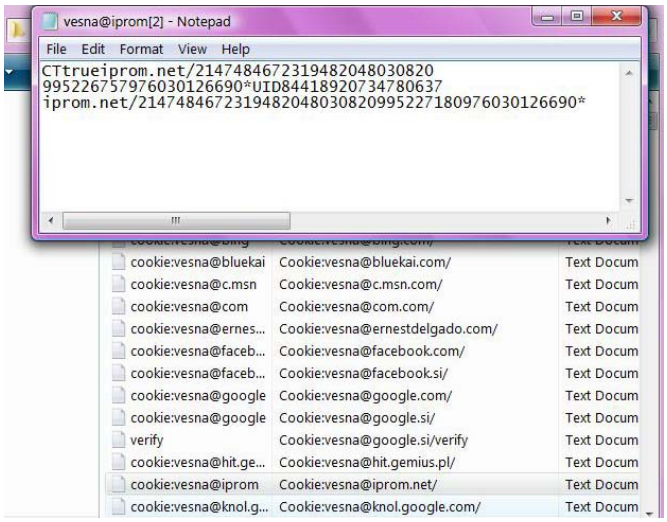
Poleg datotek aktivnosti, ki jih vzdržujejo ponudniki interneta, obstajajo tudi datoteke aktivnosti, ki jih vzdržujejo ponudniki različnih internetnih strani. Datoteke aktivnosti ponudnikov spletnih storitev zapisujejo čas in vrsto storitve, ki so jo uporabniki opravili, ter določene identifikacijske podatke, kot je na primer IP uporabnika. Poleg tega se lahko zapisujejo še nekatere spremenljivke o obiskovalčevem virtualnem okolju, kot so tip spletnega brskalnika, operacijski sistem, vrsta vključenih jezikovnih podpor, podatki, iz katere spletne strani je obiskovalec prišel na to stran itd. S pomočjo teh identifikacijskih podatkov načeloma ni mogoče ugotoviti prave identitete uporabnika, v nekaterih primerih tudi ni mogoče razlikovati med različnimi računalniki. Nekatere od zgoraj naštetih podatkov je mogoče spremeniti ali celo izbrisati, toda večina uporabnikov s tem ni seznanjena. Nekateri spletni brskalniki pa so bolj »klepetavi« kot drugi, na primer Microsoft Internet Explorer pošilja spletnim stranem nekoliko več podatkov o uporabniku kot pa drugi (Kovačič 2003, 45).

Podatki iz datotek aktivnosti se najpogosteje uporabljajo za ugotavljanje števila obiskov na posamezni spletni strani. Ti podatki so posebej pomembni za spletne strani, ki oglašujejo, saj je zaslužek od oglaševanja navadno povezan s številom obiskovalcev. Podatki o obiskih spletnih strani pa so pomembni tudi za spletne trgovine. Iz teh podatkov namreč ni mogoče izvedeti samo, katere proizvode je neki uporabnik kupil, temveč tudi to, katere si je ogledal, iz tega pa je mogoče ugotoviti potrošniški profil (Kovačič 2006, 148).

4.2 Elektronski piškotki (cookies)

Elektronski piškotki ali tako imenovani »cookies« so majhni paketi podatkov, ki jih spletni strežnik pošlje spletnemu brskalniku. S pomočjo elektronskih piškotkov spletni strežnik ob obisku nekega uporabnika lahko ugotovi, ali je uporabnik na tej strani že bil in kaj je na njej počel. Nekateri strežniki elektronske piškotke uporabljajo za sledenje uporabnikom na druge strežnike, lahko pa tudi ugotovijo uporabnikovo identiteto. Piškotki so bili sicer razviti z namenom, da omogočijo spletne nakupne košarice, danes pa so uporabljeni na vseh možnih spletnih straneh (Kovačič 2000, 1025). Uporaba piškotkov se je močno razširila, ko so ugotovili, da se en sam piškotek lahko uporablja na mnogih različnih spletnih straneh. To je pripeljalo do razvoja podjetij z oglaševalsko mrežo, ki lahko uporabnikom sledijo na tisoče spletnih straneh. Največji oglaševalski servis je podjetje »DoubleClick«, ki ima dogovore sklenjene z več tisoč spletnimi stranmi in vzdržuje piškotke več kot milijona uporabnikov (Laurant 2003).

Slika 4.1: Primer elektronskega piškotka

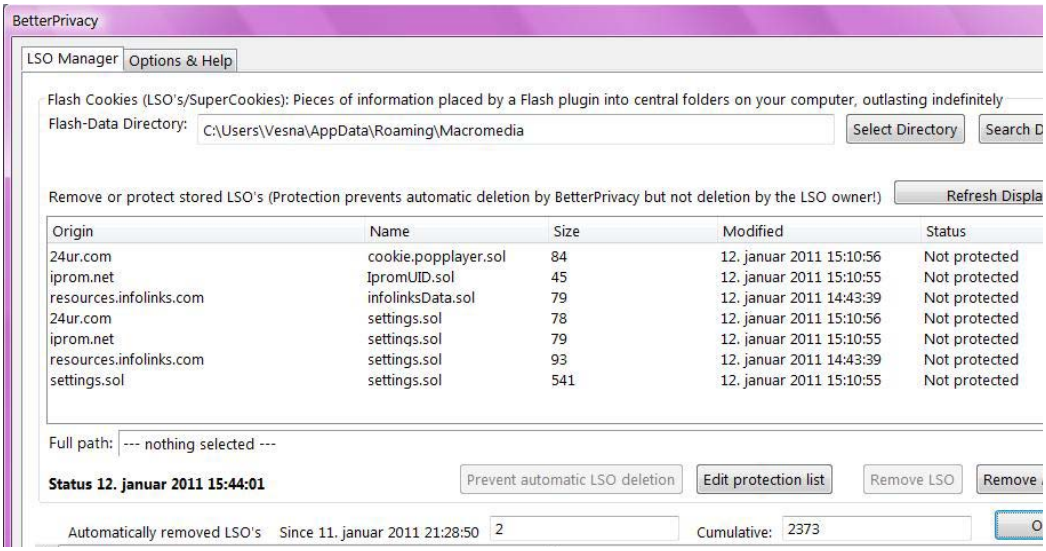


Do nedavnega smo uporabniki interneta piškotke, shranjene v naših spletnih brskalnikih, še lahko nadzorovali in jih občasno tudi izbrisali, zato so oglaševalski servisi, da bi zaščitili svoje interese, razvili nove, »superpiškotke« ali tako imenovane »Flash piškotke[15]«.

[15] Strokovno imenovani Local Shared Objects ali na kratko LSO.

Značilnost teh piškotkov je, da se ne izbrišejo tako lahko kot navadni piškotki, saj ko uporabnik briše piškotke, s tem ne izbriše tudi »Flash piškotkov«. Ob ponovnem obisku spletne strani lahko spletni strežnik s pomočjo »Flash piškotkov« identificira uporabnika in ugotovi, ali je ta izbrisal navadne piškotke. Spletni strežnik izbrisane piškotke lahko ponovno pošlje uporabniku. Tudi nekatere znane slovenske spletne strani uporabljajo »superpiškotke«, a uporabnikov o tem ne obveščajo (Kovačič 2009a).

Slika 4.2: Primer superpiškotkov



Evropska unija je leta 2002 sprejela Direktivo o zasebnosti in elektronskih komunikacijah 2002/58/EC, ki v 24. točki še posebej izpostavlja problem zbiranja osebnih podatkov s pomočjo piškotkov. Direktiva določa, da mora uporabnik imeti možnost zavrnitve piškotkov, hkrati pa mora biti seznanjen s tem, kakšne informacije o njem zbirajo spletni strežniki s pomočjo spletnih piškotkov (Kovačič 2009b).

V evropskem pravnem prostoru sta se glede zbiranja osebnih podatkov in prejemanja reklamnih e-sporočil uveljavili dve načeli. Prvo je načelo privolitve ali tako imenovano »opt-in«, ki zahteva vnaprejšnje soglasje uporabnika, drugo načelo pa je načelo odjave ali »opt-out«, ki uporabniku daje možnost odjave ali prepovedi. V uporabi je predvsem načelo soglasja, torej »opt-in«, le pri spletnih piškotkih to ni tako, saj uporabnik niti nima možnosti privolitve o uporabi spletnih piškotkov. Pri spletnih piškotkih se osebni podatki

zbirajo, vse dokler jih uporabnik ne onemogoči ali izbriše. Problem predstavljajo tudi »superpiškotki«, saj nad njimi uporabnik nima takšne kontrole kot nad običajnimi (Kovačič 2009b).

4.3 Smetje ali »spam« pošta

Izraz smetje ali »spam« označuje nezaželeno oziroma nenaročeno elektronsko pošto, pri čemer gre večinoma za oglasna elektronska sporočila za namen neposrednega trženja (Kovačič 2006, 158–161). Mnoga internetna podjetja dobavljajo drugim podjetjem, ki so specializirana za pošiljanje nezaželene komercialne e-pošte, sezname e-naslovov svojih strank. Nekatera podjetja pa e-naslove izvrtajo iz različnih virov, kot so sporočila, objavljena na »mailing« listah, novičarske skupine ali podatki o registraciji imena domene. »American Federal Trade Commission« je ugotovil, da e-naslov, ki se objavi v klepetalnici, prične prijemati »spam« pošto v osmih minutah od objave tega e-naslova (Laurant 2003).

V Sloveniji je leta 1997 pričel delovati Imenik elektronske pošte Slovenije, kjer je bilo zbranih 15.000 elektronskih naslovov, ki so bili javno objavljeni na slovenskih spletnih straneh. Slovenski uporabniki interneta so se škodljivosti tega zavedali šele, ko so jim razna marketinška podjetja na njihovo elektronsko pošto začela pošiljati reklamna sporočila ali tako imenovano »spam pošto« (Kovačič 2000, 1024).

»Spam« pošta je resen problem interneta, saj so raziskave pokazale, da se količina takih sporočil veča. Leta 2003 je obsegala že več kot 50 odstotkov vseh sporočil, kar bi utegnilo celo uničiti uporabnost elektronske pošte. »Spam« ne vdira v zasebnost neposredno, v smislu nadzorovanja, vendar pa posega v zasebnost v smislu pravice biti puščen pri miru, torej v tisti del zasebnosti, ki posamezniku omogoča, da se umakne iz družbe (Kovačič 2006, 158–161).

Področje neposrednega trženja in s tem posledično področje nezaželene elektronske pošte v Sloveniji regulirajo kar štirje zakoni: Zakon o elektronskih komunikacijah, Zakon o varstvu potrošnikov, Zakon o elektronskem poslovanju na trgu ter Zakon o varstvu osebnih

podatkov. »Če povzamemo vsebino vseh naštetih zakonov, lahko izluščimo ven tri osnovna načela neposrednega trženja: pošiljatelj mora predhodno pridobiti soglasje vsakega naslovnika, naslovnik ima pravico kadarkoli zavrniti nadaljnjo uporabo svojega elektronskega naslova, pošiljatelj mora pri obdelavi osebnih podatkov upoštevati Zakon o varstvu osebnih podatkov« (Informacijski pooblaščenec).

4.4 Vohunska programska oprema ali »spyware«

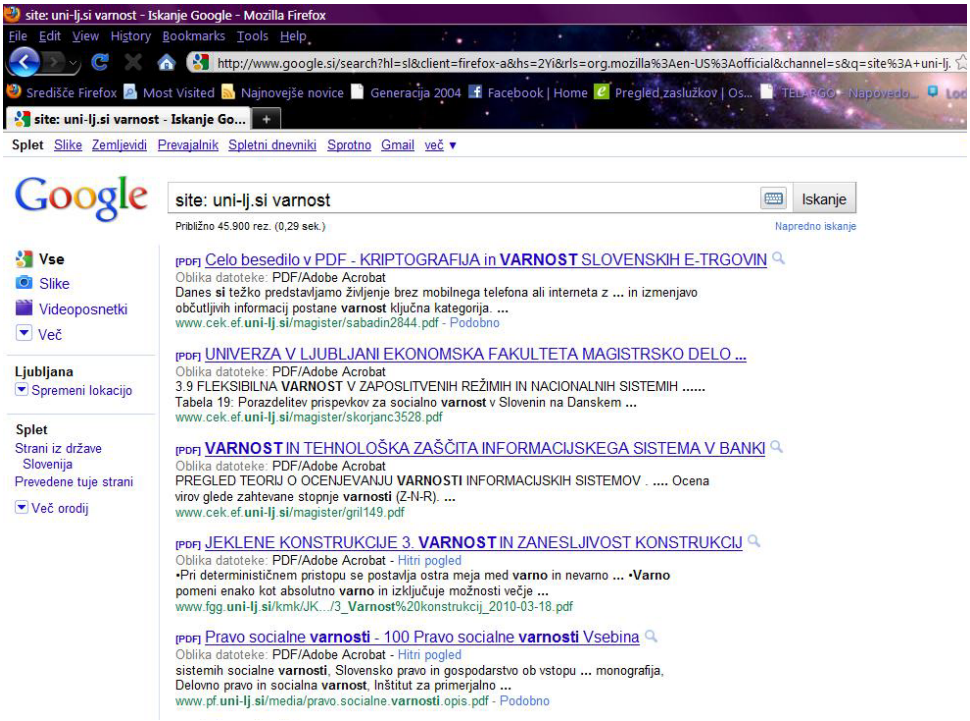
Še ena izmed tehnologij za sledenje uporabnikom interneta je »spyware«. To je invazivna programska oprema, ki drugim prenaša naše brskalne navade ali osebne podatke. Nekatere vrste »spywarea« so uporabljene komercialnemu profiliranju in so namenjene posredovanju oglasov ciljnim skupinam uporabnikov interneta. Druge vrste programov»spyware« pa so znane kot metode vohunjenja za posamezniki. Spyware je tudi pogosto povezan s krajo identitete. Vohunsko programsko opremo je pogosto težko določiti, saj lahko celo legitimna programska oprema poseduje značilnosti »spywarea«. »Spyware« je pogosto povezan z drugimi programi. Ko uporabnik prenese in naloži tak program, pogosto niti ne ve, kakšne zmogljivosti sledenja ima (Rotenberg 2006).

4.5 »Google hacking«

»Google hacking« je izraz, ki se nanaša na sposobnost, da z uporabo spletnega iskalnika Google ustvarjamo kompleksne iskalne poizvedbe, s katerimi lahko najdemo ranljive spletne strani, ki so dovzetne za vdore in na katerih je možno poiskati zasebne ter občutljive informacije o drugih, skrite delce datotek ali informacije, s katerimi se »hacker« lahko okoristi. Iskalni izraz »*site:«*, ki ga vtipkamo v Google, je neprecenljiv v vseh usmerjenih Googlovih iskanjih. Skupaj še z imenom domene se iskanje omeji na strani znotraj določene domene. Na primer, če vpišemo iskalni izraz »*site: uni-lj.si varnost«,* bomo našli vse strani, ki vsebujejo besedo varnost znotraj domene ».uni-lj.si«. Če želimo najti točno določen tip dokumenta, potem bomo v Google vpisali iskalni niz »*filetype: pdf varnost«,* Google pa nam bo našel vse pdf dokumente, ki vsebujejo besedo varnost. Obstaja še

ogromno iskalnih nizov, ki nam pomagajo pri iskanju točno določenih informacij. Lahko najdemo celo gesla in uporabniška imena, kar le še potrjuje to, kako ogrožena je naša zasebnost na internetu (Google Hacking Lab 2010).

Slika 4.3: Primer iskanja spletne strani z vsebino o varnosti znotraj domene uni-lj.si



Vir: Google.si (2011).

5 OBSTOJEČE EMPIRIČNE RAZISKAVE

Kot sem že omenila, sta bili na temo razkrivanja osebnih podatkov na internetu v Sloveniji opravljeni dve podobni raziskavi. Matej Kovačič je leta 1999 opravil raziskavo »Slovenski uporabniki interneta in zasebnost[16]«. Kovačič je v tej raziskavi lahko potrdil dve od osmih hipotez, ena izmed potrjenih hipotez pa je bila tudi ta: »Bolj in dlje kot posameznik uporablja internet, bolj je tehnološko informiran, bolj pozna šibke točke tehnologije«, kar se zdi tudi logično. Kovačič za to raziskavo pravi, da je vzorec, uporabljen v nalogi, zelo

[16] Sodelovalo je 198 uporabnikov interneta, zbiranje podatkov je potekalo prek interneta s pomočjo CAWI »Computer Assisted Web Interviewing«.

majhen, poleg tega pa še neverjetnosten. Zajema tudi dokaj specifično skupino posameznikov, zbrani rezultati pa naj bi kazali na dokaj visoko stopnjo zavedanja o pomenu zasebnosti. Internetna tehnologija se hitro spreminja in razvija, zato bi bilo treba opraviti novejšo raziskavo z večjim vzorcem.

Raziskava »Pomen zasebnosti med slovenskimi uporabniki interneta[17]«, ki jo je za svojo magistrsko nalogo opravila Darja Praprotnik, je novejša, opravljena je bila v letu 2006. Darja Praprotnik je v svoji raziskavi prišla do ugotovitev, da je slovenskim uporabnikom interneta zasebnost pomembna, vendar pa glede nje ne izražajo neke panične zaskrbljenosti. Ljudje osebnih podatkov na internetu ne razkrivajo radi, najbolj čuvajo številke kreditnih kartic, bančnega računa, podatke o svojem zdravju in EMŠO, največkrat pa razkrijejo ime in priimek ter elektronski naslov. Ugotovila je tudi, da so uporabniki interneta zelo dobro poučeni o grožnjah zasebnosti, ki jih prinaša internet. Zavedajo se, da je možno prestreči elektronsko pošto, ukrasti gesla, številke kreditnih kartic, ugotoviti, katere spletne strani obiskujejo, ugotoviti IP računalnika. Vse to ve prek 80 odstotkov uporabnikov, zdi pa se jim malo verjetno, da je možno ugotoviti njihovo fizično identiteto. Darja Praprotnik pravi, da rezultati kažejo na slabo poučenost uporabnikov o delovanju interneta. Tehnologijo za izboljšanje zasebnosti uporabniki poznajo slabo, največ jih pozna požarni zid. S to raziskavo je potrdila hipotezo, da je uporabnikom interneta zasebnost pomembna, zavedajo se groženj, premalo pa poznajo in uporabljajo tehnologijo za zaščito zasebnosti.
Darja Praprotnik podatkov iz svoje raziskave ni analizirala z nobeno analizo, ki bi lahko potrjevala zanesljivost indikatorjev ali pa vsaj preverila postavljeno hipotezo. V tej magistrski nalogi je mogoče zaslediti le tabele s frekvencami in odstotki, zato se pojavi tudi vprašanje, ali je zastavljena hipoteza res veljavna.
Čeprav je raziskava dokaj sodobna, bi lahko še bolj posodobili nekatere indikatorje. Tudi sama sem pobrskala po različnih spletnih straneh ter ugotovila, katere podatke te spletne strani od nas sploh želijo.
Čeprav se v svojem delu osredotočam na situacijo v Sloveniji, pa se mi zdi vseeno vredno omeniti raziskavo, ki jo je leta 2007 izvedel Urad informacijskega pooblaščenca v Veliki

[17] Raziskava je potekala med uporabniki interneta, starejšimi od 15 let, sodelovalo je 112 oseb od tega je 76 anketirancev sodelovalo v terenski anketi in 36 v elektronski.

Britaniji, saj proučuje, v kolikšni meri mladostniki v Veliki Britaniji razkrivajo svoje osebne podatke v socialnih omrežjih na internetu. Kot odgovor na zaskrbljujoče ugotovitve ponuja tudi nekaj nasvetov, kako zaščititi zasebnost mladostnikov. V raziskavi je sodelovalo 2000 mladostnikov starih od 14 do 21 let. Več kot polovica anketirancev ni nikoli pomislila, da so informacije, ki jih objavijo na internetu, lahko trajne ter dostopne tudi v prihodnosti. Sedem odstotkov mladostnikov meni, da zasebnostne nastavitve v njihovih profilih niso tako pomembne. Iz osebnih podatkov, ki jih mladostniki puščajo na ogled drugim, pa so ugotovili, da jih 60 odstotkov objavlja svoj datum rojstva, četrtina jih objavlja svoj zaposlitveni status ter eden od desetih objavi svoj domači naslov. Kar tretjina anketirancev ni še nikoli prebrala izjave o posredovanju osebnih podatkov na straneh s socialnimi omrežji. Ko so bili mladostniki vprašani, kaj menijo o spletnih straneh, ki bi potencialno lahko uporabljale njihove objavljene osebne podatke v marketinške namene ali pa jih celo posredovale drugim organizacijam, pa je kar 95 odstotkov anketirancev izrazilo zaskrbljenost (Information Commissioner's Office 2007).

Na podlagi teh zaskrbljujočih ugotovitev je Urad informacijskega pooblaščenca v Veliki Britaniji objavil nekaj nasvetov, kako zavarovati svojo zasebnost na internetu (Information Commissioner's Office 2007):

- Blog je za vse življenje. To si je vredno zapomniti, preden za seboj pustite elektronsko stopinjo. Če nočete, da nekaj obstaja tudi v prihodnosti, potem ne objavite.
- Zasebnost je dragocena. Izbirajte le strani, ki vam omogočajo kontrolo vidljivosti vašega profila in vaših osebnih informacij, preberite izjavo o posredovanju osebnih podatkov.
- Vaša osebna varnost je na prvem mestu. Nikoli ne razkrivajte, kje se nahajate in kje živite.
- Zaščitite se z geslom, jih redno menjajte ter kot geslo ne uporabljajte očitnih besed.
- Varujte svoj e-naslov ter za spletne strani s socialnimi omrežji uporabljajte dodaten e-naslov.

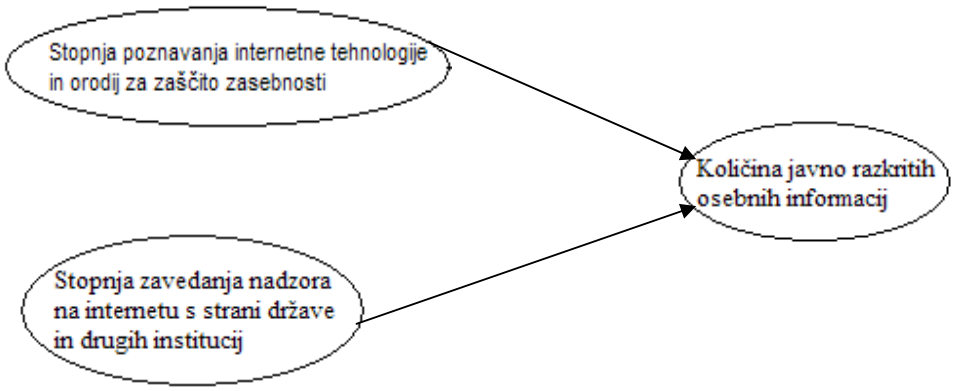
- Vaš sloves je pomemben. Kar se sedaj zdi zabavno vam in vašim prijateljem, se morda ne bo zdelo zabavno vašim učiteljem in bodočim delodajalcem ali celo vam v prihodnosti.

6 RAZISKOVALNI OKVIR

Različni avtorji vseskozi poudarjajo, da se uporabniki ne zavedajo dovolj nevarnosti, ki jim pretijo na internetu ter da uporabniki ne poznajo dovolj tehnologije za zaščito zasebnosti. Menim, da je bilo pred časom res tako, toda internetna tehnologija se je razvila, računalnik in internet uporablja vse več ljudi. Na tej podlagi sklepam, da se je povečala tudi stopnja osveščenosti o nadzoru na internetu. Zaradi množične uporabe Facebooka in preostalih spletnih socialnih omrežij je tudi v Sloveniji ta tema postala bolj aktualna, uporabnike se bolj opozarja na pomembnost zaščite zasebnosti na internetu, še vedno pa to področje v Sloveniji ni dovolj raziskano. V svoji raziskavi se ukvarjam z vprašanjem, *ali uporabnikova osveščenost o nadzoru na internetu in splošno poznavanje tehnologije za izboljšanje zasebnosti na internetu pripomoreta k temu, da uporabnik manj razkriva svoje osebne podatke in s tem izboljša informacijsko zasebnost.*

V diplomskem delu nastopa pojasnjevalni model s tremi spremenljivkami, dvema neodvisnima ter eno odvisno spremenljivko (glej sliko 6.1).

Slika 6.1: Pojasnjevalni model



6.1 Opredelitve pojmov

Stopnja poznavanja internetne tehnologije in orodij za zaščito zasebnosti je opredelitev, v kolikšni meri uporabnik interneta pozna oziroma uporablja orodja, ki zagotavljajo njegovo anonimnost oziroma ščitijo osebne podatke. K tem orodjem štejemo: zaščitnik identitete, požarni zid, upravitelj piškotkov, ponovni pošiljatelj, šifriranje ter še vrsto drugih orodij.

Stopnja zavedanja nadzora na internetu s strani države in drugih institucij je opredelitev, v kolikšni meri se uporabniki zavedajo, da lahko različne institucije brez njihovega izrecnega privoljenja o njih zbirajo podatke, na podlagi katerih je možno ugotoviti uporabnikove interese in želje, razkriti njihovo geografsko lokacijo, s povezovanjem podatkov pa je možno celo ugotoviti njihovo identiteto.

Količina javno razkritih osebnih informacij je opredelitev, koliko in katere lastne osebne podatke uporabnik prostovoljno javno objavlja na različnih spletnih straneh s socialnimi omrežji, kot so Facebook, Myspace itd.

6.2 Hipoteze

Hipoteza 1: *Uporabniki, ki bolj poznajo internetno tehnologijo in orodja za zaščito zasebnosti, manj javno razkrivajo svoje osebne podatke na internetu.*
Hipoteza 2: *Uporabniki, ki se bolj zavedajo nadzora na internetu, manj javno razkrivajo svoje osebne podatke.*

Člani socialnih omrežij na internetu so premalo seznanjeni z internetno tehnologijo, zato se niti ne zavedajo tega, kakšne zmožnosti pridobivanja osebnih podatkov imajo različni subjekti na internetu (Barnes 2006). Pri uporabi interneta puščamo elektronske stopinje, vendar povprečen uporabnik tega ne ve, kakor tudi ne ve, da se to ves čas nekje zbira in shranjuje. S sestavljanjem majhnih delčkov informacij pa je mogoče sestaviti celoten profil uporabnika (Praprotnik 2006, 24). Uporabniki, ki dobro poznajo tehnologijo za izboljšanje

zasebnosti, si lahko celo zagotovijo anonimnost, vendar pa so ponavadi takšna orodja plačljiva in v Sloveniji niso ravno razširjena.

Interes za zbiranje in shranjevanje informacij imajo različni subjekti, eden izmed njih pa je tudi država, saj zbira informacije o vsem, kar bi lahko ogrožalo njene meje in interese (Kovačič 2000, 1020). Spletna socialna omrežja dovoljujejo visoko stopnjo nadzora, saj ustvarjajo skladišče, kjer se shranjujejo osebne informacije. Ti arhivi pa omogočajo pregledovanje vseh vnosov (Barnes 2006). Uporabniki interneta se ne zavedajo, da gre na internetu čedalje bolj za nadzor nad osebnimi podatki in izdelavo uporabniških profilov za marketinške namene (Kovačič in Vehovar 2000). Poudariti pa moram, da v ta sklop nisem uvrstila nadzora, ki ga izvaja nevidna javnost v spletnih skupnostih, torej nadzor, ki ga uporabniki izvajajo med seboj, in to ne v smislu zbiranja osebnih podatkov za marketinške namene.

7 OPIS VZORCA IN ZBIRANJA PODATKOV

Podatki za raziskavo so bili zbrani v obdobju od 7. 6. 2010 do 18. 6. 2010. Podatke sem zbirala s pomočjo spletne ankete v programu Lime Survey. Enota raziskovanja so bili študenti Fakultete za družbene vede. V anketi so lahko sodelovali študenti vseh smeri, razen študentov smeri Družboslovna informatika, saj smatram, da so študenti te smeri preveč osveščeni o problematiki, ki jo raziskujem, saj zaradi vrste študija veliko časa preživijo pred računalnikom. Manjše število anketirancev je vabilo in povezavo do spletne ankete prejelo prek elektronske pošte, povezava za spletno anketo pa je bila objavljena tudi na spletnem forumu *Fdvjevka* ter na Facebook strani z imenom *Na Fdv Nisi Sam*.

Tabela 7.1: Opis vzorca anketirancev, n=102

Spremenljivka	vrednost	n	%
Spol	moški	19	18,6
	ženske	83	81,4
Starostni razredi	19 - 21	25	24,5
	22 - 24	51	50
	25 - 27	26	25,5
Smer študija	Komunikologija	28	27,5
	Kulturologija	13	12,7
	Novinarstvo	12	11,8
	Politologija	22	21,6
	Sociologija	27	26,5

V anketi je sodelovalo 81,4 odstotkov žensk in 18,6 odstotkov moških, starost anketirancev se giblje od 19 do 27 let, povprečna starost znaša 23,12 let, največ anketirancev (50 %) se nahaja v starostnem razredu od 22 do 24 let. Pri vprašanju o smeri študija so se pojavljali različni odgovori, nekateri so navajali točno smer, drugi pa samo krovno smer študija, zato sem vse odgovore uvrstila pod krovne smeri študija. Kot sem že omenila, družboslovni informatiki v anketi niso sodelovali, zato pod krovno smerjo Sociologija, tega programa ni. V največjem številu so na anketo odgovarjali komunikologi (27,5 %), takoj za njimi so bili sociologi (26,5 %), najmanj pa je v vzorcu novinarjev (11,8 %) (glej Tabelo 7.1).

8 REZULTATI ANALIZE

8.1 Osnovna statistična analiza podatkov

Tabela 8.1: Poznavanje in uporaba orodij za informacijsko varnost

Poznate ali pa uporabljate katero od spodaj naštetih orodij za informacijsko varnost?	**Poznam**		**Poznam in uporabljam**		**Ne poznam**	
	n	%	n	%	n	%
upravljanje s piškotki (»cookie manager«)	42	41,2	30	29,4	30	29,4
sistemi za anonimizacijo (zaščitnik identitete, anonimni strežnik, IPREDator, VPN …)	14	13,7	10	9,8	78	76,5
požarni zid (»firewall«)	27	26,5	73	71,6	2	2
šifriranje elektronske pošte (kriptografija)	26	25,5	9	8,8	67	65,7
varnostne posodobitve programov	27	26,5	63	61,8	12	11,8

Pri poznavanju orodij za informacijsko varnost se je izkazalo, da največji delež anketirancev (41,2 %) pozna, a hkrati ne uporablja orodij za upravljanje s piškotki, najmanj poznajo sisteme za anonimizacijo (13,7 %). Največ anketirancev pozna in hkrati uporablja požarni zid (71,6 %), sledijo pa mu varnostne posodobitve programov (61,8 %). Anketiranci najmanj uporabljajo šifriranje elektronske pošte (8,8 %) ter sisteme za anonimizacijo (9,8 %). Anketiranci so ti dve orodji navedli tudi kot najbolj nepoznani izmed vseh (glej Tabelo 8.1). Da je poznavanje orodij, kot so šifriranje elektronske pošte in sistemi za anonimizacijo, tako nizko, lahko pojasnimo s tem, da sta to najbolj kompleksni orodji za uporabo, ko želimo zaščititi našo zasebnost. Šifriranje elektronske pošte od uporabnika zahteva že nekaj več računalniškega znanja, medtem ko so sistemi za anonimizacijo velikokrat plačljivi, večina ponudnikov, ki te sisteme ponujajo, pa se nahajajo v tujini. Ravno obratno lahko visok delež uporabe požarnega zidu in varnostnih posodobitev programov pripišemo njihovi enostavni uporabi. Za uporabo teh dveh orodij

ne potrebujemo veliko, saj nas velikokrat že računalnik sam opozori, da imamo izklopljen požarni zid oziroma kdaj je čas za novo posodobitev programov. Če imamo za dostop do internetnega omrežja računalnik priklopljen na usmerjevalnik ali tako imenovani »ruter«, potem imamo hkrati priskrbljen požarni zid. Pri posodobitvah programov pa je najlažje, če imamo nastavljene tako, da se posodobitve izvajajo samodejno, saj s tem varnostne posodobitve ne zastarajo in so vedno najbolj sveže.

Tabela 8.2: Zavedanje nadzora na internetu

Označite, katere podatke je po vašem mnenju mogoče zabeležiti:	**Da**		**Ne**		**Ne vem**	
	n	%	n	%	n	%
vaš e-mail naslov	36	35,3	48	47,1	18	17,6
internetni (IP) naslov vašega računalnika	96	94,1	2	2	4	3,9
WWW stran, ki ste jo pred tem obiskali	41	40,2	33	32,4	28	27,5
vrsta in tip brskalnika, ki ga uporabljate (Mozilla Firefox, Internet Explorer ...)	87	85,3	4	3,9	11	10,8
vašo geografsko lokacijo	62	60,8	11	10,8	29	28,4
seznam datotek na vašem trdem disku	1	1	75	73,5	26	25,5
naslov WWW strani, na kateri se nahajate	86	84,3	4	3,9	12	11,8
število vaših obiskov	88	86,3	3	2,9	11	10,8
vrsto in tip vašega računalnika (procesor, RAM, trdi disk ...)	15	14,7	44	43,1	43	42,2

Anketiranci so dobro osveščeni o tem, kateri osebni podatki se lahko beležijo na internetu in kateri ne. Večina anketirancev (47,1 %) je pravilno odgovorila, da strežniki ne morejo zabeležiti njihovega e-naslova, kar 94,1 odstotkov anketiranih je tudi pravilno odgovorilo, da se IP naslov računalnika lahko zabeleži. Da se lahko zabeleži tudi WWW stran, ki so jo

uporabniki že prej obiskali, ve 40,2 odstotkov anketirancev, anketiranci pa so dobro seznanjeni tudi s tem, da se zabeležita vrsta in tip brskalnika, ki ga uporabljajo (85,3 %). 60,8 odstotkov anketirancev pravilno domneva, da se lahko zabeleži tudi njihova geografska lokacija. Pravilno so seznanjeni s tem, da se seznam datotek na njihovem računalniku ne more beležiti (73,5 %) ter da se lahko beleži naslov WWW strani, na kateri se nahajajo (84,3 %). Ponovno so pravilno odgovorili, da se lahko beleži tudi število njihovih obiskov strani (86,3 %). Največ anketirancev tudi ve, da se vrsta in tip njihovega računalnika ne more beležiti (43,1 %), ravno pri tej trditvi je bilo največ anketirancev neodločenih (42,2 %) (glej Tabelo 8.2).

Tabela 8.3: Uporaba spletnih socialnih servisov

Katere izmed naštetih spletnih socialnih servisov uporabljate, v smislu, da imate ustvarjen svoj profil:	**Uporabljam**		**Ne uporabljam**	
	n	%	n	%
Facebook	97	95,1	5	4,9
Myspace	13	12,7	89	87,3
Forum	30	29,4	72	70,6
Blog	10	9,8	92	90,2

Največ anketirancev (95,1 %) ima ustvarjen svoj profil Facebook, najmanj pa jih ima svoj blog (9,8 %) (glej Tabelo 8.3). Visok delež uporabe Facebooka je pričakovan, saj dandanes to, da nimaš profila Facebook med mladimi pomeni skoraj isto, kot da nimaš mobilnega telefona.

Tabela 8.4: Razkrivanje osebnih podatkov glede na spletni socialni servis

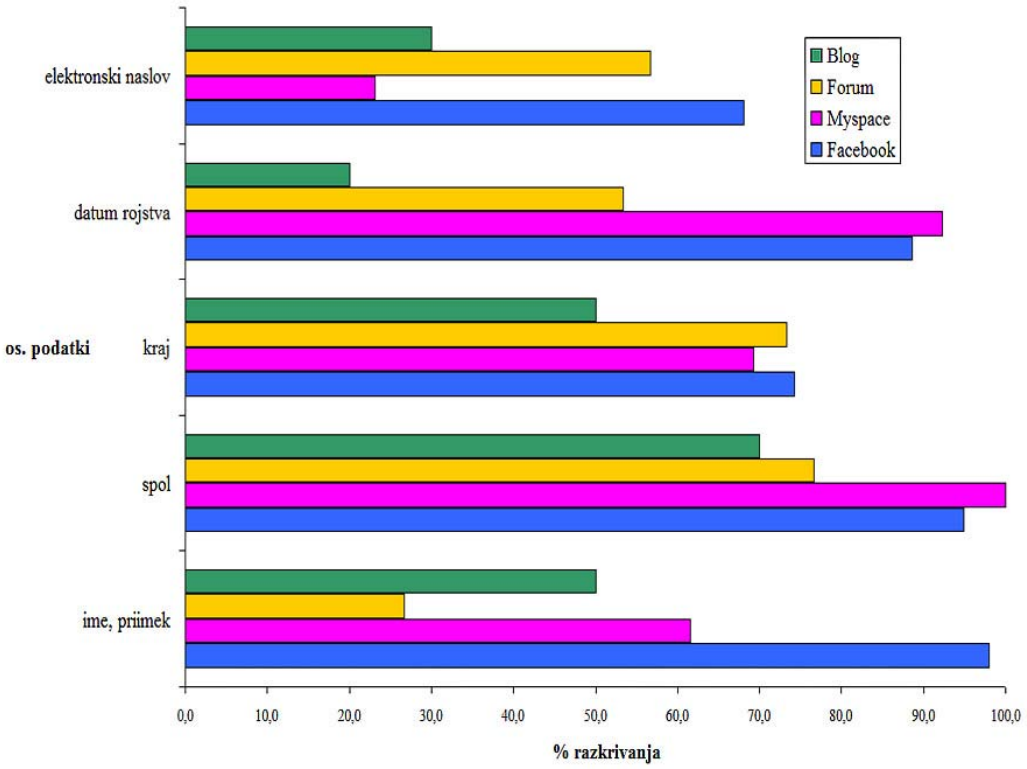
Katere izmed spodaj naštetih osebnih podatkov ste že kdaj razkrili v profilu:	**Facebook**				**Myspace**				**Forum**				**Blog**			
	Razkrivam		*Ne razkrivam*		*Razkrivam*		*Ne razkrivam*		*Razkrivam*		*Ne razkrivam*		*Razkrivam*		*Ne razkrivam*	
	n	%	n	%	n	%	n	%	n	%	n	%	n	%	n	%
ime, priimek	95	97,9	2	2,1	8	61,5	5	38,5	8	26,7	22	73,3	5	50	5	50
spol	92	94,8	5	5,2	13	100	0	0	23	76,7	7	23,3	7	70	3	30
kraj	72	74,2	25	25,8	9	69,2	4	30,8	22	73,3	8	26,7	5	50	5	50
datum rojstva	86	88,7	11	11,3	12	92,3	1	7,7	16	53,3	14	46,7	2	20	8	80
elektronski naslov	66	68,0	31	32,0	3	23,1	10	76,9	17	56,7	13	43,3	3	30	7	70
telefonsko številko	7	7,2	90	92,8	0	0	13	100	2	6,67	28	93,3	0	0	10	100
izobrazbo	53	54,6	44	45,4	2	15,4	11	84,6	8	26,7	22	73,3	3	30	7	70
zaposlitev	16	16,5	81	83,5	1	7,7	12	92,3	5	16,7	25	83,3	3	30	7	70
narodnost, veroizpoved	25	25,8	72	74,2	2	15,4	11	84,6	7	23,3	23	76,7	2	20	8	80
stan	51	52,6	46	47,4	5	38,5	8	61,5	6	20	24	80	2	20	8	80
telesno višino	0	0	97	100	0	0	13	100	3	10	27	90	0	0	10	100
spolno usmerjenost	25	25,8	72	74,2	2	15,4	11	84,6	4	13,3	26	86,7	1	10	9	90
razlog za članstvo	8	8,2	89	91,8	2	15,4	11	84,6	7	23,3	23	76,7	0	0	10	100

Anketiranci v svojem profilu Facebook najpogosteje razkrivajo ime in priimek (97,9 %), kar je tudi pričakovano, saj Facebook svoje člane vzpodbuja, da se predstavljajo z resničnimi identitetami. Za tem anketiranci razkrivajo spol (94,8 %) ter datum rojstva (88,7 %). Najmanj razkrivajo telesno višino (0 %), telefonsko številko (7,2 %) in razlog za članstvo (8,2 %). Na profilu Myspace anketiranci najpogosteje razkrivajo spol (100 %), datum rojstva (92,3 %) in kraj bivanja (69,2 %), najmanj pa razkrivajo telefonsko številko (0 %), telesno višino (0 %) ter zaposlitev (7,7 %). Na forumih anketiranci najpogosteje razkrivajo spol (76,7 %), kraj bivanja (73,3 %) in elektronski naslov (56,6 %), najmanj pa razkrivajo telefonsko številko (6,67 %), telesno višino (10 %) ter spolno usmerjenost (13,3

%). Anketiranci na blogu največ razkrivajo spol (70 %), ime in priimek (50 %) ter kraj bivanja (50 %), najmanj pa razkrivajo oziroma sploh ne razkrivajo telefonske številke, telesne višine in razloga za članstvo, saj je pri vseh treh delež enak 0 % (glej Tabelo 8.4).

Izmed petih najbolj razkritih vrst osebnih podatkov ima Facebook najvišji delež v treh. To so razkrivanje elektronskega naslova, kraja bivanja ter imena in priimka, pri zadnjem pa ima tudi daleč najvišji delež (glej Sliko 8.1). Kaj so razlogi za to, sem že omenila v interpretaciji Tabele 8.4. Izmed trinajst vrst osebnih podatkov ima Facebook najvišji delež razkrivanja kar v osmih, medtem ko imata Myspace in forumi najvišji delež v dveh (datum rojstva, spol ter razlog za članstvo, telesna višina), blogi pa v eni vrsti osebnih podatkov (zaposlitev).

Slika 8.1: Pet najbolj razkritih osebnih podatkov glede na vrsto spletnega socialnega omrežja



Za lažjo nadaljnjo statistično obdelavo pri sestavljanju izvedenih spremenljivk sem podatke o razkrivanju osebnih informacij združila, ne glede na to, v katerem spletnem socialnem servisu so bile te informacije razkrite (glej Tabelo 8.5).

Tabela 8.5: Razkrivanje osebnih podatkov - združeni spletni socialni servisi

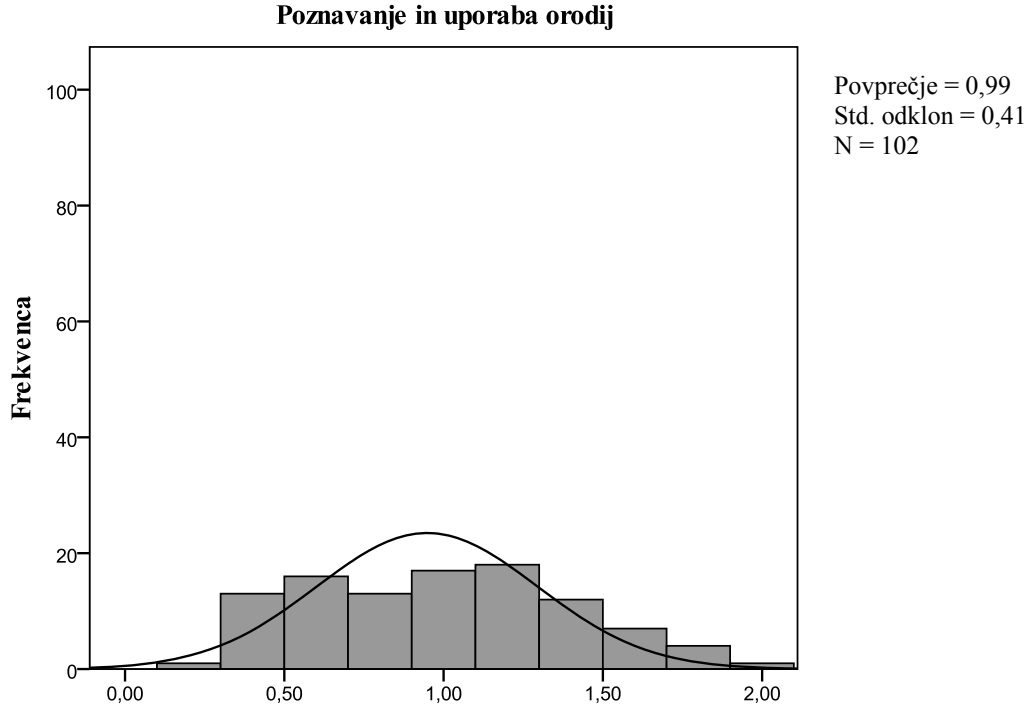
Katere izmed spodaj naštetih osebnih podatkov ste že kdaj razkrili v profilu:	***razkrivam***		***ne razkrivam***	
	n	%	n	%
ime, priimek	98	96,1	4	3,9
spol	97	95,1	5	4,9
kraj	84	82,4	18	17,6
datum rojstva	91	89,2	11	10,8
elektronski naslov	72	70,6	30	29,4
telefonsko številko	9	8,8	93	91,2
izobrazbo	58	56,9	44	43,1
zaposlitev	22	21,6	80	78,4
narodnost, veroizpoved	29	28,4	73	71,6
stan	52	51,0	50	49,0
telesno višino	3	2,9	99	97,1
spolno usmerjenost	26	25,5	76	74,5
razlog za članstvo	12	11,8	90	88,2

Anketiranci na splošno v spletnih socialnih servisih najbolj razkrivajo ime in priimek (96,1 %) ter spol (95,1 %), kar je tudi pričakovano glede na množično članstvo na Facebooku. Najmanj se razkrivata telesna višina (2,9 %) in telefonska številka (8,8 %). Za telesno višino bi lahko rekli, da je preveč neoseben podatek, da bi ga sploh razkrili, poleg tega pa opcijo razkrivanja tega podatka ponuja Myspace in ne Facebook, kar lahko pojasni tako nizek odstotek razkrivanja. Za telefonsko številko pa velja nasprotno - je preveč oseben podatek za razkrivanje, čeprav bi jo lahko objavili na vseh spletnih socialnih servisih.

8.2 Operacionalizacija teoretskih pojmov

Vsako izmed spremenljivk tvori več indikatorjev, ti pa skupaj tvorijo vsebinsko celoto. Spremenljivko **poznavanje in uporaba orodij za zaščito zasebnosti** sestavlja pet indikatorjev. Anketiranci so odgovarjali na vprašanje »*Poznate ali pa uporabljate katero od spodaj naštetih orodij za informacijsko varnost?«,* na voljo pa so imeli odgovore: poznam, poznam in uporabljam ter ne poznam. Te odgovore sem rekodirala v vrednosti 1, 2 in 0. Spremenljivko poznavanje in uporaba orodij sem tvorila tako, da sem s stavkom compute izračunala skupno aritmetično sredino vseh indikatorjev (glej Sliko 8.2).

Slika 8.2: Seštevek indikatorjev v novo spremenljivko *poznavanje in uporaba orodij za zaščito zasebnosti*



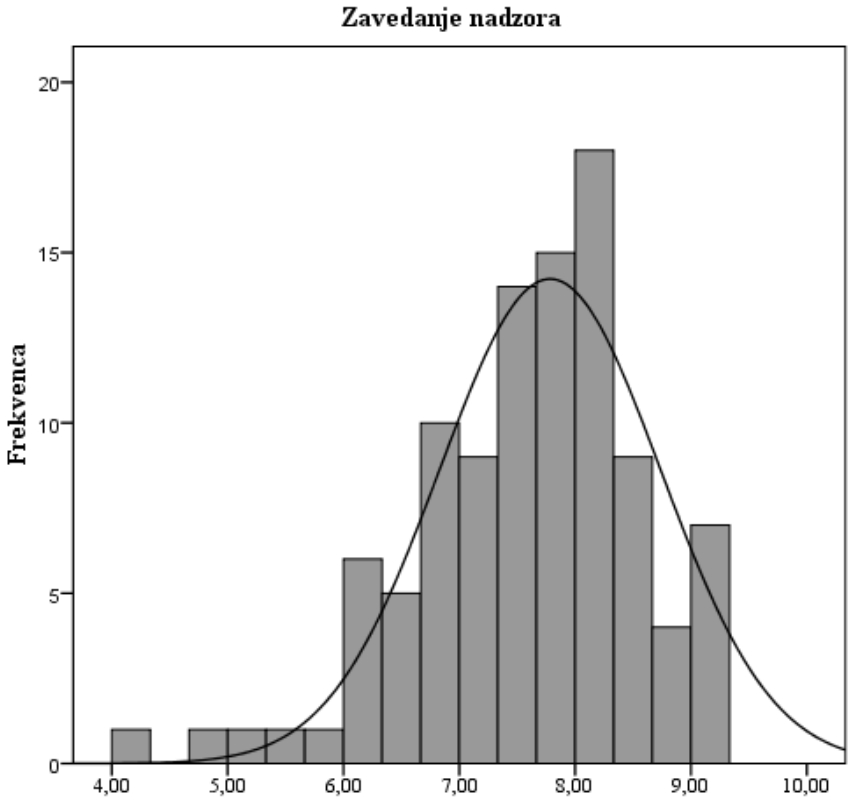
Spremenljivko **zavedanje nadzora na internetu** tvori devet indikatorjev, ki ponazarjajo nekakšen test, kjer je samo en odgovor pravilen. Našteti so bili določeni podatki, anketiranci pa so morali odgovoriti, ali se ti podatki lahko beležijo na spletnem strežniku ali ne. Ponujeni odgovori so bili, da, ne ali ne vem. Pravilne odgovore sem rekodirala v

vrednost 1, nepravilne odgovore sem rekodirala v vrednost 0, odgovore »ne vem« sem spremenila v manjkajoče vrednosti ter jih nato v SPSS-u s pomočjo ukaza »Replace missing values« spremenila v povprečja, saj odgovor ne vem ni niti pravilen, niti nepravilen. Največje možno število točk je torej devet, saj je devet indikatorjev. Indikatorje sem nato seštela ter tako tvorila spremenljivko **zavedanje nadzora na internetu**.
Kot vidimo iz spodnje tabele, se anketiranci kar dobro zavedajo nadzora, saj je povprečje kar 7,57 na lestvici do devet (glej Tabelo 8.6).

Tabela 8.6: Osnovne opisne statistike izvedene spremenljivke *zavedanje nadzora na internetu*

Ko obiščete neko spletno stran na internetu, strežnik, kjer je ta stran postavljena, zabeleži nekaj podatkov o obiskovalcu. Označite prosim, katere podatke je po vašem mnenju mogoče zabeležiti?	
N	102
Povprečje	7,57
Standardni odklon	0,98
Minimum	4
Maximum	9

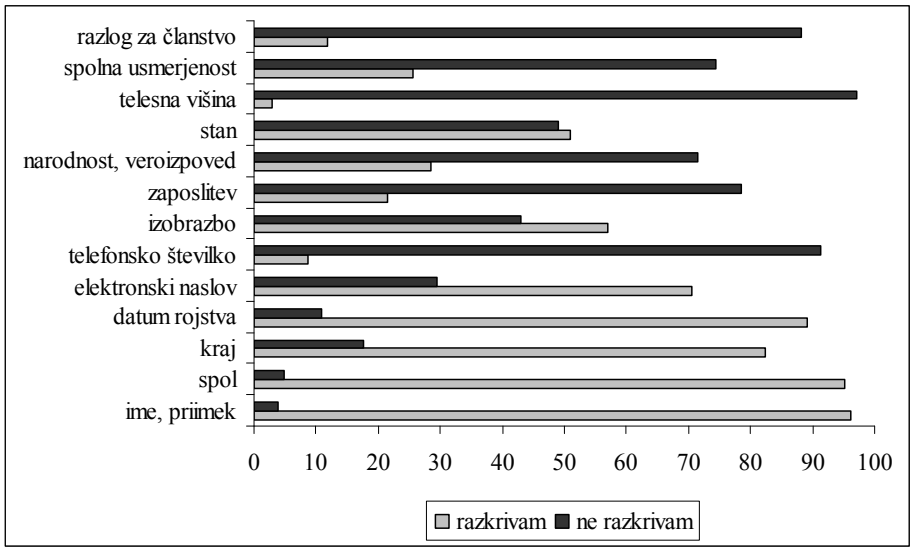
Slika 8.3: Seštevek rekodiranih indikatorjev (v 0 in 1) spremenljivke *zavedanje nadzora na internetu*



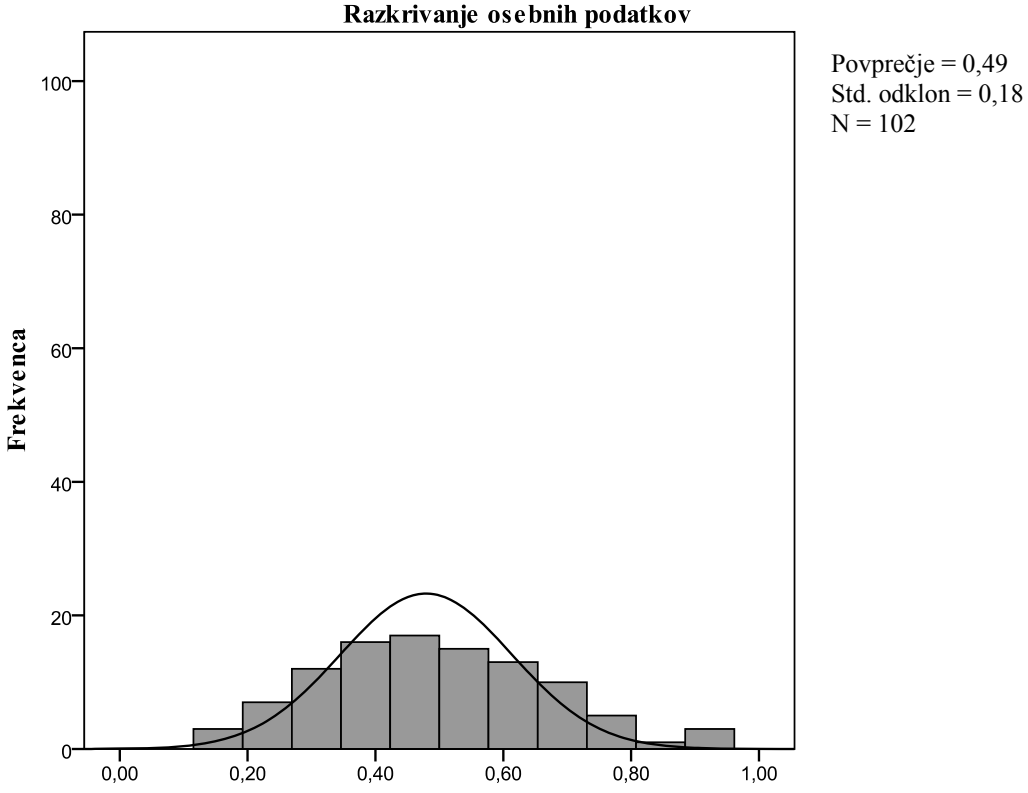
Najnižje število pravilnih odgovorov na lestvici do devet je štiri (glej Sliko 8.3).

Spremenljivko **razkrivanje osebnih podatkov** sestavlja trinajst indikatorjev. Anketiranci so odgovarjali na vprašanje »*Katere izmed spodaj naštetih osebnih podatkov ste že kdaj razkrili v profilu?«*. Na voljo so imeli odgovora razkrivam in ne razkrivam, ki sem jih rekodirala v vrednosti 1 in 0. Sprva so anketiranci odgovorili na vprašanje, katere spletne socialne servise uporabljajo, nato pa so za vsak servis posebej odgovarjali, katere podatke tam razkrivajo. Zaradi lažje statistične obdelave sem te podatke med seboj združila (glej Sliko 8.4). Spremenljivko razkrivanje osebnih podatkov sem tvorila tako, da sem s stavkom compute izračunala skupno aritmetično sredino vseh indikatorjev (glej Sliko 8.5).

Slika 8.4: Delež osebnih podatkov, ki jih anketiranci razkrivajo oziroma ne razkrivajo



Slika 8.5: Seštevek indikatorjev v novo spremenljivko *razkrivanje osebnih podatkov*

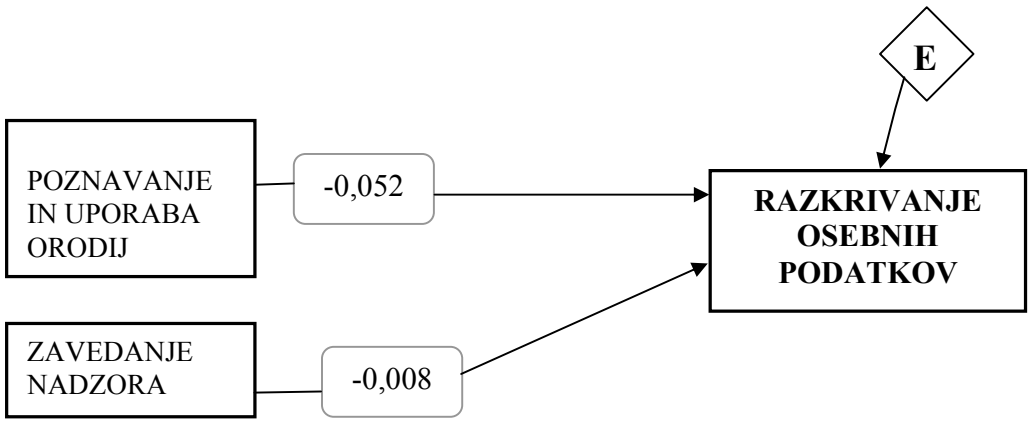


8.3 Preverjanje pojasnjevalnih modelov

Pojasnjevalni model sem preverjala s pomočjo regresijske analize z metodo enter. Model, v katerem kot odvisna spremenljivka nastopa *razkrivanje osebnih podatkov*, se ne prilega podatkom, kar nam pokaže vrednost statistike F (glej prilogo A), odstotek pojasnjene variance znaša le 0,15 odstotka, kar pomeni, da z mojim modelom lahko pojasnim le 0,15 odstotka variance odvisne spremenljivke. Vrednost popravljenega determinacijskega koeficienta R^2 je negativna, saj znaša -0,017. To se je zgodilo, ker je model zelo šibek, s tem pa pojasnim nič variabilnosti odvisne spremenljivke.

Stopnja značilnosti bi morala biti manjša od 0,1, da bi lahko govorili o statistično značilnem vplivu, idealno pa bi bila manjša od 0,05. Nobena od pojasnjevalnih spremenljivk nima statistično značilnega vpliva na odvisno spremenljivko *razkrivanje osebnih podatkov*, saj je stopnja značilnosti povsod večja od 0,05 (glej prilogo A). To se je zgodilo zaradi premajhnega vzorca, bete pa bi morale biti precej visoke, da bi postale statistično značilne. Nakazuje pa se minimalen vpliv poznavanja in uporabe orodij na razkrivanje osebnih podatkov.

Slika 8.6: Ocenjeni model razkrivanja osebnih podatkov



Z regresijsko analizo sem preverjala povezanost med neodvisnima in odvisno spremenljivko in s tem tudi, ali zastavljene hipoteze držijo. Izkazalo se je, da neodvisni spremenljivki nista statistično značilno povezani z odvisno spremenljivko.
Na podlagi dobljenih rezultatov lahko zavrnem prvo hipotezo: *uporabniki, ki bolj poznajo internetno tehnologijo in orodja za zaščito zasebnosti, manj javno razkrivajo svoje osebne podatke na internetu,* saj so rezultati pokazali, da poznavanje internetne tehnologije in orodij za zaščito zasebnosti ne vpliva na razkrivanje osebnih podatkov.
Zavrnem lahko tudi drugo hipotezo: *uporabniki, ki se bolj zavedajo nadzora na internetu, manj javno razkrivajo svoje osebne podatke,* saj so rezultati tudi tukaj pokazali, da zavedanje nadzora na internetu ne vpliva na razkrivanje osebnih podatkov.

9 ZAKLJUČEK

Zasebnost je povezana s sramovanjem, vsi se nečesa sramujemo in nočemo, da bi za to kdorkoli izvedel, zato to sramoto varujemo v zasebnosti. Kriminalci pri svojih dejanjih vedno varujejo svojo zasebnost, mi pa se sramujemo ali pa nam je zgolj nerodno za stvari, ki sploh niso povezane s kriminalom. Zato nam tudi ni mar, da se o nas razkrivajo informacije, dokler nas te informacije ne sramotijo ali spravljajo v zadrego (Baker 2010, 488–489).

Raynes–Goldie je ugotovila, da obstajata dve vrsti zaskrbljenosti za zasebnost: socialna, ki jo lahko opredelimo kot onemogočanje dostopa do podatkov drugim uporabnikom spletnih socialnih omrežij, in institucionalna, ki jo lahko opredelimo kot onemogočanje dostopa do podatkov marketinškim korporacijam, uporabniki pa so bolj zaskrbljeni za tako imenovano socialno zasebnost (Raynes–Goldie 2010). Ravno tako kot obstajata dve vrsti zaskrbljenosti za zasebnost obstajata tudi dve vrsti nadzora nad osebnimi podatki na internetu. Ena vrsta nadzora je ta, ki jo nad nami vršijo drugi uporabniki spletnih socialnih omrežij s tem, ko brskajo po naših profilih, berejo naše objave, gledajo slike itd., druga vrsta nadzora pa je ta, ki jo nad nami v marketinške namene vršijo različne korporacije. Najverjetneje so uporabniki bolj zaskrbljeni za socialno zasebnost ravno zaradi občutka sramu, ki ga imajo

pred drugimi uporabniki, saj gre za bolj osebno interakcijo, medtem ko je nadzor s strani korporacij veliko bolj neoseben, ker gre predvsem za zbiranje podatkov o nakupovalnih navadah in za potrebe ciljnega oglaševanja, zato se ob tem nadzoru tudi ne počutijo tako ogrožene. V raziskavi sem se osredotočila le na nadzor, ki ga lahko izvršujejo različne korporacije. Izkazalo se je, da se anketiranci zelo dobro zavedajo različnih zmožnosti pridobivanja podatkov s strani korporacij, toda to še vedno ne vpliva na količino osebnih podatkov, ki jo razkrivajo. Na prvi pogled bi iz navedene ugotovitve lahko sklepali, da mogoče anketiranci niso zaskrbljeni za svojo zasebnost in zaradi tega nemoteno razkrivajo svoje osebne podatke, vendar menim, da to ni tako. Če bi raziskovala drugo področje nadzora, torej nadzor, ki ga vršijo uporabniki spletnih socialnih omrežij nad drugimi uporabniki, bi najverjetneje dobila zelo drugačne rezultate, mogoče bi se celo razkrila skrb za socialno zasebnost.

V diplomskem delu sem želela proučevati, kakšen pomen ima stopnja uporabnikove osveščenosti o zasebnosti na internetu pri razkrivanju osebnih podatkov. Ugotavljala sem, ali se z večjim poznavanjem tehnologije za zaščito zasebnosti ter večjim zavedanjem nadzora na internetu količina javno razkritih osebnih podatkov manjša ali ostaja nespremenjena. V opravljeni raziskavi se je izkazalo, da model slabo pojasnjuje odvisno spremenljivko razkrivanje osebnih podatkov, nakazuje pa se minimalen vpliv, ki ga ima poznavanje in uporaba orodij na razkrivanje osebnih podatkov, vendar ta ni statistično značilen. Ker so rezultati pokazali, da neodvisni spremenljivki nista statistično značilno povezani z odvisno spremenljivko, sem morala zavrniti obe zastavljeni hipotezi. Izkazalo se je torej, da z večjim poznavanjem internetne tehnologije in orodij za zaščito zasebnosti uporabniki nič manj javno ne razkrivajo svojih osebnih podatkov na internetu ter da večje zavedanje nadzora na internetu ne vpliva na manjše javno razkrivanje osebnih podatkov. Tako sem tudi našla odgovor na zastavljeno raziskovalno vprašanje, ki se glasi, da uporabnikova osveščenost o nadzoru na internetu in splošno poznavanje tehnologije za izboljšanje zasebnosti na internetu nimata vpliva na količino razkrivanja osebnih podatkov. Pričakovala sem ravno obratne rezultate, razlogi za to, da se moja pričakovanja niso uresničila, pa se najverjetneje skrivajo tudi v velikosti vzorca. Če bi v raziskavi nastopal večji vzorec, bi bili verjetno drugačni tudi rezultati.

V teoretičnem delu sem razpravljala o tem, kako različni avtorji poudarjajo, da se uporabniki interneta ne zavedajo, da gre pri zasebnosti na internetu čedalje bolj za nadzor nad osebnimi podatki in izdelavo uporabniških profilov ter da uporabniki prav tako niso seznanjeni z obstojem datotek aktivnosti. Izkazalo se je, da je osveščenost uporabnikov o nadzoru, ki poteka na internetu, zelo podcenjena. Ravno moja raziskava je pokazala, da so uporabniki zelo dobro osveščeni o nadzoru na internetu in o orodjih za zaščito zasebnosti. Najverjetneje je k takšnemu rezultatu pripomogel tudi vzorec, ki je sestavljen iz študentov, saj bi bili mogoče rezultati pri manj izobraženem in starejšem vzorcu drugačni.

Nihče ni dobesedno prisiljen, da se priključi spletnemu socialnemu omrežju, večina omrežij, ki jih poznamo, spodbuja, toda ne sili uporabnikov k razkrivanju osebnih podatkov, kot so: datum rojstva, številka mobilnega telefona ali domači naslov. Nekatere podatke moramo razkriti že na začetku, da se sploh lahko priključimo spletnemu socialnemu omrežju. Najpogosteje moramo tako razkriti naš e-naslov, Facebook pa celo prepričuje uporabnike, da izdajo svoja resnična imena in identitete, v nasprotnem primeru je njihov profil lahko celo izbrisan.

Uporabniki Facebooka si vsak mesec med seboj izmenjajo več kot 30 milijard vsebin, vključno s spletnimi povezavami, objavami novic in zgodb, zapiskov ter fotoalbumov. To ogromno število vsebin skupaj s podatkovnimi tokovi iz drugih virov predstavlja veliko priložnost za marketinško industrijo in industrijo tržnih raziskav, hkrati pa veliko grožnjo informacijski zasebnosti uporabnikov (Hummerston in Wirth 2011). V moji raziskavi je v vzorcu nastopalo kar 95 odstotkov anketirancev, ki so uporabniki Facebooka. Ti uporabniki so imeli tudi najvišji delež razkrivanja podatkov, saj so bili deleži pri osmih od trinajstih vrst osebnih podatkov najvišji. To niti ni tako presenetljivo, saj Facebook daje svojim uporabnikom občutek varnosti, da imajo uporabniki nadzor nad zasebnostjo profilov v svojih rokah. Zaradi občutka varnosti in zasebnosti pa lahko toliko bolj razkrivajo svoje prave identitete in osebne podatke. Zaradi množičnega članstva na Facebooku in posledično množičnega razkrivanja podatkov v mojem vzorcu tako ne moremo posploševati rezultatov na člane preostalih spletnih socialnih omrežij, saj bi bili rezultati najverjetneje drugačni, če bi v vzorcu prevladovali člani nekega drugega spletnega socialnega omrežja.

V Sloveniji se osveščanje javnosti o varovanju osebnih podatkov na internetu izboljšuje, vendar Informacijski pooblaščenec javnosti še vedno ne obvešča dovolj o morebitnih nevarnostih pri razkrivanju osebnih podatkov na internetu. Nikjer ni niti zaslediti nobene raziskave, ki bi nakazovala trend razkrivanja osebnih podatkov. Tudi zakonodaja kljub evropski Direktivi o zasebnosti in elektronskih komunikacijah ni najbolje urejena, saj področje neposrednega trženja in s tem posledično področje nezaželene elektronske pošte v Sloveniji regulirajo kar štirje zakoni: Zakon o elektronskih komunikacijah, Zakon o varstvu potrošnikov, Zakon o elektronskem poslovanju na trgu ter Zakon o varstvu osebnih podatkov. Seveda bi bilo za uporabnike interneta mnogo bolj enostavno, da bi bil za to pristojen le en zakon. Varni rabi interneta v Sloveniji še največ pozornosti posveča spletna stran Safe.si, vendar pa bolj v smislu preprečevanja spletnega nadlegovanja.

Za boljše osveščanje javnosti o nadzoru na internetu bi morala vsaka spletna stran vsebovati izjavo o politiki zasebnosti, vendar samo to ni dovolj, saj obiskovalci internetnih strani takšne izjave velikokrat prezrejo, ker so te predolge, uporabljajo pa se tudi vnaprej pripravljeni vzorci izjav. Da bi obiskovalci izjave o politiki zasebnosti brali in se na ta način osveščali o svoji zasebnosti na internetu, bi morale biti izjave o politiki zasebnosti kratke in jedrnate, vsebovati bi morale podatke o tem, katere podatke obiskovalcev spletnih strani se zbira in obdeluje, za kakšen namen se te podatke potrebuje ter kdo te podatke obdeluje. Kot je že Mellors ugotovil, najboljša zaščita ni ta, da oni vedo manj o nas, ampak da mi vemo več o njih, s tem, da vemo, kaj oni vedo o nas in kako te informacije uporabljajo (Mellors v Raab v Kovačič 2003, 37).

10 LITERATURA

- Acquisti, Alessandro in Ralph Gross. 2006. *Imagined Communities Awareness, Information Sharing, and Privacy on the Facebook.* Dostopno prek: http://privacy.cs.cmu.edu/dataprivacy/projects/facebook/facebook2.pdf (6. december 2009).
- *AMPsoft.* Dostopno prek: http://www.ampsoft.net/utilities/CookieMonster.php (12. januar 2011).
- *Anonymizer.* Dostopno prek: http://www.anonymizer.com/ (12. januar 2011).
- Baker, Stewart. 2010. The Privacy Problem: What's Wrong with Privacy? V *The next digital decade: essays on the future of the internet*, ur. Berin Szoka in Adam Marcus, 483-508. Washington: TechFreedom.
- Banisar, David. 1999. *Privacy and Human Rights 1999*. An international survey of privacy laws and developments. Dostopno prek: http://www.privacyinternational.org/survey/Overview.html (13. april 2010).
- Barnes, Susan. 2006. A privacy paradox: Social networking in the United States. *First Monday* 11 (9*)*. Dostopno prek: http://131.193.153.231/www/issues/issue11_9/barnes/index.html (1. december 2009).
- Blarkom, Gilles W., John Borking in J.G.E. Olk. 2003. *Handbook of Privacy and Privacy-Enhancing Technologies. The case of Intelligent Software Agents*. Dostopno prek: http://www.cbpweb.nl/downloads_technologie/PISA_handboek.pdf (13. december 2009).
- Boyd, Danah. 2010. *»Making Sense of Privacy and Publicity«*. Dostopno prek: http://www.danah.org/papers/talks/2010/SXSW2010.html (15. maj 2010).
- Boyd, Danah. 2007. *Social Network Sites: Public, Private, or What?* Dostopno prek: http://www.danah.org/papers/KnowledgeTree.pdf (6. december 2009).
- Delovna skupina za varstvo podatkov. 2007. *Mnenje 4/2007 o pojmu osebnih podatkov*. Dostopno prek: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_sl.pdf (26. januar 2010).
- *Facebook.* Dostopno prek: http://sl-si.facebook.com/ (12. januar 2011).

- Fischer-Hübner, Simone. 2003. *Privacy-Enhancing Technologies (PET).* Dostopno prek: http://www.cs.kau.se/~simone/kau-phd-course.htm (25. april 2009).
- Goldberg, Ian Avrum. 2002. *Privacy-Enhancing Technologies for the Internet, II: Five years later.* Dostopno prek: http://www.freehaven.net/anonbib/papers/petfive.pdf (12. december 2009).
- Goldberg, Ian Avrum. 2000. *A Pseudonymous Communications Infrastructure for the Internet.* Berkeley: University of California.
- *Google.* Dostopno prek: http://www.google.si/search?client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&channel=s&hl=sl&source=hp&q=site%3A+uni-lj.si+varnost&meta=&btnG=Iskanje+Google (12. januar 2011).
- Google Hacking Lab. 2010. *Google Hacking*. Dostopno prek: http://www1.pacific.edu/~mmaxwel2/ecpe178/labs/Google-Hacks.pdf (12. maj 2010).
- Hummerston, Arno in Norbert Wirth. 2011. Behavioural and Survey Data. *The Digital Connected Consumer*, 2. februar. Dostopno prek: http://www.gfkorange.si/images/stories/2011/02-Februar/Digital_Consumer_eMagazine.pdf (10. marec 2011).
- *Information Commissioner's Office*. 2007. Dostopno prek: http://www.ico.gov.uk/upload/documents/pressreleases/2007/social_networking_press_release.pdf (16. januar 2010).
- Informacijski pooblaščenec. *Nezaželena elektronska sporočila in slovenska zakonodaja*. Dostopno prek: http://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/varstvo-osebnih-podatkov-na-internetu/#c410 (27. januar 2010).
- Kovačič, Matej. 1999. *Raziskava o odnosu do zasebnosti na internetu.* Dostopno prek: http://www.ljudmila.org/matej/zasebnost/zasebnost99/index.html (5. december 2009).
- Kovačič, --- 2000. Zasebnost v informacijski družbi. *Teorija in praksa* 37 (6): 1019-1034.
- Kovačič, --- 2003. *Zasebnost na internetu*. Ljubljana: Mirovni inštitut.

- Kovačič, --- 2006. *Nadzor in zasebnost v informacijski družbi. Filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu*. Ljubljana: Univerza v Ljubljani, Fakulteta za družbene vede.
- Kovačič, --- 2009a. Sledenje s »superpiškotki«. *Pravokator*, 16. september. Dostopno prek: http://hr-cjpc.si/pravokator/index.php/2009/09/16/sledenje-s-superpiskotki/ (6. maj 2010).
- Kovačič, --- 2009b. Evropska unija bo morda omejila uporabo spletnih piškotkov. *Pravokator*, 30. november. Dostopno prek: http://hr-cjpc.si/pravokator/index.php/2009/11/30/evropska-unija-bo-morda-omejila-uporabo-spletnih-piskotkov/ (6. maj 2010).
- Kovačič, Matej in Vasja Vehovar. 2000. *Slovenski uporabniki interneta in zasebnost.* Dostopno prek: http://backup.ris.org/si/ris2000/pub/infosoc1.pdf (6. december 2009).
- Laurant, Cedric. 2003. *Privacy and Human Rights 2003*. An international survey of privacy laws and developments. Dostopno prek: http://www.privacyinternational.org/survey/phr2003/overview.htm (27. marec 2010).
- Macaulay, Linda. 2002. *Privacy Enhancing Technologies. State of the Art Review.* Dostopno prek: http://www.lindamacaulay.com/upload/resource/7_1petreview3.pdf (8. december 2009).
- Marwick, Alice E., Diego Murgia Diaz in John Palfrey. 2010. *Youth, Privacy and Reputation*. Literature Review. Dostopno prek: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588163 (8. maj 2010).
- Ofcom. 2008. *Social Networking: A quantitative and qualitative research report into attitudes, behaviours and use*. Dostopno prek: http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/report.pdf (10. marec 2010).
- O'Neil, Dara. 2001. *Analysis of Internet Users' Level of Online Privacy Concerns.* Dostopno prek: http://ssc.sagepub.com.nukweb.nuk.uni-lj.si/cgi/reprint/19/1/17 (7. december 2009).

- Praprotnik, Darja. 2006. *Varovanje podatkov in zasebnost na internetu.* Magistrsko delo. Dostopno prek: http://www.cek. ef.uni-lj.si/magister/praprotnik2867.pdf (6. december 2009).
- Raynes-Goldie, Kate. 2010. Aliases, creeping and wall cleaning: Understanding privacy in the age of Facebook. *First Monday* 15 (1). Dostopno prek: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2775/2432 (12. maj 2010).
- Rotenberg, Marc. 2006. *Privacy and Human Rights 2006*. An international survey of privacy laws and developments. Dostopno prek: http://www.privacy international.org/article.shtml?cmd[347]%3C/a%3E=x-347559092&als[theme]= Privacy%20and%20Human%20Rights (13. april 2010).
- Seničar, Vanja, Borka Jerman-Blažič in Tomaž Klobučar. 2003. *Privacy-Enhancing Technologies-approaches and development.* Dostopno prek: http://www. sciencedirect.com/science?_ob=ArticleURL&_udi=B6TYV-47T84NY-1&_user=10&_rdoc=1&_fmt=&_orig=search&_sort=d&view=c&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=29e20b5868a165c6453a17bb5effeaa3 (13. december 2009).
- Stalder, Felix. 2002. The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy. *Sociological Research Online* 7 (2). Dostopno prek: http://www.socresonline.org.uk/7/2/stalder.html (13. marec 2010).
- Zimmer, Michael. 2008a. The Externalities of Search 2.0: The Emerging Privacy Threats when the Drive for the Perfect Search Engine meets Web 2.0. *First Monday* 13 (3). Dostopno prek: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php /fm/article/view/2136/1944 (12. maj 2010).
- Zimmer, Michael. 2008b. Preface: Critical Perspectives on Web 2.0. *First Monday* 13 (3). Dostopno prek: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm /article/view/2137/1943 (15. maj 2010).

11 PRILOGE

PRILOGA A: Rezultati regresijske analize

Tabela A.1: Rezultati regresijske analize z odvisno spremenljivko *razkrivanje osebnih podatkov*

Neodvisne spremenljivke	**Nestandardiziran regresijski koeficient B**	**Standardiziran regresijski koeficient Beta**	**t-statistika**	**Stopnja značilnosti**
poznavanje in uporaba orodij	-0,022	-0,052	-0,509	0,612
zavedanje nadzora	-0,001	-0,008	-0,081	0,936
Konstanta	0,526	/	3,783	0,000
R	0,054			
R²	0,003			
R²pop	-0,017			
F	0,145			

PRILOGA B: Anketni vprašalnik

Anketo lahko rešujejo samo študentje Fakultete za družbene vede, razen družboslovnih informatikov.

Uporaba in poznavanje orodij za zaščito zasebnosti

1. *Poznate ali pa uporabljate katero od spodaj naštetih orodij za informacijsko varnost?(Če orodje poznate in hkrati uporabljate obkrožite oba odgovora)*

	poznam	uporabljam	ne poznam
upravljanje s piškotki (»cookie manager«)			
sistemi za anonimizacijo (zaščitnik identitete, anonimni strežnik,			

IPREDator, VPN,…)			
požarni zid (»firewall«)			
šifriranje elektronske pošte (kriptografija)			
varnostne posodobitve programov			

Zavedanje nadzora

2. *Ko obiščete neko spletno stran na internetu, strežnik, kjer je ta stran postavljena, zabeleži nekaj podatkov o obiskovalcu. Označite prosim, katere podatke je po vašem mnenju mogoče zabeležiti?*

   1. vaš e-mail naslov — da / ne / ne vem
   2. internetni (IP) naslov vašega računalnika — da / ne / ne vem
   3. WWW stran, ki ste jo pred tem obiskali — da / ne / ne vem
   4. vrsta in tip brskalnika, ki ga uporabljate (Mozilla Firefox, Internet Explorer ...) — da / ne / ne vem
   5. vašo geografsko lokacijo — da / ne / ne vem
   6. seznam datotek na vašem trdem disku — da / ne / ne vem
   7. naslov WWW strani, na kateri se nahajate — da / ne / ne vem
   8. število vaših obiskov — da / ne / ne vem
   9. vrsto in tip vašega računalnika (procesor, RAM, trdi disk ...) — da / ne / ne vem

Javno razkrivanje osebnih informacij

3. *Katere izmed naštetih spletnih socialnih servisov uporabljate, v smislu, da imate ustvarjen svoj profil* ?

- Facebook
- Myspace
- Forum

- Blog

4. *Spletne strani velikokrat ponujajo možnost razkrivanja določenih osebnih informacij. Katere izmed spodaj naštetih osebnih podatkov ste že kdaj razkrili v _____ profilu? Štejejo podatki objavljeni v profilu, kot tudi v objavljenih sporočilih, komentarjih.*

*anketiranec odgovarja za tiste spletne socialne servise, ki so bili izbrani pri 3. vprašanju

		Razkrivam	Ne razkrivam
Facebook	ime, priimek		
	spol		
	kraj		
	datum rojstva		
	elektronski naslov		
	telefonsko številko		
	izobrazbo		
	zaposlitev		
	narodnost, veroizpoved		
	stan		
	telesna višina		
	spolna usmerjenost		
	razlog za članstvo		
Myspace	ime, priimek		
	spol		
	kraj		
	datum rojstva		
	elektronski naslov		
	telefonsko številko		
	izobrazbo		
	zaposlitev		
	narodnost, veroizpoved		
	stan		
	telesna višina		
	spolna usmerjenost		
	razlog za članstvo		
Forumi	ime, priimek		
	spol		
	kraj		
	datum rojstva		
	elektronski naslov		
	telefonsko številko		
	izobrazbo		

	zaposlitev		
	narodnost, veroizpoved		
	stan		
	telesna višina		
	spolna usmerjenost		
	razlog za članstvo		
Blog	ime, priimek		
	spol		
	kraj		
	datum rojstva		
	elektronski naslov		
	telefonsko številko		
	izobrazbo		
	zaposlitev		
	narodnost, veroizpoved		
	stan		
	telesna višina		
	spolna usmerjenost		
	razlog za članstvo		

Demografija

Spol: *M* *Ž*

*Starost:*_____

*Smer študija:*_____