UNIVERZA V LJUBLJANI
EKONOMSKA FAKULETA

MAGISTRSKO DELO

POMEN ZASEBNOSTI IN VARNOSTI PRI USTVARJANJU ZAUPANJA NA INTERNETU

Ljubljana, avgust 2007 ROK PRIMOŽIČ

IZJAVA

Študent Rok Primožič izjavljam, da sem avtor tega magistrskega dela, ki sem ga napisal pod mentorstvom dr. Tanje Dmitrović in somentorstvom dr. Jurija Jakliča, in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne _____

Podpis: _____

KAZALO

KAZALO SLIK

KAZALO TABEL

1 UVOD

Pojav svetovnega spleta je spremenil način dela v poslovnem svetu. Kakor je razvoj tehnologije skozi zgodovino uveljavil v vsakdanji rabi kot nujnost telefon, televizor, osebni avtomobil in še nedavno mobilne telefone, tako tudi na področju informacijskih storitev zaradi hitrosti, praktičnosti in nizkih stroškov internet počasi, a vztrajno izpodriva običajne oblike poslovanja, komuniciranja in sorodnih storitev.

Internet je danes prisoten v skoraj vsakem gospodinjstvu, podjetju in drugih organizacijah. Postal je nepogrešljiv vir informacij, komunikacijsko sredstvo in vir zabave za mnoge uporabnike po svetu. Pred običajnimi potmi nudi številne prednosti, vse od že omenjene hitrosti in nizkih stroškov pa do anonimnosti, izjemne fleksibilnosti ter visokega števila potencialnih ciljnih uporabnikov storitev.

Podjetja so bila prisiljena začeti izkoriščati nove možnosti, ki jih ponuja napredek, saj bi drugače izgubila konkurenčno bitko. Podjetja, ki jim uspeva, vedo, da je na internetu mogoče izjemno uspešno komunicirati in tudi odlično prodajati, a le pod pogojem, da razumemo vse tiste okoliščine in specifične zahteve, ki jih spletni neuspešneži prezrejo. Podjetja, ki so preživela, so ponovno preučila stanje. Inovacija, kot je internet, ni dovolj za uspeh. Potrebno je upoštevati klasična pravila trženja in jih prenesti v novo okolje, kjer kot porabniki nastopajo posamezniki z že izoblikovanimi preferencami, navadami in vrednotami.

Ena od teh prezrtih stvari je **pomen zaupanja**. Le-to je v komuniciranju izjemnega pomena, na internetu pa postane z več vidikov ključen problem. Po eni strani lahko problematiziramo zaupanje investitorjev v internet, saj lahko spletni projekti nastajajo le z njihovim kapitalom, po drugi strani pa gre za zaupanje spletnih uporabnikov, ki so vedno tisti, ki s svojim zadovoljstvom odločijo o uspehu ali propadu posameznega spletnega mesta. Gre torej za (začaran) krog, ki pa na srečo vedno bolj postaja podoben spirali – eno zaupanje spodbuja drugo (Mavsar, 2003, str. 4). Uspešni spletni projekti, ki jim uporabniki zaupajo in jih učinkovito uporabljajo, sprožajo želje po novih. Le tiste spletne strani, ki so po meri uporabnikov, naročnikom prinašajo zadovoljstvo in dobičke. To pa je tudi pogoj za večje zaupanje novih vlagateljev.

Lahko bi rekli, da je zaupanje posledica zaznane varnosti in zasebnosti. Organizacije se morajo potruditi, da bo zaznana stopnja tveganja in zaupanja pri nakupu njihovih izdelkov/storitev čim nižja, kar pomeni, da bo zaupanje uporabnikov večje. Zaupanje pa se bo večalo, če bodo izpolnjena njihova pričakovanja in če bodo z nakupom zadovoljni.

Odnos med potrošniki in podjetji se danes manifestira v načinu komuniciranja. Ta opredeljuje položaj novodobnih potrošnikov, ki je vsiljen s strani velikih podjetij. Njihova etična usmeritev se odraža v njihovem načinu komuniciranja in pri uporabi tehnik množičnega marketinga, kjer je možno pretežno enosmerno komuniciranje. Tako je potrošnik pod vplivom sporočil trgovcev,

kjer mu ni dano, da bi enakovredno sodeloval v komunikaciji, ker je ta enosmerna (Lavrenčič, 2004, str. 4).

Glavni etični problem uporabe digitalnih tehnologij je v načinu zbiranja informacij o osebah, katerim se nato ponuja različne izdelke in storitve. Tehnologija ne samo, da omogoča sledenje posameznikovih aktivnosti, temveč tudi prinaša vedno nove uporabne funkcionalnosti, ki prispevajo k lagodnosti, hkrati pa še globlje posegajo v našo **zasebnost** (Primožič, 2005, str. 2).

Uvajanje novih informacijskih tehnologij je bilo vedno tesno povezano s skrbjo glede **varnosti**. Varnost informacijskih sistemov vidimo kot metodologijo in način razmišljanja. Metodologija je po definiciji skupek postopkov, tehnik, metod, katere uporabljamo pri reševanju nekega problema. To ne pomeni le ene rešitve, ki odpravi le eno težavo, ampak nudi celovito integrirano rešitev, ki rešuje vse varnostne težave. Hudoklin in Stadler (1997, str. 291) menita, da mora vodilo pri zaščiti dela temeljiti na dejstvu, da mora varnost omogočati poslovanje, ne pa ga zavirati. Varnost informacijskih sistemov je kombinacija dobrih poslovnih pravil, dobre varnostne politike, varnostnih načrtov, sodelovanja zaposlenih, sodobne tehnologije in sodelovanja z izkušenimi strokovnjaki ter varovanja samih podatkov.

Kljub temu, da bi želeli z nalogo podati nepristranski pogled na triado dejavnikov, ki imajo ključno vlogo na svetovnem spletu, tako z zornega kota investitorjev in skrbnikov spletnih strani kot tudi uporabnikov, ne bomo mogli obravnavati interneta kot celote, temveč bomo morali izhajati s stališča prodajalca. Vpliv novih tehnologij je de facto najmočnejši na področju spletne maloprodaje (*angl. e-tailing*) (So et al., 2005, str. 1225). Glede na to, da spletno nakupovanje ne sledi tradicionalnemu načinu, se spletne trgovine soočajo z novimi izzivi, ki sovpadajo z namenom magistrskega dela.

Cilj magistrskega dela je ugotoviti, v kolikšni meri lahko na osnovi spremljanja in analiziranja zaznavanja varnosti in zasebnosti, ki sta s stališča posameznikov in podjetij že prerasla pojem skrb ter postala ovira za nadaljnji razvoj interneta, nakažemo možnosti za krepitev zaupanja v internet.

Cilj dela je testirati konceptualni model, ki proučuje zaupanje uporabnikov do novih tehnologij, s poudarkom na svetovnem spletu, in preveriti postavljene domneve ter s tem potrditi vpliv zasebnosti in zaznane varnosti na stopnjo zaupanja ter nadalje nakazati povezavo med stopnjo zaupanja in zvestobo.

Ugotovitve raziskave bodo lahko v pomoč vsem udeležencem svetovnega spleta. Uporabniki bodo dobili vpogled v aktualno stanje in napotke za preglednejše delo, skrbniki spletnih strani bodo spoznali tri prepletajoče se koncepte in odnose med njimi, ki jih je potrebno razumeti, saj v nasprotnem primeru ne bodo kos novim tehnologijam in poslovnim izzivom. Pridobljena spoznanja bodo lahko koristna tudi za nacionalne kot tudi za internacionalne organizacije, ki so vpletene v regulacijo svetovnega spleta.

Metode dela, ki smo jih uporabili pri izdelavi magistrskega dela, temeljijo na proučevanju teoretične podlage, ki nam daje osnovo oziroma celovit pregled nad obravnavano tematiko in empiričnem preverjanju zastavljenega konceptualnega modela.

Pri oblikovanju konceptualnega modela smo se naslonili na strokovno literaturo tujih in domačih avtorjev, vire, prispevke, članke z novejšimi teoretičnimi spoznanji s področja interneta, zasebnosti, varnosti in zaupanja. Spoznanja o zasebnosti, varnosti in zaupanju na internetu, ki predstavljajo prakso v tujini, smo poskušali prenesti v magistrsko delo ter opozoriti na nevarnosti in priložnosti, ki čakajo morebiti tudi nas. Poleg izbrane literature smo vključili tudi lastno znanje, pridobljeno v praksi, na področju naprednih tehnologij in tekom študija na magistrskem programu. V nalogi so vključene tudi informacije, pridobljene v pogovoru s sodelavci, iz poslovnih poročil podjetij in njihovih internih virov.

Magistrsko delo je zastavljeno tako, da smo poskušali iz obstoječe literature in s pomočjo že opravljenih raziskav izluščiti področja, ugotovitve in posebnosti, ki bi jih bilo potrebno upoštevati pri analizi treh konceptov v elektronskem okolju, kar je sicer prva faza pred empiričnim preverjanjem.

Na podlagi teoretičnih spoznanj smo se lotili kvantitativne raziskave, s katero smo poskusili najti relacije med triado že omenjenih konceptov. Raziskovalna metoda pri pridobivanju primarnih podatkov je opisna, raziskovalni instrument pa je spletni vprašalnik, ki ga sestavljajo vprašanja odprtega in zaprtega tipa:

- vprašanja tipa z več možnimi odgovori,
- dihotomno vprašanje (DA ali NE),
- Likertova lestvica strinjanja/nestrinjanja,

Na ta način smo poskušali sprejeti ali zavrniti privzete hipoteze, predvsem pa postaviti primerno podlago tudi za morebitna nadaljnja raziskovanja tega področja. Hkrati smo podali celovit pogled na analizo poslovanja elektronskih podjetij.

Struktura magistrskega dela je zasnovana na principu »od zgoraj navzdol«, kar pomeni, da smo od bolj splošnih tem prehajali na bolj podrobne. Po uvodu smo se najprej v drugem poglavju posvetili metodologiji in opredelitvam različnih izrazov, ki se pogosto uporabljajo pri opisovanju elektronskega okolja, kar je služilo za prijeme, s katerimi smo definirali termin e-okolje. Nadalje smo na kratko predstavili povezavo med elektronskim poslovanjem in ekonomijo ter družbo, s poudarkom na slovenskih razmerah. Elektronsko poslovanje namreč ni pojav, s katerim se ukvarjajo samo podjetja, in ne živi sam zase, ampak je po eni strani odraz značilnosti današnje družbe in ekonomije, po drugi strani pa je tudi dejavnik, ki to družbo in ekonomijo oblikuje. Poglavje smo zaključili s statističnimi pregledi najaktualnejših kazalnikov, s katerimi se proučuje digitalna osveščenost uporabnikov in razvitost evropskih držav.

V tretjem poglavju smo predstavili koncept zasebnosti. Najprej smo si pogledali nekatera znanstvena spoznanja uglednih avtorjev. Sledila je opredelitev zasebnosti iz pravnega oziroma

zakonskega zornega kota. Na kratko smo predstavili smisel nadzorovanja kot proces, ki poskuša zaznati in zabeležiti dejstva oziroma aktivnosti posameznika. Spoznali smo pobudnike in izvajalce nadzora ter njihov namen, ki je v nadaljevanju služil kot izhodišče za preverjanje parodoksalne dvojnosti – ali je nadzor dober ali slab. Ugotovili bomo, da se država in podjetja poslužujejo nadzora z natančno določenimi cilji. Slednje smo poskusili spoznati in preveriti z empirično raziskavo pri ponudnikih tovrstnih storitev. Ker smo želeli celotno delo pripraviti transparentno in objektivno, nas je zanimalo, kaj o ugotovljenih namenih in ciljih menijo »žrtve« nadzora – uporabniki interneta.

Predstavitev spoznanj in osvetlitev šibkih točk pri elektronskem poslovanju preko interneta ter opozorilo na potencialne nevarnosti, ki na nas prežijo ob njegovih storitvah, je tema četrtega poglavja. Ogledali smo si tehnologijo in metodologijo uvajanja sodobnih varnostnih mehanizmov, s katerimi se lahko le začasno onesposobi, ne pa tudi prepreči vdor v zasebni informacijski sistem. Seveda smo spoznali še druge metode, ki lahko ogrožajo našo varnost. Na koncu poglavja smo nakazali zaščitne ukrepe, predvsem v smislu samozaščite, s katerimi smo predstavili varnost kot proces in ne izdelek, ki se ga da kupiti.

Sledi seznanitev s konceptom zaupanja. Rdeča nit petega poglavja je misel, da je internet potrebno razumeti kot okolje, v katerem je zaupanje ključnega pomena. Gre za zaupanje, ki temelji na znanju, zato emotivno komuniciranje zaupanja ali gradnja ugleda nista dovolj. Najprej je bilo potrebno celovito opredeliti zaupanje. Pogledi različnih avtorjev so združeni v skupno celoto. Prikazani so temelji zaupanja in pogoji, ki morajo biti izpolnjeni, da se zaupanje lahko pojavi. Za njegovo natančnejšo opredelitev smo pregledali vidike zaupanja, kjer smo izmed množice opredelitev poiskali najustreznejšo. Pri pojavu zaupanja so pomembni tudi elementi racionalnosti in utilitarnosti ter temelji in viri za zaupanje, ki so opisani v nadaljevanju. Nadalje smo predstavili vrste zaupanja ter povezavo med zaupanjem, zasebnostjo in varnostjo. Strokovne opredelitve s področja odjemalcev smo smiselno povzeli ter v nadaljevanju pojasnili pomen tega koncepta za uspešno poslovanje podjetja. Peto poglavje smo zaključili z opredelitvijo ključnega odnosa med zaupanjem in nezaupanjem na spletu in navedbo rešitev, ki so potrebne, da se slednje spremeni v zaupanje.

Po predstavitvi literature na področju zasebnosti, varnosti in zaupanja na internetu smo oblikovali lasten konceptualni model. Razširjen konceptualni model sestavljajo trije glavni koncepti in en pomožen, ki bo nakazal možnosti nadaljnjih raziskav.

V šestem poglavju smo oblikovali raziskovalne domneve, opisali metodologijo in operacionalizirali spremenljivke, katere smo izmerili z empirično raziskavo. V raziskovalnem načrtu smo tudi predvideli postopek zbiranja podatkov in opisali strukturo raziskave. Menili smo, da je najboljša komunikacijska pot, ki bi služila za raziskavo javnega mnenja, ravno internet. Izvedli smo spletno anketo, s katero smo preverili osveščenost naključnega uporabnika internetnih tehnologij. V tem poglavju so tudi prikazani rezultati. S pomočjo analize preizkušanja domnev smo preverili veljavnost postavljenih raziskovalnih domnev. Na koncu poglavja smo ovrednotili raziskavo in povzeli ugotovitve teoretičnega dela konceptualnega

modela. Sledijo odprta vprašanja za prihodnje raziskave in predstavitev perspektivnosti razvoja spleta kot varnega medija za prenos elektronskih informacij, elektronskega poslovanja in drugih oblik komuniciranja.

Magistrsko delo smo zaključili s sklepnim poglavjem, kjer smo ugotovitve prejšnjih poglavij povezali z osnovnimi hipotezami dela.

2 TEMELJNI POJMI

Razširjenost in pomembnost elektronske tehnologije sta dandanes že tako veliki, da vsepovsod govorimo o elektronskem okolju, elektronski ali digitalni družbi in ekonomiji, novi ekonomiji, elektronskem poslovanju. Tehnologija je zares posegla v večino dejavnosti človeške družbe, njen vpliv pa bo po vsej verjetnosti v prihodnosti še večji. Velikokrat so izrazi, s katerimi skušamo opisati to dogajanje, zelo slikoviti, vendar zavajajoči in nenatančni. Čeprav je intuitivno mogoče razumeti, o čem je govora, manjka natančnost in konsistentnost izrazov, zato bomo najprej poskušali opredeliti, kaj razumemo z izrazoma: "nova ekonomija" in "elektronsko poslovanje", ki se pogosto uporabljata in ju uporabljamo tudi v magistrskem delu.

Preden začnemo s preučevanjem elektronskega poslovanja, bomo zavoljo jasnosti in razumljivosti opredelili nekatere pogosto uporabljene pojme.

2.1 EKONOMIJA NOVIH RAZSEŽNOSTI

Dramatična rast elektronskega poslovanja prek interneta in svetovnega spleta na številne načine spreminja naše življenje, delo in zabavo. Ena izmed najpomembnejših sprememb, ki smo jim priča, je prehod iz "industrijske ekonomije" v "novo ekonomijo"[1]. Prehod iz ekonomije, ki temelji na preverjenih kapitalističnih vrednotah in proizvodnji, k ekonomiji, ki temelji na računalnikih, povezljivosti in človeškem znanju. Vse to povzroča spremembe v načinu ustvarjanja, proizvajanja, prodajanja ter distribucije izdelkov in storitev (McKeown, 2001, str. 1).

Izrazi, kot so nova ekonomija (*angl. new economy*; npr. v Tyson, 1999, str. 1 ali Tapscott, 1995, str. 44), digitalna ekonomija (*angl. digital economy*; npr. v Brynjolfsson in Kahin, 2000, str. 2 ali Tapscott, 1995, str. 2), internetna ekonomija (*angl. internet economy*; npr. v Choi in Whinston, 2000, str. 2), ekonomija znanja (*angl. knowledge economy*; npr. v Kim, Mauborgne, 2003, str. 134), ekonomija omrežij[2] (*angl. network economy*; npr. v Achrol, Kotler, str. 147), so danes

[1] Namesto izraza nova ekonomija se pogosto pojavljajo tudi izrazi internetna ekonomija, digitalna ekonomija, mrežna ekonomija in informacijska ekonomija.

[2] Slovenski pravopis (2001, str. 887) ločuje pri izrazu "mreža" dva pomena. Prvi se nanaša na fizičen predmet (npr. ribiška mreža), drugi pa na povezave med osebami, objekti (npr. cestne, trgovske). Za mrežo v drugem smislu (torej povezave) najdemo na istem mestu sopomenko "omrežje". Izraz *network* zato prevajam z omrežje, saj ne gre za mrežo v smislu predmeta, ampak za mrežo v smislu povezav med posamezniki, organizacijami, računalniki in podobnim.

splošno uporabljani v množičnih medijih in tudi strokovni literaturi, ker želijo poudariti nekatere značilnosti, ki jih opažamo v sodobnih gospodarstvih, in do sedaj niso bile prisotne v večjih razsežnostih. Tapscott (1995, str. 44–68) navaja 12 pojavov, ki oblikujejo značaj ter podobo nove ekonomije in zaradi katerih se le-ta razlikuje od "stare", tradicionalne ekonomije. Ti pojavi so znanje, digitalnost, virtualnost, molekularnost, omrežja, zmanjšanje vloge posrednikov, konvergenca, inovativnost, zbliževanje potrošnikov in proizvajalcev, hitrost, globalizacija ter neravnovesje in jih v nadaljevanju kratko povzemamo po avtorju ter dopolnjujemo z drugimi pogledi.

1. **Znanje**. Nova ekonomija je ekonomija znanja (*angl. knowledge economy*): pomembna konkurenčna prednost za podjetja so ljudje, torej zaposleni in njihovo znanje, vedno več dodane vrednosti ustvarja intelekt in ne fizična moč. Proizvodi in storitve vsebujejo vedno več znanja, saj postajajo zamisli potrošnikov, informacije in tehnologija njihov pomemben del: "pametne kartice", "pametni avtomobili", "pametni telefoni", "pametni spletni portali" predstavljajo le nekaj primerov dobe "pametnih proizvodov", ki pričenjajo radikalno spreminjati različne aspekte sodobne družbe. Choi in Whinston (2000, str. 8) uporabljata zato izraz "pametna ekonomija" (*angl. smart economy*).

   Tapscott (1995, str. 7) poleg tega ugotavlja, da je tudi v kmetijstvu in industriji vedno več delovnih mest, kjer je pomembno predvsem znanje (*angl. knowledge work*). Skoraj 60 % Američanov dela na delovnih mestih, ki zahtevajo uporabo človeškega znanja, medtem ko je kar 80 % novih delovnih mest nastalo v informacijsko intenzivnih sektorjih gospodarstva. Avtor tako trdi (1995, str. 47), da bo v novi ekonomiji kapital vedno bolj postajal funkcija znanja, zato je za podjetja pomembno, da pridobijo, zadržijo in povečujejo znanje svojih zaposlenih ter zagotovijo kreativno in inovativno delovno okolje. Edina dolgoročno vzdržljiva konkurenčna prednost pa bo postala sposobnost organizacije za neprestano učenje (*angl. organizational learning*).

2. **Digitalnost**. Nova ekonomija je digitalna ekonomija (*angl. digital economy*): podjetja uporabljajo informacije v digitalni oziroma elektronski obliki, podatki so spravljeni na elektronskih nosilcih podatkov in v računalniških bazah podatkov, omrežjih, sistemih in podobno. Izmenjava podatkov in informacij ter poslovne transakcije potekajo preko elektronskih omrežij. Analogne in fizične informacije, ali, kot pravi Negroponte (1996, str. 12), atome zamenjujejo biti, analogno komunikacijo in tehnologijo pa digitalna vsebina.

3. **Virtualnost**. Zaradi digitalizacije lahko postajajo fizične stvari virtualne, kar vpliva na metabolizem gospodarstva, tip možnih institucij in odnosov ter naravo same ekonomske aktivnosti, na primer: virtualne volilne skrinjice, virtualne oglasne deske, virtualne konference, virtualna podjetja, virtualne državne agencije, virtualni trgovski centri, trgi, trgovine in drugo.

4. **Molekularnost**. Nova ekonomija je molekularna ekonomija (*angl. molecular economy*): organizacijska struktura, ki je značilna za tradicionalna podjetja, se razgrajuje, postaja bolj sploščena, nadomeščajo jo dinamične molekule in grozdi (*angl. clusters*) posameznikov ali skupin, ki oblikujejo osnovo za ekonomsko aktivnost. Podjetja z molekularno strukturo temeljijo na posameznikih (zaposlenih z znanjem), ki delujejo kot posamična poslovna enota. Takšna struktura se lahko razširi tudi na celotno ekonomijo in tako se bomo, namesto z množičnimi mediji ali množično proizvodnjo, srečevali z molekularnimi mediji ter molekularno proizvodnjo. To pomeni, na primer, da posamezniki (uporabniki, kupci) ne bodo več omejeni na program, ki ga je zanje pripravila televizijska hiša, ali proizvod, ki ga je izdelalo podjetje, ampak bodo lahko izbirali med velikim številom posameznih oddaj in jih kombinirali v "svoj" program, ali pa sami določali lastnosti, ki jih zahtevajo pri želenem proizvodu.

5. **Omrežja**. Nova ekonomija je ekonomija omrežij (*angl. networked economy*): povezovanje v omrežja ni značilno le za tehnologijo, ampak tudi za ljudi, podjetja, organizacije, interesne skupine in družbo. Povezovanje z drugimi podjetji za izvajanje poslov in projektov je postalo običajen način dela in priložnost za majhna podjetja, da premagajo glavni prednosti velikih konkurentov: ekonomijo obsega in dostop do virov.

6. **Zmanjšanje vloge posredništva** (*angl. disintermediation*). Digitalna omrežja odpravljajo potrebo po posrednikih med proizvajalci in potrošniki. Posredniki (podjetja, poslovne funkcije ali posamezniki) morajo odkriti novo dodano vrednost, ki jo lahko ponudijo, sicer ne bodo več potrebni. Sledili bodo novi načini podjetniškega sodelovanja z novimi tipi posredništva (*angl. reintermediation*).

7. **Konvergenca**. Ključni sektor nove ekonomije predstavljajo novi mediji, ki so rezultat konvergence različnih panog: računalniške, komunikacijske in panog, ki ustvarjajo vsebino (*angl. content industry*, na primer založbe, zabavna industrija, televizijska in kabelska omrežja in podobno).

8. **Inovacije**. Nova ekonomija temelji na inovacijah, ki so gibalo ekonomske aktivnosti in poslovnega uspeha, glavni vir vrednosti pa postaja človeška domišljija. Podjetja si morajo prizadevati k razumevanju potreb kupčevega kupca in si zamišljati tisto, česar si na trgu še ne predstavljajo. Za to je potrebno tudi poslovno okolje, ki ne kaznuje tveganih potez in kjer lahko cvetita kreativnost in človeška domišljija.

9. **Zbliževanje proizvajalcev in potrošnikov** (*angl. prosumption*). Potrošniki so v novi ekonomiji soudeleženi v dejanskem proizvajalnem procesu, saj posamezniku prilagojena množična proizvodnja (*angl. mass customization*) zahteva, da podjetja izdelujejo proizvode, ki vsebujejo in odražajo zahteve in okuse posameznih potrošnikov. Uporabniki (proizvodov, tehnologije, informacij) postajajo tudi oblikovalci in včasih proizvajalci, s tem pa se hkrati briše meja med njimi.

10. **Hitrost**. Nova ekonomija je ekonomija, ki poteka v dejanskem času (*angl. real time economy*): digitalizacija je omogočila elektronsko poslovanje, ki se odvija v trenutku, zato je za uspeh podjetja pomembna hitrost poslovnih transakcij, hitrost komunikacije in tudi hitrost, s katero se prilagaja spreminjajočim se pogojem poslovanja ter vedno krajšim življenjskim ciklom proizvodov.

11. **Globalizacija**. Nova ekonomija je globalna ekonomija: znanje, kot ključni vir konkurenčne prednosti podjetij, ne pozna meja, zato so tudi za podjetja vedno manj pomembne nacionalne ekonomije, vedno bolj pa ena sama, svetovna ali globalna ekonomija. Z razvojem globalnih omrežij imajo podjetja lažji dostop tudi do geografsko oddaljenih trgov in potrošnikov, prav tako pa do znanja oziroma ljudi na oddaljenih lokacijah.

12. **Neravnovesje**. Nova ekonomija poglablja socialna neravnovesja, na primer med dobro plačanimi zaposlenimi, ki imajo ustrezno znanje, in odvečnimi zaposlenimi z neustreznim znanjem, med ljudmi, ki imajo dostop do znanja, in tistimi, ki ga nimajo in podobno.

Goldhaber (1997) poleg tega opaža, da je zaradi prenasičenosti okolja z vsakovrstnimi informacijami in omejenim časom posameznika vedno težje vzbuditi pozornost potencialnih kupcev, dobaviteljev ali investitorjev, zato govori o "ekonomiji pozornosti" (*angl. attention economy*), saj meni, da je ravno to tista redka dobrina, ki lahko prinese uspeh podjetju.

Do sedaj smo izraz "nova ekonomija" razlagali v njegovem širšem pomenu. Bolj ozko pa se takšno poimenovanje večinoma nanaša na del celotne ekonomije oziroma gospodarstva, kjer so zgoraj navedene lastnosti še posebej očitne in relativno bolj pomembne glede na ostale panoge; temu delu ali sektorju gospodarstva pravimo "nova ekonomija" (v tem smislu ga uporabljamo tudi v nadaljevanju magistrskega dela, zato bodo narekovaji izpuščeni). Tvorijo ga predvsem podjetja, ki se ukvarjajo z dejavnostmi, za katere je informacijska tehnologija (če uporabimo najbolj splošen izraz) osrednjega pomena, bodisi v smislu, da je to proizvod oziroma storitev podjetja, bodisi v smislu infrastrukture, ki je potrebna za izvajanje dejavnosti podjetja. Sem spadajo na primer telekomunikacijska podjetja (operaterji fiksne in mobilne telefonije, proizvajalci telekomunikacijske opreme), podjetja, ki proizvajajo računalniško strojno opremo (*angl. hardware*), podjetja, ki razvijajo programsko opremo (*angl. software*), ponudniki internetnih storitev (*angl. internet service providers – ISP*), podjetja, ki ponujajo storitve na področju informacijske tehnologije ostalim podjetjem (svetovanje, vzdrževanje infrastrukture, nastop na internetu in podobno) in podjetja, ki svojo dejavnost opravljajo v internetnem prostoru (Marc, 2003, str. 8).

Choi in Whinston (2000, str. 5) opredeljujeta tudi izraz "internetna ekonomija" v širšem ali ožjem pomenu. V širšem pomenu gre za del gospodarstva, ki se ukvarja z informacijskimi dobrinami (programska oprema, vsebina na spletnih straneh, novi mediji, podpora podjetjem). V ožjem pogledu pa uporabita internet in omrežja za osnovo definicije. Internetna ekonomija se odvija na internetu, vanjo pa so vključena podjetja, ki se ukvarjajo predvsem z e-poslovanjem (*angl. e-business sector*). V tem smislu bomo izraz uporabljali tudi v magistrskem delu.

2.2 POJEM ELEKTRONSKEGA POSLOVANJA

Nekatere opredelitve razumejo elektronsko poslovanje le v ožjem smislu, preprosto kot izmenjavo podatkov med računalniki ali kot elektronsko trgovanje (*angl. electronic commerce*). Pojem elektronsko poslovanje res izhaja iz angleškega izraza "electronic commerce", vendar pa le-ta ne odraža polne vsebine pojma elektronskega poslovanja.[3] Zato se v angleškem jeziku vse bolj uporablja pojem "electronic business", ki je širši in zato pravilneje odseva vsebino pojma elektronskega poslovanja. Večina opredelitev si je tako enotna v tem, da pojma elektronsko poslovanje ne moremo več razumeti le v ožjem smislu. Elektronsko poslovanje (*angl. electronic business*) je širši pojem in se nanaša na vse, pri čemer s pomočjo interneta lahko omogočamo večjo učinkovitost, hitrost, inovacije in ustvarjanje nove vrednosti v organizacijah. To je taktična ali strateška uporaba interneta, ki spremeni poslovna razmerja med podjetjem in strankami, med podjetji, znotraj enega samega podjetja ali celo med samimi strankami.

Podobno definira elektronsko poslovanje Jerman Blažičeva (2001, str. 11), ki pravi, da imenujemo elektronsko poslovanje "vse, kar danes delamo v sklopu svoje poslovne dejavnosti s pomočjo računalniških aplikacij in računalniških omrežij". Ta pojem zajema: elektronsko bančništvo, elektronsko trženje, elektronsko trgovanje, spletno trgovino, svetovanje na daljavo, elektronsko zavarovalništvo, računalniško podprto skupinsko delo ter delo, pouk in dražbe na daljavo.

Tudi Cunningham in Fröschl (1999, str. 9) se strinjata, da zajema elektronsko poslovanje veliko več kot le elektronsko trgovanje. Pomeni povezovanje informacijske tehnologije, predvsem interneta, v poslovne procese, ki spreminjajo organizacije in ustvarjajo nove. Informacijska tehnologija je v zadnjih tridesetih letih povečala učinkovitost in produktivnost poslovnih procesov, ni pa jih spremenila. Spremenilo jih je elektronsko poslovanje. V elektronskem poslovanju in poslovnih procesih je informacijska tehnologija postala nepogrešljiva, medtem ko je bila v prejšnjih modelih le podporna funkcija.

V preteklosti je elektronska izmenjava podatkov po zasebnih omrežjih zahtevala velike finančne naložbe in je bila zato za mnoga mala in srednje velika podjetja praktično nedosegljiva. S prihodom interneta pa sta RIP[4] in elektronsko poslovanje postala dostopna tudi najmanjšim podjetjem, kar je povzročilo pravi razcvet in eksponentno rast elektronskega poslovanja. Podjetja vseh velikosti lahko sedaj med seboj komunicirajo elektronsko in sicer preko javnega omrežja (internet), preko omrežij znotraj podjetij (intranet) oz. omrežij, namenjenim za izbrana podjetja in njihovim poslovnim partnerjem (ekstranet) ter preko privatnih omrežij (Radoš, 1999, str. 35).

---

[3] Zato se zdi primerno za angleški izraz "electronic commerce" uporabiti prevod elektronsko trgovanje ter definicijo Svetovne trgovinske organizacije, ki elektronsko trgovanje opredeljuje kot proizvodnjo, distribucijo, trženje, prodajo ali dostavo blaga in storitev po elektronski poti. Konkretna transakcija elektronskega trgovanja lahko vsebuje več elementov oziroma sestavin poslovnih transakcij, med katerimi sta najbolj določujoča dostava ter plačilo.

[4] Računalniška izmenjava podatkov (*angl. EDI – Electronic Data Interchange*)

TABELA 1: Razlika med tradicionalnim elektronskim poslovanjem in elektronskim poslovanjem na internetu

Tradicionalno elektronsko poslovanje	Elektronsko poslovanje na internetu
• Podjetje – podjetje • Podjetje – državna uprava	• Podjetje – podjetje • Podjetje – državna uprava • Porabnik – podjetje • Porabnik – državna uprava
Zaprti "klubi", največkrat panožno specifični	Neomejen trg, globalen obseg
Omejeno število partnerjev	Neomejeno število partnerjev
Zaprta zasebna omrežja	Odprta omrežja
Poznani in preverjeni partnerji	Poznani in nepoznani partnerji

Vir: Radoš, 1999, str. 36.

Iz zgornje tabele lahko vidimo, da imamo opravka z dvema različnima modeloma e-poslovanja. Na eni strani je tradicionalni model, ki je visoko strukturiran in reguliran, na drugi pa internetni model, ki to ni. Internet je zameglil tradicionalno elektronsko poslovanje in hkrati pospešil uvajanje novih tehnologij. Odprto omrežje je privabilo nove uporabnike, ki lahko na enostaven in relativno ugoden način vzpostavijo stike s svojimi partnerji preko novega komunikacijskega kanala – svetovnega spleta.

2.3 ELEKTRONSKA DRUŽBA PRIHODNOSTI

Elektronsko poslovanje je relativno nov pojav, vendar postaja vse bolj samoumeven način poslovanja v sodobni razviti družbi in ekonomiji, zlasti v poslovanju podjetij. Izvedljivost in uspešnost elektronskega poslovanja, ki ju nameravamo analizirati, sta odvisni tudi od značilnosti elektronskega okolja. S tem mislimo na infrastrukturo, ki omogoča takšno poslovanje in na razširjenost uporabe ter obvladovanje potrebne tehnologije med prebivalci in podjetji.

Prihod informacijske dobe pomeni, da se znanje oziroma informacije v vedno večji meri uveljavljajo kot sredstva za doseganje družbene blaginje. V poslavljajoči se industrijski dobi je vloga nosilcev blagostanja pripadala kapitalu, delu in zemlji. S prihodom informacijske dobe so našteti dejavniki izgubili relativen pomen. Odločilen dejavnik blagostanja posameznikov, poslovnih organizacij in držav je postala zmožnost obdelovanja informacij.

Premik težišča od dela, kapitala in zemlje k informacijam in znanju opisujemo z več enakovrednimi pojmi. Naj navedemo nekaj najbolj značilnih (Boar, 1997, str. 5):

- Informacijska doba: uporaba in izkoriščanje informacij v vseh oblikah je osnova za ustvarjanje vrednosti. Interaktivne, operativne večpredstavne vsebine (besedilo, slika, zvok, video) bodo prevladovale v vseh oblikah človeške dejavnosti.

- Kibernetska korporacija: poslovanje je popolnoma informatizirano. Zbiranje, obdelovanje in razširjanje informacij popolnoma prežema vse vidike poslovanja, tako osnovne, podporne in navidezne procese kot odnose s kupci, dobavitelji, poslovnimi partnerji in zaposlenimi.
- Digitalna ekonomija temelji na elektronskem trgovanju. Tržišče se premika v navidezni prostor, izdelki in storitve postajajo informacijsko intenzivni, namesto vrednostne verige za blago in storitve se uveljavlja informacijska veriga za blago in storitve.
- Navidezno podjetje: poslovanje poteka v navideznem, kibernetskem prostoru. Zaposleni so medsebojno povezani z elektronskimi sredstvi, zato lahko delajo kjerkoli in kadarkoli je to potrebno. Podjetja se z uporabo elektronskih sredstev med seboj dinamično povezujejo in vstopajo v poslovna zavezništva, pri čemer tradicionalno razumevanje podjetja izgublja pomen.
- Obdobje omrežne povezanosti: Poslovanje se preobraža iz hierarhične v horizontalno organizacijsko strukturo. Delo opravljajo omrežno povezane skupine, ki se osredotočajo na vrednostne tokove, nasprotno od tradicionalne, hierarhično organizirane birokracije, ki se osredotoča na opravila.
- Družba znanja (*angl. knowledge society*): proizvodnja dobrin je tesno povezana z uporabo znanja, ki v tej vlogi izpodriva zemljo, kapital ali delo. Ustvarjanje, procesiranje in razpečevanje informacij postaja osnovna zaposlitev večine ljudi.

Prehod v informacijsko družbo zahteva temeljito preobrazbo vseh družbenih struktur in povzroča vrednostno, kulturno, organizacijsko, lastninsko, institucionalno in tehnično prestrukturiranje družbe. Novo obdobje zaznamuje velika dinamika, ki jo povzroča uporaba informacijskih tehnologij. Čas za razvoj novih izdelkov in storitev se krči, poslovne priložnosti so vedno bolj kratkotrajne, zato so podjetja prisiljena iskati rešitve v globalnih strateških partnerstvih in povezavah. Konkurenca na globalnih trgih je čedalje ostrejša, zato morajo podjetja odkrivati nove tržne niše in jih izkoristiti pred prihodom konkurence. Lokalni trgi se umikajo globalnemu tržišču, nacionalnih gospodarstev ne bo mogoče zaščititi pred prihodom globalne konkurence. Vse to je pripeljalo do trdega boja za obstanek. Nekatera podjetja so začela iskati nove priložnosti, s pomočjo katerih bi pridobila konkurenčno prednost in včasih jih to pripelje na rob, bodisi pravne ali družbene sprejemljivosti.

Za informacijsko dobo je značilna dematerializacija poslovanja in vztrajna rast storitev. Vedno večji del poslovanja postaja odvisen od zbiranja in obdelovanja informacij ter njihovega distribuiranja. Spremenjen način poslovanja omogoča nove storitve in izdelke. Z uporabo informacijskih in komunikacijskih tehnologij se povečuje mobilnost ljudi, izdelkov in storitev. Mobilnost uporabnika, ki je omogočena z brezžičnim dostopom do interneta, odpira možnosti za nove načine dela (npr. Delo na domu, delo na terenu ...). Elektronski prostor predstavlja tudi za industrije, katerih poslovanje je pretežno materialnega značaja, pomemben komunikacijski in tržni kanal. Informacijska doba prispeva k reorganizaciji družbe in industrije in v temelju spreminja sistem proizvodnje in izmenjave dobrin ter storitev. Poleg pozitivnih lastnosti prinaša nova ekonomija tudi nekaj negativnih. Ena izmed negativnih posledic nove ekonomije, ki

sovpada s temo magistrskega dela, je nevarnost pred vdorom v zasebno sfero posameznika in težave z zagotavljanjem varnosti, kar prispeva k nastajanju vedno bolj trnate poti za pridobivanje zaupanja uporabnikov interneta.

Čeprav so trditve, ki jih lahko pogosto prebiramo v tisku, da je internet največja iznajdba v zgodovini človeštva in pomeni revolucijo tudi na področju ekonomije in poslovanja podjetij, nekoliko pretirane, ne moremo mimo dejstva, da je informacijska tehnologija, vključno z internetom, postala pomemben del našega življenja. Hitra rast zmogljivosti računalniške tehnologije in razširjenost njene uporabe je zares impresivna.

2.4 RAZVOJ IN UPORABA INFORMACIJSKIH TEHNOLOGHIJ MED PREBIVALCI SLOVENIJE

Prehod v informacijsko družbo vnaša v sodobni svet korenite spremembe. Večina držav se zaveda tveganja, ki bi ga povzročilo zaostajanje za državami, ki uporabo informacijske tehnologije uspešno vključujejo v preobrazbo gospodarstva in družbe v celoti ter s tem omogočajo državljanom sodelovanje in aktivno udeležbo v procesih razvoja na vseh ravneh bivanja (Republika Slovenija v informacijski družbi, 2003, str. 5).

Tudi v Sloveniji se začenjamo zavedati pomena informacijske tehnologije v sodobnem življenju. Vlagamo v gradnjo infrastrukture in v izobraževanje, pričeli smo z uvajanjem e-poslovanja (v podjetjih in bankah, javni upravi, zavodu za zdravstveno zavarovanje, carinski službi), predvsem pa smo v letu 2000, kot ena prvih držav, dobili zakon o elektronskem poslovanju in podpisovanju, ki je usklajen z evropsko zakonodajo. Sprejet je bil nacionalni program razvoja telekomunikacij, ustanovljeno je bilo posebno (sedaj preteklo) Ministrstvo za informacijsko družbo (MID), ki pa je po drugi strani ugotavljalo, da imamo še vedno neliberaliziran trg telekomunikacijskih storitev, nepovezana omrežja za prenos podatkov in zato tudi visoke cene storitev (Ministrstvo za informacijsko družbo, 2000). Danes ni več tako. Pomembna konkurenca na področju fiksne telefonije so postali ponudniki govornih storitev preko protokola IP in operaterji mednarodnih prenosnih omrežij s ponudbo posredovanja mednarodnih klicev. Julija 2004 so začeli ponujati svoje storitve tudi operaterji mednarodnih telefonskih storitev na podlagi izbire in predizbire operaterja.

Direktorat za informacijsko družbo na Ministrstvo za visoko šolstvo, znanost in tehnologijo (2007) ugotavlja, da nas stanje informacijske družbe v RS v primerjavi z državami EU uvršča v povprečje. Delež širokopasovnega dostopa do interneta je leta 2006 v Sloveniji znašal 34 % (povprečje držav članic EU je 32 %). Ravno tako je visoka uporaba mobilne tehnologije, saj imamo 90 priključkov na 100 prebivalcev. S to razvitostjo sodi Slovenija v vrh držav članic EU (povprečje držav članic EU je 87). Po drugi strani pa je poslovanje preko interneta še na začetku svojega razvoja. Poleg nezainteresiranosti so uporabniki interneta navedli predvsem skrb za varnost (24 %), zasebnost (21 %) in pomisleke glede prejemanja in vračanja blaga (17 %). Ravno tako je v Sloveniji pomanjkljiva ponudba e-vsebin. Predvsem je opazno pomanjkanje

ponudbe kakovostnih e-vsebin na področju e-zdravja, e-učenja, kulturne dediščine, e-poslovanja, e-prostora in e-vsebine za informiranje in podporo potrošnikov.

Ministrstvo za visoko šolstvo, znanost in tehnologijo (2007) je v letošnjem letu pripravilo strategijo razvoja informacijske družbe po strateškem okviru i2010[5]. Strategija obsega tri osnovna področja izvajanja ukrepov:

- dokončna vzpostavitev enotnega evropskega informacijskega prostora, ki spodbuja odprt in konkurenčen notranji trg za informacijsko družbo in medije;
- povečanje inovacij in investicij v raziskave na področju IKT za spodbujanje rasti ter večjega števila in boljših delovnih mest;
- vzpostavitev vključujoče evropske informacijske družbe, ki spodbuja rast in zaposlovanje na način, ki je skladen z načeli socialnega vključevanja, trajnostnega razvoja in daje prednost boljšim javnim storitvam in kakovosti življenja.

Prednost elektronskega poslovanja in interneta za potrošnike je priročnost, omogoča nižje cene, osebno prilagajanje, celovitost in večjo širino ter globino ponudbe informacij, proizvodov in storitev interaktivne skupnosti. V Sloveniji je bila širitev interneta zaradi odprtosti do novih tehnologij razmeroma poceni (za evropske razmere) telefonskih impulzov ter Arnesove politike v prvih letih ena hitrejših v Evropi. Predvsem izobraženi in računalniško orientirani uporabniki so začeli uporabljati internet zelo zgodaj, ustavljalo se je pri preostali populaciji. Za glavnino populacije, ki je računalniško nepismena, niti ne zna angleško, bi bilo potrebno poslovanje z institucijami, kot so banke, javna uprava ali zdravstvene ustanove, s katerimi se vsakdo srečuje, prenesti na elektronske medije, kar bi ljudi "sililo" v uporabo interneta. Problem vsebin pa bo ostajal aktualen tudi takrat. (Vehovar, 2000).

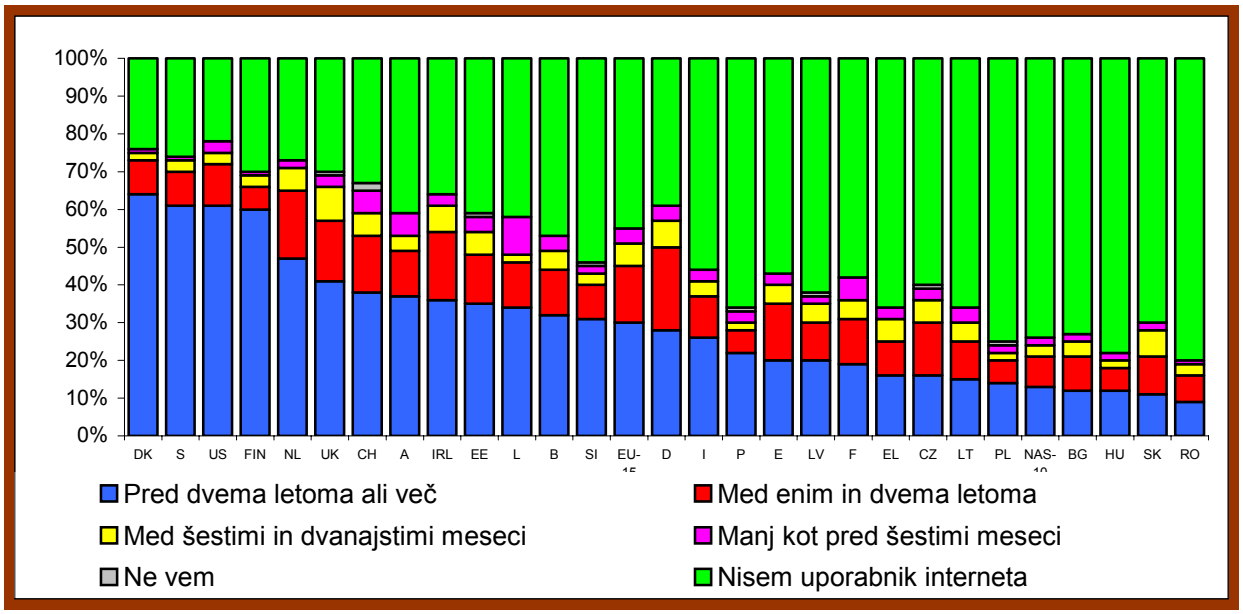
V nadaljevanju bomo predstavili nekaj izbranih in obdelanih podatkov, ki so se zbirali v času od leta 1998 do 2002. Podatki so bili zbrani z nacionalnimi raziskavami pod istimi merili in pogoji. Glavni pobudnik in vodja projekta je bila Evropska komisija, ki je pripravila projekt SIBIS (Statistical Indicators Benchmarking the Information Society), katerega slovenska članica je tudi Fakulteta za družbene vede. SIBIS-ov glavni cilj je bil proučiti stanje informacijske družbe po posameznih državah, ob tem pa tudi postaviti pilotne indikatorje, s pomočjo katerih bi lahko v prihodnje nadzirali napredek in razvoj. Zaradi obširnosti obravnavanega področja bomo le na kratko predstavili nekaj ugotovitev ter jih povezali z drugimi primerljivimi raziskavami na področju Slovenije.

Evropske države lahko po kriteriju razvitosti spletnih storitev in deležu "izkušenih" uporabnikov razdelimo v tri skupine. Države, ki beležijo podobno ali višjo razvitost kot ZDA, so: Danska, Švedska in Finska. V drugo skupino bi lahko razvrstili države, ki imajo med 50 in 30 %

[5] Pobuda i2010 je nastala pod okriljem Evropske komisije in njen namen je spodbuditi odprto in konkurenčno digitalno gospodarstvo in poudariti informacijsko komunikacijsko tehnologijo (krajše IKT) kot gonilno silo večje socialne vključenosti, kakovosti življenja, gospodarske rasti in konkurenčnosti (Ministrstvo za visoko šolstvo, znanost in tehnologijo, 2007).

uporabnikov interneta med celotno populacijo (Nizozemska, Velika Britanija, Avstrija, Irska, Estonija, Luksemburg, Belgija in Slovenija). Zanimivo je tudi to, da lahko skoraj vedno najdemo Estonijo v samem vrhu med takratnimi pridružitvenimi članicami EU. Preostanejo nam še predvsem mediteranske države, ki imajo le 30 % uporabnikov interneta z vsaj dvoletnimi izkušnjami.

SLIKA 1: Prva uporaba interneta v izbranih evropskih državah v letu 2002



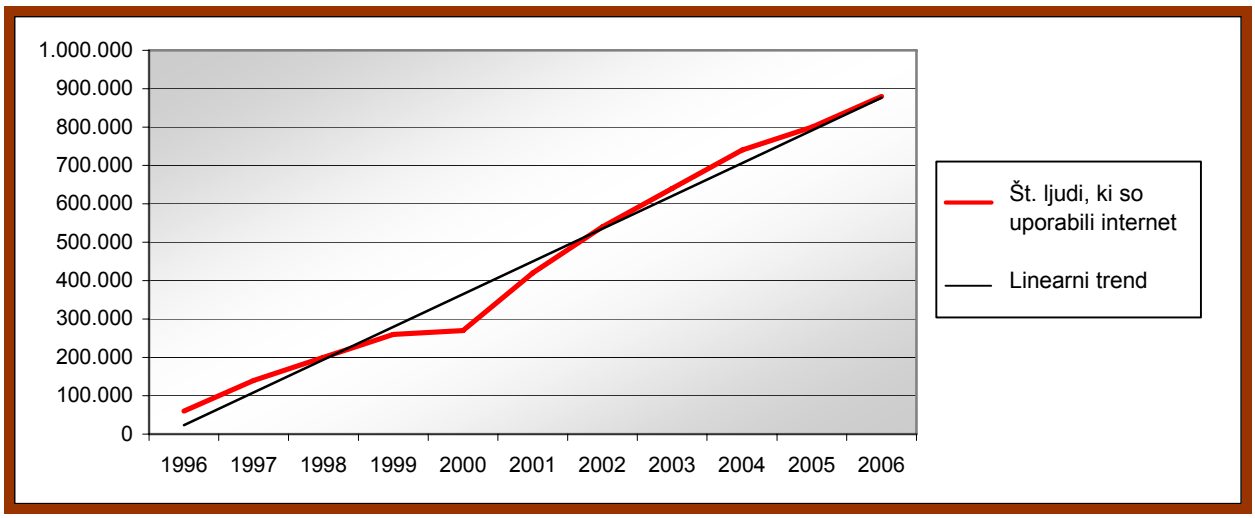
Vir: SIBIS, 2002/2003.

Podatki o prvi uporabi interneta so leta 2003 uvrščali Slovenijo tik nad evropsko povprečje, saj je 31 % populacije prvič uporabilo internet pred letom 2000 (EU-15: 30 %). Po drugi strani je bil delež manj izkušenih uporabnikov v Sloveniji med najnižjimi: 3,2 odstotka uporabnikov je začelo uporabljati internet med letoma 2001 in 2002 ter 1,5 odstotka uporabnikov je pričelo uporabljati internet v letu 2003 (EU-15: 5,9 in 3,8). Nižji odstotek uporabnikov, ki so začeli uporabljati internet v letu 2003, lahko opazimo le na Danskem, Finskem, Švedskem in v Romuniji. V Sloveniji je prišlo do te razlike zaradi visoke penetracije uporabe interneta na začetku in pojemanja v kasnejšem obdobju. To opažanje tudi potrjuje razlago o počasnejšem naraščanju številu novih uporabnikov v naslednjih nekaj letih. Kot kaže, se populacija, ki še ni nikoli uporabila interneta, zelo težko odloči za uporabo le-tega.

Število uporabnikov interneta se iz leta v leto veča. Zadnje merjenje, katerega rezultati so objavljeni na spletni strani www.ris.org, kaže, da je bilo leta 2006 880.000 aktivnih mesečnih uporabnikov interneta v Sloveniji. Slednja vrednost narašča z letno rastjo pod 10 %, kar potrjujejo tudi podatki Eurosata 2006, kjer je Slovenija na povprečju EU-25. Ocene projekta RIS

temeljijo na telefonskih anketah[6] (n=605). V spodnjem grafu so prikazani uporabniki, ki aktivno uporabljajo internet.

SLIKA 2: Uporabniki interneta v Sloveniji



Vir: Prirejeno po RIS, 2006.

Slovenija po številu aktivnih uporabnikov sovpada s povprečjem EU. Približno tretjina ga uporablja vsak dan, polovica pa skoraj vsak dan oziroma od pet- do sedemkrat na teden. Uporabniki interneta so mlajši, izobraženi in aktivni. To je populacija, ki jo je z drugimi mediji težko doseči.

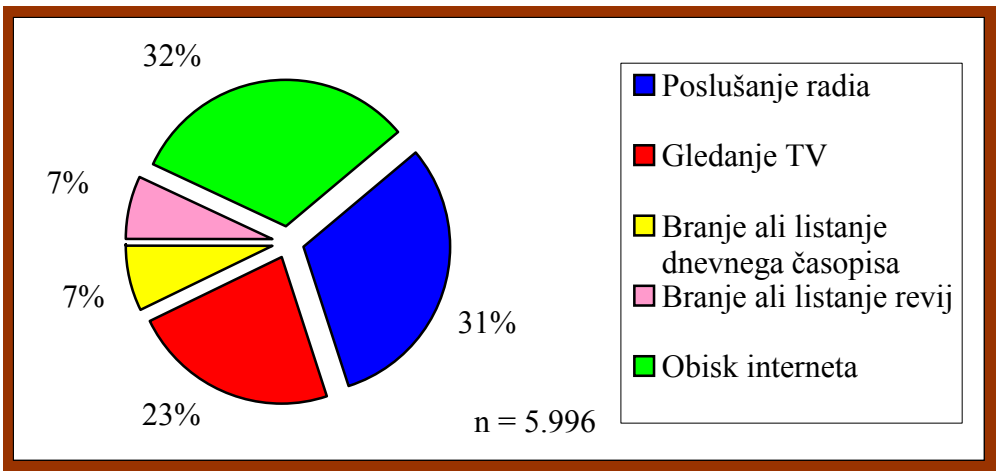
Internet je postal močno prodajno orodje, saj skoraj osem od desetih uporabnikov na internetu išče informacije o izdelku ali storitvi, ki jih zanima. Šest od desetih poskuša na internetu dobiti dodatne informacije o izdelku ali storitvi, za katero so videli oglas v drugem mediju, pet od desetih pa primerja cene istih ali sorodnih izdelkov ali storitev. Internet jim omogoča hiter in obsežen dostop do informacij, ki jih ne more zagotoviti noben drug medij. Podjetja, ki svojih izdelkov ali storitev na internetu ne oglašujejo, izgubljajo veliko morebitnih kupcev (Petrov, 2004).

Medijski načrtovalci, pa tudi oglaševalci, se navedenih dejstev čedalje bolj zavedajo in zato internet postaja sestavni del medijskih načrtov oglaševalskih kampanj. Biti ali ne biti na internetu ni več vprašanje. Vprašanje je, kako in koliko. To potrjuje podatek, da so v Sloveniji izdatki za oglaševanje na internetu letos prvič postali enakovreden sestavni del oglaševalskih oziroma trženjskih proračunov podjetij (Petrov, 2004).

[6] Ankentirancem je bilo zastavljeno naslednje vprašanje: »Ali uporabljate internet … pri tem mislimo tudi elektronsko pošto, www, ftp, WAP ali katerokoli drugo internet storitev«? (Možna odgovora: da, ne)

Anketa, ki je bila izvedena na spletnih straneh Najdi.si (2004), je pokazala, da je povprečni anketiranec pripravljen porabiti največ svojega časa za pregledovanje vsebine na internetu, sledi poslušanje radia (31 %) in gledanje televizije (23 %). Branje revij in listanje dnevnega časopisja se nahaja na zadnjem mestu. Zavedati se moramo, da to ni bil ravno reprezentativen vzorec, saj so vsi anketiranci tudi uporabniki interneta. Glede na to, da so preko slednjega oddali svoje glasove, lahko sklepamo, da bi bili rezultati na ravni celotne populacije oziroma naključnega vzorca nekoliko drugačni.

SLIKA 3: Dnevna uporaba posameznega medija



Vir: Najdi.si, 2004.

V prihodnje lahko pričakujemo, da se bo delež obiska interneta v primerjavi s pregledom oziroma poslušanjem medijev še povečeval. Vse večjo popularnost vsekakor spodbujajo vse boljši spletni informativni portali, kar povzroča izreden padec prodaje tiskanih medijev. Uporabniki so vse bolj pripravljeni verjeti novicam, ki jih dobijo preko spleta. Ponudniki radijskih, televizijskih in tiskanih vsebin so/bodo pričeli zbrane informacije posredovati tudi vzporedno preko interneta. Internet postaja globalno informacijsko središče, ki pridobiva vedno več uporabnikov, pripravljenih (deloma) opustiti obstoječe množične medije in preiti na uporabo medija z dodano vrednostjo.

Menimo, da bo rast uporabe interneta – tako v Sloveniji kot v EU – zmerna v obsegu nekaj odstotnih točk, kar je značilno, ko penetracija interneta preseže 50-odstotno raven, na kar nakazujejo izkušnje iz ZDA in skandinavskih držav. Ob tem ne gre pozabiti na izjemno rast interneta v zelo kratkem času. Da bi posamezen medij dosegel 50-odstotno penetracijo v gospodinjstvih, so na primer v ZDA časopisi potrebovali 100 let, telefon 70 let, kabelska televizija 40 let, računalniki pa 20 let; televizija in svetovni splet sta polovico gospodinjstev dosegla v samo osmih letih.

3 KONCEPT ZASEBNOSTI

Zasebnost[7] je temelj človeškega dostojanstva in drugih vrednot, kot npr. svobode združevanja in svobode govora. Pravica do zasebnosti je najpogosteje določena kot "meja, do katere družba lahko vdre v posameznikove zadeve" (Banisar et al., 1999).

3.1 NADZOR IN ZASEBNOST

Različni avtorji vidijo več dimenzij zasebnosti. Čebulj (1992, str. 7) navaja tri sestavine zasebnosti: zasebnost v prostoru (možnost posameznika, da je sam), zasebnost osebnosti (svoboda misli, opredelitve, izražanja) in informacijska zasebnost (možnost posameznika, da obdrži podatke in informacije o sebi, ker ne želi, da bi bili z njim seznanjeni drugi). Medtem, ko poročilo Privacy & Human Rights (Banisar et al., 1999) loči: prostorsko zasebnost, zasebnost telesa, informacijsko zasebnost in zasebnost komunikacij. V magistrskem delu se bomo opredelili predvsem na informacijsko zasebnost, saj je le-ta v sodobni družbi, poleg zasebnosti komunikacij, najbolj ogrožena.

Vprašanje (družbenega) nadzora je bilo eno pomembnih vprašanj v sociologiji 19. stoletja. Družbeni nadzor je predstavljal nekaj pozitivnega, nekaj, kar omogoča red in sobivanje posameznikov v družbi. Ross (1969, str. 2) trdi, da uspešno sodelovanje posameznikov zahteva visoko stopnjo družbenega reda, visoka stopnja družbene organizacije pa predstavlja nadzor. Hkrati pa je družbi potrebna še kakšna avtoriteta, ki razmejuje konflikte interesov posameznikov.

Marx govori o nadzoru kot o nečem, s čimer kapitalistični menedžer sili delavce k povečanju produktivnosti (Lyon, 1994, str. 25–26). Facault povezuje nadzor z disciplino, disciplinskimi mehanizmi, ki so jih razvile sodobne družbe, ki subtilno in posredno vsiljujejo normativno delovanje posameznikov in ker se za discipliranje posameznikov uporablja nadzor, je po Facaultu le-ta sredstvo podrejanja (Facault, 1984, str. 137–138). Zelo zanimiv je Facaultov t.i. panoptični učinek. Njegova moč ni posest, pač pa strategija. Tu gre predvsem za to, da veš, da te ta čas lahko nekdo opazuje. Doseže se neka negotovost, ki povzroči prostovoljno podrejanje posameznikov. Kovačič (2003, str. 21) navaja kot primer vsakdanjega opazovanja nadzor anketarjev ali pa videonadzor v veleblagovnicah.

Pomemben element nadzora je danes v dobi nove ekonomije "proizvodnja" dosjejev o posameznikih (tvorijo se baze podatkov), zato Lyon govori o družbi dosjejev (Lyon, 1994, 29–30). Posamezne ustanove in podjetja ves čas zbirajo, obdelujejo in posodabljajo evidence o subjektih. V vsakem trenutku se v neki bazi dopolni nov zapis, ki ga je povzročil naš obstoj. S pomočjo dosjejev lahko nadzorujemo dejavnosti in potrebe ljudi, baze podatkov pa omogočajo vpogled v pretekle dogodke. Nadzor nad posamezniki izvajajo tako vladne službe kot tudi

[7] Začetki zakonodaje, ki ščiti zasebnost, segajo že v leto 1361, ko je zakon Justices of the Peace Act predvidel kazni za osebe, ki so skrivaj opazovale druge posameznike ali jim prisluškovale (Kovačič, 2003, str. 35).

podjetja; menimo, da si bodo slednji pridobili v prihodnje vedno več podatkov o potrošnikih in to samo z enim ciljem – ugotoviti potrošnikove želje in navade ter prilagoditi ponudbo.

Beseda nadzor ima negativen prizvok, vendar ne smemo zanemariti njegove pozitivne plati, saj pripomore k zagotavljanju varnosti, vzdrževanju reda in udobja. Posvetili se bomo predvsem nadzoru, ki s pomočjo (orodja) interneta posega v našo zasebnost.

Pravica do informacijske zasebnosti se danes opredeljuje kot "pravica posameznika, ki zahteva, da se podatki in informacije o njegovih zasebnih razmerjih ne sporočajo komurkoli" (Čebulj, 1992, str. 7), in sicer tistim, ki za uporabo določenih podatkov in informacij niso pooblaščeni. Značilnost informacijske zasebnosti je torej nadzor pretoka in posredovanja podatkov, ki se nanašajo na nekega posameznika.

3.2 PRAVNI VIDIKI VARSTVA OSEBNIH PODATKOV NA INTERNETU

V Sloveniji je pravica do zasebnosti zajamčena z Ustavo Republike Slovenije[8], varstvo osebnih podatkov pa ureja Zakon o varstvu osebnih podatkov (ZVOP-1, Ur.l. RS, št. 86/2004). Predhodnik ZVOP-1 je bil ZVOP (ZVOP, Ur.l. RS, št. 59/2001), ki je bil za tiste čase med modernejšimi v Evropi (Čebulj, 1992, str. 48) in gledano primerjalno precej restriktiven, torej nudi posamezniku precejšnjo varstvo. Nadzor nad izvrševanjem Zakona o varstvu osebnih podatkov izvaja Inšpektorat za varstvo osebnih podatkov, ki rešuje tudi pritožbe posameznikov v zvezi z varstvom osebnih podatkov in zasebnosti. Poleg ZVOP-1 se varstva osebnih podatkov na internetu dotakne tudi Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP)[9], vendar le v obsegu, ki se nanaša na ureditev izdajanja kvalificiranih potrdil. Zakon je namenjen predvsem urejanju izmenjave in hranjenju sporočil v elektronski obliki. Na deklarativni ravni pravico do informacij zasebnosti zagotavlja tudi vrsta mednarodnih dokumentov. V izvedbeni ravni pa je v prvi vrsti pomemben Zakon o telekomunikacijah.

Berčič (2006) navaja še dva zakona, ki sta zelo pomembna, če gledamo z zornega kota tega dela, saj urejata problematiko pošiljanja vsiljene elektronske pošte (več o slednji je zapisano v

[8] Ustava RS vsebuje vrsto pravic, ki se nanašajo na osebno sfero. Pri tem magistrskem delu je pomembna določba 38. člena Ustave RS, ki zagotavlja varstvo osebnih podatkov. S tem se naša ustava uvršča med tiste redke ustave, ki vsebujejo določbe o varstvu osebnih podatkov in jih uvrščajo med temeljne pravice in svoboščine (Ude, 1996, str. 895–896).

[9] ZEPEP je v Sloveniji stopil v veljavo junija 2000. Skupaj z Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje predstavlja pravno podlago za proces, v katerem se bo zmanjšala količina dokumentnega poslovanja (Zdovc, 2002, str. 8). V veljavo pa prihaja novi zakon o elektronskem poslovanju in elektronskem podpisu, ki natančno določa odgovornosti za vsebino na internetu. Spremembe zakona so ugodne za ponudnike internetnih storitev, saj jih odvezujejo določenih odgovornosti za prepovedano ali škodljivo vsebino na njihovih strežnikih. Ponudniki ne bodo odgovorni za morebitno neprimerno vsebino, ki jo kdo drug objavlja na njihovih strežnikih ali se prek njih le prenaša, vendar le, če ne vedo zanjo. Če bodo vedeli za protipravno vsebino (pedofilsko gradivo, gradivo, ki spodbuja k rasni nestrpnosti, dokumente, ki kršijo varstvo osebnih podatkov, itd.), jo morajo nemudoma odstraniti ali onemogočiti dostop do nje (Zmagaj, 2004, str.10).

poglavju 4.3.2). Prvi je Zakon o varstvu potrošnikov (ZVPot), ki kot prejemnike nenaročenih reklamnih sporočil varuje potrošnike oziroma fizične osebe, drugi pa Zakon o elektronskem poslovanju na trgu (ZEPT). Slednji je bil sprejet lani, predvsem zaradi doslednega izvajanja določb EU o elektronskem poslovanju in velja za pravne osebe. Oba zakona delujeta po načelu »opti-in«[10] pošiljanja vsiljene pošte.

Za učinkovito zaščito zasebnosti na internetu pogosto ne zadoščajo splošni predpisi o varstvu osebnih podatkov. Globalna narava interneta pomeni hiter in nenadzorovan prenos podatkov čez državne meje. Ravno zaradi tega pravno varstvo zasebnosti in osebnih podatkov na internetu ne more biti učinkovito brez mednarodnega pravnega urejanja.

Pri vprašanjih zasebnosti in interneta je treba ves čas imeti v mislih naslednje vodilno načelo: pravo ne ščiti zgolj prostorov, lastnine in lastnikov, temveč posameznike, ki v določenem prostoru ali pri določenem ravnanju pričakujejo zasebnost. Pravno obravnavanje zasebnosti na internetu zadeva predvsem naslednje sklope med seboj povezanih vprašanj: tajnost in dostop do vsebine sporočil, posredovanih po internetu, ravnanje in dostop do "prometnih podatkov", ki so potrebni za posredovanje vsebinskih sporočil, identifikacijo udeležencev pri komuniciranju, varstvo osebnih podatkov ter samodejno obdelavo podatkov.

Zoran Perše (2000, str. 5) pravi, da je potrebno postaviti merila in različne načine učinkovitega varovanja osebnih podatkov in zasebnosti, ki se jih upošteva v ureditvi, pri čemer ne gre pozabiti na samozaščito, ki tudi zagotavlja učinkovite postopke za neposredno varstvo prek omrežij. Pripravi zakonodaje naj sledi ustrezna implementacija, predvsem z uporabo novih postopkov in tehnoloških orodij. Za kršitelje zakonskih predpisov o varstvu osebnih podatkov morajo biti določene primerne kazni. Le-te pa obravnava Kazenski zakonik RS, ki zlorabo osebnih podatkov opredeljuje v 154. členu[11] (Ur. l. RS. Št. 63/94, 70/94, 23/99).

3.3 ZASEBNOST NA SPLETU: PREMIKAJOČA SE TARČA

Povprečni uporabnik interneta za osebne in službene potrebe najpogosteje uporablja naslednje storitve interneta: elektronsko pošto, deskanje po svetovnem spletu, klepetalnice, novičarske

[10] Načelo opti-in zahteva predhodno privoljenje prejemnikov za prejemanje komercialnih sporočil. Slednje načelo določajo vsi omenjeni zakoni razen najliberalnejšega zakona – Zakona o varstvu osebnih podatkov, ki pa predpisuje načelo opti-out. ZVOP-1 pošiljatelju dovoljuje pošiljanje takih sporočil, če prejemniku obenem da na voljo tudi možnost, da se izpiše iz njegovega pošiljateljskega seznama. Na prvi pogled je videti, kot da je prišlo do zmede, vendar ni tako. Načelo opti-out iz ZVOP-1 ne velja, ker zakon sam nakazuje drugačno rešitev, če bi tako zapovedali drugi zakoni (Berčič, 2006, str. 8–10).

[11] Določeno je, da se z denarno kaznijo ali zaporom do enega leta kaznuje, kdor v nasprotju z zakonom uporabi osebne podatke, ki se smejo voditi samo na podlagi zakona ali na podlagi osebne privolitve posameznika, na katerega se podatki nanašajo, ali kdor vdre v računalniško vodeno zbirko podatkov, da bi zase ali za koga drugega pridobil kakšen osebni podatek.

skupine[12], elektronsko poslovanje[13] in elektronsko oglaševanje. Vsaka od naštetih storitev predstavlja določeno tveganje s stališča varnosti osebnih podatkov in zasebnosti v širšem smislu.

3.3.1 Načini zbiranja osebnih podatkov

Osebne podatke je prek interneta možno zbirati in shranjevati na različne načine. Prvi, ki ga bomo omenili, se nanaša na postavitev **predstavitvene strani**. Vsak uporabnik ima možnost, da na internetu postavi predstavitveno stran, na kateri običajno objavlja svoje osebne podatke. Ne zaveda pa se, da je z razvojem informacijsko komunikacijske tehnologije (*angl. information comunication technology - ICT*) omogočeno avtomatsko zbiranje podatkov, objavljenih na internetu, saj ICT omogoča rutinsko, namensko pa tudi "naključno" zbiranje, hitro procesiranje, klasificiranje ter povezovanje podatkov. Tako je npr. Telekom Slovenije zbral elektronske naslove in jih izdal v Imeniku elektronske pošte Slovenije. Čeprav je tovrstno zbiranje na prvi pogled nenevarno, lahko njegove podatke zbere spretna reklamna agencija in nam v elektronski predal začne pošiljati reklamna sporočila oziroma tako imenovano pošto z elektronskimi "smetmi" (*angl. junk mail oz. spam*).

Drugi način zbiranja podatkov o uporabnikih je, da spletne strani na internetu od uporabnikov v zameno za informacije ali določene ugodnosti zahtevajo osebne podatke. Na straneh, kjer se ti podatki zbirajo, ponavadi ne piše oziroma ni razvidno, za katere namene (večinoma prodajne) bodo tako zbrani podatki uporabljeni.

V kolikor bi za prva dva načina zbiranja lahko rekli, da gre za javno oziroma odkrito zbiranje podatkov, pa novejše tehnologije omogočajo zbiranje podatkov s pomočjo tako imenovanih **piškotkov** (*angl. cookies*). Piškotke uporabniku pošlje računalnik, kjer je postavljena spletna stran, ki si jo uporabnik ogleduje. Upravitelj spletne strani, ki piškotek pošilja, od njega dobi nekaj informacij o uporabniku, ne da bi le-ta za to vedel (Žurej, 2001, str. 39). Piškotek je namreč poseben program, ki lahko na uporabnikovem računalniku izvede določene ukaze. V piškotku so osnovni podatki o našem obisku posamezne spletne strani. Podatki o posameznikovem on-line obnašanju, pridobljeni z uporabo piškotkov, sami po sebi načeloma še ne omogočajo identifikacije konkretnega posameznika. Mogoče bi bilo celo trditi, da piškotki nimajo za tarčo posameznika, ampak le posamezen računalnik. Pot do identifikacije uporabnika je zelo kratka. Zadošča namreč, da je uporabnik na katerikoli izmed povezanih spletnih strani izpolnil kakšen obrazec in s tem razkril svojo identiteto ali podatke, iz katerih jo je moč ugotoviti. Nekateri ponudniki storitev shranijo tako pridobljeno ime oziroma nadaljnje podatke o uporabniku v svoj sistem, v uporabniku nameščenem piškotku pa pustijo označbo, s katero se lahko pri njegovem ponovnem obisku ti podatki preberejo in dopolnijo z eventualnimi novimi

[12] Izmenjava mnenj z določenega interesnega področja ali komuniciranje med več sogovorniki.

[13] Vsakodneven primer elektronskega poslovanja je npr. ko si preko interneta kupimo neko oblačilo. Blago plačamo s kreditno kartico, katere številko moramo posredovati po internetu, razkrijemo pa tudi poštni naslov, na katerega nam trgovina pošlje kupljeno blago (Perše, 2000b, str. 39–40).

podatki. Nekateri podatki se shranjujejo direktno v piškotkih. Spletni iskalniki lahko uporabnika posvarijo, da bo dobil piškotek, vendar namen le-teh ni le zbiranje informacij, zato uporabnik ne more vedeti, za kakšen piškotek gre (Možina, 2000, str. 23–25). Vedno pogostejše osveščanje uporabnikov o možnostih spremljanja in beleženja aktivnosti je povzročilo, da sedaj že 39 odstotkov uporabnikov interneta vsaj enkrat na mesec izbriše shrambo piškotkov iz osebnega računalnika (Marshall, 2005).

Oglaševalske agencije, katerim je bilo "odvzeto" strateško orodje, so pričele iskati druge možnosti spremljanja uporabnikov interneta. Pojavila se je nova serija piškotkov, ki so pametnejši in se znajo bolje skriti v majhen kot računalnika. Novi piškotki, ki nosijo tehnično ime "**vztrajen identifikacijski element**" (*angl. persistent identification element – PIE*) so plod nove tehnologije, ki prispeva k uspešnemu skrivanju tako pred ročnim brisanjem kot tudi pred odstranjevalci vohunskih programov. Njihova vztrajnost se kaže v tem, da so se sposobni samodejno arhivirati in skrivati na mestih, kjer nanje nihče ne pomisli; skrijejo se v lokalne objekte Macromedia Flash predvajalnika, ki ga ima nameščenega več kot 98 odstotkov računalnikov. PIE je možno izklopiti le, če se uporabnik odloči, da bo zavračal vse piškotke. Takih drastičnih ukrepov se ne pričakuje, ker bi to pomenilo, da se uporabniki odpovedujejo tudi piškotkom svojih priljubljenih spletnih strani. Posledično bi morali slednji vsakokrat, ko bi želeli dostopiti do portalov, vnesti uporabniško ime in geslo. Tu so še spletne strani, ki so vidne le, v kolikor imamo aktivirane piškotke.

Veliko ljudi, ki se zaveda vdora v njihovo zasebnost, je javno pozvalo podjetje United Virtualities – avtorja tehnologije PIE, da naj le-teh ne ponujajo svojim strankam. Na drugi strani je Macromedia, ki velja za zaupanja vredno podjetje. Njeni piškotki sledijo prvotnemu namenu, saj se uporabljajo izključno za shranjevanje večjih datotek, predvsem z avdio in video vsebino. Lahko se zgodi, da bodo uporabniki zahtevali, da sistemi za odstranjevanje vohunskih programov odstranijo vse; tudi flash piškotke, kar bo povzročilo veliko škodo in nepotreben spletni promet. Pri Macromedii so se že odzvali in ponudili novo nastavitev, ki ponudi možnost samodejnega brisanja objektov, ki niso del Flash predvajalnikov.

Poleg piškotkov obstajajo tudi manj agresivne tehnologije, ki ne posegajo toliko v zasebnost, ravno tako pa lahko podajo zanimive rezultate v zvezi z obiskom. Ena izmed slednjih je beleženje obiskov in klikov, ki se ne odvija na računalnikih uporabnikov, temveč na strežnikih ponudnikov spletnih vsebin. Spremljanje uporabnikov poteka v posamičnih sejah, ko se sledi njihov iskalnik. De facto se uporabnike prepozna le preko IP naslova in verzije iskalnika. Oba podatka služita upravljavcu spletne strani, da lahko poda dokaj natančno oceno, koliko uporabnikov je obiskalo spletno stran v nekem časovnem obdobju. Sedaj, v dobi nove ekonomije, samo ti podatki niso dovolj oglaševalcem oziroma upravljavcem spletnih portalov. Njihova želja je ugotoviti vzorec uporabnika, ki ni IP številka, temveč ime, in predvideti njegove prihodnje aktivnosti z namenom ustvarjanja ekonomske koristi.

Naslednja nevarnost, s katero običajni uporabnik večinoma ni seznanjen, so **LOG datoteke**, z drugo besedo "datoteke aktivnosti". LOG datoteke so posebne datoteke, kamor računalnik avtomatsko vpisuje aktivnosti uporabnikov. To pomeni, da se vse aktivnosti posameznega uporabnika (kdaj je prebral elektronsko pošto, katere spletne strani je obiskal in kdaj, itd.) avtomatsko zapisujejo na internetni strežnik podjetja ali organizacije, ki ga oskrbuje z internetom. Dostop do tako "naključno" zbranih podatkov ima upravitelj sistema in verjetno še kdo (Odlazek, 2003, str. 16).

Poleg naštetih načinov zbiranja podatkov obstajajo še drugi (npr. prestrezanje elektronskih sporočil), katerih seznam se z iznajdljivostjo upraviteljev interneta in trženjskih agencij veča. S pravnega vidika pomeni največjo nevarnost v zvezi z zbiranjem zlasti nenatančnost, napačnost, nepopolnost ali neažurnost zbranih podatkov (Čebulj, 1992, str. 8). Ob tem je potrebno imeti v mislih tudi samo zbiranje podatkov, ki lahko pomeni potencialno grožnjo zasebnosti. Vojske, obveščevalne službe ter policije držav namreč namenjajo ogromno denarja za nakup in razvoj sistemov za opazovanje akcij sovražnikov ter odkrivanje potencialnih nevarnosti (Webster, 1995, str. 63), vse v smislu "zaščite nacionalnih interesov". To pomeni, da se nadzor vrši tudi preventivno, to pa že lahko ogroža svobodo in pravice posameznika.

Z razvojem novih tehnologij in z večanjem procesorske moči nastajajo novi načini vdorov v našo zasebnost. Med novodobne tehnologije sodijo **brezžična omrežja**, ki prinašajo poleg pozitivnih lastnosti tudi nekatere slabosti; največja je slaba varnost. Dahl (Fuchs, 2005) navaja kot primer osebo, ki vstopi v stavbo, v kateri uporabljajo brezžična omrežja, se s prenosnikom usede v avlo in z nekaj znanja ter spretnosti pride v zelo kratkem času do pomembnih podatkov. V primeru, da ne more vstopiti v stavbo, lahko sedi v avtu, ki se nahaja znotraj območja, pokritega s signalom. Brezžična omrežja so kot odprte knjige, ki vabijo hekerje, da vdrejo vanje. Z razvojem novih tehnologij so se vzporedno začela pojavljati tudi svetovalna podjetja, ki pregledajo celotno omrežje med drugim tudi z vidika varnosti, z namenom odkrivanja šibkih točk, ki bi jih bilo potrebno odpraviti. Slednja podjetja ne bodo le pregledala infrastrukture in svetovala glede varnosti, pač pa bodo tudi poskusila izvršiti zunanji vodeni vdor. Kot rezultat obiska takega podjetja sledi poročilo, v katerem so zabeležena vsa opažanja in koraki za odpravo oziroma izboljšanje odkritih pomanjkljivosti. Predvsem podjetja iz finančnega sektorja se že sedaj poslužujejo teh storitev, ki vsekakor ne smejo biti enkratne narave. Te si morajo slediti, saj že odprtje enih virtualnih vrat na usmerjevalniku zaradi namestitve novega programa lahko popolnoma ogrozi celoten sistem.

Spletne kamere nas snemajo na vsakem koraku. Programska in strojna oprema za izvajanje nadzora je postala dostopna vsakomur. V milijonih domov so nameščene kamere z dostopom do interneta, z namenom video pogovora, starševskega nadzora, varstva poslopij, itd. Zaradi varnostnih razlogov jih je možno zaslediti tudi na tisočih drugih javnih mestih. Nepremišljena uporaba slednjih lahko privede do nasprotnega učinka. Namesto, da bi naredila naše življenje varnejše, dejansko omogočimo vpogled v naše zasebno življenje. Video oziroma slike, ki se prenašajo preko spleta, so zelo enostavno dostopna vsebina, ki jo je možno pregledovati kjer koli

na svetu. Spletne kamere (IP kamere) imajo kot vsaka spletna stran svoj IP naslov. Večina kamer uporablja enak vzorec in kode, ki niso nobena skrivnost za poznavalce. Vse, kar slednji potrebujejo, da odkrijejo kamere, je le nekaj črk in številk, ki so tipične za spletne strani, na katerih gostujejo ciljne kamere. In ne samo, da lahko opazujejo dogajanje v nekem prostoru oziroma v okolju, včasih je možno tudi prevzeti kontrolo nad upravljanjem. Če se želimo zaščititi, moramo začeti uporabljati požarne zidove in gesla, saj že osnovni varnostni ukrepi odvrnejo večino nepooblaščenih dostopov. Znani so tudi primeri, ko so se ljudje prepoznali na slikah, objavljenih na spletu, ki so bile posnete z domačimi kamerami (WorldNow, 2005). Pravni strokovnjaki opozarjajo, da v takem primeru ne moremo storiti kaj dosti, saj so zakoni medli in nedorečeni. Tudi v primeru, da se zavaruje dostop do kamer v domačem okolju, še vedno nimamo vpliva in kontrole nad kamerami, ki so nameščene v zdravstvenih domovih, nakupovalnih središčih, šolah, vrtcih in drugih javnih prostorih. Prenovljeni Zakon o varstvu osebnih podatkov je to področje načeloma uredil, le od sprejetja slednjega ni bilo opaziti nobene kontrole, ki bi jo morale izvajati pristojne inšpekcijske službe.

Medtem ko še vedno mislimo, da je internet brezplačen, uporabniki slednjega postajajo vedno pogosteje "tarča" spletnih oglaševalcev oziroma podjetij, ki uporabljajo internet kot del medijskega načrta. Zaradi trenutne aktualnosti vprašanja in pomembnosti tematike smo slednjemu namenili poglavje, ki sledi.

3.3.2 Oglaševanje na internetu

Prihodki od spletnega oglaševanja so dosegli v zadnjem četrtletju leta 2006 nov rekord, kar 4,8 milijard dolarjev. V celotnem lanskem letu so znašali prihodki kar 16,8 milijarde dolarjev, kar je 34 odstotkov več kot v letu 2005. Direktorica podjetja IAB (Interactive Advertising Bureau) Marla Nitke (2007) meni, da se oglaševalci vse bolj strinjajo, da je internet najbolj učinkovit medij za povezovanje s potrošniki. Internet je postal zanimiv za oglaševalce tudi zato, ker so uporabniki slednjega mlajši, izobraženi in aktivni. To je populacija, ki jo je z drugimi mediji težko doseči.

Povečan obseg oglaševanja tudi potrjuje, da se z internetom lažje gradi blagovne znamke ter prodaja storitve in proizvode. Prav tako je spletnim potrošnikom celotna informacija o predmetu oglaševanja na voljo hitro in enostavno z enim klikom.

Slovenski medijski načrtovalci v medijske načrte oglaševalskih akcij vse pogosteje vključujejo tudi internet. Splet postaja glavni vir informacij o izdelku ali storitvi v procesu nakupne odločitve kupca. Tega se zavedajo tudi oglaševalci, ki so za oglaševanje prek interneta v Sloveniji v letu 2004 porabili med 700 in 800 milijonov tolarjev bruto (Petrov, 2004). Povedano drugače, bruto vložek v oglaševanje prek interneta je v Sloveniji leta 2004 prvič presegel odstotek celotnega oglaševalskega kolača.

Tehnologija za ciljanje na podlagi vedenjskih vzorcev pri prikazovanju oglasov na spletu uporablja enostavno logiko, ki "upošteva" aktivnosti (potencialnega) uporabnika na spletni strani. Če se glede na njegovo aktivnost ugotovi, da se uvršča med potencialne kupce določenega izdelka, mu oglasni strežnik prikaže spletni oglas za takšen izdelek. Lahko bi rekli, da je doseženo dvoje. Oglaševalec je pokazal oglasno sporočilo potencialnemu kupcu, uporabnik interneta pa je videl oglasno sporočilo za izdelek, ki bi mu lahko ustrezal (Struna, 2004). In ne samo, da strežniki zbirajo podatke o zgodovini naših obiskov in klikov, slednji beležijo tudi tehnologijo, ki jo uporabljamo, in sicer način povezave, hitrost in ponudnika dostopa do interneta, državo dostopa, operacijski sistem, spletni iskalnik, različico Flash predvajalnika, ločljivost zaslona ter druge tehnične podrobnosti. Analize bodo oglaševalcem v pomoč pri načrtovanju prihodnjih oglaševalskih akcij (Cetin, 2005).

Oglasni strežniki uporabljajo virtualno identiteto kot ključni referenčni element. Z besedno zvezo "virtualna identiteta" (*angl. virtual identity*) razumemo IP številko oziroma IP naslov (*angl. IP address*), ki predstavlja virtualni naslov računalnika. IP naslov namreč pove, kje v omrežju se nahaja določen računalnik, s tem pa je znana tudi pot do njega. Vsakdo se je že srečal s spletno anketo ali nagradno igro, s katero obiskovalca pozivajo, naj jo izpolni, saj bo lahko na ta način sodeloval v nagradni igri in si priboril eno od nagrad, le redki pa so se vprašali, s kakšnim namenom se osebni podatki zbirajo in kakšna je varnostna politika.

Simon Cetin (Vagaja, 2005) navaja kot primer preproste in vsakdanje uporabe zbirk podatkov v spletnem oglaševanju upravljanje frekvence prikazovanja oglasnega sporočila. Posamezen oglas lahko uporabniku spletnega medija prikazujemo z natančno določeno frekvenco, saj se v zbirko podatkov zapisuje tudi to, kolikokrat je posameznik oglasno sporočilo že videl in kolikokrat ga mora glede na nastavitve še videti. Oglasni strežnik te podatke obdeluje in jih v nadaljevanju uporablja za ustrezno posredovanje oglasa posamezniku. Posamezniku lahko oglasno sporočilo prikažejo le enkrat ali pa večkrat, odvisno od ciljev akcije. Velikost zbirke ni tako pomembna, bolj je pomembna kakovost podatkov. Pri načrtovanju in izvajanju akcij na podlagi vedenjskih vzorcev namreč ne iščejo statističnih približkov, temveč operirajo s konkretnimi podatki. Slednje predstavljajo kot prednost sodobnih orodij za ciljanje v elektronskih medijih.

Ciljanje na podlagi vedenjskih vzorcev je ena od najbolj naprednih možnosti uporabe zbirk podatkov. Oglasni strežnik zapisuje gibanje uporabnika po spletni strani z določenimi vsebinami in to shranjuje v zbirko. Primer: če nekdo v tednu dni petkrat obišče določene nepremičninske vsebine in tam išče cene ter druge informacije, povezane z nakupom nepremičnine, potem je verjetno, da bi rad kupil nepremičnino. Če ta isti uporabnik obiskuje tudi vsebine, povezane z vzgojo otrok, poleg tega pa na podlagi geografske kode ugotovimo še, da do interneta dostopa iz Kranja, potem lahko sklepamo, da bi ga utegnil zanimati oglas za nepremičninsko agencijo v Kranju. Oglasni strežnik podatke o aktivnosti tega uporabnika shranjuje, jih obdela in ob obisku spletne strani temu uporabniku prikaže oglasno sporočilo za agencijo v Kranju, ki posreduje pri najemu stanovanj za mlade družine. Tako prikazan oglas je za uporabnika smiseln in manj moteč, oglaševalec pa nima nepotrebnih izgub, saj ne prikazuje oglasov vsem uporabnikom

določenega spletnega medija, od katerih jih nameravata kupiti takšno nepremičnino denimo le dva odstotka.

Skrbniki spletnih portalov trdijo, da potrebujejo za svoj obstoj finančne prilive iz naslova oglaševanja. V kolikor že morajo oglaševati, je najbolje za obe strani – tako za oglaševalce kot tudi za kupce – da se prikazujejo oglasi, ki so sestavljeni iz vsebine, ki je aktualna za posameznika (Wired News, 2005).

Nekaj spletnih strani je svojim uporabnikom ponudilo izbiro med oglasi, ki se pojavljajo naključno, ali oglasi, ki so bili selekcionirani glede na njihove potrebe. Na žalost večina upravljavcev ne opozarja na svoje početje.

Oglaševalska podjetja niso edina, ki zbirajo naše podatke za komercialne namene. Zanimivo je, da so največji trije ponudniki brezplačne pošte (Yahoo, Google in Microsoft) hkrati tudi ponudniki spletnih iskalnikov. Slednji so ugotovili, da lahko med tema dvema navidez brezplačnima storitvama ustvarijo sinergijo in to predvsem na področju oglaševanja. Uporabniki morajo ob odpiranju brezplačnega elektronskega naslova navesti tudi osebne podatke, le-ti pa se kasneje uporabijo pri prikazovanju sponzoriranih povezav oziroma štejejo in razvrščajo potencialne uporabnike, ki so kliknili na določeno povezavo.

Yahoo in Google že nekaj časa ponujata plačane komercialne storitve v svojih iskalnikih. V prihodnje se jima ima namen pridružiti tudi Microsoft. Microsoftova platforma bo ponujala podrobne informacije o uporabnikih, kot so spol, starost in lokacija, da bi si podjetja, ki bodo pri njih oglaševala, lahko izbirala ciljno publiko. To je že sprožilo kritike zagovornikov zasebnosti na internetu, vendar pri Microsoftu pravijo, da se uporabnikov na podlagi ponujenih podatkov še vedno ne bo dalo identificirati (Linn, 2005).

Chris Hoofnagle iz centra EPI (za varovanje elektronske zasebnosti podatkov) pravi, da postaja "prodajanje" uporabnikov interneta vse bolj ustaljen trend za povečevanje oglaševalskega prihodka (Linn, 2005). Podoben primer, ki je sprožil val ogorčenja, je Googlova storitev, ki beleži zgodovino iskanja in obiskov, imenuje se *My Search History*. Pri ponudniku pravijo, da so slednjo ponudili kot eno izmed dodanih vrednosti, ki bo uporabnikom omogočila prikaz predhodnega gibanja po spletu; na ta način se bodo slednji izognili ponovnemu postopku iskanja. Največji problem, ki zbuja skrb, je zgodovina obiskov in iskanja, ki je shranjena na centralnem strežniku. Ne glede na to, da Google hrani podatke skladno z izjavo o varovanju zasebnih podatkov, lahko javni računalnik (v knjižnicah, šolah, barih, itd.) razkrije marsikaj o preteklih iskanjih in tu so seveda še hekerji. Sama funkcionalnost je zanimiva tudi z oglaševalskega vidika. V kolikor imamo shranjeno in obdelano zgodovino uporabnikov, lahko na podlagi slednje zelo enostavno prikazujemo dinamične reklamne pasice in oglase (Koprowski, 2005). Pri Googlu pravijo, da to zaenkrat ni mogoče (lahko pa je to smer, v katero so se namenili).

O zbiranju in prodaji podatkov o spletnih klikih svojih uporabnikov je nedavno spregovoril tudi David Cancel, direktor podjetja Compete Inc. Cancel je na konferenci Open Data 2007 razkril, da internetni ponudniki na veliko prodajajo sporne podatke. Podatki so sicer anonimni in iz njih ni mogoče razkriti identitete uporabnikov. Ob tem pa se vseeno postavljajo vprašanja o obsegu podatkov, ki jih prodajajo podjetja. Neimenovan udeleženec konference je ocenil, da je v Združenih državah Amerike ta hip od 10 do 12 velikih kupcev podatkov. Zanje so pripravljeni odšteti od 0,4 pa vse do enega dolarja na mesec za posameznega uporabnika (Henderson, 2007).

3.4 POZITIVNI IN NEGATIVNI UČINKI NADZORA

Pri preučevanju zasebnosti in nadzora nujno trčimo na paradoksalno dvojnost. Nadzor ima hkrati pozitivne in negativne učinke. Danes je nadzorovanje posameznikov sredstvo družbenega nadzora, kakor tudi sredstvo za zagotavljanje pravic družbene participacije. Prav tako tudi ne moremo mimo dejstva, da je nadzor tesno povezan s tehnologijo. Informacijske tehnologije so med drugim tudi namenjene zbiranju in obdelavi vseh vrst podatkov in informacij. Tako podatkov in informacij o okolju, družbi, v kateri živimo, in posameznikih, ki nas obdajajo. Informacijska družba je družba nadzora (Kovačič, 2003, str. 11), zato ni presenetljivo, da imajo informacijske tehnologije danes izjemen pomen za nacionalno varnost, z vprašanji zasebnosti pa se čedalje bolj ukvarjajo politični aktivisti, civilna družba in delavski sindikalisti.

3.4.1 Zbiranje osebnih podatkov kot pogoj za demokratičnost oziroma avtoritarnost družbe

Pri nadzoru so pogosto izpostavljene predvsem njegove negativne plati, a ima tudi pozitivne strani, saj pri zagotavljanju varnosti in vzdrževanju reda v povezovanju z organizacijo služi tudi urejanju življenja v družbi. Nadzor je prerasel v nujno zlo, ki se ga nikakor ne moremo več otresti. Sprva je bil njegov namen omogočiti red in sobivanje posameznikov, kaj kmalu pa so ga pričeli uporabljati tudi v druge namene. Dandanes lahko govorimo o množičnem nadzoru in oblikovanju dosjejev posameznikov, ki so s svojo participacijo v družbi (uveljavljanje državljanskih, zdravstvenih, zaposlitvenih in drugih pravic) izpostavljeni nadzoru.

Zasebnost posameznika je postala ogrožena z zbiranjem, obnavljanjem in dopolnjevanjem vladnih zapisov ter podatkovnih baz. Vladne institucije so z namenom organiziranosti in učinkovitosti delovanja avtomatizirale določene procese ter jih centralizirale na ravni celotne javne uprave. Določeni zapisi, kot na primer: plačilo davkov, socialna blaginja in kriminalna preteklost, so zaupne narave ter dosegljivi določenim pristojnim uradnikom. Tu so še javno dostopni podatki (nekateri le, če izkazuješ pravni interes), med katere sodijo zapisi o lastništvu, datum rojstva, smrti in zakonski stan. Država se ne poslužuje nadzora le zaradi poenostavitve izvajanja administrativnih nalog, temveč tudi za zagotavljanje zunanje in notranje varnosti.

Sistem e-države zbuja kar nekaj skrbi. Ena izmed skrbi je možnost prodaje podatkov o posameznikih in organizacijah ponudniku spletnih storitev, ki se ponavadi ukvarjajo z ugotavljanjem kreditne sposobnosti in z izdelovanjem kreditnih profilov, ali pa posredovanje drugi vladni instituciji z namenom preverjanja določenih podatkov. Še ena skrb je varnost povezanih podatkovnih zbirk, ki poleg potrebnih podatkov vsebujejo tudi druge informacije (družinski podatki, finančni podatki, zdravstvene informacije), s pomočjo katerih se lahko izdela popoln osebni profil. Tveganje nepooblaščenega dostopa in zunanjih napadov na državne strežnike je postalo večje kot kdajkoli prej. Zaupnost, integriteta in dostopnost državnih podatkov ogrožajo amaterski hekerji, virusi in črvi. Državne institucije se zavedajo tveganja, kar potrjujejo tudi izvedeni varnostni ukrepi.

Združene države Amerike namenijo milijone dolarjev letno, da bi se ubranile pred virtualnim kriminalom, kot je na primer kraja identitete. Poskrbeti bi bilo potrebno za visoko izobražene kadre na področju virtualne varnosti in zasebnosti, ki bi se lahko soočili z vse večjim valom kriminala, vendar pridemo do ugotovitve, da se slednjim ne namenja toliko pozornosti, kot bi sprva pričakovali. Peterson (2005) je izpostavil, da v ZDA vsako leto doktorira približno 100 ljudi, ki so postali strokovnjaki na področju zasebnosti ter varnosti na internetu. Informacijska družba lahko preživi le, če bo temeljila na znanju, ki je edina perspektiva globalne ekonomije v razmerah sorazmerno velikih napadov s strani vedno bolj specializiranih hekerjev, ki lahko ure in ure svojega časa porabijo, da bi prišli do želenega cilja. Mnogi menijo, da imamo znanja dovolj in celo preveč. Treba bi ga bilo le pametno uporabiti. Živimo v času hitrih sprememb in hitrega nastajanja novega znanja in novih tehnologij. Le družbe, v katerih imajo osnovne in uporabne raziskave dominantno vlogo, se lahko uspešno prilagajajo hitrim spremembam in gradijo blaginjo v svetu nepredvidljivih odkritij, kjer bogastvo temelji na novih in boljših ne pa na cenejših rešitvah. Sodobne države brez znanstvenikov in znanosti ni.

Pri vzpostavljanju zakonskega varstva posameznikove zasebnosti seveda nujno trčimo na že omenjeno kolizijo med svobodo in poseganjem vanjo. Določitev meje posegov v zasebno sfero posameznika in podeljevanja dovoljenj za izvajanje nadzora ter nadzor nad izvajalci nadzora bi nas pripeljal v absurdno situacijo. Mellors (v Raab 1997, str. 158) zato ugotavlja, da "najboljša zaščita ni ta, da oni (država) vedo manj o nas, pač pa, da mi vemo več o njih: da vemo, kaj vedo o nas in kako te informacije o nas uporabljajo". Glavna sestavina zaščite informacijske zasebnosti je torej nadzor pretoka in posredovanja podatkov, ki se nanašajo na nekega posameznika. Zato se sodobna zakonodaja za zaščito zasebnosti ukvarja predvsem s transparentnostjo uporabe osebnih podatkov. Zbiranje podatkov se torej ne omejuje, imeti pa mora zakonsko podlago. Namen zbiranja in uporaba podatkov morata biti vnaprej znana in transparentna (Kovačič, 2003, str. 37).

Nadzor posameznikov se izvaja tudi pri kriminalnih raziskavah. Statistične analize pravijo, da se v ZDA izvaja snemanje telefonskih pogovorov na vsakega stotisočega prebivalca. Če ta podatek primerjamo z drugimi državami, lahko ugotovimo, da so ZDA veliko bolj konservativne pri izdajanju nalogov za nadzor telefonskih pogovorov kot Evropa. Država, ki je v letu 2004 izdala

največ nalogov za snemanje pogovorov na svetu, je Italija. Italijanski časopis La Repubblica je objavil, da so v Italiji prisluškovali kar 172-im telefonskim priključkom na 100.000 prebivalcev. Prišlo je že tako daleč, da je eden izmed večjih operaterjev mobilne telefonije izjavil, da nima več prostih prisluškovalnih kapacitet. Nemški inštitut Max Planck, ki se ukvarja z mednarodnim kriminalom, je ugotovil, da Italijanom sledijo Nizozemci s snemanjem 62-ih priključkov na 100.000 prebivalcev. S snemanjem devetih priključkov na 100.000 prebivalcev se na dnu lestvice zahodnoevropskih držav nahaja Avstrija (Hesseldahl, 2005).

Stališče držav v Evropski uniji ni enotno glede zakona, ki naj bi zahteval shranjevanje poročil o mobilni in internetni uporabi z namenom boja proti terorizmu. Predlog Evropske komisije[14] bo potreboval približno tri leta za uveljavljanje, saj potrebuje soglasje evropskega parlamenta, ki je zelo občutljiv, ko gre za državljanske pravice, in bolj odprt za lobiranje telekomunikacijskih podjetij. Medtem ko bi Velika Britanija, ki jo podpirajo Irska, Francija in Švedska, želela to uveljaviti čim hitreje in znotraj vseh štirih držav posamezno, Evropska komisija išče zdravo razmerje med potrebami boja proti kriminalu in pravicami do zasebnosti. Po madridskih bombnih napadih leta 2004 so štiri države predlagale, da se podatki o telekomunikacijski uporabi hranijo vsaj eno leto, predlog Evropske komisije pa je bil od 6-ih mesecev do enega leta (Reuters, 2005).

Britanski informacijski pooblaščenec priznava, da so se uresničili strahovi, da bi Velika Britanija postala družba nadzora. Kot ugotavlja poročilo Mreže za študije nadzora, je na Otoku kar 4,2 milijona video nadzornih kamer oziroma ena kamera na 14 prebivalcev. Eden izmed avtorjev poročila je dejal, da je Britanija najbolj nadzorovana zahodna družba (BBC, 2006). Nadzor telekomunikacij in video nadzor sta le dve izmed oblik nadzora posameznikov. Pridružujejo se jima med drugim še nadzor prometa, uporabe vozil, nakupovalnih navad, finančnih transakcij, medicinskih podatkov ter sledenje s pomočjo mobilnih telefonov.

Zadnjih nekaj let se ves svet bori proti terorističnim organizacijam, ki z množičnimi napadi ogrožajo življenja nedolžnih. Države so poostrile nadzor določenih ključnih komunikacijskih in transportnih poti z namenom preventive. Posledico nadzora na višji ravni občutimo prav vsi. Tehnologija je šla že tako daleč, da je možno izvajati fotografiranje ozemlja kar preko satelitov. Nekateri strokovnjaki menijo, da visokoločljivostni posnetki, ki nastanejo s sateliti, omogočajo prepoznavo oseb in drugih podrobnosti. Kot argument o predhodno zapisanem Friedenberg (2005) navaja primer Googla, ki ponuja brezplačno storitev Google Maps. S pomočjo slednje se išče mesta ali zgradbe po njihovem naslovu oziroma po drugih kriterijih. Glede na to, da so že Googlovi posnetki s ptičje perspektive relativno natančni, si ne moremo zamisliti, kaj vse ima še država (npr. ZDA).

[14] Svet Evrope je na pobudo Evropske komisije 29. januar razglasil za dan varstva osebnih podatkov.

3.4.2 Akterji nadzora

Ves svet čaka, da bodo vodilna ameriška podjetja za informatiko skupaj z glavnimi ponudniki kreditnih kartic dokončno oblikovala strojne rešitve (pametne kartice) in kodirne programe za zagotavljanje visoke varnosti in zasebnosti podatkov med prenašanjem po internetu. Težave pri tem pa niso tehnološke, ampak politične. Ameriška vlada se že vrsto let bori proti uporabi zanesljivih postopkov za šifriranje sporočil v javnih omrežjih – in za izvoz teh postopkov iz ZDA – preprosto zato, ker želi nadzorovati vsebino sporočil. Vlada pravi, da je to pomembna zmožnost v boju proti mednarodnemu terorizmu in kriminalu. Tem zahtevam se pridružujejo vlade večine razvitih (in demokratičnih) držav, od katerih so nekatere že prepovedale uporabo težko zlomljivih šifer (Pahor, 2003). Ameriška vlada že vrsto let razvija enkripcijske metode za lastne potrebe, če pa se pojavi nekdo, ki bi jih želel ponuditi za komercialne namene, ga hitro ustavijo. Še več, analitska hiša Gartner (2006) že vrsto let pred vsakim koncem leta objavi deset napovedi za prihajajoča leta na področju informacijske tehnologije. Čeprav gre pogosto za drzne napovedi, so se pričakovanja Gartnerja večkrat izkazala za pravilna. Le-ti so konec leta 2006 med drugim tudi napovedali bojazen glede zasebnosti uporabnika v prihodnosti. Kljub temu, da so mnoge države sprejele zakone, ki ščitijo zasebnost državljanov, so vse glasnejše zahteve, zlasti v ZDA in zahodni Evropi, po katerih naj bi bila nacionalna varnost pomembnejša od zasebnosti, zato je velika verjetnost, da bo do leta 2010 mogoče slediti prek mobilnega telefonskega omrežja okrog 60 % uporabnikov.

Odkar je februarja 2000 o ameriškem sistemu za prestrezanje elektronskih komunikacij Echelon razpravljal celo evropski parlament, se večina uporabnikov zaveda, da nam med brskanjem po spletu prisluškujejo. A podatkov o naših spletnih navadah ne zbirajo le vladne agencije.

Podatke kupujejo agencije, ki analizirajo spletno poslovanje. Nekatere manjše spletne predstavitve s takim vohunjenjem financirajo večino svojih obratovalnih stroškov. Za spletno knjigarno je koristno, če lahko izve, katere knjige si uporabniki ogledujejo ali kupujejo v drugih spletnih prodajalnah. Take analize je mogoče kupiti s prepoznavnostjo uporabnikov, od katerih so bili zbrani podatki. Če je računalnik okužen z vohunskim programom, nas včasih spletna stran, ki je še nikoli nismo obiskali, pozdravi z imenom in priimkom ter ponudi vsebinsko podobno knjigo, kot smo si jo pred tedni ogledovali nekje drugje (Vagaja, 2004).

Med največje akterje nadzora se vsekakor uvrščajo novodobna podjetja, ki so v dobi nove ekonomije našla novo tržno nišo. Slednjo so zapolnili z novimi rešitvami, po katerih povprašujejo predvsem oglaševalska podjetja (kot vmesni člen) in ponudniki raznolikega blaga. Vsi stremijo k istemu cilju: spoznati v realnem času čimbolj natančne potrebe strank in jim ponuditi blago, ki bi jih morebiti zanimalo. Tradicionalna podjetja se že leta in leta trudijo zaznati potrebe potencialnih strank, vendar, resnici na ljubo, pogosto niti ne vedo, koliko strank imajo.

Zadnja leta je bilo že veliko slišati o CRM-ju. Modna kratica, ki stoji za tremi angleškimi besedami – customer (stranka, kupec, odjemalec), relationship (odnos) in management (ravnanje). Na prvi pogled izgleda, kot da je CRM nekaj, kar zanima samo velika podjetja, če pa si zadevo pobližje ogledamo, pa kaj hitro ugotovimo, da si lahko koristi od njega obetajo tudi manjše organizacije.

Podjetja imajo opravka z več ali manj kupci, vsa pa imajo podobne probleme, kako kupce zadržati, kako jim prodati še več enakih stvari, oziroma kako jim prodati še kakšno drugo stvar. Lep primer so zavarovalnice. Te morajo imeti vse podatke o nas zavarovancih, če ne zaradi drugega, zato, da nam izstavljajo račune, potrebujejo pa tudi druge kontaktne podatke, da nas lahko opomnijo, če nismo dobri plačniki. Včasih pa nas pokličejo po telefonu kar tako in nam poskušajo prodati še kaj več; v nekaterih primerih jim uspe, v večini pa ne. Za podjetja pomenijo ti stiki strošek. V njihovem interesu je uspešna prodaja s čim manj osebne interakcije (Batagelj, 2004, str. 15).

Tu nastopi CRM – na podlagi podatkovnih zbirk računalniški programi prek zapletenih računskih algoritmov določajo, katerim kupcem kaj ponuditi in kakšna je verjetnost, da bodo sprejeli njihovo ponudbo.

Ni pa nujno, da se CRM uporablja samo pri telefonski prodaji, poteka lahko pri vsakem stiku, ki ga ima podjetje z odjemalci. Menedžment odnosov z odjemalci ni nekaj novega. Lokalni prodajalci imajo svoje stranke preprosto v glavi; o nas vedo vse. Tega veliki trgovski sistemi ne zmorejo, si pa želijo. Ne samo, da bi lahko opozarjali na artikle, ki se jih običajno kupi, lahko bi tudi pošiljali letake samo s tistimi izdelki, ki stranko zanimajo – ponavadi je na njih veliko izdelkov, ki jih res ne potrebujemo. Sistem bi imel veliko večjo uporabno vrednost, sploh pa bi prihranili kar nekaj časa – čas pa postaja čedalje pomembnejši!

Kljub vsem tem pozitivnim vidikom so tudi pomisleki. Teh je seveda veliko – glavni pomisleki proti CRM-ju izhajajo iz pravice do zasebnosti in načela enakosti. Pravica do zasebnosti je ena temeljnih pravic. Obdelava in uporaba teh zbirk podatkov ni vedno v skladu z zakonodajo, ki s tega vidika potrošnike zelo ščiti. Pri drugem vidiku pa je pomembno, da podjetja kar naenkrat vedo o nas zelo veliko.

Ena izmed posledic je tudi ta, da nas razvrščajo v skupine zelo dobrih, srednjih in slabih kupcev. Boljši kot smo kupci, zanimivejši smo zanje, trgovci nas bolj nagrajujejo, banke nam ponujajo boljše kredite, policaji so na nas pozornejši ... Kar naenkrat nismo vsi kupci enako obravnavani, kar marsikoga moti, lahko pride tudi do napak in pomot.

Pravne in fizične osebe, ki uporabljajo nepravilno zbrane osebne podatke, oziroma so jih pridobili za drug namen, lahko doletijo nepričakovane posledice (ZVOP-1, Ur.l. RS, št. 86/2004 in 113/2005):

- Posameznik lahko zahteva izbris iz zbirke osebnih podatkov ter **povrnitev morebitne povzročene škode**.
- Pristojni inšpektorji lahko izrekajo relativno **visoke kazni**.
- Zloraba osebnih podatkov je lahko pod pogoji Kazenskega zakonika tudi **kaznivo dejanje**.

Iz tega razloga je potrebno v primeru, da se neko podjetje (pravna ali fizična oseba) odloči za uporabo osebnih podatkov, to prijaviti pri informacijskem pooblaščencu, posamezniku pa mora dati v podpis izjavo, s katerim da soglasje za uporabo svojih osebnih podatkov (Informacijski pooblaščenec, 2007).

Za varovanje pravne oz. fizične osebe, ki zbira osebne podatke posameznikov, je primerno, da izjava vsebuje naslednje elemente:

- opredelitev, katere osebne podatke posameznik posreduje v uporabo,
- namen obdelave osebnih podatkov in namen njihove uporabe,
- čas shranjevanja osebnih podatkov.

Register zbirk osebnih podatkov je javno dostopen register[15], ki ga je bilo treba vzpostaviti tudi zaradi evropskih direktiv. V njem lahko vsak posameznik preveri, katere podatke o njem na primer vodi določena banka, mobilni operater ali zasebni zdravnik in druga podjetja. Za primer: NLB v zbirki osebnih podatkov o potrošniških kreditih vodi 15 podatkov o posameznem posojilojemalcu, kar je razvidno iz registra.

Čeprav se je 1. oktobra leta 2006 iztekel rok za vpis zbirk v register, je bilo do novembra 2006 vpisanih le nekaj več kot 3.700 zbirk, tretjina šele v zadnjih dveh mesecih. Lahko zaključimo, da je tako večina zavezancev (približno 136 tisoč) formalno v prekršku. Kazni, ki so predvidene za kršitelje, se za pravne osebe gibljejo od enega do treh milijonov tolarjev. Tako bi se – če bi informacijski pooblaščenec vsem 136 tisočim zavezancem, ki zbirk niso vpisali v register, izrekel najnižje kazni – v proračun lahko nateklo 136 milijard tolarjev (Basle, 2006).

3.4.3 Smiselnost nadzora v očeh nadzorovanih

Vdori v zasebnost niso povsem nov pojav, vendar je v zadnjem času ta nadloga začela dobivati skoraj alarmantne razsežnosti. Zgovoren je podatek ameriškega ponudnika internetnih storitev EarthLink, ki mu je od začetka leta 2004 prek svoje storitve za nadzor internetnih dejavnosti (in nevarnosti) uspelo pregledati čez dva milijona osebnih računalnikov. Dobljeni podatki so domala alarmantni: v vsakem tretjem računalniku je vsaj en vohunski program, v povprečju pa imajo "okuženi" računalniki kar 28 različnih vohunskih programov (Djurdjič, 2004, str. 20).

[15] Register zbirk osebnih podatkov je objavljen na spletnem naslovu http://www.ip-rs.si/index.php.

Raziskave kažejo, da se v zadnjem času težave zaradi vohunskih programov vse bolj kopičijo. S tem pa se to področje uvršča že med največje razloge za težave pri delovanju sistemov, čemur lahko takoj na drugi strani pripišemo posledice, kot je slabša storilnost uporabnikov, ki se morajo ubadati s tem namesto s prvotnimi zadolžitvami. Motenje normalnega dela se lahko kaže na različne načine, od oken, ki se nepredvidoma prikazujejo na zaslonu in nas odvračajo od trenutnega dela, do upočasnitve delovanja, ker računalnik streže potrebam vohunskih programov namesto uporabniških. Pri večjih podjetjih, kjer imajo lastno informacijsko službo, slednjo obremenijo zaradi čiščenja sistemov, ki je ponavadi zelo zamudno delo in dostikrat zahteva ponovno namestitev operacijskega sistema. Najhujši vidik tega pojava pa je ta, da se uporabniki tega večinoma sploh ne zavedajo. Podjetja, v katerih so okuženi računalniki, pa podcenjujejo nevarnosti, ki iz tega izhajajo.

Zanimivo pa je, da so nad vohunskimi programi precej bolj zaskrbljeni posamezniki kakor odgovorne osebe v podjetjih, ki skrbijo za računalniško podporo. Nenavadnost tega položaja razkriva raziskava med upravitelji računalniških sistemov, med katerimi jih je le 25 odstotkov izjavilo, da so vohunski programi velika nevarnost za njihova podjetja. V isti sapi pa je raziskava pokazala, da se je z vohunskimi programi srečalo že 92 odstotkov vprašanih (Djurdjič, 2004, str. 21). Taka razlika v odgovorih jasno kaže, da tudi specialisti podcenjujejo pojav in s tem povezane nevarnosti, posledično pa v ta namen tudi niso vpeljani ustrezni varnostni ukrepi. Analitiki zato menijo, da bo do streznitve prišlo šele tedaj, ko se bo iz tega naslova dogodila kakšna večja afera kraje podatkov, nakar bodo vsi množično hiteli krpati svoje “nove” razpoke v varnosti (Djurdjič, 2004, str. 21).

Strokovnjaki pravijo, da napoved družbenih sprememb zaradi digitalnih sledi in dosjejev ni enostavna naloga. Ljudje imajo radi storitve, kjer privarčujejo tako na času kot tudi na denarju, vendarle so kljub temu jezni, če kdo poskuša v zameno za slednje vstopiti v njihovo zasebnost.

3.4.3.1 Orodja in metode za znižanje tveganja in posegov v zasebnost

Internet je res postal sestavni del našega življenja in poslovanja in ker gre za milijone ljudi po vsem svetu, moramo imeti vedno v mislih, da nismo sami. Skoraj nerazumljivo je, da varno zaklepamo predale svoje pisalne mize in vrata svojega stanovanja, ko pa večina vstopa v internet, počne to tako, kot bi si želela, da bi se ljudje sprehajali skozi njihov najbolj intimen kotiček stanovanja. Spletno okolje je postalo zelo nevarno, razen če imamo ves čas v mislih skrb za varno delo z računalnikom in internetom. Pri stotinah milijonov uporabnikov interneta je zagotovo nekdo, ki ima slabe namene, kar pomeni: stalna previdnost ni nikoli odveč in velja osnovno pravilo, da neznancem v svetovnem omrežju nikoli ne zaupamo. Anonimnost je v svetu interneta še posebej pomembna, in če nam jo ponujajo v bankah, na poštah in še kje npr. z zeleno črto pred okencem, ki varuje našo zasebnost, poiščimo to črto tudi na spletnih straneh. Za zagotovitev višjega nivoja varnosti ne zadošča le uporaba strojne ali programske opreme, temveč je to proces, v katerega morajo biti vključeni vsi udeleženci.

Pravilen pristop organizacije varovanja in zaščite podatkov je pristop od zgoraj navzdol. Najprej je treba postaviti strategijo varovanja ter ustrezen program informacijske varnosti. Šele nato prek varnostne politike, usposabljanja in varovanja informacijskih virov prehajamo na nižje ravni varovanja. Vse ravni moramo varovati enakomerno in dosledno, sicer tvegamo, da bo ravno najšibkejši člen tarča napada in bo posledično ogrozil tudi vse druge ravni. Ob tem ostajajo problemi realnosti še vedno nezadostna zavzetost vodstva, neformalni pristopi k organiziranju varovanja, prepad med dodelitvijo virov in pričakovanji ter odsotnost funkcije neodvisnega preverjanja delovanja in urejanja varnosti v organizacijah.

V svetu interneta zasebnost varuje izjava o varovanju zasebnosti (*angl. privacy policy*). V tej izjavi upravljavci strani izjavljajo, kakšno stopnjo zasebnosti zagotavljajo z našimi podatki. Ta izjava je temelj za komuniciranje s spletnimi stranmi, kje se posluje ali daje podatke o sebi. Na spletnih portalih TRUSTe, TrustWise in VeriSign se lahko preveri, katere spletne strani so zaupanja vredne (Šalamon, 2004, str. 61). Stopnjo zasebnosti se nastavi tudi v spletnih iskalnikih. V povezavi z zasebnostjo je tudi skoraj nasilno ponujanje piškotkov. Ko se prvič vstopi na spletno stran, se v računalnik namesti piškotek s te spletne strani, ki kdaj kasneje omogoča hitrejši dostop do spletne strani, ali pa si zapomni podatke, ki so bili podani ob spletnem nakupu oziroma ob neki drugi aktivnosti in nam s tem prikrajša ponovne vnose. Datoteka oziroma piškotek beleži podatke gostitelja, med drugim tudi osnovne podatke o obisku spletne strani, ime računalnika, dan in uro obiska, uporabljena gesla in nenazadnje tudi preference. V izjavah o varovanju zasebnosti je ponavadi zapisano, da bo spletna stran zbirala le podatke, ki so potrebni za hitrejše odvijanje prihodnjih nakupov oziroma obiskov v korist uporabnika. Ponavadi ti piškotki ne zbirajo samo informacij, kaj vnašamo v polja na portalu, kjer smo dobili piškotek, temveč beležijo tudi naše obiske njim konkurenčnih portalov ter spletnih strani, ki niso v njihovi domeni. Nevarnost slednjih se kaže predvsem v dveh smereh: ali gre zaupati upravljavcu spletnega portala, da bo naše podatke hranil skladno z izjavo, ki jo je podal na dnu spletne strani, in kaj narediti, v kolikor gre za javni računalnik, ki bo naslednjemu obiskovalcu ponudil naše osebne podatke. Piškotki so v resnici vdor v zasebnost (tudi zasebnost računalnika), zato se jim je najbolje odreči, pa naj bodo še tako dobri, oziroma naj omogočajo še toliko hitrejše delo. Več kot tretjina uporabnikov se jim je že bila pripravljena odreči. Brisanje piškotkov je najbolj prizadelo oglaševalsko industrijo, ki uporablja slednje kot orodje za beleženje aktivnosti, na drugi strani pa so ponudniki programskih rešitev za odstranjevanje vohunskih programov (*angl. anti-spayware software*), med katere sodijo tudi piškotki, ki beležijo hitro rast povpraševanja po njihovih programskih paketih. Vojna s piškotki pridobiva nove razsežnosti, ki smo jih v grobem poskusili predstaviti v poglavju 3.3. V računalniku se hranijo tudi podatki o straneh, ki smo jih že obiskali, t.i. (*angl. cache*). Z njimi je lahko ponovni obisk spletnih strani hitrejši. Takšen seznam se seveda lahko izbriše.

TABELA 2: Varnejše spletno nakupovanje

Napotek	Opis
Pred spletnim nakupom si oglejte **izjavo o zasebnosti**.	Poiščite pogoje zaupnosti (ali izjavo) na dnu domače strani (oziroma vsake strani) ali v dokumentih, ki se imenujejo *angl. terms & conditions* in *angl. terms of use*. Izjava naj določa: • Katere informacije spletno mesto o vas zbira in kako jih zaščiti. • Dostop do osebnih podatkov; vsak priznani prodajalec bo ponudil preprosto urejanje in brisanje neprimernih podatkov. • Način, kako ustavite zbiranje osebnih podatkov. • Odgovorna oseba za varovanje podatkov (*angl. privacy officer*). Če ta ni omenjena, morda nihče ne nadzira, ali podjetje izpolnjuje svoje obljube.
Bodite pazljivi, **katere osebne podatke delite**.	Vprašajte se, ali spletno mesto podatek potrebuje. Naslov in številka kreditne kartice sta najverjetneje potrebna (a le na varni strani!). Bodite previdni pri objavi enotne matične številke, materinega dekliškega priimka, številke bančnega računa in podobno.
Bodite pazljivi pri **nakupovanju z enim klikom**.	Ko ustvarite račun ali opravite nakup, uporabite povečevalna očala in si dobro oglejte kljukice v poljih. Nekatera mesta si vzamejo pravico do skupne rabe osebnih podatkov in označijo polja namesto vas. Odgovorna mesta vam ponudijo možnost odjave.
Bodite pazljivi pri **nakupovanju z enim klikom**.	Spletna stran shrani podatke o kreditni kartici, naslovu in druge osebne podatke, ki vam omogočajo nakup le z enim klikom miške. To je izjemno priročno, vendar, če delite računalnik z drugimi osebami ali uporabljate javni računalnik, se odjavite takoj po opravljenem nakupu. Sicer bosta morda tuja diamantna zapestnica ali ogromen televizijski sprejemnik plačana z vašo kreditno kartico.

Vir: Povzeto po Microsoft, 2004.

Zelo pomembno je osveščanje uporabnikov o možnih situacijah, ki pripeljejo do namestitve vohunskega programa, in kakšne so posledice. Opozarjanje na nevarnosti je potrebno začeti že pri otrocih, pri katerih je internet zelo razširjen, saj kar 58 odstotkov slovenskih otrok uporablja internet. Med najpogostejša pravila, ki jih svojim otrokom postavljajo starši iz držav EU-25, sodi prepoved izdajanja osebnih informacij. Starši si zelo želijo boljše informiranosti o možnostih kako zavarovati svoje otroke pred škodljivimi in nelegalnimi vsebinami. Kot najbolj zaželen vir

informacij o tem navajajo šole (41 %), medije (30 %), ponudnike spletnih storitev (24 %) in državo (14 %) (Eurobarometer, 2004). Naslednji korak je lahko omejevanje pravic – kaj uporabniki lahko počnejo in kaj ne. Uporabniki morajo redno nameščati ustrezne popravke (npr. Service Pack 2 za Windows okolje) in nadgradnje, s katerimi se dvigne nivo zaščite pred nezaželenimi in nedovoljenimi akcijami tovrstnih programov. Eden izmed ukrepov bi lahko bil uporaba alternativnih programov (predvsem spletnega iskalnika[16], katerega pomanjkljivosti in varnostne luknje izkorišča večina znanih in razširjenih vohunskih programov).

Vse odkar je Microsoft v operacijski sistem Windows 98 vključil Internet Explorer (IE), je slednji najpogosteje uporabljeni iskalnik. Eden izmed problemov, ki nastopijo, če si vodilni v panogi, je, da si izpostavljen, in na spletu to pomeni, da so te opazili hekerji (Surmacz, 2005). Slednji so našli na IE-ju šibke točke in jih izkoristili. S pozivom svetovno priznanih ustanov, kot na primer Computer Emergancy Readiness Team in German Federal Office for Information Security, k uporabi alternativnega iskalnika se število uporabnikov IE-ja hitro znižuje. Microsoft bi moral za ohranitev tržnega deleža ponuditi popravke, ki so bili izvedeni za Windows XP s Service Pack 2, tudi za starejše verzije operacijskih sistemov, vendar slednjih ne bo. IDC[17] ocenjuje, da je bilo leta 2005 še vedno 390 milijonov uporabnikov operacijskih sistemov Microsoft, ki še niso prešli na verzijo XP. Zavedati se moramo, da bodo s tem, ko vedno več ljudi preizkuša alternativne iskalnike, tudi hekerji postali pozorni na njih. Vincent Weafer iz Symantech-a, priznanega podjetja na področju varnosti, napoveduje, da bomo v bližnji prihodnosti priča večji ranljivosti in napadom vseh tipov iskalnikov in ne samo Internet Explorerja. Bolj ko bodo popularni, bolj bodo zanimivi kot tarča napada (Janelle, 2005). In to se že dogaja; alternativni iskalniki so že začeli izdajati varnostne popravke.

Pomaga tudi, če poostrimo pravila in pravice na nivoju požarnih zidov in internetnih prehodov, v pomoč pa so lahko orodja za nadzor nameščene programske opreme na odjemalcih v omrežju. Večina teh prijemov sicer ne bo povsem odpravila nevarnosti, vendar nam bo omogočila zmanjšanje stopnje tveganja. In ob vsem tem je pomembno, da se zavedamo, da je ob vseh posledicah, tudi katastrofalnih, ob napačni ali površni uporabi računalnika in interneta nujno potreben nadzor nadzorovanega.

[16] Poznavalci predlagajo kot alternativo Internet Explorer-ju naslednja dva iskalnika: Firefox ali Opera.

[17] IDC velja za eno največjih ameriških analitičnih organizacij, ki preučuje predvsem globalne dejavnike v informacijski in telekomunikacijski industriji ter z njima povezane finančne tokove.

TABELA 3: Grožnje varnosti

Področje varnosti IS	Delež
Virusi	22 %
Hekerji	21 %
Nadzor dostopa na daljavo	17 %
Internetna varnost	10 %
Zaščita osebnih podatkov	5 %
Izobraževanje uporabnikov	5 %
Poslovanje med podjetji	5 %
Notranje grožnje	4 %
Kraja ali poškodba podatkov	4 %
Drugo	7 %

Vir: Zupan, 2004, str. 11.

Po raziskavah META Group-a po svetu namenijo za varnost povprečno 3–4 % celotnega IT proračuna. Ocenjuje se, da se bo delež povečal na 8–12 %. Po drugi strani raziskovalne institucije – kot je KPMG – ugotavljajo, da se še vedno porabi milijone dolarjev zaradi izvedenih incidentov (Zupan, 2004, str. 11).

4 KONCEPT VARNOSTI

Z nastankom interneta se je razvil nov družbeni prostor, ki ga je nemogoče nadzorovati v celoti in ki omogoča tako stare kot tudi povsem nove oblike računalniške kriminalitete[18]. Omrežje internet samo po sebi ne zagotavlja potrebnih pogojev za varno komunikacijo in e-poslovanje. Varnost računalniških sistemov in drugih pomembnih virov, ki jih obravnavamo v sklopu računalniškega omrežja, je potrebno zaščititi z izbiro ustreznih tehnologij, metod in rešitev, s kombinacijo ukrepov ter jih povezati v celoto tako, da bo varnost komunikacije prek interneta največja.

Število možnih žrtev računalniške kriminalitete raste iz dneva v dan. Tako je že vsak uporabnik interneta postal potencialna možna žrtev. Pri tem je opaziti, da naraščata tako obseg kot tudi

[18] Računalniški kriminal je nasilno dejanje na računalniku, s čimer trpi žrtev zaradi nezakonite namere kršitelja. Računalniški kriminal je relativno nov pojem, ki se je pojavil zaradi povečane uporabe računalniških sistemov za shranjevanje podatkov. Vse oblike organizacij, ki uporabljajo računalniške sisteme, so potencialne žrtve napada računalniškega napada (Forcht, 1994, str. 297). Danes se pojavljajo poleg klasičnih načinov kriminala tudi novejše oblike, ki so povezane s trendom digitalne tehnologije. Glavne oblike nasilja računalniškega kriminala so: telekomunikacijske prevare, poneverbe kreditnih kartic in drugo, vdori v sisteme, nepooblaščeno reproduciranje izdelkov, otroška pornografija, organiziran kriminal, itd.

raznovrstnost načinov in oblik izvajanja računalniškega kriminala. Zato nekatere, zlasti razvite države, ki so se že soočile z njimi, razmišljajo o zakonodajnih rešitvah, ki bi omogočile pregon tovrstnih kaznivih dejanj.

4.1 KONCEPT ČLOVEKOVE VARNOSTI

Varnost je ena izmed najbolj osnovnih in najpomembnejših vrednot, h kateri težijo vse družbe. Je neizbežna sestavina sodobnih družbenih odnosov, ki pomembno ali celo usodno vpliva na razvoj in obstoj posameznika, skupin ter družbe, kakor tudi na vse njihove duhovne in materialne vrednote. Zavestno prizadevanje za vzpostavitev stanja varnosti je civilizacijska in kulturna kategorija, ki zajema vse vidike varnosti. V različnih družbah in različnih zgodovinskih obdobjih so ljudje na pojem varnosti gledali na različne načine.

Grizold (2001, str. 123) opredeli varnost kot stanje, v katerem je zagotovljen uravnotežen fizični, duhovni in duševni ter gmotni obstoj posameznika in družbene skupnosti v razmerju do drugih posameznikov, družbene skupnosti in narave.

Razvojno gledano je varnost vgrajena kot biološki mehanizem, kot težnja organizma po obstoju, kot prilagajanje organizma na ogrožajoče vplive okolja. Biološko je torej varnost pogoj za delovanje osnovnih življenjskih funkcij in je tako vzgib za razvoj, zavestno dejanje, da bi se stanje varnosti (kot pozitivno dejanje) zmeraj znova vzpostavilo (Grizold, 2001, str. 126).

Lahko bi rekli, da je varnost nejasen in večpomenski koncept, ki ga običajno štejemo med temeljne družbene vrednote, hkrati pa trdimo, da gre pri tem konceptu za okoliščine, v katerih so zagotovljene oziroma zaščitene vse temeljne družbene vrednote. Varnost je torej mogoče opredeliti kot sredstvo za dosego nekega cilja ali pa kot cilj sam (Jelušič, 1997, str. 70). Jelušičeva definira varnost kot stanje ravnotežja mednarodnih, meddržavnih, medskupinskih, družbenih interpersonalnih in intrapersonalnih procesov, zaradi česar se v zavesti posameznika oblikuje občutek stabilnosti, homeostatičnosti, torej tudi zagotovljenih pogojev za življenje in preživetje (Jelušič, 1997, str. 70).

Anžič (2002, str. 455) varnost opredeljuje kot imanentno prvino družbe, ki zajema stanje oziroma lastnost stanja in dejavnost oziroma sistem. Pojem varnost se nanaša tako na posameznika, na državo oziroma družbo v celoti kot tudi na mednarodno skupnost. Sodobna varnostna paradigma zahteva nujnost trinivojskega pristopa h konceptu varnosti in sicer kot varnost posameznika, kot varnost skupine ter kot varnost mednarodnega sistema. Posameznik vedno najprej občuti potrebo po svoji lastni varnosti in zadovoljitev le-te mu omogoča kakovosten obstoj in razvoj. Varnost je torej človekovo zavestno prizadevanje za vzpostavitev takšne civilizacijske in kulturne kategorije, ki bo zajemala vse vidike varnosti: politične, gospodarske, pravne, zdravstvene, socialne, kulturne in številne druge. Razumevanje pojava sodobne varnosti mora nujno vključevati vse vidike človeškega obstoja in delovanja v družbi ter

vse ravni njegovega povezovanja in oblike družbenega organiziranja (regionalno, nacionalno, mednarodno in svetovno) (Grizold, 2001, str. 83). Varnost ni vezana samo na eno področje človekovega delovanja, ampak je potreba po varnosti prisotna na vseh področjih človekovega delovanja in delovanja širše skupnosti, v katere se povezuje človek (države, naroda, podjetja, itd.).

Človekovo varnost je lažje definirati ob njeni odsotnosti, vendar pa je dobro, da imamo vsaj neko bolj definirano opredelitev. Tako lahko za človekovo varnost rečemo, da ima dva glavna vidika; prvi je varnost pred tako bistvenimi grožnjami, kot so lakota, bolezni in represija, drugi vidik pa je varnost in zaščita pred nenadnimi in škodljivimi razdori v vsakdanjem življenju, pa najsi bo v domovih, službah ali skupnostih (UNDP, 1994, str. 24).

Kot je bilo že omenjeno, velja, da je varnost povezana z možnostjo svobodnega uresničevanja posameznika, zato lahko rečemo, da se svoboda in varnost medsebojno določata in dopolnjujeta. Šele varnost omogoča svobodo posameznika ali družbe in je zato njen predpogoj.

4.2 RAZSEŽNOSTI VARNOSTI

Če si res želimo razumeti problematiko varnosti v realnem svetu, potem moramo nameniti več pozornosti netehnološkim vidikom (Odlyzko, 2003). Potrebno se je namreč zavedati že samo obstoječega ekonomskega ozadja – o potrebi po tehtanju med koristmi in stroški dane rešitve. Tudi s tem v mislih bi bilo dobro preučiti spodbude posameznih igralcev, saj imajo mnogi interes preložiti stroške varnosti na druge subjekte ali pa uporabiti sredstva zaščite npr. za ohranjanje monopolne situacije (zlorabo tržnega položaja).

Vsebina informacije zatorej ni edini merodajni dejavnik pri opredelitvi problematike njene zaščite, ampak je potrebno upoštevati še kopico drugih, tj. kontekst. Poleg omenjene ekonomske plati pa nastopajo sicer še npr. tako sociološki kot psihološki dejavniki – in vsi ti dejansko združno ovirajo uspešno uvedbo in uporabo varnostnih mehanizmov.

Odlyzko poudarja, da je eden osnovnih problemov pri varnosti podatkov in informacij v sorazmerni nezdružljivosti človeške narave s formalnimi sistemi – izkaže se namreč, da je izjemno težko uravnovesiti zahteve po varnosti na eni strani ter fleksibilnostjo na drugi. Ljudje smo pogosto nagnjeni prilagajati pravila našim željam – in ne obratno. Seveda smo tudi pri svojem medsebojnem delovanju pod vplivom kulture, ki jo v dani skupnosti delimo. Težava pa je tudi v tem, da formalne sisteme gradi ožja skupina ljudi, ki so formalnih sistemov navajeni – običajno pa imajo le-ti bore malo potrpljenja za omenjene človeške dejavnike in za družabne odnose nasploh, saj od drugih ljudi pričakujejo razumevanje in vedenje podobno svojemu. Po drugi strani so te iste človekove značilnosti tiste, ki lahko ugodno prispevajo k varnosti, saj se ljudje bolje znajdejo v negotovih, nedoločenih situacijah – sem pa sodijo tudi družbene okoliščine. In ravno takšne značilnosti imajo pogosto situacije v stvarnosti, kjer potekajo e-

transakcije v določenem kontekstu – to pa omogoča neko dodatno raven varnosti. Odlyzko navaja kot primer sorazmerno hiter uspeh in široko razširjenost faksirnih naprav, čeprav je faksiran podpis vis-a-vis originalnemu pravzaprav bistveno zmanjšal objektivno raven varnosti podpisa, je ta tehnologija bistveno pripomogla h gospodarskemu razcvetu svetovnega gospodarstva. To pa zato, ker ljudje ocenjujemo varnost glede na kontekst (družbeni, pravni, ekonomski) – in je varnost dejansko do neke mere od teh odvisna.

Nadaljnji problem pri varnosti informacij v povezavi z ljudmi je po istem viru v naslednjem. Na mnogih področjih je mogoče poznavanje tehnologije oddaljiti od končnih uporabnikov – in pri tem varnost ne trpi. Pri varovanju informacij temu v splošnem žal ni tako. Življenje v informacijski družbi pomeni čedalje večjo vpletenost ljudi s tehnologijo – in ljudje so kot rečeno prav najpogostejši vzrok ranljivosti sistemov. Namreč, kljub obširni razpoložljivosti informacij o tematiki varnosti se še vedno (znova) dogaja, da ljudje nasedajo na različne zlonamerne trike, kot je npr. "nigerijska potegavščina" in različni primerki t.i. družbenega inženiringa.

Na psihološki oziroma sociološki ravni se ljudje in skupnosti ljudi ravnamo po neki vrsti analize stroškov in koristi (*angl. cost benefit analysis*) – sprejemamo rešitev problema le do tiste mere, dokler čutimo, da nam neugodnosti od dodatne varnosti ne presežejo koristi od le-te. Tako v realnem kot tudi v virtualnem svetu smo nekako pripravljeni živeti v ne povsem varnem okolju. Odlyzko pa opozarja, da je pri tem problem tudi v tem, da sta lahko v kibersvetu tako hitrost napadov kot njihova magnituda mnogo večji.

Da pa se ne kaže ravno vdati črnogledosti, je razvidno iz dejstva, da so tudi tisti posamezniki, ki namerno škodijo sistemom, zgolj ljudje in se prav tako ne vedejo vedno racionalno, delajo napake in se soočajo z zapletenostjo sistemov, katere tako ali drugače napadajo. Pa tudi primer boja medijev plačljive televizije s pirati jasno kaže, da ustrezna uporaba nabora pravnih, tehnoloških in poslovnih prijemov omogoča ohranitev rasti in donosnosti dane dejavnosti kljub nevarnostim in škodi.

4.3 INFORMACIJSKA VARNOST

Državni slovar informacijske sistemske varnosti informacijsko varnost sistemov opredeljuje kot zaščito informacijskih sistemov pred nepooblaščenimi dostopi ali modifikacijami informacij, najsi bo v shranjeni obliki, v procesu ali prenosu, ter zaščito pred zatajitvijo delovanja (DOS) pooblaščenim uporabnikom in zagotovitvijo delovanja nepooblaščenim uporabnikom, vključno z vsemi ukrepi za odkrivanje, dokumentiranje in zavračanje tovrstnih groženj (Hayden, 2003, str. 33). IBM-ov računalniški slovar informacijsko varnost opredeljuje kot koncepte, tehnike, tehnične in administrativne ukrepe, ki se jih uporablja za zaščito informacij pred namernimi ali nenamernimi nepooblaščenimi pridobitvami, povzročanjem škode, razkritjem informacij, spremembo informacij, manipuliranje z njimi ali izgubo in uporabo informacij (McDaniel, 1994, str. 94).

Večina opredelitev informacijske varnosti se osredotoča na specifično uporabo in specifičen medij (primer: zaščititi elektronske podatke pred nepooblaščeno uporabo). V bistvu pa je to napačna predstava ali nesporazum, ker se informacijsko varnost enači z računalniško varnostjo, ki je ožji pojem. Tovrstne definicije glede prenosa informacij (komunikacijski vidik) in uporabniškega vidika informacijsko komunikacijske tehnologije (IKT) opredeljuje in obravnava omrežna varnost. Koncept informacijske varnosti pa je širši in kot cilj ogroženosti vključuje celotno IKT, vključno z zbiranjem in obdelavo podatkov, in delovanje strojne opreme nasploh (Svete, 2005, str. 107).

Podjetja se v današnjem poslovnem okolju soočajo z zahtevnim izzivom ohranjanja konkurenčnosti. S ciljem racionalizacije stroškov in približevanja kupcu prilagajajo obstoječo informacijsko infrastrukturo, s čimer odpirajo vrata svojega sistema. V tej točki se pojavi vprašanje informacijske varnosti, ki zajema zaščito podatkov in fizičnih komponent sistema pred nenamerno ali namerno zlorabo. Najpogosteje izvirajo iz raznih prevar, kraj storitev, intelektualne lastnine, privatnih podatkov ter vsakdanjega vandalizma (Gordon et al., 2004).

Mnoga podjetja razmišljajo v duhu »nam se to ne more zgoditi«, vendar spregledajo dejstvo, da lahko tudi računalniki brez pomembnejše vsebine omogočajo nepridipravom podlago za napade na druge računalniške sisteme (Houle et al., 2001). Zanimivo je, da utegnejo biti podjetja, ki za svoje računalnike in mreže ne skrbijo z vestnostjo dobrega gospodarja, pravno formalno odgovorna za škodo, ki je preko njihovega sistema povzročena drugim podjetjem (Greene, 2000). Mnoga podjetja o varnosti razmišljajo kot o kategoriji, ki bo dodana, ko bodo imeli čas ali ko bodo to storitev uporabniki pripravljeni plačati (Acar et al., 2002).

Vendar lahko pogledamo na problem z drugega zornega kota in ugotovimo, da je za dolgoročni obstoj podjetja ključno zaupanje potrošnikov in dobaviteljev. Posledično si podjetja s svojo malomarnostjo ne bi smela privoščiti izgube zaupanja. Raziskava Giga Information Group ugotavlja, da je zaupanje uporabnikov ključna kategorija, ki odloča o uspehu ali neuspehu posamezne spletne storitve. Res je tudi, da popolne varnosti ni. Vprašanje je, do katere mere zaščititi sistem, kajti več ni nujno bolje. Z naraščanjem števila varnostnih ukrepov hitro pada verjetnost zlorabe, vendar prav tako hitro (eksponentno) narašča težavnost uporabe sistema (Eckel et al., 1996). Tako vstopimo v krog varnosti, stroškov in enostavnosti uporabe ter iščemo kompromise.

Strokovnjaki za informacijsko varnost se strinjajo, da je potrebno pri elektronskem poslovanju zadostiti naslednjim varnostnim zahtevam:

- Zaupnost. Pošiljanje podatkov mora biti tako zaščiteno, da je vsebina skrbno varovana, pošiljatelja in prejemnika sporočila pa ni možno identificirati.
- Neokrnjenost. Podatki, poslani v elektronski obliki, se med prenosom ne smejo popačiti, izgubiti ali kako drugače spremeniti. Celovitost podatkov je lahko npr. potrebna pri prenosu FTP-ja ali datotek elektronske pošte po internetu. Pri tem je potrebno ovreči

dvom, da je bilo sporočilo med prenosom oz. shranjevanjem spremenjeno, skrajšano ali mu je bilo kaj dodano.

- Razpoložljivost. Komunikacijska infrastruktura in računalniška mreža morata permanentno omogočati pošiljanje in sprejemanje podatkov, kar je pogoj za izvajanje elektronskega poslovanja.
- Pristnost. Pri pošiljanju sporočila moramo biti prepričani, da bo poslano točno določenemu naslovniku. Prav tako mora biti naslovnik prepričan, da je sporočilo poslal točno določen pošiljatelj in ne kakšna tretja oseba (Lawrence et al., 2000) in (Šinigoj, Turk, 1999).
- Avtorizacija. Pri avtorizaciji gre za nadzor dostopa do določenih informacij. Uporabnik, ki želi informacije dostopa, se mora identificirati in hkrati dokazati svojo pristnost, da je res objekt, ki ima pravico do teh podatkov. Največkrat gre za uporabo gesla in uporabniškega imena. Pojma avtorizacija in pristnost se v praksi večkrat mešata.
- Nadzor pretoka. Privatne mreže posameznih bank ali ustanov imajo vozlišča, ki prestrezajo in analizirajo sporočila, ki prihajajo iz ali pa so namenjena v internet. To vozlišče prestreza vsa sporočila, ki prihajajo z interneta in preveri pristnost vsakega izmed njih. Poleg tega ta vozlišča filtrirajo pakete, ki temeljijo na naslovih IP[19] storitev interneta (Šinigoj, Turk, 1999).
- Nezanikanje. Sistem mora zagotavljati, da niti pošiljatelj niti prejemnik ne moreta zanikati pošiljanja oziroma prejema sporočila (Stallings, 1995). Prejemnik sporočila lahko dokaže, da je bilo sporočilo res poslano od omenjenega pošiljatelja in pošiljatelj lahko dokaže, da je prejemnik sporočilo res prejel. Najpogosteje gre v tem primeru za najrazličnejše pravne spore med dvema poslovnima strankama.

Da pa bi lažje razumeli vseobsežnost informacijske varnosti, si lahko pogledamo samo njene grožnje. Svete (2005, str. 107) je grožnje razdelil v dve skupini. Prva skupina groženj se nanaša na informacijsko zagotovitev oz. fizične oblike ogrožanja, druga skupina pa obsega uporabniški vidik ogrožanja informacijske varnosti. V spodnji tabeli so prikazane oblike ogrožanja informacijske varnosti.

[19] Internet Protocol.

TABELA 4: Oblike ogrožanja informacijske varnosti

Višja sila	Pomanjkanje programske in strojne opreme	Človeški dejavnik	
		(nenamernost)	(namernost)
• potres • nevihte • poplave • strele • požar • visoka temperatura • visoka vlažnost • onesnaženost • radarsko sevanje • akustično sevanje • elektromagnetno sevanje • nestabilnost napajanja z električno energijo • izredne razmere • vojno stanje	• izpad sistema • tehnične napake na strežniku • tehnične napake na odjemalcih • logične napake v strežnih programih • logične napake v aplikativnih programih	• slaba organizacija • nedisciplina • nemarnost • nestrokovnost • monotonost • utrujenost	• kraje • prevare • poneverbe • izsiljevanje • grožnje • kršenje zasebnosti • sabotaže • sporočanje zaupnih podatkov • vohunjenje • pornografija • propaganda • vandalizem (cracking) • terorizem • umori • vdiranje v računalnike (hacking) • izdelava in širjenje piratstva na področju programske opreme • napadi DOS
INFORMACIJSKA ZAGOTOVITEV		DRUŽBENO IN KULTURNO OGROŽANJE	

Vir: Svete, 2005, str. 108.

Varnost lokalnih sistemov je mogoče doseči s fizičnimi varnostnimi ukrepi, kar je razmeroma enostavno. Korak naprej predstavlja elektronsko poslovanje, ki v marsičem presega meje organizacije. V takšnih in podobnih primerih si pri zagotavljanju informacijske varnosti pomagamo z zahtevnimi kriptografskimi mehanizmi.

4.3.1 Vrste napadov in zaščita

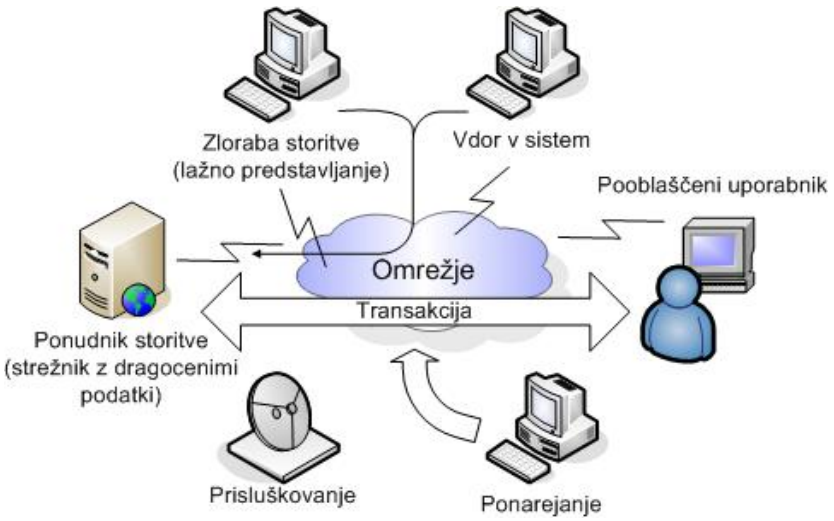
Zaščiteni oziroma zaupni podatki, ki so shranjeni na računalniških sistemih in potekajo preko omrežij, predstavljajo za posameznike, podjetja in ostale ustanove nevarnost razkritja podatkov, kar lahko pripelje do hudih posledic, kot je na primer finančni primanjkljaj. Zaupni podatki so številke kreditnih kartic, poslovne skrivnosti, elektronsko-zdravstvene kartice, programska oprema sistemov, torej razne aplikacije, ki služijo za način izvedbe določene naloge.

V računalniškem sistemu varujemo shranjene podatke, ki so ponavadi končni cilj potencialnega napadalca. Zaradi tega moramo zagotoviti (Pepelnjak, Bradeško, 1997, str. 157):

- varnost dostopa, kjer so predmet zaščite viri in storitve v sistemu;
- varnost uporabe, kjer je potrebno zagotoviti, da za dostop pooblaščeni uporabniki v sistemu počno le tisto, kar jim glede na njihov položaj pripada; zaščito potrebujejo tudi uporabniki sami – v banki ne pustijo, da bi uporabnik storitve (npr. pri vpogledu v bančni račun) pri tem doživel zlorabo s strani tretje osebe;
- varnost transakcij – vsi pomembni podatki, ki se izmenjujejo preko komunikacijskih poti, morajo preko teh potovati varno, brez možnosti, da bi jih kdo prestregel ali celo poneveril;
- vdori v sistem – ti imajo lahko za posledico le nepooblaščen dostop do podatkov in njihovo krajo, lahko pa tudi spremembo, ali še huje, uničenje podatkov (med te napade lahko uvrstimo večino današnjih računalniških virusov, ki se prikradejo do sistema in povzročijo določeno škodo);
- prestrezanje sporočil – tu napadalec ne vdre v sam sistem, pač pa za dostop do podatkov (in tudi morebitno spremembo le-teh) uporabi prenosne poti, kjer z ustrezno strojno in programsko opremo prisluškuje ali spreminja podatke, ki potujejo po napadeni poti;
- onemogočanje storitev (*angl. denial-of-service*) – kjer napadalec poskuša poslabšati kakovost storitve ali jo povsem onemogočiti (npr. z izjemno povečanim številom zahtev po določeni storitvi na sistemu, ki pod tako obremenitvijo ne deluje več optimalno, ali pa z umetnim ustvarjanjem nepotrebnega omrežnega prometa, ki zasiti prenosne poti);
- povzročanje stroškov – tu napadalec izkoristi določene varnostne pomanjkljivosti in uporabi storitev, do katere sicer ni upravičen – to napadenemu povzroča nepotrebne stroške, druge škode ponavadi nima; ti napadi so danes zelo popularni, saj napadalec pride do informacijskih virov zastonj ali mnogo ceneje kot sicer.

Omenjene napade srečujemo tudi v kombinirani obliki. Z nedolžnim prisluškovanjem se napadalec lahko prikoplje do podatkov (npr. gesel), s katerimi lahko povzroči veliko škode.

SLIKA 4: Vrste napadov v omrežjih



Vir: Pepelnjak, Bradeško, 1997, str. 159.

V današnjem času so najbolj pogosti vdori v sistem, ki imajo lahko za posledico ogromno škodo, kar še posebej velja za banke, ki se varujejo pred nepooblaščenimi dostopi do podatkov in njihovo krajo. Zato obstajajo določeni programi, ki zaščitijo računalnik oziroma strežnike pred potencialno nevarnimi vsebinami, ki prihajajo z interneta. Eden izmed teh je požarni zid. Z njegovo pomočjo se pridobi večji nadzor nad tem, kateri podatki prihajajo v računalnik in kateri gredo iz njega. Naposled se uveljavlja tudi spoznanje, da končni rezultat povezave na internet ni samo požarni zid, ampak tudi posamezni računalniki, ki so za njim skriti. V večjih podjetjih hitro naraste možnost vdora in kraje informacij, saj je priključkov za dostop do omrežja veliko. Zato obstajajo npr. omejitve omrežnega priključka na strojni naslov omrežne kartice, kar pa vseeno ni dovolj, saj je mogoče strojni naslov omrežne kartice dokaj enostavno poneveriti. Zaradi tega so spisali standard (802.1x), ki omogoča dinamični vklop in izklop omrežnega priključka. Še večjo nevarnost predstavlja brezžična dostopna točka, saj je medij prenosa podatkov tu zrak in lahko vsak, ki ima prenosnik, prisluškuje pogovoru med posameznimi brezžičnimi napravami, kar še posebej oteži zagotavljanje varnosti omrežja.

4.3.2 Pasti in nevarnosti

Internet je neprecenljivo orodje za delo, raziskovanje ter tudi dobra zabava. Ogromen, neomejen svet vsebin je dostopen vsem in ta virtualni svet konstantno raste. Problem, ki pri tem nastaja, je seveda ta, da nikoli ne vemo, na kaj bomo naleteli, ko ga naključno raziskujemo. Še več, nenehno smo soočeni z različnimi reklamami in podstranmi, ki nam jemljejo čas, nas ne zanimajo, so nespodobne, nekatere nelegalne ali celo nasilne (Kavran, 2004, str 23).

Pred nekaj leti se je zdelo, da je internet tehnologija svobode, danes pa se zdi, da je panoptičnost že vgrajena vanj. Aktivno vlogo pri nadzoru na internetu imajo države in njihovi organi, še posebej pa to velja od terorističnega napada 11. septembra 2002 v ZDA. Za podjetja je zanimivo nadzorovanje potrošnikov oziroma zbiranje podatkov o slednjih, lahko pa tudi nadzorujejo aktivnosti svojih zaposlenih (Kovačič, 2003, str. 40).

Država in podjetja se torej nadzora poslužujejo z natančno določenimi nameni in cilji. Nadzorovanja po internetu se poslužujejo tudi hekerji[20] (*angl. hacker*), ki pa navadno ne vdirajo v računalnike samo zaradi finančne koristi, pač pa zgolj za zabavo, zaradi samodokazovanja (poskusi vdorov v čim bolj zavarovane sisteme), postavljanja rekordov ali povzročanja škode. Število napadov je tesno povezano tudi s šolskim urnikom, kar kaže, da za napadi stoji veliko mladoletnikov.

[20] V nadaljevanju magistrskega dela bomo besedi heker in vdiralec uporabljali kot sopomenki.

4.3.2.1 Zahrbtni programi

Zahrbtne programe lahko definiramo kot programsko opremo, ki ima za osnovni namen povzročanje škode, izgube ali vohunjenje. Razdelimo jo lahko na naslednje skupine:

- virusi,
- črvi,
- trojanski konji,
- miselni virusi,
- kombinirani virusi.

Povprečen uporabnik interneta je najpogosteje žrtev računalniškega **virusa**. Gre za zahrbten program, ki se vključi v algoritem drugega programa. S tem ga tako okuži. Ko poženemo okuženi program, se lahko z njim požene virus, ki se hkrati samo razmnožuje, tako da se priključi drugemu še ne okuženemu programu in povzroči več ali manj škode.

Posebni primeri virusov so makro virusi, ki se širijo preko aplikacij, kot so urejevalniki besedil ali preglednice, še posebno veliko pa jih za svoje razširjanje uporablja Microsoft Word in Excel. Virusi se prenašajo s kopiranjem podatkov med sistemi in lahko povzročijo veliko škode. Podobni virusom pa so **črvi**, vendar za razliko od virusov le-ti delujejo v računalniškem omrežju in za svojo širitev ne potrebujejo drugega programa (Bertoncelj, 2000, str. 135). Črvi izdelajo svoje kopije in za širjenje izkoriščajo obstoječe povezave med računalniki. Ker je danes večina računalnikov povezanih v omrežje, kot je internet, se lahko preko omrežja v zelo kratkem času okuži ogromno računalnikov.

Trojanski konji se ne znajo sami razmnoževati. Namesto tega ponudijo uporabniku kakšno zanimivost, v ozadju pa počno druge nedovoljene reči, npr. sporočajo podatke iz računalnika, omogočijo dostop do računalnika napadalcu, počnejo določene stvari v imenu uporabnika in podobno.

Poleg naštetih vrst zlonamerne programske opreme pa poznamo še tako imenovane **miselne viruse** ali potegavščine (angl. hoaxes). To so razna obvestila v slogu:
»Pojavil se je nov nevaren virus, ki lahko pobriše vse podatke v računalniku. Preglejte, če je ta in ta datoteka na vašem računalniku in jo nemudoma pobrišite ...«

Navadno taka besedila navajajo kakšno znano računalniško podjetje, preveč poveličujejo zmožnosti virusa in svetujejo, da sporočilo takoj pošljete prijateljem. Taka obvestila niso nič manj nevarna kot virusi, saj lahko z njihovo "pomočjo" uporabnik sam onesposobi računalnik tako, da si pobriše kakšno pomembno datoteko, ki je potrebna za delovanje računalnika.

4.3.2.2 Zasipanje z vsiljeno pošto

Z izrazom »spam« (slednjega smo že spoznali v tretjem poglavju) označujemo vsiljeno elektronsko pošto. Večinoma gre za oglaševanje, pogosto tudi različnih goljufivih ali nezakonitih izdelkov ali storitev. Raziskave kažejo, da količina takšnih sporočil narašča in krni uporabnost elektronske pošte. Zaradi možnosti velikih zaslužkov je spam tudi eden izmed pomembnih dejavnikov za razmah kiberkriminala. Poleg spama, povezanega z elektronsko pošto, poznamo še spam na konferencah USENET, sistemih za klepet preko interneta (MSN, ICQ, itd), v zadnjem času pa tudi dopisovanje reklamnih komentarjev na t.i spletne dnevnike (*angl. bloge*).

V splošnem lahko za spam sporočilo smatramo vsako sporočilo, ki je poslano večjemu številu naslovnikov z namenom vsiljevanja vsebine, ki se je naslovniki sami ne bi odločili prejemati. V veliki večini primerov gre za oglaševanje plačljivih storitev ali izdelkov. Ponavadi se s spam pošto oglašujejo izdelki ali storitve dvomljive kvalitete, velikokrat pa gre za goljufije[21]. Ker ponudniki dostopa do interneta kot zaščitni ukrep pogosto omejujejo dostop do strežnikov za pošiljanje odhodne pošte, so pričeli vdirati v računalniške sisteme z namenom pošiljanja vsiljene elektronske pošte, delno pa tudi postavljanja lažnih spletnih strani, preko katerih prodajajo npr. (otroško) pornografijo ali ponarejena zdravila. Pri tem si pomagajo z računalniškimi virusi in črvi.

4.3.2.3 Prevare, sleparije

V informacijski dobi je zlonamerno delovanje pogosto delo sleparjev ali pravih zlonamernežev, skritih za neko prevleko, masko. Vse to pa ima za sabo nek skrit namen, ki je uporabniku neznan. Ti napori pa imajo nekaj skupnega. Njihov glavni namen je prevarati uporabnika, da sprejme napačne informacije oziroma naredi napačne poteze na podlagi napačnih informacij. Te napačne informacije pa pridobi iz vira, za katerega misli, da je avtentičen, vendar je ta vir lahko s pomočjo prevare ponarejen in tako informacije, ki so na voljo, ne služijo prvotnemu namenu.

Prevara v računalništvu predstavlja situacijo, v kateri se neka oseba ali program uspešno zamaskira kot nekdo drug s ponarejanjem podatkov in tako dobi neko nelegitimno prednost ali korist.

Elektronsko vohunjenje je tehnika, ki pregleduje in izloča informacije iz informacijskih paketov, ki potujejo po internetnem omrežju. Izluščene informacije lahko vsebujejo uporabniška imena, gesla in druge pomembne informacije, ki potujejo v omrežju v čisti tekstovni obliki. S pomočjo stotih ali tisočih gesel, ki jih program pridobi, lahko vsiljivec sproži obsežen napad na sisteme. Namestitev omenjenega programa ne zahteva administratorskih pravic na računalniku, kjer program nameščamo.

[21] Tipičen primer je nigerijska prevara, ki prevarantom včasih uspe tudi pri nas. Primer slednje si je moč ogledati na Arnesovi spletni strani [URL:http://www.arnes.si/spam/nigerijska-prevara.txt].

Danes se na internetu zbira velikansko število osebnih podatkov in to seveda brez privolitve ali celo brez vednosti posameznikov (Data Protection Working Party, 2000, str. 19). Odprta omrežja in večji pretok informacij spodbujata razvoj novih proizvodov in storitev, doseganje družbenih in ekonomskih koristi, ustvarjata pa tudi nove probleme glede varstva in zaščite osebnih podatkov. Velika večina uporabnikov se namreč ne zaveda, da vsaka transakcija na internetu za seboj pušča elektronske sledi (Žurej, 2001, str. 38). Nekateri jih z vsako uporabo računalniške tehnologije puščajo namerno (npr. na svoji spletni strani), kakor tudi nevede (npr. z obiskom spletne strani). Obstaja tudi nevarnost vdora v računalniški sistem. Zlorabe niso povzročene samo s tehničnimi sredstvi, pač pa tudi z različnimi goljufijami, ko skušajo napadalci žrtev prepričati oziroma pretentati, da jim posreduje dostop do sistema ali posreduje želene podatke oziroma informacije ali pa se do želenih podatkov celo dokopljejo s tajnim opazovanjem. Govorimo o zamaskiranih straneh (*angl. phishing sites*), ki slonijo na uporabi socialnega inženiringa in sodobne informacijske tehnologije.

Zamaskirane strani so ponavadi skrite v spletne banke z namenom napeljevanja uporabnika k vpisu osebnih podatkov in gesel. Zaradi slabe uporabe slovnice in črkovanja so zaenkrat zlahka prepoznavne, vendar se njihova oblika vse bolj spreminja in postajajo vse bolj podobne resničnim stranem bank (Ward, 2005). Znani so tudi primeri, ko so se napadalci lažno predstavili kot osebje tehnične pomoči in se tako dokopali do uporabniških imen in gesel ali pa so celo postavljali lažne spletne strani[22]. Uporabniki namreč večinoma ne vedo, da lokacija spletne strani v splošnem zapisu lahko vsebuje tudi uporabniško ime in geslo za dostop do strani v obliki http://ime:geslo@www.streznik.com. Seveda večina spletnih strani tega ne zahteva, saj je dostop prost za vse. Ker je do javno dostopnih spletnih strani mogoče dostopiti z vpisom kateregakoli imena in gesla, obstaja nevarnost, da uporabnik zamenja uporabniško ime s spletnim mestom (Kovačič, 2003, str. 42). Izdelava zamaskiranih strani je postala resna grožnja družbi. Dobičkonosen posel z minimalnim začetnim kapitalom, majhnimi možnostmi za izsleditev in visokim izkupičkom privablja vse več nepridipravov. Slednje dokazuje tudi Anti-Phishing Working Group, ki poroča, da se je število zamaskiranih strani v letu 2005, glede na preteklo leto, povečalo za dobro četrtino (Ward, 2005).

Pred kratkim smo bili priča prvemu »phising« napadu na uporabnike Nove Ljubljanske banke, kar dokazuje, da so napadi in varnostni incidenti, bazirani na socialnem inženiringu, resen varnostni izziv, tako za ponudnike storitev na internetu kot tudi za uporabnike teh storitev. Že v času hladne vojne so vohunske organizacije z vzhoda nadomeščale svojo tehnološko inferiornost z uporabo metod, baziranih na socialnem inženiringu, in s tem vzdrževale ravnovesje. Danes pa se moramo vprašati, kaj vse zmore kombinacija sodobnih internetnih tehnologij in socialnega

[22] Lep primer je bil npr. decembra 2002, ko se je pojavila spletna stran ebayupdates.com. Uporabniki nakupovalnega spletišča eBay so bili po elektronski pošti naprošeni, naj na spletno stran ebayup-dates.com vpišejo številko svoje kreditne kartice in geslo. Seveda je bila spletna stran lažna in ni bila nikakor povezana s podjetjem eBay, namenjena pa je bila izključno kraji številk kreditnih kartic (http://story.news.yahoo.com/news?tmpl= story2&cid=575&ncid= 738&e=6&u=/nm/20021211/wr_nm/crime_ebay_email_dc).

inženiringa ob tovrstnih napadih, kaj lahko naredimo kot posamezniki, podjetja in družba, da se ubranimo takih napadov.

Kot v vsaki vojni imamo za zmago na voljo več različnih orožij. V primeru »phishinga« in podobnih načinov goljufanja je učinkovita le kombinacija naslednjih: socialni odgovor, uporaba sodobnih tehnologij in ustrezna pravna ureditev ter praksa.

Analitiki in raziskovalci, specializirani za zaščito, namreč ocenjujejo, da bodo napadi virusov ter črvov, trojanskih konjev, klicalnikov in drugih hekerskih orodij vsako leto hujši, s težjimi morebitnimi posledicami za poslovanje. Po oceni META Group so podjetja v letu 2004 porabila 8,2 % informacijskega proračuna za zaščito pred virusi in podobnimi nevšečnostmi, kar je za 44 % več kot v letu prej. Kljub splošnim gospodarskim težavam je kar 66 % podjetij povečalo delež sredstev, namenjenih zaščiti. Ne glede na omenjeno povečanje sredstev za zaščito so v letu 2005 virusi in črvi, po oceni podjetja Trend Micro, povzročili škodo v vrednosti okoli 55 milijard dolarjev, za 45 % več kot v letu prej in celo 76 % več v primerjavi z letom 2001 (Jakupović, 2005, str. 66).

Glavno sredstvo njihovega hitrega širjenja je elektronska pošta, preko katere prihaja 95 odstotkov vseh virusov in drugih škodljivih programov. Še hujši kot napadi samih virusov so vdori črvov[23], ki se prek e-pošte hitro širijo po celem svetu in povzročajo škodo največjega obsega. Veliko škode lahko prinesejo tudi vohunski programi, ki po vdoru zbirajo podatke in jih pošiljajo na določene e-naslove s ciljem nadaljnje zlorabe. Podobno delovanje imajo tudi trojanski konji in druga hekerska orodja, ki med drugim lahko odprejo stranska vrata za nadaljnje hekerske vdore. Zanimivo je, da najpogosteje lahko zasledimo kot razlog hekerskega napada ravno preizkušanje lastnega znanja in sposobnosti. Omrežja raznih institucij jim služijo kot igrišče, do katerega dostopijo preko interneta in na katerem testirajo svoja orodja – programe. Vse bolj nevarna in na druge načine škodljiva postaja tudi že nekajkrat omenjena vsiljena e-pošta, ki je po obsegu že dosegla "običajno" e-pošto, danes tako pomembno za poslovanje. Vsiljena e-pošta poleg ogromne izgube časa, zaradi njenega pregledovanja in brisanja, prinaša še dodatne nevarnosti in škodo, ker jo hekerji pogosto uporabljajo tudi kot sredstvo širjenja virusov in drugih zlonamernih programov.

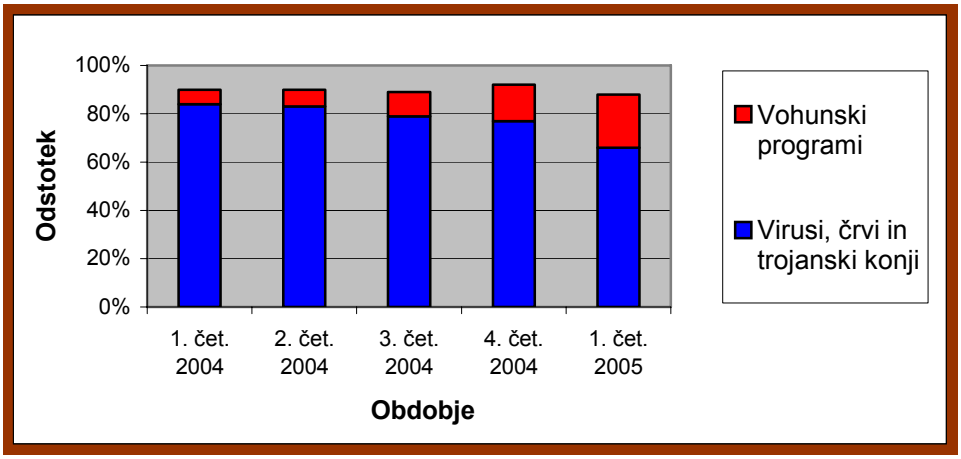
V nadaljevanju magistrskega dela se bomo posvetili predvsem elementom, ki posegajo v našo zasebnost oziroma vplivajo na naše zaupanje in ne toliko ostalim nevšečnostim (virusi in črvi), ki nam načeloma le otežujejo delo. Zavedati se moramo, da je zelo težko zapisati ločnico med le-temi, saj tudi virusi in črvi ogrožajo našo socialno varnost. Eden izmed primerov je kraja identitete – ko se virus na okuženem računalniku samostojno razmnožuje tako, da v žrtvinem imenu pošilja škodljive datoteke.

[23] Prvi črv, imenovan Morris, katerega avtor je bil Tappan Morris, se je pojavil pred sedemnajstimi leti in od takrat ima pojem spletna varnost nove dimenzije. V samo nekaj urah je uspešno okužil nekaj tisoč računalnikov in povzročil precej težav administratorjem.

4.3.2.4 Vohunski programi: nadloga ali nevarnost?

Izraz vohunski programi (*angl. spyware*) je generično ime za cel niz programov, ki lahko v ciljnih sistemih povzročajo bolj ali manj resne nevšečnosti. Sem sodijo s stališča nevšečnosti tudi povsem navadni programi, ki ne počnejo drugega, kakor da nas motijo z reklamnimi sporočili ali pa pri nemotenem brskanju po spletnih straneh. Precej bolj nevarni so programi, ki zapisujejo naše delovanje ali pa iščejo podatke v naših sistemih in jih brez naše vednosti posredujejo na neznano zbirališče podatkov (v tem konceptu jih bomo obravnavali tudi v nadaljevanju magistrskega dela). Ti programi ne samo da vdirajo v našo zasebnost, temveč nam tudi upočasnijo računalnik (kadar spyware oddaja podatke, lahko med deskanjem opazimo zastajanje pri prenosu strani), s čimer se po definiciji že zelo približajo temu, kar pojmujemo kot računalniški virus. Ne smemo mimo internetnih piškotkov, ki jih lahko iznajdljivi avtorji uporabijo za zbiranje podatkov o navadah uporabnikov, kar je vsekakor vdor v zasebnost. Potem so tu še programi, ki izvajajo akcije, ki so v korist vdiralcu – prek modema kličejo plačljive telefonske številke ali pa "obiskujejo" spletne strežnike s ciljem večanja zadetkov.

SLIKA 5: Odstotek računalnikov s prisotnostjo vohunskih programov med ameriškimi uporabniki v obdobju 1. četrtletje 2004 – 1. četrtletje 2005



Vir: eMarketer.com, 2005.

Iz zgornje slike je razvidno, da se kljub konstantni okuženosti računalnikov (okoli 90 %) delež vohunskih programov iz obdobja v obdobje povečuje. Po drugi strani je opaziti upad virusov in ostalih nadlog.

Nekatere[24], ponavadi brezplačne (vohunske) programe, si uporabniki sami namestijo, saj se ne zavedajo oziroma ne pričakujejo, kaj vse je bilo v namestitveni datoteki poleg obljubljene vsebine. Spet drugi se celo jasno predstavijo in obljubijo nekaj v zameno – ponavadi neko

[24] Eden takih je znani program Gator, ki uporabniku sicer povsem jasno razloži pogoje uporabe, pa ga še vedno kljub temu srečamo na številnih računalnikih. Tu zbira podatke, prikazuje (nezaželene) reklame, v praksi pa tudi precej obremenjuje komunikacijske povezave.

programsko rešitev. Posledice, ki so rezultat nameščenih vohunskih programov, so ponavadi naslednje (povzeto po Djurdjič, 2004, str. 20–22):

- motenje z reklamnimi sporočili,
- povzročanje sprememb v delovanju računalnika in upočasnitev delovanja,
- izvajanje akcij z namenom zaslužka v korist vdiralcu,
- spremljanje navad uporabnikov in zapisovanje slednjih v oddaljene baze,
- beleženje natipkanega besedila,
- posredovanje uporabnikovih dokumentov, ki so na krajevnih diskih in v omrežnih strežnikih, vidnih iz lokalnega sistema.

Vohunskih programov se marsikje lotevajo povsem brezskrbno in nepripravljeno. Medtem ko si danes pri virusih prizadevamo, da bi bile definicije za protivirusne programe ažurne domala vsako minuto, ima le malo podjetij aktivno politiko glede vohunskih programov. Analitiki, ki se ukvarjajo z varnostjo v informacijskih sistemih, so zato vohunske programe začeli postavljati med nevarnosti z največjim tveganjem, na kar bi morali biti pozorni prav vsi.

4.4 NAPREDNE TEHNIČNE REŠITVE IN VARNOSTNE KOMPONENTE

V računalniških omrežjih je prestrezanje podatkov po omrežju podobno prisluškovanju v telefonskem omrežju. Elektronsko sporočilo je mogoče še bolj preprosto prestreči, saj se elektronska pošta po internetu načeloma prenaša nešifrirano, torej kot navadno besedilo. Podatke pa lahko spremenimo v tako obliko, da si prisluškovalec, ki jih prestreže, z njimi ne more pomagati.

Zaradi narave interneta, ki je zaenkrat v veliki meri pravno neurejen navidezni prostor, ki ne priznava državnih meja ter posledično predstavlja veliko oviro državnemu nadzoru, je za varovanje lastnih pravic najprej odgovoren uporabnik. Tako kot razvoj tehnologije nenehno prinaša nova in učinkovitejša orodja, s katerimi lahko posega v posameznikove osebne pravice, nova tehnologija ponuja tudi vrsto rešitev, ki lahko služijo zavarovanju različnih interesov glede zasebnosti in anonimnosti dejavnosti posameznikov in podjetij pri uporabi internetnih storitev. Paleta tovrstnih rešitev je široka in obsega tako strojne kot programske rešitve: požarna stena (*angl. firewall*), anonimni pošiljatelj e-pošte (*angl. anonimous remailer*), programska oprema za filtriranje e-pošte, programska oprema za anonimno deskanje po svetovnem spletu, "ubijalci piškotov", šifriranje elektronske pošte, posameznih datotek ali celotnega računalniškega diska, digitalni podpis, digitalni certifikat ipd. Večina te programske opreme, ki je dostopna na internetu, je poceni ali pogosto celo zastonj. Vendar pa marsikateri delodajalec namestitev tovrstnih programov na službene računalnike prepoveduje.

Omrežje internet samo po sebi ne zagotavlja potrebnih pogojev za varnost osebnih podatkov in elektronskega poslovanja. Za varnost je potrebno poskrbeti z izbiro ustreznih tehnologij, metod in rešitev ter jih povezati v celoto tako, da bo varnost osebnih podatkov prek interneta največja. Za varno uporabo interneta predstavljamo nekaj aktualnih pristopov in zaščit.

1. **Kriptografija**. Najbolj znana in učinkovita tehnika zaščite zasebnosti je kriptografija[25] (Kovačič, 2003, str. 64). Z besedo kriptografija označujemo metode za zaščito vsebine podatkov. Sporočilo zakrijemo z enkripcijsko metodo in enkripcijskim ključem in dobimo kriptogram, ki ga lahko pošljemo naslovniku. Naslovnik nato kriptogram s pomočjo dekripcijske metode in dekripcijskega ključa predela v izvorno obliko sporočila (Vidmar, 1997, str. 162–164).

2. **Varni protokoli**. Osnovna ideja varnih protokolov je vzpostavitev varnega kanala med dvema računalnikoma, ki zagotavlja zaupnost, neokrnjenost podatkov in možnost preverjanja identitete. Najbolj znana metoda za zaščito podatkov na mrežni ravni je standard IPSec. IPSec nam omogoča vzpostavitev navideznega zasebnega omrežja znotraj javnega omrežja, kot je internet.

3. **Požarne pregrade**. Požarna pregrada (*angl. firewall*) je omrežna naprava, ki nadzoruje dostop do oziroma iz omrežja. Njena osnovna funkcija je spremljanje in omejevanje prometa. Nahaja se na robovih omrežja in mora biti postavljena na vseh vhodno/izhodnih točkah. Največkrat zagotavlja varen dostop iz intraneta v internet ter obratno in je zato postavljena med notranjim in zunanjim omrežjem.

4. **Elektronski podpis**. Zakon o elektronskem poslovanju in elektronskem podpisu določa, da je elektronski podpis enakovreden lastnoročnemu podpisu. Elektronski podpis lahko uporabljamo zgolj kot dodaten varnostni mehanizem, ki poviša nivo varnosti v računalniški aplikaciji. Vendar tu ne gre samo za tehnični, temveč tudi za pravni termin. Elektronski podpis je namreč tisti varnostni element, ki zagotavlja dokumentu v elektronski obliki pravno veljavo, npr. računu v elektronski obliki status verodostojne knjigovodske listine.

5. **Gesla in druge zaščite**. Najstarejši in najenostavnejši način preverjanja identitete je identifikacija s pomočjo gesla oziroma določene informacije, ki določa neko osebo ali subjekt. V e-poslovanju se z gesli ali identifikacijskimi številkami srečujemo praktično na vsakem koraku. Predstavljajo najenostavnejši način identifikacijske uporabnosti in so ključ dostopa do varovanih podatkov.

Varnostna politika je kompromis med stroški in tveganji. Sistem je varen, ko imajo napadalci večje stroške od koristi vdora v sistem. Povedano drugače, najšibkejši člen v verigi zagotavljanja informacijske varnosti je običajno človek. Tudi najmodernejše tehnologije varovanja ne pomagajo, če uporabnik izbere slabo geslo ali nasede na prevaro, izvedeno s pomočjo socialnega inženiringa. Zatorej bi *družba* (šole, podjetja in ostale ustanove, ki imajo vpliv na vedenje spletnih uporabnikov) morala poskrbeti za ustrezno izobraževanje ter hkrati zahtevati dosledno izvajanje varnostnih ukrepov.

[25] Kriptografija je veda o tajnosti, šifriranju, zakrivanju sporočil in o razkrivanju šifriranih podatkov (kriptoanaliza).

5 KONCEPT ZAUPANJA

Koncept zaupanja so sprva obravnavali zlasti na področju sociologije, zadnja leta pa ga vse bolj omenjajo tudi na področju ekonomije, kot osnovni pogoj za uspešne ekonomske transakcije. Zaupanje predstavlja pripravljenost uporabnikov oziroma kupcev za nakup izdelka ali storitve ter pri tem sprejem določene stopnje tveganja. Organizacija lahko poveča zaupanje svojih uporabnikov z ustreznimi certifikati o kakovosti izdelkov, z garancijami, z možnostjo vračila izdelkov in podobno (Compagno, 1999, 120–123).

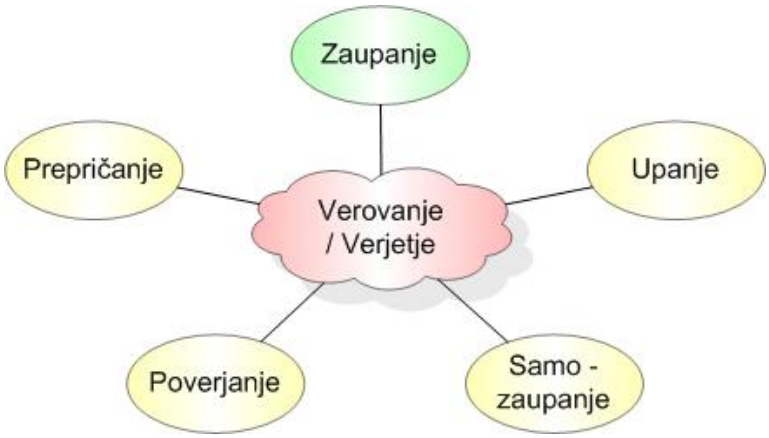
Preden bomo podrobneje spoznali različne opredelitve zaupanja priznanih svetovnih avtorjev, bi želeli predstaviti opredelitev zaupanja, ki jo je podal Warren E. Buffett. Le-ta je dejal: »Zaupanje je kot zrak, ki ga vdihavamo. Ko je prisoten, ga nihče ne opazi, ko ga ni, pa vsi«.

5.1 OPREDELITEV ZAUPANJA

Če poskusimo temo zaupanja internetu umestiti v sistem znanosti, smo naleteli na trd oreh in zabredli v široko temo, ki jo lahko obravnavamo z več stališč. Zaupanje je po eni strani psihološka tema, proučevali pa so jo tako ekonomisti, sociologi, politologi kot tudi drugi družboslovci. Spletno zaupanje bi nenazadnje lahko proučevali tudi s popolnoma tehničnega vidika, saj pomemben del gradnje zaupanja predstavlja zagotavljanje varnosti skozi zapletena kodiranja gesel in ključev, ki zahtevajo visoko strokovna tehnična znanja.

V literaturi lahko najdemo veliko različnih opredelitev zaupanja, ker gre dejansko za večrazsežnostni koncept. Izvor besede zaupanje lahko med drugim najdemo tudi v antropološki kategoriji verovanja oziroma verjetja. Iz Slike 6 je razvidno, da razsežnost verovanja obsega pet pomembnejših sestavnih delov: prepričanje, poverjanje, upanje, zaupanje in samozaupanje. Verovanje obsega široko pomensko področje, od zavesti o obstoju določenih nadnaravnih sil, prepričanja o obstoju česa skrivnostnega, umišljenega, domnevnega, predpostavljenega, do verovanja v ljudi in prepričanja o njihovi poštenosti, nadarjenosti, učinkovitosti ter iskrenosti. Prepričanje je verovanje, da je povedano ali navedeno v skladu z resnico. Poverjanje pomeni verjeti ali zaupati nekomu, da bo po svojih najboljših močeh izpolnil nalogo. Upanje izraža pričakovanje, da bo dogovorjena naloga izvedena. Samozaupanje temelji na zaupanju vase. Kdor ne zaupa v svoje sposobnosti, bo težko izkoristil svoje zmožnosti, saj jih ne bo upal pokazati drugim. Lahko ima dobre zamisli, a ne verjame, da jih lahko uresniči (Mayer, 2004, str. 57–61). Zaupanje določa odnosno komponento do stvari, pojavov, drugih ljudi in samega sebe. S tem se približujemo Dunnovemu konceptu, da je zaupanje človeška strast in hrepenenje (De Vos, Wielers, 2003, str. 81).

SLIKA 6: Razsežnosti verovanja/verjetja



Vir: Mayer, 2004, str. 58.

Whitney (1994, str. 16) razloži zaupanje kot vero in prepričanje v poštenost, zanesljivost in pravičnost drugih ljudi. Vsebuje nagonsko, nevprašljivo in nedvomljivo prepričanje, vendar je kljub temu lahko le začasen pojav. Zaupanje mora biti vedno zasluženo, njegov pomen pa jasen in razumljiv.

Pri zaupanju lahko razlikujemo (Whitney, 1994, str. 16):

- med zaupanjem, ki pomeni nagonsko in brezpogojno prepričanje oz. vero,
- med zaupanjem, ko se zavedamo pozitivnih razlogov in
- med zagotovilom, ki vsebuje popolno prepričanje in gotovost.

Sitkin in Roth (1993, str. 378) predlagata, da se zaupanje razdeli na štiri velike skupine: zaupanje kot individualna lastnost, zaupanje kot situacijska značilnost in zaupanje kot institucionalni dogovor. Zaupanje lahko poleg tega opredelimo tudi kot odnos in lahko predstavlja tudi kakovost določenega razmerja. Tako lahko najširše opredelimo zaupanje kot pozitivno pričakovanje, da naš partner ne bo skozi besede, dejanja ali odločitve ravnal preračunljivo (izkoristil ranljivosti druge strani) ne glede na možnosti in priložnosti. Pri tem mislimo, da je zaupanje brezpogojno in omejeno. Obstajajo določene omejitve oziroma meje, ki jih okolje postavlja združbam in posameznikom pri zaznavi in razlagi zaupanja. (Kovač, Jesenko, 2004, str. 41).

Zaupanje je neposredno povezano z odvisnostjo in tveganjem. Podobno, kot gre za razmerje med varnostjo in nevarnostjo, gre lahko za razmerje med zaupanjem in tveganjem. Ljudje zaupamo v nekaj ali nekomu, pri čemer se pojavi možnost, da pričakovanja ne bodo izpolnjena in zadovoljena, oziroma se stvari ne bodo odvijale v skladu s pričakovanji. Zaupanje nam tako omogoča sprejemati tveganja, čeprav je vedno prisotna stopnja negotovosti. Prav ta odvisnost od dejanj drugih, na katere nimamo vpliva in pri čemer nimamo vnaprejšnjih dokazov, nas naredi ranljive (Pečovnik, 2001, str. 54).

Zaupanje ne more obstajati v okolju gotovosti, saj se v takšnem okolju dogovorjene stvari dogajajo samoumevno in zaupanje zato ni potrebno, ali pa ima samo obrobnejši pomen. Iz tega sledi, da zaupanje obstaja v negotovem in tveganem okolju, kot je na primer internet.

5.2 RAZSEŽNOSTI ZAUPANJA

Zaupanje je odvisno tako od zaupnika kot tudi od pogojev in okoliščin. Različnim zaupnikom različno zaupamo in določenemu zaupniku zaupamo odvisno od situacije. Nekdo zaupa nekomu ali v nekaj z obzirom na nekaj (sposobnosti, namere) v odvisnosti od pogojev. Zaupanje je odvisno od zunanjih in notranjih pogojev. Zunanji vsebujejo trge, pravne sisteme, običaje, norme in pravila upravljanja. Notranji pa zajemajo združbo kot prizorišče za preživetje njenih članov. Ostali notranji pogoji so značilnosti delovnih nalog, organizacijska struktura, vodenje, kultura, proces vzajemnega delovanja in komunikacija.

Ljudje so na začetku življenja popolnoma odvisni od drugih, kasneje biološka potreba postane bolj psihološka zahteva, saj si želimo določeno mero predvidljivosti, stabilnosti, zanesljivosti in varnosti. Zaupanje je biološko določeno in ima prav tako lahko tudi biološke posledice. Giddens v svoji teoriji razlaga, da je bistvena sestavina človeškega obstoja ontološka varnost, ki se nanaša na osnovni občutek varnosti v svetu in temeljno zaupanje v druge ljudi in pripomore k določeni stopnji čustvenega ravnovesja, ugodja in blagostanja (Layder, 1994, str. 135). Poleg tega je zaupanje temelj za spoštovanje samega sebe in je temelj za odnose. Odnosi brez zaupanja so bolj podobni transakcijam (Marshall, 2000, str. 49–52). Vsi ti elementi nujnosti in potrebnosti zaupanja so prikazani na Sliki 7.

SLIKA 7: Elementi nujnosti in potrebnosti zaupanja

Vir: Marshall, 2000, str. 50.

Za zaupanje je značilno, da nastaja počasi na podlagi pozitivnih izkušenj. Z napačnim vedenjem (s posmehovanjem, zavračanjem, z navajanjem neresničnih podatkov ...) pa se zelo hitro izniči (Možina, 2004, str. 67). Zaradi tega je potrebno zaupanje v združbah spodbujati in ga stalno krepiti. To pomeni, da mora preiti koncept zaupanja iz teoretičnega okvira v kulturo. Kulturo

označimo kot celovit sistem vrednot, norm, predstav, prepričanj in simbolov, ki določajo način obnašanja in odzivanja na probleme (Rozman et al., 1993, str. 169).

Poznamo dve temeljni obliki zaupanja: osebno in neosebno. Neosebno zaupanje lahko nadalje razdelimo še na sistemsko in institucionalno zaupanje (Bachmann, 2003, str. 63):

- osebno zaupanje. Pri osebnem zaupanju gre za odnos med posameznikoma in temelji na dobrem poznavanju in zaupnosti, ki sta se razvili z vzajemnim delovanjem. V združbi ga je težko vzpostaviti, poleg tega pa je potrebno dosti časa, da se oblikuje. V večini primerov je nemogoče usklajevati posameznikova pričakovanja. Osebno zaupanje je zelo pomembno v združbah, še posebej v razmerjih med vodji in vodenimi.
- sistemsko zaupanje. Zaupanje v sistem je pojav, ki je zakoreninjen v antropološki osnovi človeškega delovanja. Zaupanje je pomembno v sami družbi in pridobiva na pomenu, saj je človeštvo oblikovalo veliko število tehničnih in družbenih sistemov. Gre za abstraktne sisteme, ki jih upravlja majhno število visoko specializiranih strokovnjakov. Institucionalno zaupanje se nanaša na formalne, družbene in legitimne strukture, ki jamčijo zaupanje.
- institucionalno zaupanje. Institucionalno zaupanje pa zajema prenos organizacijske kontrole od individualnega na raven kolektivnega odločanja oziroma soodločanja. Ta oblika pojasnjuje institucionalne vzorce odgovornosti, nalog in drugih elementov strukturnega kapitala, ki so temelj zaupanja in pričakovanj pri sodelovanju med posamezniki. Na oblike zaupanja imajo na tem mestu vpliv predvsem regijski in nacionalni sistemi poslovanja, v katerih deluje združba. Pri sistemskem zaupanju je za Luhmanna sistem tako objekt kot vir zaupanja (Lane, 1998, str. 17).

5.2.1 Zaupanje v trženju

Pomembnost zaupanja v trženju neprestano raste (Sahay, 2003). Zaupanje je poleg predanosti, komunikacij in zadovoljstva eden izmed osnovnih stebrov, ki podpirajo teorijo trženjskih odnosov. Zaupanje lahko definiramo kot skupek kupčevih prepričanj o dobaviteljevih značilnostih (Ganesan, 1994). V literaturi lahko najdemo več dimenzij zaupanja. V kolikor je govora o kupčevem zaupanju, se največkrat omenjata odkritost (*angl. honesty*) in dobrohotnost (*angl. benevolance*). Odkritost odraža neko gotovost, iskrenost in prepričanje kupca, da bo dobavitelj izpolnil svoje obljube (Gundlach in Murphy, 1993). Dobrohotnost pa izraža kupčevo prepričanje, da je podjetje zainteresirano za njegovo blaginjo, in da slednje nima edinega cilja zgolj ustvariti dobiček (Larzelere in Huston, 1980), temveč da je motivirano za iskanje skupnih koristi (Doney in Cannon, 1997).

5.2.2 Zaupanje uporabnikov v internet

Zaradi svoje mladosti in neobvladljivosti internet velja za najbolj demokratično, hkrati pa precej kaotično okolje, v katerem je treba še posebej paziti, kateri informaciji zaupaš. Spletni obiskovalec zato išče spletna mesta, ki vzbujajo zaupanje, ter se za spletni nakup odloči na podlagi večkratnega obiska (Cheskin, 2000).

Internet se neprestano razvija, kar pomembno vpliva na večino komercialnih sektorjev. Slednji vpliv ni povzročil visokih prodajnih rezultatov, saj še vedno ostaja pomanjkanje zaupanja, posledično pa je moč zaznati odpor do e-poslovanja (Gefen, 2000). Nezaupanje izvira iz posameznih lastnosti, ki jih ima internet v primerjavi s tradicionalnimi načini (Yousafzai et al., 2003). Torej, ko stranka izvede transakcijo v spletni trgovini, ki deluje v okolju, ki mu ne zaupa v celoti – kot je na primer internet – (Fung in Lee, 1999) je manjša verjetnost, da bo zaupala v zanesljivost in pravilnost postopka plačila v primerjavi s transakcijo v običajni trgovini. Glede na to, da kupec pri spletnem nakupu nima nobene interakcije s prodajalcem, ne more preučiti proizvoda in preveriti istovetnosti prodajalca. Nadalje, spletna plačila se običajno izvedejo s kreditnimi karticami, kar še poveča možnost prevar. Obstaja tudi možnost, da nismo prejeli tistega blaga, ki smo ga naročili. Pritožbe podjetjem, ki poslujejo brez fizične prisotnosti, oziroma, ki imajo pisarne v oddaljenih državah, in ob dejstvu, da so še vedno nekateri uporabniki interneta premalo osveščeni o morebitnih nevarnostih, so otežene oziroma včasih celo nemogoče. Tu moramo tudi omeniti nedorečeno, heterogeno ter neučinkovito zakonodajo, večanje števila težav z vsiljeno elektronsko pošto, neprestanih novic o hekerskih napadih in virusih. Na podlagi zgoraj zapisanega lahko zaključimo, da je dvom o nevarnostih na internetu upravičen in nenazadnje tudi zelo močan (Koufaris in Hampton-Sousa, 2002). Načeloma bi lahko zapisali, da je spletni nakup tvegan postopek (Taylor Nelson Sofres Interactive, 2002) in pridobitev zaupanja pri poslovanju prek slednjega medija je bistveno težje kot v tradicionalnem okolju (Bitting in Ghorbani, 2004).

Glede na zgoraj omenjene lastnosti spletnih nakupov je potrebno ob nadaljnjem proučevanju zaupanja upoštevati tudi vidike, ki niso (bili) znani oziroma navedeni v klasični trženjski literaturi. Večina raziskav, ki proučujejo zaupanje na spletu, se osredotoči predvsem na dimenziji odkritosti in dobrohotnosti. Nekateri avtorji so mnenja, da na zaupanje vplivajo tudi drugi faktorji, kot na primer zaznavanje sposobnosti (*angl. competence*) (Sirdeshmukh et al., 2002). Zaznavanje sposobnosti je še zlasti pomembno, ko govorimo o internetu. Vzroke lahko najdemo v internetnem poslovnežu, ki se mora izkazati s poštenostjo in z zaupanja vrednimi dejanji, ki bo s tehničnim in finančnim znanjem ter človeškimi viri prispeval k uspešno zaključeni transakciji; blago bo dobavljeno do predvidenega roka in vsi bančni podatki bodo varno shranjeni ter nedostopni tretjim osebam. Z drugimi besedami, ni dovolj, da damo obljube in da imamo dobre namene, temveč, da obljube in namene tudi realiziramo.

Zanimivo študijo na temo zaupanja na spletu je v sodelovanju s tržno-raziskovalnim podjetjem Cheskin Research izvedlo podjetje Archetype/Sapient.[26] Glavna ugotovitev je bila, da je zaupanje v spletno stran (*angl. trusthworthiness*) dolgoročna lastnost, ki se gradi skozi uporabnikove izkušnje s spletno stranjo. Zaupanje raste, ko uporabniki dobijo želene rezultate in se ob tem ne počutijo ignorirane ali prevarane. Zaupanje naj bi izhajalo iz dejanskega obnašanja organizacije, ki se pokaže skozi več pozitivnih epizod z uporabniki. Za zaupanje velja, da ga je

[26] Gre za mnogokrat citirano študijo, ki so jo komentirali mnogi pomembni praktiki in teoretiki spletnega oblikovanja in uporabnosti (kot je na primer znani strokovnjak za spletno uporabnost Jakob Nielsen).

težko zgraditi, a zelo lahko izgubiti: že ena sama zloraba zaupanja lahko uniči leta akumuliranja verodostojnosti (Cheskin, 2000 in Nielsen, 1999).

5.2.2.1 Vzroki nezaupanja

Tveganje je prisotno že pri običajnem poslovanju in komuniciranju, še bolj pa je značilno za internetno okolje. Znane so goljufije in poneverbe spletnih kartic, vdori v sisteme, prevare spletnih komunikatorjev. Internet je neobvladljiv in marsikdaj je težko ugotoviti, ali je posamezna stran in podatki na njej avtentični ali ne[27]. Internetni uporabniki se teh tveganj vedno bolj zavedajo in že podzavestno podatke s spleta jemljejo z določeno mero rezerve.

Vzroki nezaupanja v internet so med drugim verjetno tudi v tem, da gre za razmeroma mlado inovacijo. Internet je bil namreč »odkrit« šele v 60-ih letih 20. stoletja. Začetna ideja je bila, da bo služil vojaški stabilnosti, saj gre za mrežno infrastrukturo, ki lahko deluje tudi v primeru, če se kak njen del pokvari, ali je uničen na primer v primeru jedrskega napada (Verčič et al., 2000). Koncept se je kasneje izkazal za uporabnega tudi na drugih področjih, pravo ekspanzijo v javni rabi pa je internet doživel v prvi polovici devetdesetih, po sprejetju protokolov http in www ter po razvoju prvega spletnega brskalnika.

Napačna uporaba in neuspehi pri internetnem komuniciranju in poslovanju so najverjetneje ravno rezultat te mladosti interneta. Ljudje smo nagnjeni k temu, da nove pojme in stvari umestimo v že obstoječe mentalne sheme, ker pa je internet v nekaterih lastnostih zelo podoben klasičnim medijem, je mogoče sklepati, da so starejši uporabniki, ki so se interneta priučili, internet uvrstili v shemo medijev. Ravno ti, starejši uporabniki, pa so trenutno najmočnejša družbena skupina, ki usmerja in odloča o investicijah. Ker pa njihovo razumevanje interneta temelji na stereotipnem pojmovanju, da je internet le še en medij, ki povrhu sploh ne kaže rezultatov, so temu primerno skromne tudi investicije. Pripravljeni so vlagati le v spletno oglaševanje, ne pa tudi v aktivno dolgoročno spletno prisotnost, ki edina ustvarja odnose zaupanja in ugodne poslovne rezultate.

Razlog nezaupanja gre morda iskati tudi v pravni neobvladljivosti spletnega prostora v primerjavi z nespletnim. Pri običajnem poslovanju je zakonodaja dorečena, goljufije pa so v veliki meri sankcionirane, za spletno okolje pa to nikakor ne drži. Zaenkrat še niso iznašli učinkovitega načina, kako pravno urediti internet. Vse prelahko je na primer skriti svojo identiteto, ukrasti bazo podatkov in na njeni podlagi nadlegovati uporabnike z oglasno pošto.

[27] Primer za to neobvladljivost je spletni naslov ameriške Bele hiše. Na domeni www.whitehouse.gov je prava stran domovanja ameriškega predsednika, na www.whitehouse.com se nahaja klasični iskalnik oseb in podjetij, www.whitehouse.net in www.whitehouse.org pa sta strani, ki se na prvi pogled sicer zdita pravi, gre pa za ponaredek, ki za pridobitev večjega obiska izkorišča ime znane institucije. Ameriška administracija, ki svojo voljo in gospodarsko-politični vpliv brez težav širi po vsem svetu, nikakor ne uspe odkupiti ali prevzeti teh nekaj krovnih domen.

5.2.2.2 Gradnja zaupanja na spletu

Ker se zaupanje dogaja v obiskovalčevi glavi, so se v skladu z upravljavsko logiko razvile metode za vzbujanje zaupanja. Za občutek zaupanja v uporabnikovih glavah je zaupanje seveda treba znati predstaviti, a metode delujejo le, če kasnejša kupčeva izkušnja pokaže, da se je zaupati izplačalo. Če dejansko stanje ne ustreza obljubam, danih v komunikaciji, se zaupanje hitro podre: »Izkušnja pove dejstvo, ki hitro zamenja iluzije in domneve.« (McKnight v Murphy 2003, str. 75).

Murphy v svoji raziskavi potrdi hipoteze, da naslednji pristopi pozitivno vplivajo na mero zaupanja v spletnega trgovca (Murphy, 2003, str. 77–81):

- prenos zaupanja z uporabo blagovnih znamk in oseb, ki jim ljudje zaupajo,
- sporočanje sposobnosti s pomočjo pričevanj strank,
- strukturalna zagotovila o procesu (varnost nakupa, možnost pritožbe),
- komunikacija in izvedba uspešnih zadovoljitev; večkrat ko je kupec po nakupu zadovoljen, bolj zaupa,
- pojasnitev dodane vrednosti,
- personalizacija.

Čeprav se zdi, da bi pri zaupanju na internetu lahko imele odločilno prednost že uveljavljene blagovne znamke, Cheskin ugotavlja, da vnaprejšnja poznanost ni odločilni dejavnik. Mali in novi spletni projekti lahko s pravo strategijo in taktikami dosežejo uspeh tudi brez vnaprejšnje poznanosti podjetja ali blagovne znamke (Cheskin, 2000).

Houston oceno tveganja (*angl. risk assessment*) najprej razdeli na (1) *kalkulativno* (seštevanje prednosti), (2) *empatično* (čustveno zgrajeno na osebni ravni v manjših skupinah) in pa (3) *zaupanje, temelječe na znanju* (*angl. knowledge based*). Ko so naše transakcije preproste, je ekonomska kalkulativnost pomembna pri zagotavljanju prostega trga, v primeru, da gre za odnose, pa se lahko zanesemo na empatično zaupanje (Houston, 2001, str. 42).

V e-poslovnem okolju pa gre za zanimivo posebnost. Pomembna naj bi bila namreč predvsem zadnja vrsta, na znanju temelječe zaupanje. V e-okolju gre večinoma za visoko kolaborativne odnose, v katerih delimo kompleksne informacije, odnosi pa hkrati trajajo le kratek čas (Houston, 2001, str. 42). Po tej razlagi naj bi večina e-poslov zahtevala zaupanje med ponudnikom in uporabnikom, ni pa nujno, da ta odnos traja.

Houston je uvrstil ugled med kalkulativne načine ocene tveganja, ki pa na internetu niso najpomembnejši[28]. Ugled (kot umetno skonstruirana slika v očeh potrošnikov) naj na spletu ne bi imel pomembne vloge, saj se informacije na internetu širijo tako bliskovito, da se le težko kaj prikrije (Houston, 2001, str. 40).

[28] S tem Houston potrdi že prej omenjeno Cheskinovo študijo.

5.2.2.3 Konkretni pristopi in dejanja za gradnjo zaupanja v internet

Iz teoretično ocenjenih smernic spletnega komuniciranja so v nadaljevanju izpostavljene praktične stvari, kako se obnašati, da obiskovalci zaupajo in da stran učinkuje kot zaupanja vredna:

- Ker se zaupanje gradi skozi čas, ne smemo ničesar prepustiti naključju. Treba je *pristopiti strateško* in biti pripravljen na najhujše škandale. S tem v zvezi je pomemben krizni menedžment in preigravanje možnih scenarijev. Ker pa se informacije na internetu širijo zelo hitro, je koristna takojšnja reakcija (Nielsen, 1999).
- Spletne strani je potrebno *oblikovati z mislijo na uporabnika*, tehnologije pa uporabljati s premislekom. Pomembno je varovanje podatkov in to, da je poskrbljeno za hitrost in gladkost nalaganja spletne strani (Nielsen, 1999).
- Spletna stran se mora *naložiti v trenutku* in dobro je, da je obiskovalcu hitro jasno, kje je in kaj bo tu našel. Najhujši primeri se zgodijo, ko oblikovalci ustvarijo izredno lepo stran, ki izkorišča najnovejše animacijske tehnike, na koncu pa se izkaže, da je oblikovalec edini, ki stran zna uporabljati, vsem ostalim pa se niti ne ljubi čakati, da se stran naloži. Kakovostna in preprosta oblika, dobri teksti, brez izjeme delujoče povezave in logična navigacija strani implicitno vsebujejo podatek o pričakovani kakovosti storitve.
- *Takojšnja navedba vseh stroškov* pove, da avtor strani ničesar ne skriva. Podobno velja tudi za navajanje virov in povezav na druge spletne strani, ki večajo kredibilnost (Nielsen, 1999).
- Pomemben je *način uporabe elektronske pošte*, ki jo je treba uporabljati s premislekom in le z dovoljenjem. Preveč je vsiljene pošte, ki jo vsak dan brišemo iz svojih e-nabiralnikov, saj se njihovi avtorji ne zavedajo, da je elektronska pošta lahko odličen trženjski pripomoček le v primeru, da prejemniki že iz zadeve sporočila razberejo, da piše nekdo, ki ga poznajo in mu lahko zaupajo. Zato je potrebno uporabnike seznaniti, da kadarkoli prejmejo našo pošto, dobijo pomembne, objektivne informacije in ne oglaševalskih smeti. Trend gradnje odnosov s pomočjo e-pošte so redni izobraževalni spletni časopisi, ki večino sporočila namenijo izobraževanju, le majhen del pa promociji avtorjevih storitev.

Razvijati je potrebno dolgoročen odnos in vzpodbuditi čimveč transakcij s pozitivnim občutkom obiskovalca. Šele, ko se spletna stran redno polni z informacijami, ki zanimajo obiskovalce, lahko upamo, da se bodo večkrat vrnili. Če obiskovalcu informacije koristijo, je dodan en kamenček k mozaiku spletnega zaupanja, hkrati pa se poveča možnost, da bo obiskovalec izvedel akcijo, ki se od njega pričakuje. Zadovoljen obiskovalec se vrne in o strani pove še prijateljem. Na spletu se informacije, zaupanje in tudi nezaupanje širijo bliskovito!

5.3 VPLIV ZASEBNOSTI IN ZAZNAVANJA VARNOSTI NA ZAUPANJE TER ZVESTOBO

Osrednja tema tega magistrskega dela je proučitev povezav med zaupanjem, zasebnostjo in varnostjo ter nadalje zvestobo do spletne strani. Koncepta zasebnosti in varnosti sta dva pojava, ki ju na področju odnosov na spletu najpogosteje povezujemo s konceptom zaupanja. V nadaljevanju sledi analiza povezave med prvima konstruktoma in njunega vpliva na zaupanje in zvestobo. Vpliv na konstrukt zvestobe bo le nakazan, ne pa tudi podrobneje analiziran, saj bi v nasprotnem primeru presegli predviden obseg tega dela.

O konceptu zasebnosti je bilo že veliko govora. Različni avtorji ga različno opredeljujejo. Če povzamemo njihove definicije, lahko rečemo, da je zasebnost posameznikova zmožnost nadzora pogojev, pod katerimi se pridobivajo in uporabljajo njegovi osebni podatki. Če prenesemo slednjo definicijo v virtualni svet, lahko zapišemo, da se zasebnost navezuje na postopke pridobivanja, distribuiranja ali nepooblaščene uporabe osebnih podatkov (Wang et al., 1998). Nove kompleksne tehnologije z vedno večjimi možnostmi za obdelavo podatkov vedno bolj potencirajo vprašanje zasebnosti. Uporabniki interneta so posledično postali nezaupljivi do ponudnikov spletnih storitev in vedno bolj jih zanima, s kakšnim namenom se podatki zbirajo, na kakšen način bodo zbrani, kako bodo obdelani in nenazadnje, kje bodo shranjeni.

Na razvoj spletnega poslovanja negativno vplivata dve oviri. Prvo smo omenili v zgornjem odstavku – pomanjkanje zasebnosti – in druga pomanjkanje varnosti (Dong-Her et al., 2004). Razlog za drugo oviro lahko najdemo v možnosti prestrezanja finančnih podatkov in njihovi nezakoniti uporabi. Kolsaker in Payne (2002) trdita, da varnost odraža videnje zanesljivosti uporabe plačilnih metod in postopkov prenosa ter hranjenja podatkov. Posamezniki bi želeli, da njihovi osebni podatki (zasebni in finančni) ne bodo dani v vpogled tretjim osebam, nepotrebno shranjeni in upravljani v času tranzita in kasnejšega hranjenja ter, da se bo z njimi ravnalo zaupno in skladno z danimi obljubami. Tu gre predvsem za tehnični aspekt, ki bo zagotovil integriteto, tajnost, avtentikacijo in skrb za nezanikanje spletnih transakcij. Z integriteto informacijskega sistema mislimo predvsem na nezmožnost vpliva na postopek prenosa podatkov in njihovo hranjenje s strani tretjih oseb, v kolikor le-ti nimajo pooblastila. Tajnost podatkov pomeni, da le-ti ne bodo dani v vpogled neavtoriziranim posameznikom. Avtentikacija nastopa kot predpogoj za izvedbo identifikacije. Zadnji element je skrb za nezanikanje, ki se nanaša na postopke, ki preprečujejo tako na strani uporabnika kot tudi na strani organizacije zanikanja določenih operacij oziroma postopkov (na primer: spletno naročilo).

Kupec je ključni udeleženec vsake trgovske transakcije. Neustrezen nivo varnosti elektronske transakcije lahko povzroči kupcu znatno škodo. Nezadovoljni kupec pa ne bo hotel več elektronsko trgovati. Pravilna izbira med različnimi možnostmi varovanja transakcije, ki jih nudijo trgovci, bi znižala kupčevo tveganje. Težava pa je v tem, da povprečni kupec ni strokovnjak za varnost in se ne zaveda posledic uresničenih groženj varnosti transakcije. Zato tudi ne zna presoditi, katere varovalne funkcije zadoščajo njegovim varnostnim potrebam. Komunikacijski protokoli za elektronsko trgovanje bi morali biti predstavljeni kupcu; kakšen

nivo varnosti transakcije zagotavlja določena kombinacija varovalnih funkcij in katerim njegovim zahtevam ustreza ta nivo varnosti. Kupčeve zahteve glede nivoja varnosti so odvisne predvsem od vrednosti in vrste naročenega blaga; čim večja je vrednost nakupa, višji je zahtevani nivo varnosti trgovske transakcije (Hudoklin in Stadler, 1997, str. 291).

Driscoll in drugi so v raziskavah ugotovili, da je strah pred zlorabami pri pošiljanju finančnih podatkov po internetu najpomembnejši dejavnik, ki ovira hitrejši razvoj nakupovanja in plačevanja po internetu. Raziskava je pokazala, da se 43 odstotkov uporabnikov interneta boji možnosti zlorabe kreditne kartice pri plačevanju po internetu. Te ugotovitve jasno kažejo, da je strah pred možnostjo goljufije in zlorabe pri plačevanju po internetu posledica zaznanega pomanjkanja varnosti z vidika uporabnikov interneta in resna ovira za nadaljnji razvoj elektronskega poslovanja. Spoznanja raziskav kažejo tudi, da sta strah pred zlorabo in strah pred goljufijo ključna dejavnika, ki vplivata na pripravljenost nakupovalca plačati in prodajalca sprejemati plačila po internetu. Zaskrbljenost glede varnosti in možnih zlorab pri plačevanju po internetu se bo zmanjšala, ko bodo posamezniki in organizacije verjeli, torej zaupali, da je plačevanje prek interneta varno (Bračun, 2003, str. 152).

Vzpostavitev zaupanja med kupci, prodajalci in finančnimi ustanovami je najboljši način za povečanje zaupanja v plačevanje po internetu. Kupca je potrebno prepričati, da imajo izdelki in storitve pričakovano kakovost in da jih bo pravočasno prejel. Kupec mora tudi verjeti, da pri plačilu po internetu ne bo prišlo do zlorabe njegove kreditne kartice in da bo za plačilo prejel pričakovani izdelek. Podobna pričakovanja imajo tudi prodajalci izdelkov oziroma ponudniki storitev na internetu. Prodajalec mora biti prepričan, da bo za dobavljen izdelek oziroma opravljeno storitev prejel plačilo, da pri sprejemanju plačil po internetu ne bo prišlo do zlorabe in da bodo kupci njegovih izdelkov oziroma uporabniki njegovih storitev pošteni (Bračun, 2002, str. 145).

Pogled na problematiko smo v večji meri naredili z zornega kota uporabnika. Sklepamo lahko, da k zaupanju v spletne komunikacije sicer res pripomorejo varnostni ključi, pomembno pa je predvsem to, kako posamezniki te varnostne ukrepe doživljajo in kako se ob uporabi spletne strani ali aplikacije počutijo.

Organizacije se morajo potruditi, da bo zaznana stopnja tveganja pri nakupu njihovih izdelkov/storitev čim nižja, kar pomeni, da bo zaupanje uporabnikov večje. Zaupanje pa se bo večalo, če bodo izpolnjena njihova pričakovanja in če bodo z nakupom zadovoljni. Uporabniki bodo bolj zaupali organizaciji z dobrim imidžem in bodo bolj pripravljeni kupiti izdelek pri organizaciji, ki slovi na trgu po dobri kakovosti svojih izdelkov ali storitev, kot pa pri neki nepoznani organizaciji. Vsekakor pa si mora organizacija pridobiti zaupanje v očeh uporabnikov ter ga z ustreznimi ukrepi tudi ohranjati in večati.

5.3.1 Povezava med zaznavanjem zasebnosti in varnostjo na internetu

Na osnovi zgoraj zapisanega lahko sklepamo, da med zasebnostjo in varnostjo na internetu obstajajo določene povezave, ki pa so prešibke in nejasne. Zasebnost se navezuje predvsem na pravni vidik in dobro poslovno prakso upravljanja osebnih podatkov[29]. Pri varnosti nas zanimajo tehnične rešitve, ki bodo zagotovile uspešno izvedbo postopkov, predvidenih s strani pravnega vidika in dobre poslovne prakse[30]. Da bi se izognili posegom v zasebnost uporabnikov spletnih strani, se moramo poslužiti varnostnih ukrepov. Povezavo med konceptoma zasebnosti in varnosti bi lahko našli na treh ravneh. Prvič, lahko rečemo, da si uporabniki predstavljajo povezavo le v svojih mislih. Uporabniki včasih ne vedo, kdaj se en koncept zaključi in drug začne in to jih lahko zbega. Glede na to, da uporabnik želi ohraniti določeno mero zasebnosti, mu prej omenjena nejasnost ne predstavlja težave. On želi le ohraniti integriteto in ostale osebnostne pravice, pa naj si bodi z uporabo pravno-formalnega pristopa, dobre poslovne prakse, varnostnih sistemov, ali pa s kombinacijo vseh treh. Drugič, podjetja želijo oba koncepta obravnavati hkrati. V poslovnem svetu obstaja prepričanje, da osnova za zaščito zasebnosti ni samo dobra poslovna praksa in zakonodaja, temveč tudi zanesljivi informacijski sistemi (Lyman, 2003). In tretjič, videli smo, da uporabniki postavljajo varnost ob bok zasebnosti. Enako velja za zakonska merila, ki obravnavajo poleg načina zbiranja osebnih podatkov, njihove uporabe ter prenosa tudi zahteve po tehničnih rešitvah.

Koncepta zasebnosti in varnosti se morata zaradi pomanjkanja skupnih točk obravnavati ločeno. Vendar, kot smo videli, ne samo uporabniki, tudi podjetja in zakonodaja oba koncepta povezujejo.

5.3.2 Opredelitev zvestobe in povezanost le-te z zadovoljstvom

V literaturi je veliko opredelitev zvestobe kupcev. Po Veselu in Žabkarjevi (2003, str. 42) je le-ta sledeča: "Zvestoba kupcev je močna zavezanost k ponovnemu nakupu proizvoda ali storitve, ki se odvija konsistentno v prihodnosti kljub situacijskim vplivom in trženjskim naporom, ki lahko to preprečijo."

Zvestoba je fizična in čustvena obveza s strani kupcev v zameno za zadovoljitev njihovih potreb. Podjetja morajo gledati na odnose s svojimi strankami z njihovega vidika, kar jim bo pomagalo razumeti obstoječo stopnjo zvestobe. Raziskave o obstoječih kupcih so ključni prispevek pri načrtovanju ohranjanja. Zvestobe ne dosežemo s trženjskimi programi, revijami, ustanavljanjem klubov ali predstavljanjem kartic. Zvestoba se razvije sčasoma, če so parametri za odnos načrtovani in pravilno izvedeni. Najbolje je definirana kot mišljenje, skupek stališč, prepričanj, hotenj, itd. (Stone et al., 2000, str. 102–103).

[29] Primer: Spletnega uporabnika je potrebno obvestiti o namenu zbiranja in uporabe osebnih podatkov.

[30] Primer: Podjetje lahko obljubi, da pridobljenih osebnih podatkov ne bo dalo v vpogled tretjim osebam, kar pa še ne pomeni, da so podatki varni. Ne smemo pozabiti na hekerje, ki slednje z nelegalnimi metodami zbirajo in prodajajo.

Griffin (1995, str. 4) pravi, da se pravi pristop za ponavljajoče nakupe skriva v zvestobi kupcev. Za napovedovanje prodaje in finančne rasti je bolj zanesljiva mera, kot je zadovoljstvo kupcev, saj zadovoljni kupci kupujejo tudi pri konkurenci brez kančka oklevanja. Nakupno vedenje zvestega kupca ni slučajno, ampak se pojavi po določenem času skozi več odločitvenih faz. Takšen kupec točno ve, kaj in od koga bo kupil. Zvestoba je definirana v pogojih nakupnega vedenja. Zvesti kupec je tisti, ki (Griffin, 1995, str. 31):

- redno ponavlja nakupe;
- kupuje vse izdelke ali storitve;
- daje priporočila drugim;
- je konkurenca zanj nedotakljiva.

Mnoga podjetja zmotno mislijo, da so kupci, ki jih obdržijo, že avtomatično tudi zvesti. Problem leži v deležu kupca, torej v deležu razpoložljivih sredstev, ki jih porabi pri podjetju. Z zvestobo sta povezana dva pogoja (Griffin, 1995, str. 5):

- trajanje-ohranjanje kupca (dolžina trajanja odnosa s kupcem) in
- celoten delež kupca (prikaže odstotek porabljenega proračuna pri podjetju).

Imeti zvestega kupca pomeni imeti stalen vir dohodka skozi večletno obdobje. Pojavi se, kadar kupec občuti, da so njegove potrebe najbolje zadovoljene. Takrat kupuje skoraj izključno samo od izbranega podjetja in izključi iz upoštevanja obstoječo konkurenco. Vendar pa tudi zvestoba ni popolnoma zanesljiva, nadaljevala se bo samo, dokler bo kupec čutil, da prejema boljšo vrednost, kot bi jo sicer prejel drugje. Vedno torej obstaja tveganje, da bo kupec nezvest, če mu bo konkurenca ponudila več. Zvestoba je zelo ranljiva (Mcllroy et al., 2000, str. 348).

Obstaja več stopenj zvestobe, medtem ko so nekateri kupci bolj zvesti, so drugi manj. Zvestoba se razvije s pristopi, ki okrepijo pozitivna stališča in z njimi povezana vedenja. Cilj podjetij nikakor ni narediti vseh kupcev zvestih, ampak se je treba osredotočiti na izboljšanje zvestobe pri tistih strankah, ki se bodo in se verjetno odzivajo na razne spodbude, na diferencirano storitev, ki je na razpolago samo zvestim kupcem ali pa na kombinacijo obeh (Stone et al., 2000, str. 105).

Raziskave o ugotavljanju zadovoljstva so dokazale, da obstaja povezava med zadovoljstvom in zvestobo tako za izdelke kot storitve. Potrebno pa je poudariti, da zadovoljni kupci niso nujno tudi zvesti (Kostanjšek et al., 2000, str. 3).

Zadovoljstvo ni natančen in zadosten pokazatelj kupčeve zvestobe, je pa nujen. Torej lahko obstaja zadovoljstvo brez zvestobe, toda težje je doseči zvestobo brez zadovoljstva (Mcllroy et al., 2000, str. 349). Dokler ni nobene garancije, da se bo zadovoljen kupec vrnil, pa je skoraj zagotovljeno, da se nezadovoljen kupec, ki ima na voljo več ponudnikov, ne bo vrnil.

Podjetja v storitvenem sektorju ugotavljajo na podlagi svojih raziskav, da se kar 80–90 % njihovih uporabnikov opredeli za zadovoljne ali zelo zadovoljne, vendar pa kljub temu obstaja še zelo velik delež tistih, ki zamenjajo ponudnika (Kostanjšek et al., 2000, str. 4).

Ni presenetljivo, da so mnoga podjetja odkrila močno vzajemnost med zadovoljstvom in zvestobo samo pri najvišjih stopnjah kupčevega zadovoljstva. Spodnja preglednica, ki temelji na pridobljenih podatkih podjetij, kot so AT&T, Rank Xerox in The Royal Bank of Scotland, prikazuje, da v povprečju ostanejo 95 % zvesti tisti kupci, ki so na lestvici zadovoljstva najvišje (izvrstno/zelo zadovoljni). Po pričakovanju začne stopnja zvestobe nato strmo padati skupaj z nižje opredeljenimi stopnjami zadovoljstva. Tako je ocena zvestobe pri nezadovoljnih kupcih pičla 2 %, pri zelo nezadovoljnih čisto na dnu lestvice zadovoljstva pa zvestoba sploh nima več prihodnosti (Hill et al., 2004, str. 2–3).

TABELA 5: Povezava med zadovoljstvom in zvestobo

Kupčeva potrjena stopnja zadovoljstva	Ocena zvestobe
izvrstna / zelo zadovoljen	95 %
dobra / zadovoljen	65 %
povprečna / niti zadovoljen niti nezadovoljen	15 %
skromna / nezadovoljen	2 %
zelo skromna / zelo nezadovoljen	0 %

Vir: Hill et al., 2004, str. 108.

Odnos med zadovoljstvom in zvestobo ni linearen in strmo narašča tako, kot se veča zadovoljstvo kupca. Podobno dokazujejo podjetja z uporabo številčnih lestvic, ki prav tako prikazujejo pozitivno vzajemnost med zadovoljstvom in zvestobo. V splošnem se odraža 60 % ocena zadovoljstva s samo 35 % zvestobo, več kot 80 % ocena zadovoljstva pa z 90 in večodstotno zvestobo (Hill et al., 2004, str. 108).

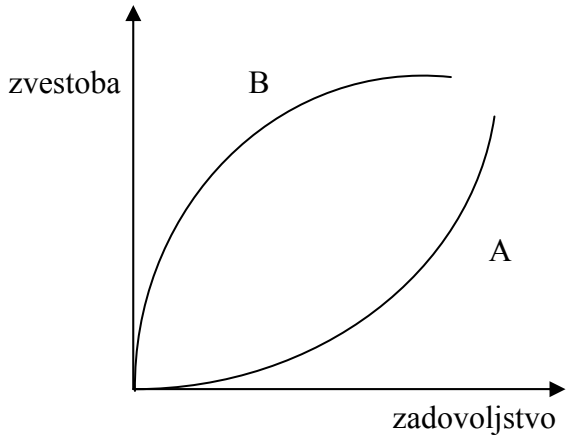
Organizacije, ki imajo več izkušenj z merjenjem zadovoljstva kupcev, se zavedajo, da je sprejemljiva raven zadovoljstva samo tista, ki je najvišje uvrščena na lestvici. Kritično področje zadovoljstva je nekje na sredini zgornje tabele, kjer je možno z majhnim povečanjem stopnje zadovoljstva tehtno povečati zvestobo. Podatki kažejo, da je ogromno organizacij, katerih merilo zadovoljstva lebdi okoli 80 % ali manj. Slednji lahko dosežejo pomembne izboljšave v zvestobi (Hill et al., 2004, str. 108).

Za razmerje zadovoljstvo-zvestoba ni enotnega pravila, ki bi veljalo za vse trge. Na nekaterih trgih, na tistih značilno konkurenčnih z visokimi ravnemi zamenjave dobaviteljev, bo zvestoba postopoma naraščala samo pri najvišjih stopnjah zadovoljstva. To je prikazano s krivuljo A na spodnji sliki. Na drugih trgih, tistih, za katere veljajo visoki stroški prehoda na druge dobavitelje

in večje ravni vztrajnosti kupcev, pa je dopuščen precejšen padec zadovoljstva kupcev, preden začne to vidno izpodkopavati zvestobo. To je na sliki prikazano s krivuljo B.

Dobro je vedeti, kateri tip krivulje je primernejši za posamezno podjetje, za kar pa je potrebno razviti lasten model (Hill et al., 2004, str. 108).

SLIKA 8: Povezava zadovoljstva in zvestobe na različnih trgih



Vir: Hill et al., 2004, str. 108.

E-poslovanje vsekakor sodi pod krivuljo A. Internet je prostor, na katerem se srečuje veliko število ponudnikov in kupcev. Ponudniki oziroma spletni trgovci imajo zelo težko nalogo, ko želijo obdržati kupca. Le-ta ima z nekaj kliki na dosegu celotno svetovno ponudbo konkurenčnih ponudnikov s primerljivimi substituti. Ne glede na to, da bo stranka še tako zadovoljna z neko spletno trgovino, bo kaj hitro pripravljena kupiti blago pri konkurenci, ki bo ponudila boljše pogoje. Spletni trgovci se bodo morali neprestano truditi, da bi dosegli čim večje zadovoljstvo. Kot smo že ugotovili, je internet globalno okolje, ki se zelo razlikuje od tradicionalne prodaje in je zato eden izmed najpomembnejših faktorjev, ki vpliva na ponakupno odločitev, še vedno cena.

6 RAZISKAVA O VPLIVU ZASEBNOSTI IN VARNOSTI NA ZAUPANJE UPORABNIKOV NA SVETOVNEM SPLETU

V tem poglavju bomo najprej predstavili osnovna izhodišča za spletno raziskavo. Opredelili bomo cilje raziskave ter opisali čas in način izvedbe raziskave. Zastavili bomo načrt same raziskave, kjer bomo navedli vir podatkov in predstavili metodologijo, nato pa bomo postavili hipoteze in konceptualni model. Sledila bo opredelitev raziskovalne metode in raziskovalnega instrumenta. Na koncu bomo predstavili še rezultate raziskave, omejitve in možne napake ter smernice za nadaljnje raziskovalno delo.

6.1 OPREDELITEV PROBLEMA IN CILJA RAZISKAVE

Cilj raziskave je analizirati vpliv zasebnosti in varnosti na stopnjo zaupanja med internetnimi uporabniki ter nakazati povezavo med zaupanjem ter zvestobo do spletne strani.

Konceptualni model naj bi prikazal vzročno-posledične povezave med različnimi internetnimi dejavniki. Shema, ki je prikazana v Sliki 9 na strani 69, grafično povzema bistvene elemente in predhodne ugotovitve v zvezi z analizo uporabnikovega vedenja na svetovnem spletu, do katerih so prišli različni avtorji, ki so proučevali podobno tematiko. Poskuša nam podati celovit pogled na analizo uporabe interneta od prve uporabe pa vse do zvestobe spletni strani. Ker obstaja kar nekaj povezav med posameznimi koncepti in je nemogoče zajeti vse možne relacije, smo v model vključili samo nekaj (po našem mnenju) pomembnejših. Pri izbiri konceptov smo predvsem upoštevali trenutno aktualnost.

6.2 NAČRTOVANJE RAZISKAVE

Načrt raziskave je sestavljen po Kotlerju (1996, str. 133) iz naslednjih petih postavk: viri podatkov, raziskovalne metode, raziskovalni instrumenti, načrt vzorčenja ter oblike komuniciranja.

6.2.1 Viri podatkov

Ločimo dve vrsti virov podatkov: primarne in sekundarne podatke. Sekundarne podatke predstavljajo podatki, ki so navadno zbrani za nek drug namen, so najcenejši in najlažji način pridobivanja podatkov, ki pomagajo pri identifikaciji problema. Poleg tega so idealen vir idej za nadaljnje raziskovanje (Kumar et al., 1999, str. 109–110). Zbrani in strnjeni sekundarni podatki predstavljajo teoretični del magistrskega dela.

Sprva je bilo potrebno preučiti sekundarne podatke in se podrobno seznaniti z globino in širino raziskovalnega problema in na ta način priti do raziskovalnih izhodišč. Naslonili smo se predvsem na članke raznih tujih strokovnih revij, ki smo jih našli v bazah člankov. Za pridobitev prave predstave aktualnosti raziskave smo preučili tudi novejše domače strokovno gradivo.

Na osnovi sekundarnih podatkov smo oblikovali anketo, s katero smo želeli pridobiti primarne podatke. S pomočjo elektronske pošte smo k sodelovanju povabili 6.172 naključnih uporabnikov interneta. Zaradi starejše baze elektronskih naslovov smo zabeležili 806 nedostavljenih sporočil. Osrednji vir primarnih podatkov predstavlja 462 izpolnjenih spletnih vprašalnikov (stopnja odziva je bila 7,54-odstotna), od katerih smo jih 62 izločili, ker niso vpisali spletne strani, ki je zahtevala njihove osebne podatke. Vse statistične analize so bile opravljene na vzorcu 400-tih popolno izpolnjenih anketnih vprašalnikov.

Glede na temo in problem dela smo se odločili za neverjetnostni priložnostni vzorec. Zanj je značilno, da je z vidika reprezentativnosti boljši od priložnostnega. Raziskovalec sam sebi vnaprej postavi nalogo, da mora izbrati take enote preučevanja, ki so po njegovem mnenju tipične glede na opazovani pojav v osnovni populaciji (Rojšek, 1997, str. 47). Anketa je bila poslana na naključne naslove, ki so v upravljanju podjetja Zaslon Telecom d.o.o., ki vodi, vzdržuje in nadzoruje zbirko osebnih podatkov posameznikov v skladu z zakonom o varstvu osebnih podatkov.

Pri vzorčenju nismo postavili demografskih omejitev, smo pa slednje podatke uporabili pri pripravi analiz in pri pripravi zaključnih ugotovitev.

6.2.2 Metodologija

Raziskovalna metoda pri pridobivanju primarnih podatkov je bila opisna, **raziskovalni instrument** pa je bil spletni vprašalnik, ki so ga sestavljala vprašanja odprtega in zaprtega tipa:

- vprašanja tipa z več možnimi odgovori,
- dihotomno vprašanje (DA ali NE),
- Likertova lestvica strinjanja/nestrinjanja.

Glede na postavljene hipoteze smo oblikovali različna vprašanja in trditve. Anketa je bila testirana in večkrat spremenjena. Končna verzija se nahaja v Prilogi 1.

Slabosti metode anketiranja preko elektronske pošte so predvsem nizka stopnja odziva, slab nadzor nad anketirancem, pridobljene informacije pa ponavadi niso tako kakovostne kot v primeru osebnega spraševanja, saj je težje postavljati odprta vprašanja. Prednosti omenjene metode so predvsem nizki stroški pridobivanja podatkov, hitrost metode, široka distribucija vzorčnih enot, lažja analiza pridobljenih podatkov ter bolj popolni odgovori pri osebnih in občutljivih vprašanjih (Churchill, 1991, str. 341; Tull, Hawkins, 1993, str. 172; Bergstein, Estelami, 2002, str. 303–319).

Kot raziskovalni instrument smo uporabili vprašalnik, ki je daleč najpogostejši instrument za zbiranje primarnih podatkov. Sestavlja ga sklop vprašanj, na katera mora vprašani odgovoriti. Pri oblikovanju vprašalnika smo se osredotočili na to, da bodo pridobljeni odgovori na vprašanja podali čim bolj realno sliko glede porabnikovega stališča do proučevane tematike. Pri samem sestavljanju vprašalnika smo se poslužili postopka razvijanja vprašalnika, kot ga je predlagal Churchill (1991, str. 360). Postopek obsega naslednjih devet korakov: specifikacija potrebnih informacij in hipotez, izbira vrste vprašalnika in metode zbiranja podatkov, opredelitev vsebine posameznih vprašanj, oblikovanje možnih odgovorov za vsako vprašanje, oblikovanje vprašanja, določitev zaporedja vprašanj in oblike vprašalnika, pregled vseh preteklih korakov, testiranje vprašalnika in morebitni popravki.

6.2.3 Vsebina vprašalnika

Vprašalnik je bil sestavljen iz 34-ih vprašanj zaprtega tipa ter dveh odprtega tipa, ki so si med seboj logično sledila. Vprašalnik je bil razdeljen na šest sklopov. S prvim sklopom vprašanj smo poskušali pridobiti splošni vtis o anketirancu in njegovem stališču do interneta. Tu smo uporabili Likertovo lestvico (prvo in drugo vprašanje), ki sodi med posredne lestvice za merjenje stališč. V tretjem in četrtem vprašanju smo prosili anketiranca, da naj izbere med dvema odgovoroma. V kolikor je anketiranec na četrto vprašanje odgovoril negativno, je sledilo še podvprašanje. Šesto vprašanje, ki je spraševalo po pogostosti uporabe interneta za spletne nakupe, je bilo osrednje vprašanje prvega sklopa. Možni odgovori so se nahajali v spustnem meniju. Zadnje vprašanje prvega sklopa je bilo pomožno vprašanje, da bi si skozi celotno izpolnjevanje vprašalnika lažje zapomnili, za katero spletno stran odgovarjajo na vprašanja. Odgovor na slednje vprašanje se je preslikal v vsa vprašanja, ki so sledila v nadaljevanju. To vprašanje je bilo tudi izločitveno, tako da so bili tisti anketiranci, ki niso podali odgovora, oziroma njihov odgovor ni bil naslov ali ime spletne strani, pri končnem pregledu izločeni. Takšnih anketirancev je bilo 62. Sledili so štirje sklopi vprašanj, ki so merili varnost, zasebnost, zaupanje in zvestobo spletni strani. Vsa vprašanja so bila zaprtega tipa z Likertovo lestvico strinjanja. Zadnji sklop vprašanj so sestavljala demografska vprašanja. Zanimal nas je spol, starost in izobrazba anketirancev.

6.2.4 Izvedba anketiranja

Kot smo že navedli v podpoglavju Metodologija, smo podatke pridobili s pomočjo spletne ankete, ki se je nahajala na dveh spletnih naslovih[31]. Na anketo, ki se je nahajala na prvem naslovu, so odgovarjali anketiranci, ki so zasledili povabilo k sodelovanju na spletnih straneh iskalnikov Najdi.si ter Matkurja.si. Na drugo, identično anketo so odgovarjali anketiranci, ki so dobili povabila za sodelovanje po elektronski pošti. Za elektronsko anketiranje smo se odločili, ker najbolj sovpada s tematiko tega dela. Zbirka 6.172-ih elektronskih naslovov je bila obdelana s programom Atomic Email Logger. Slednji program je poskrbel, da so bila vsa sporočila pravilne sintakse in hkrati odstranil vse podvojene naslove. Sporočila so bila poslana preko programa za masovno pošiljanje elektronskih sporočil – Mach5 Mailer. Na ta način smo dosegli, da so bila sporočila videti bolj osebna (vsak prejemnik je dobil svoje sporočilo). Vprašalnik se je nahajal na spletnih straneh podjetja Zaslon Telecom d.o.o. Vsi podatki so se po končanem preverjanju zapisali v SQL podatkovno bazo. Sporočila so bila razposlana v obdobju od 23. 4. do 4. 5. 2007. Pri analizi smo upoštevali vse odgovore, ki so prispeli do 21. 5. 2007.

6.2.5 Analiza rezultatov

Konstrukte smo preverili z metodo glavnih komponent. Povezave med konstrukti so bile testirane z regresijsko analizo, kjer smo kot spremenljivke uporabili posamezne konstrukte, izračunane kot povprečje mejnih spremenljivk.

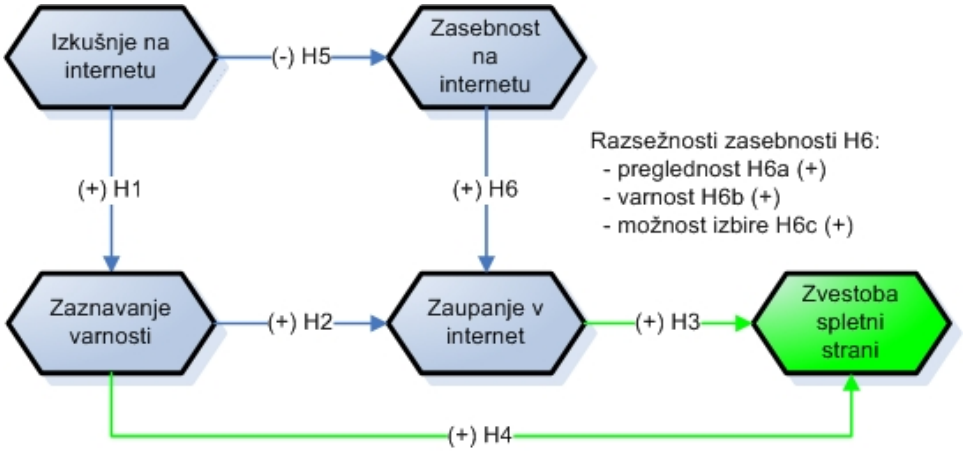
[31] http://www.zaslon-telecom.si/anketa/index.html in http://www.zaslon-telecom.si/anketa/index2.html

Podatki so bili obdelani s statističnim programskim paketom SPSS 12.0 for Windows. Rezultati so prikazani v prilogi.

6.3 HIPOTEZE

Po dosedanjem teoretičnem pregledu in snovanju konceptualnega modela smo postavili raziskovalne domneve ter izvedli empirično raziskavo, ki je obravnavala zastavljene domneve. Za ta namen smo pred raziskavo opredelili spremenljivke in jih združili v pet skupin, kar prikazujemo v nadaljevanju. Na vzorcu smo tako preverjali veljavnost naših domnev.

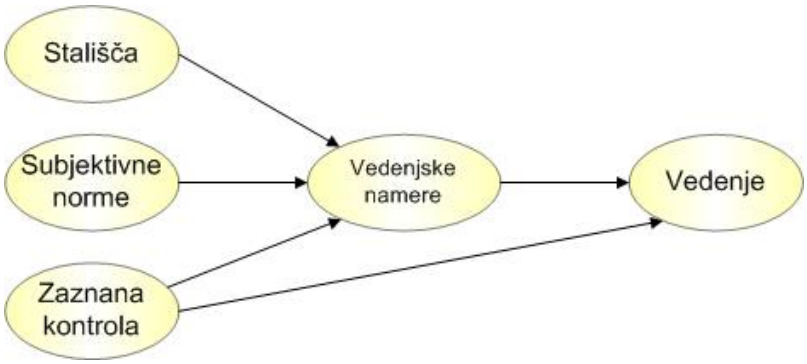
SLIKA 9: Konceptualni model



Vir: Lasten.

Pri razvoju konceptualnega modela smo si pomagali s teorijo planiranega vedenja (TPV), ki jo razvija Icek Ajzen (1991). TPV je v bistvu dopolnjena različica teorije razumne akcije (TRA), ki sta jo v 70-ih letih začela razvijati Ajzen & Fishbein (1980) in spada med t.i. odločitvene motivacijske modele. Za te je značilno, da analizirajo posamezne psihološke in socialne pogoje, ki vplivajo na zastavljanje ciljev (namen) in akcijo v zvezi z njimi. TPV temelji na predpostavki, da ljudje v vsakdanjem življenju sprejemajo veliko število odločitev, od katerih so nekatere avtomatizirane, nekatere pod vplivom nezavednega, večji del pa temelji na podlagi prejšnjih izkušenj posameznika in po premisleku. Pri takšnem odločanju upoštevamo tako notranje kot zunanje informacije. Na podlagi zbranih informacij, ki jih pridobimo preko socialnih skupin, medijev ipd. na eni strani in tudi na podlagi naših želja, prepričanj, možnosti na drugi strani, sprejmemo končno odločitev.

SLIKA 10: Teorija planiranega vedenja



Vir: Ajzen, 1991, str. 182.

Naša raziskava temelji na predpostavki, da stališča do zasebnosti, varnosti in zaupanja v internet vplivajo na odnos do same uporabe slednjega medija. Teorija planiranega vedenja predstavlja teoretične temelje za testiranje naših hipotez, vključno z osnovami za testiranje; ali so stališča resnično povezana z vedenjskimi nameni, ki so nadalje povezani z dejanskim vedenjem posameznika. Izhajajoč iz teorije, bi morala mnenja drugih uporabnikov interneta vplivati na uporabo interneta. In nenazadnje, če se potencialni uporabniki zavedajo možnosti in resursov za uporabo interneta, bi morali ti dejavniki imeti pozitivni vpliv na njihove namere in vedenje.

Da bi torej ugotovili, kaj motivira posameznika za uporabo interneta, se je najbolj primerno opreti na cilje, pričakovanja in tudi na ovire. Cilji in pričakovanja posameznika nam povedo, kaj je tisto, kar posameznika spodbuja k zadovoljitvi individualne potrebe.

Izkušeni uporabniki interneta bodo imeli zaradi časa, ki so ga preživeli na spletu in izkušenj, ki so jih pridobili, boljše znanje o varnosti na internetu kot uporabniki, ki niso izkušeni. Izkušeni uporabniki so se naučili zaznati in se izogniti nevarnostim, zato internet uporabljajo varneje. Lenhart (2000) je na podlagi raziskave, ki jo je opravil raziskovalni institut Pew Internet and American Life Project, zaključil, da večina neizkušenih uporabnikov interneta verjame, da je internet »nevaren« in da mu ni mogoče zaupati, medtem ko izkušnje vodijo v »znanje«. Torej:

H1 Več, ko ima posameznik izkušenj z internetom, bolj je dovzeten za zaznavanje varnosti na svetovnem spletu.

Nekatere raziskave so nakazale možno povezavo med nižjo stopnjo zaupanja pri spletnih interakcijah in visoko stopnjo zaskrbljenosti o internetni varnosti. Povedano drugače, ljudje, ki imajo skrbi glede varnosti, ne morejo zaupati spletni strani. Rezultati raziskave, ki jo je izvedla Evropska unija (European Commission, 2004) kažejo, da le 23 % Evropejcev, ki so opravili spletni nakup, popolnoma zaupa internetu kot nakupnemu kanalu. 48 % spletnih nakupovalcev je dejalo, da jih pri spletnih nakupih najbolj skrbi varnost. Do podobnih rezultatov so prišli tudi v

ZDA. Študija, ki je proučevala navade uporabnikov interneta, je v sklopu ugotovitev izpostavila tri glavne vzroke za nezaupanje v internet (Harris Interactive, 2002):

1. podjetja lahko prodajo zaupne podatke drugim podjetjem brez privolitve subjektov, katerih osebni podatki so shranjeni v bazah,
2. spletna transakcija ni varna in
3. hekerji bi lahko ukradli osebne podatke.

Lahko bi rekli, da so ljudje seznanjeni z vprašanjem varnosti, vendar ne znajo sami presoditi v konkretnem primeru, če je skrb de facto upravičena. Povprečen uporabnik interneta je podzavestno prepričan, da je internet nevaren (So et al., 2005, str. 1238). V kolikor bi le-ta znal sam presoditi, ali gre za (ne)varno spletno stran, bi tudi lažje vzpostavil zaupanje.

Na podlagi gornjih ugotovitev lahko zapišemo, da je povezava med konceptoma zaupanja in zaznavanja varnosti uporabe interneta verjetna in vredna proučitve. V kolikor v idejo, zapisano pod prvo hipotezo, vključimo tudi zaupanje, potem lahko zapišemo, da zaupanje pride z znanjem, znanje pa je posledica izkušenj. Za potrebe testiranja povezave smo zastavili naslednjo hipotezo:

H2 Z dvigovanjem nivoja zaznavanja varnosti na internetu prispevamo k pozitivnejšemu povečanju zaupanja v internet.

Pri tretji hipotezi se bomo osredotočili na zvestobo določeni spletni strani, zato je hipoteza bolj specifična kot ostale, ki se nanašajo na splošno uporabo interneta. Nekateri avtorji (Goldman, 1978) so zapisali, da so ljudje bolj predani podjetjem, ki jim dajo največ razlogov za zaupanje. Lojalnost lahko razložimo s strategijo zmanjšanja tveganja, pri čemer se po eni strani daje prednost zaupanja vrednim podjetjem, po drugi strani pa se izogibamo tveganim alternativam (Assael, 1992). Slednji koncept je možno prenesti v virtualni svet, kjer je znano, da je ena izmed največjih ovir za širjenje e-poslovanja ravno zaupanje. Glede na zgoraj zapisano lahko upravičeno sklepamo, da bo višja stopnja zaupanja uporabnika vodila do krepitve zvestobe v spletno stran.

H3 Močnejše, ko je zaupanje uporabnika v spletno stran, višja bo raven zvestobe do te strani.

Število odjemalcev, ki kupujejo preko interneta, je še vedno relativno majhno. V Evropski uniji je do leta 2003 le 16 % internetnih uporabnikov izjavilo, da so izvedli spletni nakup (European Commission, 2004). Med vsemi razlogi, ki so jih navajali kot vzrok izogibanju spletnim nakupom, sta se največkrat pojavljali negotovost in skrb za zaščito zasebnosti. Upoštevajoč slednje podatke, in na osnovi poročila, ki so ga pripravili pri Taylor Nelson Sofres Interactive (2002), lahko navedemo dva glavna vzroka, zakaj uporabniki interneta ne kupujejo preko spleta:

1. ker niso pripravljeni razkriti podatkov o svojih kreditnih karticah in

2. ker imajo ideološko prepričanje, da je varneje kupovati v tradicionalnih trgovinah kot pa preko spleta.

Vsiljena elektronska pošta je druga največja ovira spletnih nakupov, takoj za stroški pošiljanja (CIB, 2003). Potemtakem je videti razumljivo, da ima proces zaznavanja varnosti glede osebnih podatkov s strani uporabnika neposreden vpliv na njegovo lojalnost.

H4 Dvig ravni zaznavanja varnosti, predvsem z vidika osebnih podatkov, bo pozitivno vplival na zvestobo določeni spletni strani.

Hoffman et al. (1999) so ugotovili, da so bili izkušeni uporabniki interneta bolj zaskrbljeni glede vprašanj, povezanih z upravljanjem njihovih osebnih podatkov, v primerjavi z manj izkušenimi uporabniki. Pričakujemo, da bodo posameznikove izkušnje, povezane s svetovnim spletom, negativno povezane s stališčem do zasebnosti na internetu.

H5 Več, ko ima posameznik izkušenj z internetom, bolj negativno bo njegovo stališče do zasebnosti na internetu.

Zvezna trgovinska komisija ZDA (engl. Federal Trade Commision) je zapisala, da poštena informacijska praksa sloni na štirih dimenzijah (FTC Report to Congress, 2000):

- Preglednost: uporabnike se seznani z namenom zbiranja osebnih podatkov.
- Dostopnost: uporabnikom se omogoči dostop in vpogled v podatkovne zbirke ter podatke posameznika.
- Možnost izbire: organizacija, ki zbira podatke, mora uporabnikom omogočiti možnost izbire; ali dovolijo, da se podatki uporabijo oziroma izmenjajo z drugimi organizacijami.
- Varnost: podjetja morajo zagotoviti, da so osebni podatki varni in da ne bo prišlo do zlorabe.

Dimenzije zasebnosti, kot jih je predstavila ameriška Zvezna trgovinska komisija, predstavljajo praktične in teoretične temelje konstrukta zasebnosti. Rezultati raziskave, ki sta jo izvedla Liu in Arnett (2002), so pokazali, da le nekaj več kot 50 % spletnih strani večjih podjetij vsebuje tudi izjavo o zasebnosti. Avtorja nadalje sklepata, da je delež podjetij, ki imajo v izjavah predstavljene vse štiri dimenzije, bistveno manjši.

Têrmin zaupanje si lahko pogledamo z več zornih kotov (Houston, 2001). Je kompleksen socialni fenomen, ki odseva tehnološki, vedenjski, psihološki in organizacijski vidik interakcij med različnimi človeškimi in nečloveškimi predstavniki. Vse poslovne aktivnosti zahtevajo določeno mero zaupanja, še posebno pa tiste, ki izvirajo iz negotovih okolij (Lee, 1998). Uporabniki interneta morajo zaupati spletu in aktivnostim, ki se odvijajo na njem. V nasprotnem primeru se ga bodo bali in začeli izogibati (Gefen, 2000). V e-poslovanju je stopnja zaupanja videna kot osebno dojemanje posameznika, ki verjame, da bodo dejanja osebe na drugi strani opravljena s poštenimi nameni, integriteto in v skladu s poslovno etiko. (Jarvenpaa et al., 1998).

Slednja stopnja zaupanja predstavlja skupek različnih lastnosti, ki si jih (po svojem lastnem videnju – percepciji) ustvari določena oseba o osebi, s katero posluje. Vanjo spadajo integriteta, zmožnost in prepričanje v spletno poslovanje (Gefen et al., 2003). Zaščita zasebnosti uporabnika interneta je lahko pomembna osnova za pridobitev zaupanja (primer: stranka spletne trgovine mora verjeti, da se bo spletna transakcija odvijala skladno z njenimi pričakovanji) (Culnan, 1999). Na osnovi ugotovitev iz literature bomo preverili naslednje povezave:

H6 Med zasebnostjo in ravnijo zaupanja obstaja pozitivna povezava.
H6a Seznanjenost z načinom uporabe osebnih podatkov bo pozitivno vplivala na raven zaupanja.
H6b V kolikor bodo spletni uporabniki dobili občutek, da so njihovi osebni podatki varni, se bo posledično dvignila raven zaupanja.
H6c Možnost izbire med sistemoma opti-in in opti-out bo pozitivno vplivala na raven zaupanja.

Namen raziskave je testiranje hipotez oziroma določitev dejavnikov, ki so pomembni pri odločitvi uporabnika za uporabo internetnih storitev.

6.4 REZULTATI SPLETNE RAZISKAVE IN NJIHOVA INTERPRETACIJA

Podatke, ki smo jih pridobili z anketiranjem, smo obdelali s programskim paketom SPSS in s pomočjo programa Excel, v katerem smo lahko grafično ponazorili vse pridobljene rezultate.

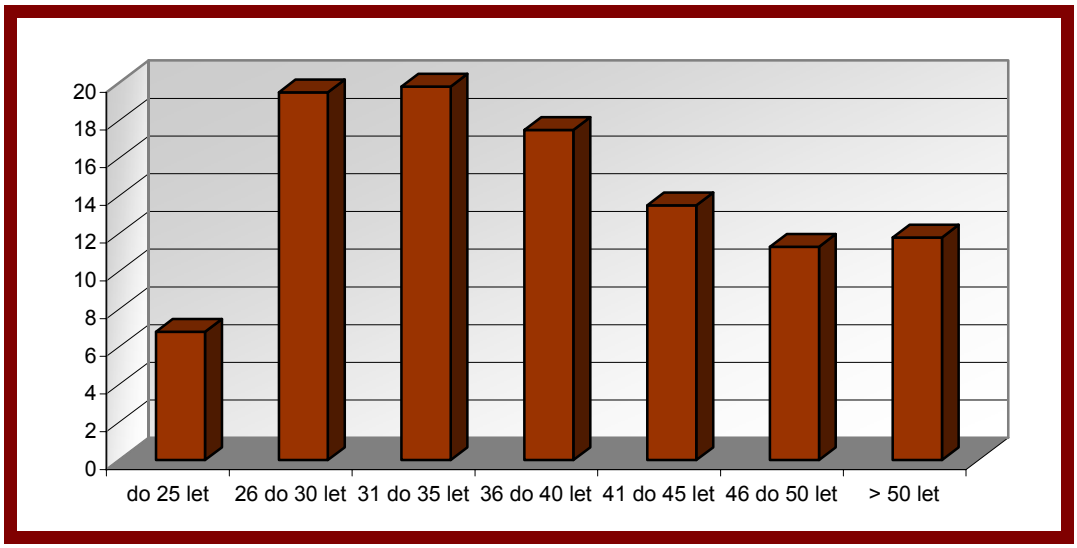
6.4.1 Opis vzorca

Najprej bomo predstavili zbrani vzorec anketiranih, in sicer sociodemografske značilnosti vzorca, nato pa bomo analizirali preostale trditve.

Izmed 400-tih anketiranih uporabnikov interneta je v vzorec zajetih 46,5 odstotka žensk (186 anketiranih) in 53,5 odstotka moških (214 anketiranih). Kot prikazuje Slika 11, je največ anketiranih (79 oseb, 19,8 odstotka), starih od 31 do 35 let, 19,5 odstotka jih je starih od 26 do 30 let, sledijo anketirani, stari od 36 do 40 let, teh je 17,5 odstotka, 13,5 odstotka je starih od 41 do 45 let, 11,8 odstotka je starih več kot 50 let, sledi 11,3 odstotka anketirancev, starih od 46 do 50 let, 6,8 odstotka pa je starih do 25 let.

Prvotno je anketa vsebovala 9 starostnih razredov in ne 7. Pri analizi podatkov smo prve tri razrede (do 17 let, od 17 do 20 let, od 21 do 25 let) združili v en razred – do 25 let.

SLIKA 11: Prikaz strukture anketiranih oseb po starosti

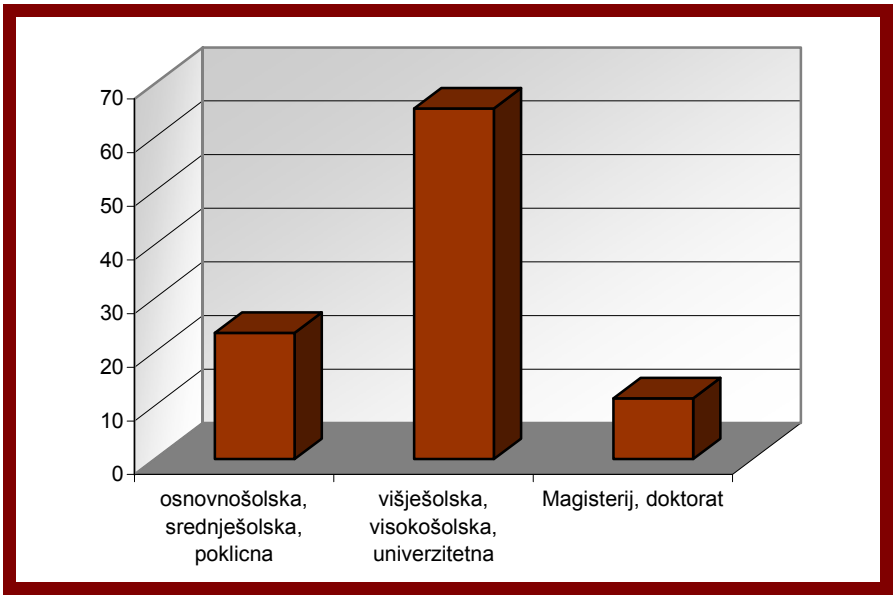


Vir: Anketa, 2007.

Pri strukturi anketiranih po dokončani izobrazbi, kar prikazuje Slika 12, močno prevladujejo anketirani z višješolsko, visokošolsko in univerzitetno izobrazbo, saj je le-teh 65,3 odstotka, 23,5 odstotka anketiranih ima osnovnošolsko, srednješolsko in poklicno stopnjo izobrazbe. Najmanj je magistrov in doktorjev, in sicer 11,3 odstotka.

Tudi tu smo prvotno najnižja dva razreda – osnovnošolska izobrazba ter srednješolska in poklicna – združili v enega, saj sta le dva anketiranca imela osnovnošolsko izobrazbo.

SLIKA 12: Prikaz strukture anketiranih porabnikov glede na dokončano izobrazbo



Vir: Anketa, 2007.

6.4.2 Opisne statistike

V tem poglavju bomo predstavili opisne statistike za vpliv izkušenj na internetu na zaznavanje varnosti ter vpliv slednjega na zaupanje. Proučili bomo tudi dva dejavnika, ki vplivata na zvestobo spletni strani; to sta zaupanje in varnost. Sledila bo tudi predstavitev vpliva spletnih izkušenj na zaznavanje zasebnosti ter vpliv le-te na zaupanje v internet.

Najprej smo analizirali trditve oziroma odgovore na prvih sedem splošnih vprašanj o internetu.

- zaskrbljenost glede varnosti na internetu

Vprašanje »*Ali ste zaskrbljeni glede varnosti na internetu?*« je na lestvici od 1 do 5 doseglo povprečno oceno 3,38. Kar pomeni, da so anketiranci bolj kot ne zaskrbljeni glede splošne varnosti na internetu. 37 odstotkov anketirancev je izrazilo skrb glede varnosti; 35,5 odstotka niti so niti niso zaskrbljeni; sledi 13 odstotkov, ki pravijo, da ni bojazni glede varnosti; 10,8 odstotka je zelo zaskrbljenih in 3,8 odstotka anketirancev sploh ni zaskrbljenih.

Spremenljivka je porazdeljena rahlo asimetrično v levo in je sploščena. Standardni odklon znaša 0,968.

- zaskrbljenost glede varnosti pri opravljanju spletnega nakupa

Vprašanje »*Ali ste zaskrbljeni glede varnosti pri opravljanju spletnega nakupa ali elektronskega bančništva?*« je na lestvici od 1 do 5 v povprečju doseglo nekoliko višjo povprečno oceno kot predhodno vprašanje. Le-ta znaša 3,68; kar nam pove, da je v povprečju večina anketirancev izrazila skrb glede varnosti pri opravljanju spletnega nakupa. 62,6 odstotka je izrazilo skrb; 20,3 odstotka niti so niti niso zaskrbljeni glede varnosti; 17,3 odstotka pa niso oziroma sploh niso zaskrbljeni glede varnosti.

Spremenljivka je porazdeljena rahlo asimetrično v levo in je sploščena. Standardni odklon je 1,131.

- zasebnost ali praktičnost

Na vprašanje »*Kaj je za vas bolj pomembno: praktičnost ali zasebnost?*« je 58,5 odstotka anketirancev odgovorilo v prid zasebnosti.

- nakup preko spleta s kreditno kartico

228 (57 %) sodelujočih je na vprašanje »*Ali ste pripravljeni uporabiti vašo kreditno kartico za plačilo spletnega nakupa?*« odgovorilo, da so pripravljeni uporabiti kartico za plačilo spletnega nakupa.

- zakaj niso pripravljeni uporabiti kreditne kartice za plačilo spletnega nakupa

43 odstotkov anketirancev, ki je na predhodno vprašanje odgovorili negativno, je odgovarjalo še na naslednje odprto vprašanje »*Zakaj ne?*«. Namen tega vprašanja je bil pridobiti čim bolj

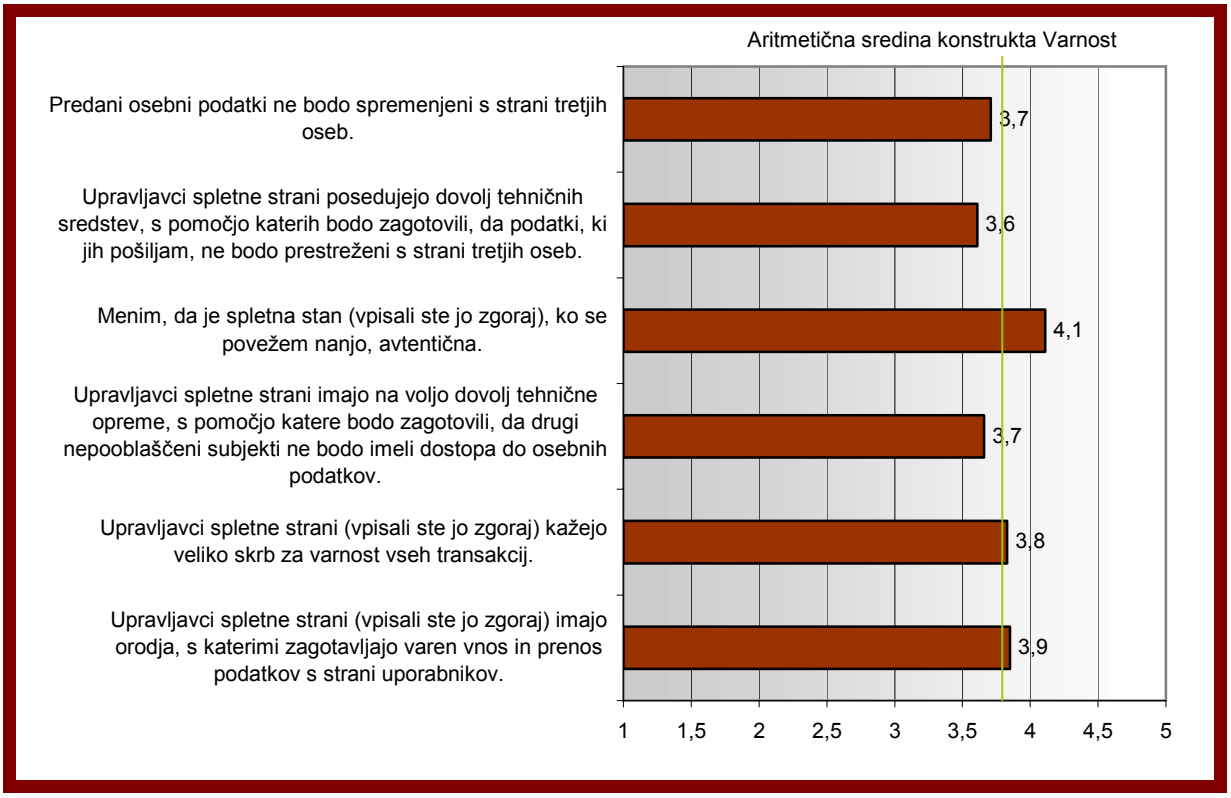
nepristransko mnenje posameznih anketirancev (brez pomoči). Odgovori so bili zelo raznoliki, možno pa jih je združiti v tri skupine: nezaupanje, pomanjkljiva varnost in možnost zlorab.

- uporaba interneta

Anketiranci so na vprašanje »*Kako pogosto ste uporabili internet v zadnjih šestih mesecih za spletne nakupe?*« najpogosteje odgovorili z »*manj kot enkrat na mesec*« (37,8 odstotka). Le 3,8 odstotka uporabnikov interneta uporablja internet za spletne nakupe vsak dan. 30,3 odstotka uporabnikov interneta ni še nikoli kupovalo preko spleta.

V nadaljevanju so anketiranci s pomočjo petstopenjske Likertove lestvice izražali stališča do serij trditev, ki so se nanašale na proučevane konstrukte. Konstrukt varnosti smo merili s 6-imi trditvami, povprečne ocene so prikazane v Sliki 13.

SLIKA 13: Povprečne ocene strinjanja za trditve, ki proučujejo področje varnosti

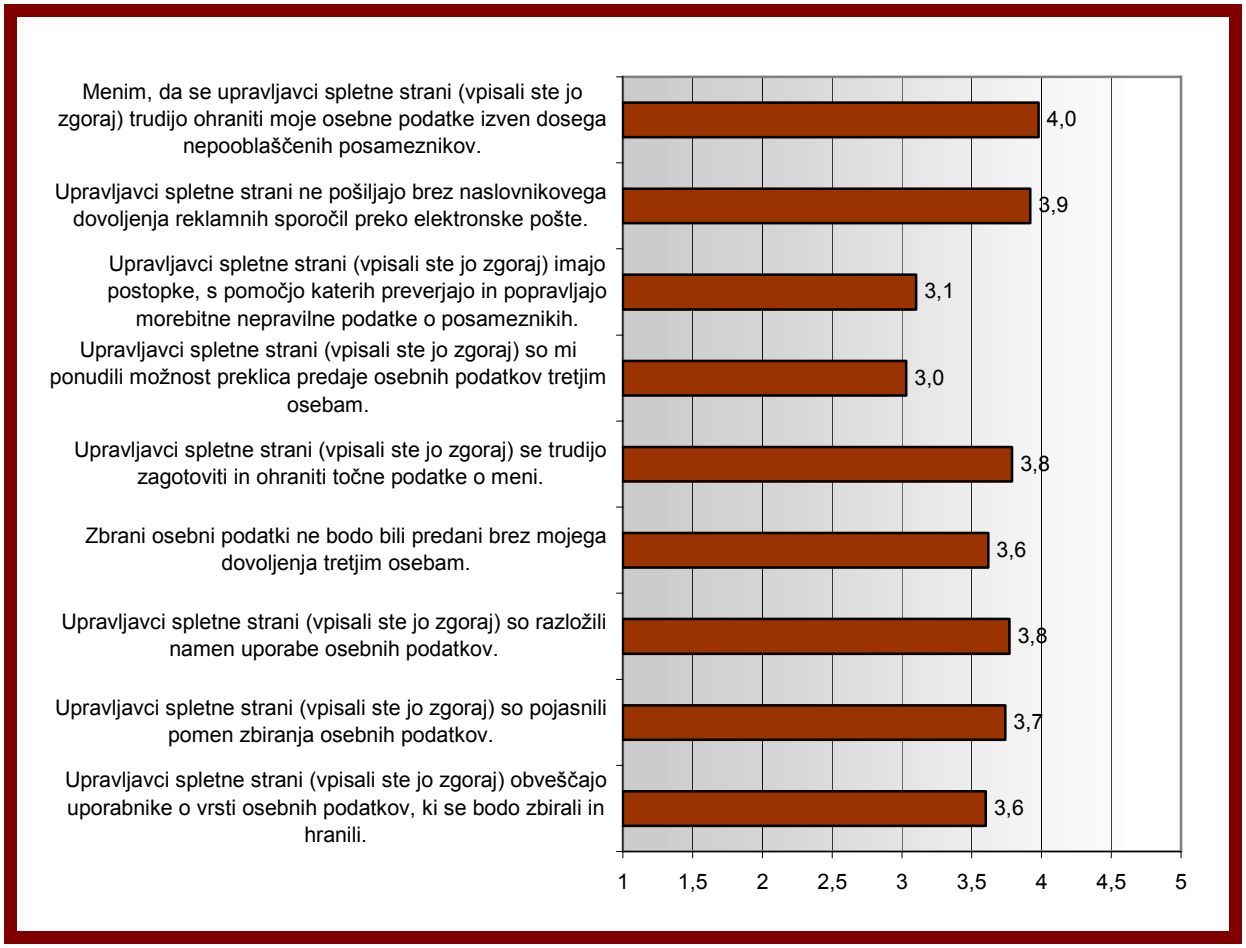


Vir: Anketa, 2007.

Anketiranci so se z vsemi trditvami glede varnosti precej strinjali, saj je povprečna vrednost nad srednjo vrednostjo 3. Najbolj so se strinjali s trditvijo, ki govori o avtentičnosti spletne strani (4,1), najmanj pa s trditvijo o posedovanju tehničnih sredstev za zagotavljanje varnosti (3,6). Najbližje povprečju konstrukta je trditev »*Upravljavci spletne strani kažejo veliko skrb za varnost vseh transakcij.*«.

V naslednjem sklopu so anketiranci ocenjevali 9 trditev, ki se nanašajo na zasebnost. Slika 14 prikazuje povprečne vrednosti.

SLIKA 14: Povprečne ocene strinjanja za trditve, ki proučujejo področje zasebnosti

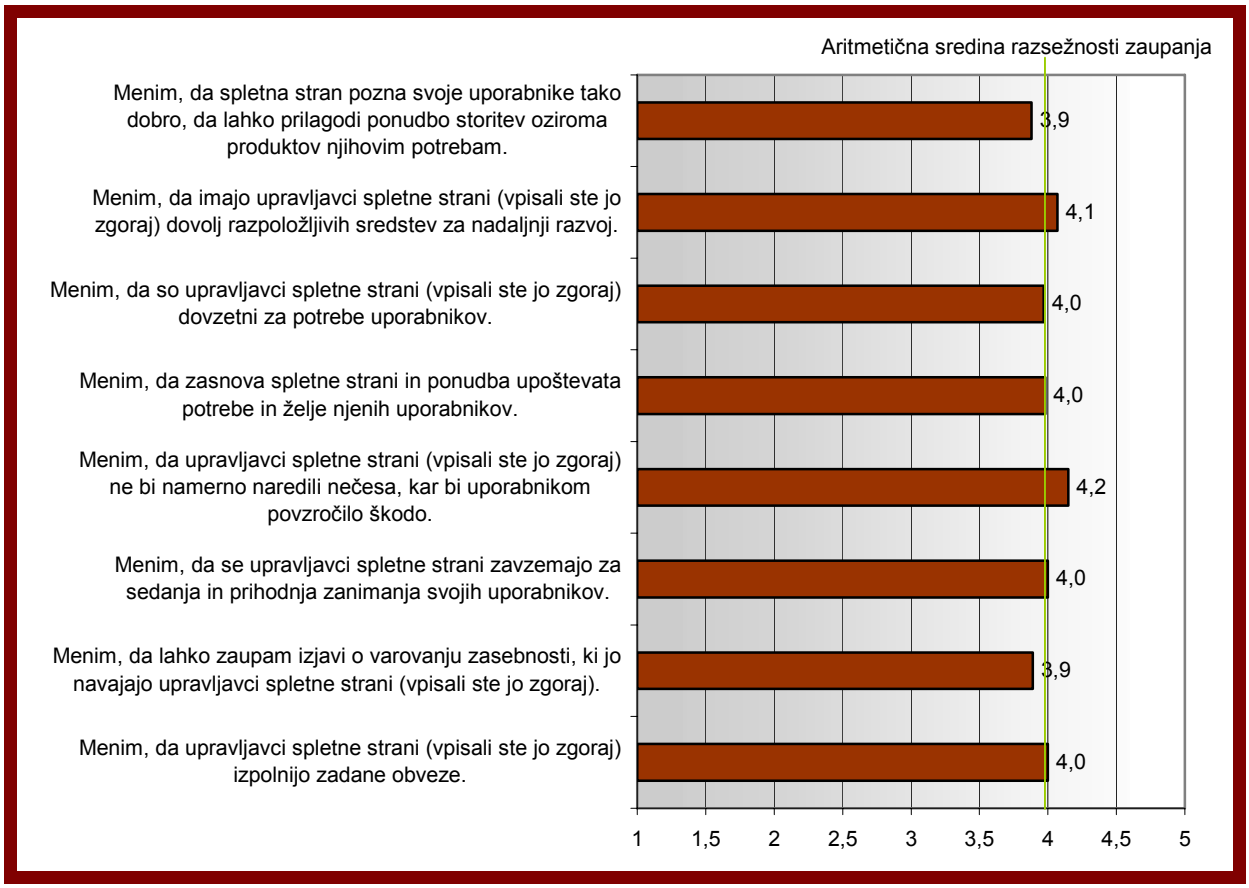


Vir: Anketa, 2007.

Anketiranci so se precej strinjali tudi s trditvami, ki so proučevale področje zasebnosti, saj je tudi tu povprečna vrednost nad srednjo vrednostjo 3. Najbolj so se strinjali s trditvijo, ki govori o dostopu do podatkov s strani nepooblaščenih uporabnikov (4,0). Najnižjo oceno (3,0) je dobila trditev, ki pravi, da so upravljavci ponudili možnost preklica predaje osebnih podatkov tretjim osebam. Trditvi »*Zbrani osebni podatki ne bodo bili predani brez mojega dovoljenja tretjim osebam.*« in »*Upravljavci spletne strani obveščajo uporabnike o vrsti osebnih podatkov, ki se bodo zbirali in hranili.*« imata povprečni vrednosti odgovorov najbližje povprečju razsežnosti zasebnosti; aritmetična sredina odgovorov znaša 3,6 in 3,62, celotnega konstrukta pa 3,61.

Konstrukt zaupanja smo merili s pomočjo 8-ih trditev, katerih povprečne vrednosti so prikazane v Sliki 15.

SLIKA 15: Povprečne ocene strinjanja za trditve, ki proučujejo področje zaupanja

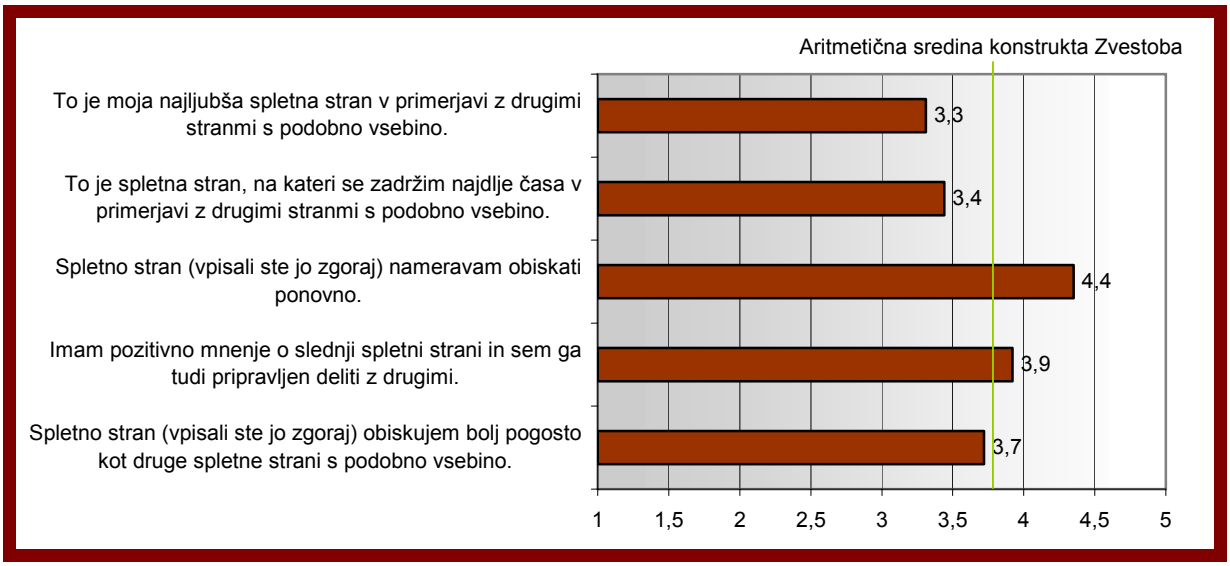


Vir: Anketa, 2007.

Povprečna ocena ni bila pri nobenem odgovoru, ki se navezuje na področje zaupanja, nižja od 3,8, kar pomeni, da so se z vsemi trditvami strinjali. Anketiranci so izmed vseh trditev najbolje ocenili (4,2) trditev, ki govori o namerni povzročitvi škode. Najslabše, vendar še vedno pozitivno, pa so ocenili zadnjo trditev tega sklopa, ki pravi, da spletna stran pozna svoje uporabnike tako dobro, da lahko prilagodi ponudbo storitev ali produktov potrebam uporabnikov. Aritmetična sredina konstrukta zaupanja znaša 4.

Konstrukt zvestobe spletni strani smo merili s 5-imi trditvami. Povprečne vrednosti prikazuje Slika 16.

SLIKA 16: Povprečne ocene strinjanja za trditve, ki proučujejo področje zvestobe



Vir: Anketa, 2007.

Tudi v zadnjem sklopu vprašanj so bili vsi odgovori nad vrednostjo 3. Anketiranci so se z vsemi trditvami precej strinjali, saj je povprečna vrednost nad srednjo vrednostjo 3. Srednja vrednost vseh trditev se giblje na intervalu med 3,3 in 4,4, kar pomeni, da povprečne vrednosti spremenljivk v konstruktu zvestobe dosegajo največji razpon (1,1) v primerjavi z drugimi konstrukti proučevanega modela. Izmed vseh trditev, tako na ravni konstrukta kot tudi celotnega vprašalnika, je najvišjo vrednost (4,35) dobila trditev, ki govori o namenu ponovnega obiska spletne strani. Najbližje povprečju dimenzije (3,7) pa je bila trditev »*Spletno stran obiskujem bolj pogosto kot druge spletne strani s podobno vsebino.*«.

6.4.3 Oblikovanje konstruktov ter preverjanje njihove zanesljivosti

Pojasnjevalne spremenljivke v konceptualnem modelu so v svojem bistvu sestavljene spremenljivke.

Najprej bomo izvedli redukcijo podatkov z metodo glavnih komponent. Slednja metoda je ena najpogosteje uporabljenih multivariantnih metod. Kovačič (2001) v svojem On-line slovarčku statističnih pojmov navaja kot cilj te metode iskanje nekaj prvih komponent, ki pojasnjujejo čim večji del razpršenosti analiziranih podatkov. Metoda glavnih komponent torej zmanjša razsežnost podatkov, pri tem pa poizkuša izgubiti čim manj informacij. Metodo bomo uporabili za določitev vsakega konstrukta posebej in sicer za naslednje konstrukte:

- varnost,
- zasebnost,
- zaupanje in
- zvestoba.

Za posamezne konstrukte bomo poskušali ugotoviti zanesljivost modela. V kolikor bo zanesljivost konstruktov sprejemljiva, bomo v drugi fazi preverjali postavljene hipoteze. Če to ne bo tako, bo pred preverbo hipotez sledil popravek modela.

Da bi ugotovili, ali izbrani indikatorji res merijo zgolj eno dimenzijo, to preverimo z analizo glavnih komponent. Proučiti moramo komunalitete, ki nam povedo, koliko variance spremenljivk je zajete v modelu, ki smo ga dobili z analizo glavnih komponent.

KMO statistika (Priloga 7) pri vseh dimenzijah presega vrednost 0,8, kar kaže na ustreznost vzorca za faktorizacijo. Za preverjanje zanesljivosti merskega instrumenta za posamezne dimenzije smo uporabili Cronbachov koeficient (Priloga 7). Pri vseh dimenzijah vrednost koeficienta presega 0,6, ki predstavlja mejo zanesljivosti. Večina koeficientov je celo večja od 0,8, kar kaže na zelo dobro zanesljivost.

VARNOST

Iz Tabele 13 v Prilogi 3 je razvidno, da ima najnižjo vrednost po ekstrakciji trditev »*Menim, da je spletna stran (vpisali ste jo zgoraj), ko se povežem nanjo, avtentična.*«; to je 0,504, kar je dovolj, da spremenljivko ohranimo v modelu. Z eno dimenzijo pojasnimo okoli 71 % celotne variance spremenljivk, kar pomeni, da lahko uporabimo vse trditve za to dimenzijo (Priloga 3, Tabela 14). Faktorske uteži so pri vseh trditvah visoke in približno enake (razen pri zgoraj omenjeni trditvi), kar pomeni, da vse podobno prispevajo h konstruktu (Priloga 3, Tabela 15).

V naslednjem koraku naredimo sestavljeno spremenljivko Likertovega tipa, ki je povprečje na vseh trditvah.

ZASEBNOST

Z analizo glavnih komponent smo odgovorom na devet trditev iskali skupne razsežnosti (prikaz razdelitve spremenljivk po posameznih razsežnostih je v Prilogi 7) in jih skušali izraziti s faktorjem. Komunalitete pa nam kažejo, da je faktor ustrezen in pojasnjuje velik delež variance posameznih kategorij. To prikazujemo v Tabeli 17 (Priloga 4). S tremi komponentami pojasnimo 75,4 % celotne variance spremenljivk (Priloga 4, Tabela 18). S poševno rotacijo komponentnih uteži (izbrali smo jo zato, ker predvidevamo, da so dimenzije med seboj povezane) smo potrdili napovedano povezanost trditev znotraj konstrukta zasebnosti (Priloga 4, Tabela 19). Razsežnosti konstrukta zasebnosti so:

- seznanjenost,
- varovanje zasebnosti in
- možnost izbire.

Trditvi Q17 in Q18 imata dokaj močne uteži tako pri razsežnosti varnosti kot pri možnosti izbire, vendar smo ju zaradi vsebinskih razlogov, podprtih s teorijo, uvrstili v dimenzijo varnost in tudi sicer se izkaže, da imata pri tej dimenziji večje uteži.

TABELA 6: Korelacijska matrika

Komponenta	Seznanjenost	Varnost	Možnost izbire
Seznanjenost	1	0,526	0,508
Varnost	0,526	1	0,402
Možnost izbire	0,508	0,402	1

Vir: Anketa, 2007.

Korelacijska matrika nam pokaže vrednosti Pearsonovih korelacijskih koeficientov med posameznimi faktorji. Vrednosti koeficientov so pozitivne in precej visoke, kar kaže na to, da so dimenzije med seboj precej povezane.

ZAUPANJE

Komunalitete oz. deleži varianc, pojasnjeni s faktorjem, kažejo, da vse spremenljivke sodijo k izbranemu faktorju. To prikazujemo v Tabeli 21 (Priloga 5). Vse neodvisne spremenljivke lahko prikažemo s samo enim faktorjem. Faktor pojasnjuje 65,30 % variance (Priloga 5, Tabela 22). Faktorske uteži so pri vseh trditvah visoke in približno enake, kar pomeni, da vse podobno prispevajo h konstruktu (Priloga 5, Tabela 23).

ZVESTOBA

Komunalitete (delež pojasnjene variance s faktorjem) nam kažejo, da vse spremenljivke sodijo k faktorju (Priloga 6, Tabela 25). Z enim faktorjem smo pojasnili 68,1 % skupne variance. Iz analize izhaja, da njegova lastna vrednost znaša 3,403. Lastna vrednost faktorja je dovolj visoka za primernost analize (Priloga 6, Tabela 26). Iz Tabele 27 (Priloga 6) je razvidno, da so tudi pri konstruktu zvestobe faktorske uteži pri vseh spremenljivkah približno enakih vrednosti.

Najvišjo stopnjo strinjanja ima konstrukt Zaupanje (4). Dimenzije Zasebnosti so ocenjene dokaj različno. Najvišjo povprečno oceno znotraj konstrukta zasebnosti ima poddimenzija Pričakovano varovanje zasebnosti (3,8), sledi poddimenzija Preglednosti (3,7), najnižjo oceno pa ima poddimenzija Možnost izbire (3,1), ki je med vsemi sestavljenimi spremenljvkami tudi najnižje ocenjena.

TABELA 7: Opisna statistika sestavljenih spremenljivk

Dimenzija	N	Minimum	Maksimum	Aritmetična sredina	Standardni odklon
Varnost	400	1	5	3,79	0,78
Zasebnost-preglednost	400	1	5	3,70	1,02
Zasebnost-varnost	400	1	5	3,82	0,84
Zasebnost-možnost izbire	400	1	5	3,07	1,03
Zaupanje	400	1	5	3,99	0,70
Zvestoba	400	1	5	3,75	0,91

Vir: Anketa, 2007.

6.4.4 Statistično preizkušanje domnev

Domneve smo postavili v skladu s konceptualnim modelom, katerega smo oblikovali na podlagi ugotovitev, ki so jih dale predhodne empirične raziskave. V konceptualnem modelu imamo na eni strani neodvisne, na drugi pa odvisne spremenljivke. Slednje pri nadaljnjih preverjanjih hipotez nastopijo tudi v vlogi neodvisne spremeljivke. Za preverjanje koncepta smo uporabili enostavno in multiplo regresijsko analizo. Rezultati regresijskih analiz so objavljeni v Prilogah 9 do 14.

V Tabeli 8 so prikazani rezultati regresijskih analiz med pari konstruktov.

TABELA 8: Rezultati enostavne regresijske analize

Neodvisna spremenljivka	Hipoteza	Odvisna spremenljivka	B	Beta	P	R^2
Izkušnje	H1 +	Varnost	0,232	0,302	0	0,091
Varnost	H2 +	Zaupanje	0,64	0,716	0	0,513
Zaupanje	H3 +	Zvestoba	0,7	0,536	0	0,288
Varnost	H4 +	Zvestoba	0,515	0,442	0	0,195
Izkušnje	H5 -	Zasebnost	0,137	0,171	0,001	0,029
Zasebnost	H6 +	Zaupanje				0,585*
- *Preglednost*	H6a +	Zaupanje	0,088	0,129	0,003	
- *Varnost*	H6b +	Zaupanje	0,543	0,653	0	
- *Možnost izbire*	H6c +	Zaupanje	0,031	0,045	0,258	

Legenda: ☐ - nepotrjene hipoteze
* - prilagojen R^2

Vir: Anketa, 2007.

Ker konceptualni model (Slika 9 na strani 69) kaže, da obstajajo sočasni vplivi več odvisnih spremenljivk (konstruktov) na posamezno neodvisno spremenljivko, smo za testiranje vpliva vseh neodvisnih spremenljivk na izbrano spremenljivko uporabili multiplo regresijsko analizo. Rezultate prikazujeta Prilogi 15 in 16.

Pri preučevanju vpliva zasebnosti in varnosti na zaupanje smo izvedli multiplo regresijo, s katero smo pojasnili 65,1 % variance odvisne spremenljivke. Model je statistično značilen ($F=187,18$, $P<0,01$). Varnost, zasebnost-preglednost in zasebnost-varnost zasebnosti statistično značilno pozitivno vplivajo na zaupanje, medtem ko vpliva zasebnosti-možnost izbire ne moremo potrditi. Na zaupanje najmočneje vpliva varovanje zasebnosti, najmanj pa seznanjenost.

$$\text{Zaupanje} = 1{,}093 + \overbrace{0{,}057\ \underset{(0{,}027)}{\textit{Preglednost}} + 0{,}381\ \underset{(0{,}038)}{\textit{Varovanje zasebnosti}} + 0{,}004\ \underset{(0{,}025)}{\textit{Možnost izbire}}}^{\textit{Zasebnost}} + 0{,}321\ \underset{(0{,}037)}{\textit{Varnost}}$$

Ravno tako smo izvedli multiplo regresijo za model, v katerem proučujemo vpliv zaupanja in varnosti na zvestobo. Tudi ta model je statistično značilen (F=82,873, P<0,01). Zaupanje statistično značilno pozitivno vpliva na zvestobo. Vpliv varnosti na zvestobo je na meji sprejemljive statistične značilnosti (P=0,052), vendar smo ga zaradi minimalnega odstopanja, potrditve vpliva pri merjenju z bivariatno regresijsko analizo in pričakovanega predznaka povezave potrdili.

$$\text{Zvestoba} = 0{,}87 + \underset{(0{,}079)}{0{,}059\ \textit{Zaupanje}} + \underset{(0{,}07)}{0{,}138\ \textit{Varnost}}$$

H1 Izkušnje na internetu so pozitivno povezane z zaznavo varnosti.

Korelacijski koeficient med izkušnjami na internetu in zaznavanjem varnosti na svetovnem spletu je enak 0,302, kar pomeni, da je odvisnost med slednjima spremenljivkama šibka in pozitivna. Skupaj z linearno regresijo lahko pri stopnji značilnosti P=0 potrdimo postavljeno domnevo in sprejmemo sklep, da izkušnje na internetu pozitivno vplivajo na zaznavanje varnosti na svetovnem spletu.

H2 Med zaznavanjem varnosti in zaupanjem je pozitivna povezava.

Korelacijski koeficient 0,716 kaže, da je povezava med zaznavanjem varnosti in zaupanjem pozitivna in močna. Skupaj z linearno regresijo lahko potrdimo postavljeno domnevo in sprejmemo sklep, da sta konstrukta varnosti in zasebnosti pozitivno povezana; pri stopnji značilnosti P=0.

Domneva je potrjena tudi z uporabo multiple regresije (b=0,321, P<0,05).

H3 Zaupanje je pozitivno povezano z zvestobo spletni strani.

Na podlagi korelacijske analize lahko rečemo, da sta zaupanje in zvestoba spletni strani pozitivno povezana. Korelacijski koeficient med slednjima znaša 0,536, kar pomeni, da je odvisnost med njima pozitivna ter srednje močna. Tudi regresijska analiza kaže, da je pozitiven vpliv zaupanja na zvestobo statistično značilen (P=0).

Podobne rezultate z malo nižjim beta koeficientom smo dobili tudi z uporabo multiple regresije (b=0,59, P<0,05). S tem lahko potrdimo hipotezo H3.

H4 Zaznana varnost ima pozitiven vpliv na zvestobo.

Korelacijski koeficient 0,442 kaže, da je povezava med zaznavanjem varnosti in zvestobe spletni strani pozitivna in srednje močna. Rezultati korelacijske analize in bivariatne regresije potrjujejo postavljeno domnevo, multipla regresijska analiza pa je pokazala statistično značilnost povezave

na meji sprejemljive stopnje tveganja (P=0,052). Možen razlog je v multikolinearnosti, saj sta konstrukta, ki nastopata kot pojasnjevalni spremenljivki (Zaupanje in Varnost), močno medsebojno povezana (r=0,716). Ker je predznak parcialnega regresijskega koeficienta v skladu s pričakovanim, lahko hipotezo 4 sprejmemo.

H5 Izkušnje na internetu vodijo k negativnemu stališču do zasebnosti na internetu.

Na podlagi korelacijske analize lahko rečemo, da so izkušnje na internetu in stališče do zasebnosti pozitivno povezani. Korelacijski koeficient med slednjima znaša 0,171, kar pomeni, da je odvisnost med njima pozitivna ter zelo šibka. Tudi regresijska analiza kaže, da je pozitiven vpliv izkušenj na stališče do zasebnosti statistično značilen (P=0,001). V modelu smo predvidevali negativen vpliv. Iz tega sledi, da hipoteze H5 ne moremo potrditi.

H6 Zasebnost na internetu in zaupanje v le-tega sta pozitivno povezana.

Konstrukt zasebnosti ima tri razsežnosti.

H6a Preglednost nad zbiranjem podatkov in zaupanje na internetu sta pozitivno povezana.

Korelacijski koeficient med seznanjenostjo z načinom uporabe osebnih podatkov in zaupanjem je enak 0,129. To pomeni, da je povezava med njima pozitivna in zelo šibka. Tudi na podlagi regresije ugotavljamo, da je pozitiven vpliv preglednosti oziroma seznanjenosti na zaupanje statistično značilen (P=0,003).

Podobne rezultate smo dobili tudi pri uporabi multiple regresijske analize (b=0,057, P<0,05).

H6b Varovanje zasebnosti bo pozitivno vplivalo na zaupanje v internet

Na podlagi korelacijske analize lahko rečemo, da sta varovanje zasebnosti ter zaupanje v internet pozitivno povezana. Korelacijski koeficient med slednjima znaša 0,653, kar pomeni, da je odvisnost med njima pozitivna ter srednje močna. Tudi linearna regresija kaže, da varovanje zasebnosti pozitivno vpliva na zaupanje (P=0). S tem lahko potrdimo hipotezo H6b.

Multipla regresijska analiza je pokazala, da znaša parcialni regresijski koeficient b=0,381 ob stopnji značilnosti P<0,05, kar potrjuje vpliv Varovanja zasebnosti na Zaupanje v internet.

H6c Možnost izbire glede uporabe osebnih podatkov in zaupanje v internet sta pozitivno povezana.

Korelacijska analiza je pokazala, da povezava med možnostjo izbire glede uporabe osebnih podatkov in zaupanjem ni statistično značilna (P=0,258). Temu sledi, da ne moremo trditi, da sta možnost izbire glede uporabe osebnih podatkov in zaupanje v internet med seboj povezana. Enak rezultat kažeta tudi linearna in multipla regresija. Iz tega sledi, da hipoteze H6c ne moremo potrditi.

6.4.5 Povzetek ugotovitev

Z opravljeno raziskavo smo s pomočjo statističnih testov preverili zastavljene hipoteze:

- Prvo hipotezo smo potrdili. Raziskava je pokazala, da več, ko ima posameznik izkušenj z internetom, bolj je dovzeten za zaznavanje varnosti na svetovnem spletu.
- Drugo hipotezo smo ravno tako potrdili, in sicer smo ugotovili, da višji nivo zaznavanja varnosti na internetu prispeva k pozitivnejšemu stališču do interneta.
- Tretja hipoteza je tudi potrjena. Z raziskavo smo ugotovili, da močnejše, ko je zaupanje uporabnika v spletno stran, višja bo raven zvestobe tej strani.
- Četrta hipoteza je potrjena. Ugotovili smo, da dvig ravni zaznavanja varnosti, predvsem z vidika osebnih podatkov, pozitivno vpliva na zvestobo določeni spletni strani.
- Peto hipotezo smo zavrnili, ker smo ugotovili, da posameznikove izkušnje zelo šibko, pa vendar pozitivno vplivajo na njegovo stališče do zasebnosti na internetu.
- Šesto hipotezo smo deloma potrdili.
- Šesta »a« hipoteza je tudi potrjena. Z raziskavo smo potrdili, da seznanjenost z načinom uporabe osebnih podatkov pozitivno vpliva na raven zaupanja.
- Šesta »b« hipoteza je ravno tako potrjena, saj smo ugotovili, da se bo posledično dvignila raven zaupanja, v kolikor bodo spletni uporabniki dobili občutek, da so njihovi osebni podatki varni.
- Šesta »c« hipoteza je bila zavrnjena, ker povezanosti med možnostjo izbire sistema množičnega obveščanja z zaupanjem nismo potrdili. Ne moremo trditi, da možnost izbire vpliva na raven zaupanja do interneta.

6.4.6 Omejitve in možne napake pri raziskavi

Rezultati raziskave, ki so del tega magistrskega dela, so v večini primerov potrdili zastavljene hipoteze. Vseeno je ob tem potrebno upoštevati tudi nekatere omejitve, ki so nastale zaradi izbrane metode zbiranja podatkov.

Raziskava, ki smo jo izvedli na namenskem vzorcu 400-tih enot, je bila deskriptivne narave. Rezultate lahko uporabimo za predvidevanje, vendar jih ne moremo posplošiti na celotno populacijo. Vzorec je pokrival le slovenske uporabnike interneta, kjer pa spletni nakupi niso ravno globalna aktivnost kot na primer v ZDA. Prav tako moramo na rezultate raziskave gledati z določeno mero previdnosti, saj pri spletnem anketiranju anketirani ni v osebnem stiku s spraševalcem.

Način izvedbe vprašalnika je sicer časovno in stroškovno zelo učinkovit, vendar pa je posledica tega načina izvedbe relativno majhen odziv anketirancev, vzrok pa je zaznava vabila kot nezaželene elektronske pošte.

Med celotno raziskavo smo poskusili zmanjšati možnost napake. S testiranjem vprašalnika smo se izognili nerazumljivim in dvoumnim vprašanjem, zato smo tudi postavili jasna in enostavna

vprašanja ter možne odgovore. Spletni vprašalnik je pri vseh vprašanjih izvajal kontrolo odgovorov, kar pomeni, da so bila vsa vprašanja popolno izpolnjena. Žal pa se nismo mogli izogniti napakam neodziva in napakam, ki so posledica merjenja pojava, saj lahko le predvidevamo, da so anketiranci odgovarjali pošteno in le enkrat.

Težava, ki se je pojavila pri anketiranju, je bila nezaupanje do vprašalnika oziroma vira, kar tudi nekako sovpada s tematiko naloge. Prejeli smo nekaj deset elektronskih sporočil, s katerimi so potencialni anketiranci spraševali, od kod imamo njihove kontaktne podatke in ali bodo rezultati ankete resnično uporabljeni v magistrski nalogi.

Ko govorimo o pomanjkljivosti raziskovalnega dela – njegovi omejenosti – pa lahko hkrati to razumemo kot možnost nadaljnjega raziskovalnega dela.

6.4.7 Smernice za nadaljnje raziskave

Zastavljen konceptualni model je pokrival tri med seboj povezane osrednje konstrukte (zasebnost, varnost in zaupanje na internetu). Pri pripravi modela smo že upoštevali in tudi proučili spremenljivko, ki nekako logično sledi celotnemu procesu – zvestoba. Število opravljenih poslov prek interneta in vrednost le-teh se vsako leto veča. Model bi bilo potrebno razširiti v smeri proučitve dejavnikov, ki vplivajo na stranko, da se odloči za spletni nakup. Nova dimenzija bi zahtevala proučitev, poleg že omenjenih faktorjev, tudi drugih dejavnikov, ki lahko vplivajo na spletni nakup. Ugotovili smo, da so uporabniki interneta zelo neodločni glede spletnih nakupov, predvsem s stališča (v njihovih očeh) pomanjkljive varnosti in vprašljive zasebnosti. In ravno zato je pomembno razumeti dejavnike, ki vplivajo na stališča potencialnih kupcev o internetu, prikazati internet v boljši luči in posledično vplivati na njihov namen po spletnem nakupu.

V obstoječem modelu bi bilo smiselno testirati tudi navzkrižne povezave med posameznimi spremenljivkami. Tukaj mislimo na povezavo med varnostjo in zasebnostjo ter zasebnostjo in zvestobo. Predvidevamo, da lahko v obeh primerih pričakujemo pozitivno povezavo.

Omeniti je potrebno tudi vedno pogosteje uporabljeno novo opremo, ki omogoča brezžični dostop do interneta; Wi-Fi in Wi-Max. Tehnologiji omogočata dostop do interneta brez fizične povezave. Posledično se spletni trg hitreje širi, saj tradicionalna telefonska ali kabelska omrežja niso več potrebna. Nova tehnologija bo tako prispevala k novim poslovnim priložnostim, kot tudi predstavila določen izziv, kar se tiče zaupanja do spleta. Glede na to, da nove tehnologije lahko predstavljajo določeno oviro pri nadaljnjem razvoju interneta, je potrebno le-te nemudoma proučiti. Predvsem je potrebno preveriti, ali imajo uporabniki interneta, v primerjavi s tradicionalnim spletnim okoljem, enako stališče do problematike varnosti osebnih podatkov.

Na osnovi teoretičnega konceptualnega modela, ki smo ga predstavili in skoraj v celoti potrdili pri svoji raziskavi, se lahko oblikuje naprednejši strukturni model. Ta ima lahko za izhodišče

prikazani model, potrjen pa je lahko z drugačnimi statističnimi metodami. Tako lahko v prihodnje pride do splošno veljavnega modela spletnega komuniciranja.

Svetovni splet je dokaj novo okolje, ki je pod vplivom demografskih dejavnikov. Pri izdelavi naloge smo se srečali z določenimi ljudmi, ki so izrecno proti internetu in ga ne mislijo uporabljati. V Sloveniji je kar nekaj območij, kjer še nimajo interneta; govorimo o digitalnem razkoraku. Tehnologija se iz dneva v dan spreminja in to neposredno vpliva na stališča in mnenja posameznikov. Vse te dejavnike bi bilo potrebno periodično spremljati ter na podlagi rezultatov prilagoditi ponudbo vsebin, poskrbeti za pereča vprašanja in pospešiti nadaljnji razvoj interneta.

7 SKLEP

V zadnjih nekaj letih je moč opaziti stagnacijo interneta in telekomunikacijskega sektorja. Kljub temu bo spletno poslovanje nadaljevalo z rastjo in poslovne spletne strani bodo pomemben komunikacijski kanal. Še vedno pa ostajajo področja zasebnosti, varnosti in zaupanja, tako z vidika posameznika kot tudi podjetja, upravičena skrb in posledično tudi ovira za nadaljnjo rast interneta.

Spletna podjetja so začela izkoriščati oziroma uporabljati nove tehnologije za potrebe zbiranja, obdelave in preučevanja navad ter lastnosti spletnih uporabnikov, le-ti pa so postali zaskrbljeni glede uporabe podatkov, njihovega obdelovanja in možnosti prenosa v povezane informacijske sisteme (European Commision, 2004). V medijih se pojavlja vedno več člankov, ki podajajo dvom o varnosti na internetu (na primer: širjenje virusov in napadi hekerjev), s čimer pa slabšajo že tako nizko zaupanje spletnih uporabnikov, predvsem kar se tiče spletnih nakupov (Consumer Union, 2002). Kot primer navajamo podatke študije, ki jo je pripravil Hoffman et al. (1999). Ugotovil je, da več kot 40 odstotkov spletnih nakupovalcev meni, da je njihova zasebnost ogrožena. 45 odstotkov vprašanih je prepričanih, da so zakoni preohlapni in njihovo izvajanje ni dosledno. Skrb za morebitno pomanjkanje zasebnosti pri opravljanju spletnih transakcij postaja, zaradi izgube nadzora nad uporabo osebnih podatkov, vedno večja ovira pri širjenju spletnega poslovanja.

Ljudje imajo različne interese, ki opredeljujejo količino in vrsto informacij, ki jih želijo deliti z zunanjim svetom, vendar pa se ob vsem tem pretoku informacij dostikrat zgodi, da je ogrožena elektronska zasebnost. Na eni strani nevarnost predstavljajo nekateri načini zbiranja podatkov, na drugi strani pa nevarnost predstavljajo nekatere storitve interneta, pri katerih gre za izmenjavo določenih podatkov in informacij. Večina nevarnosti za zlorabo posameznikove elektronske zasebnosti izhaja iz dejavnikov, ki jih omogoča sodobna informacijska tehnologija. Posegi v zasebnost in osebne podatke lahko pomenijo ogromno izgubo, posledično pa materialno škodo tako za organizacijo kot tudi upravljavca, ki osebno odgovarja za nastalo škodo. Ozaveščen uporabnik lahko še pred novimi tehnološkimi zaščitami sproži odziv na nevarnosti v internetnem okolju.

Potrebno se je zavedati, da je varnost spremenljivka toka in ne stanja. Če je podjetje danes varno, še ne pomeni, da bo varno tudi jutri. Seveda pa je treba imeti pred očmi tudi dejstvo, da upravljavec spletne strani ne more zagotavljati varnosti v samem računalniku uporabnika. Zato ni dovolj, če za varnost pri spletni izmenjavi podatkov skrbi le upravljavec, temveč mora za varnost poskrbeti tudi uporabnik. V prihodnosti se pričakuje vedno večja grožnja s strani interneta, zato je treba temu področju posvetiti veliko pozornost. Poskrbeti bo potrebno za neprestano izobraževanje in seznanjanje z novimi grožnjami, da bomo kos vedno novim napadom, ki pretijo z interneta. Vendar pa samo tehnična znanja, brez osveščanja uporabnikov, ne bodo zadostovala.

Mnenje je, da se bo zaskrbljenost glede varnosti in možnih zlorab pri uporabi interneta zmanjšala, ko bodo posamezniki in organizacije verjeli, torej zaupali, da so spletne strani varne. Eden izmed ključnih dejavnikov, ki prispeva k pomanjkanju zaupanja, je nizka stopnja zaznane varnosti. Menimo, da sta splošno zaupanje v varnost osebnih podatkov in nenazadnje plačevanje prek interneta tista dejavnika, ki pomembno vplivata na njun osnovni partnerski odnos. Problem zaupanja na internetu je dvojen: uporabnik, ki nastopa v vlogi plačnika oziroma dajalca podatkov, mora verjeti, da bo upravljavec spletne strani izpolnil dano obljubo, upravljavec, ki nastopa v vlogi prejemnika plačila in/ali skrbnika informacij, pa mora verjeti, da bo uporabnik izpolnil dano obljubo. Oba pa morata verjeti, da je izmenjava podatkov prek interneta varna.

Na podlagi proučevanja ustrezne literature in izkušenj v praksi smo zastavili raziskavo, v kateri smo želeli doumeti in pojasniti dejavnike zaupanja. Namen raziskave je pojasniti problematiko povezave med zaupanjem, zasebnostjo in varnostjo na internetu. Zanimala nas je predvsem zveza med naslednjimi dejavniki: izkušnje na internetu, zaznavanje varnosti, zaupanje v spletno stran, zvestoba spletni strani in zasebnost na spletni strani.

Z raziskavo smo želeli ugotoviti, ali lahko na osnovi spremljanja in analiziranja zaznavanja varnosti in zasebnosti nakažemo možnosti za krepitev zaupanja v internet. Rezultati raziskave so pokazali, da imata oba dejavnika pozitiven vpliv na zaupanje v internet. Z analizo prispelih odgovorov smo ugotovili, da izkušnje na internetu pozitivno vplivajo tako na konstrukt zasebnosti kot tudi na zaznavanje varnosti. Slednji spremenljivki nadalje pozitivno vplivata na stopnjo zaupanja in ta je skupaj s konceptom varnosti v pozitivni povezavi z zvestobo spletni strani.

Glede na rezultate, ki so potrdili vpliv zasebnosti in varnosti pri ustvarjanju zaupanja na internetu, predlagamo spletnim upravljavcem, da opravijo podrobnejše raziskave, v katere naj uvrstijo tudi tržne faktorje, s pomočjo katerih bodo dobili pravo predstavo o obiskovalčevih stališčih in tendencah glede spletnih nakupov. Na ta način bodo lahko proučili zadovoljstvo svojih kupcev, poiskali vzroke morebitnega nezadovoljstva, preverili možnosti ponovnega nakupa in nenazadnje tudi ustrezno ukrepali.

LITERATURA

1. Acar Tolga, Michener R. John: Risks in Features vs. Assurance, CACM Inside Risks, [URL:http://www.csl.sri.com/users/neumann/insiderisks.html], 2002.
2. Achrol S. Ravi, Kotler Philip: Marketing in the Network Economy. Journal of Marketing, vol. 63, št. 4, 1999. str. 146–163.
3. Ajzen Icek, Fishbein Martin: Understanding Attitudes and Predicting Social Behavior. Prentice-Hall, Englewood Cliffs, 1980. 278 str.
4. Ajzen Icek: The theory of planned behavior. Organizational Behavior and Human Decision Processes, vol. 50, 1991. str. 179–211.
5. Anžič Andrej: Mednarodni terorizem - varnostni izziv in dileme. Teorija in praksa, letnik 39, št. 3, [URL:http://dk.fdv.uni-lj.si/tip/tip20023Anzic.pdf], 2002. str. 454–466.
6. Assael Henry: Consumer Behaviour and Marketing Action. PWS-Kent, Boston : 1992. 746 str.
7. Bachmann Reinhard: Trust and power as means of coordinating the internal relationships of the organization. Nooteboom Bart, Six Frederique, ur., The Trust Process in organization. Cheltenham. UK, Northampton : Edward Elgar, 2003. str. 58–74.
8. Basle Andreja: Nemarno upravljanje osebnih podatkov je lahko drago. Ljubljana : Finance, št. 218/2006, [URL:http://www.finance-on.net/?MOD=show&id=167957&src=pj141106], objavljeno: 14. 11. 2006.
9. Batagelj Zenel: CRM te opazuje ... Ljubljana: Delo revije, Moj mikro, št. 1, Ljubljana : 2004. str. 7–15.
10. BBC: Britain is 'surveillance society'. United Kingdom : BBC, [URL:http://news.bbc.co.uk /2/hi/uk_news/6108496.stm], 19. 11. 2006.
11. Berčič Boštjan, Bojanec Anton, Krkoč Peter, Mrhar Peter, Patru Primož, Šinigoj Aleksander, Valenčič Iztok: Ukrepi v primeru informacijskih nesreč. Inštitut Za Informacijsko Varnost, Šempeter pri Gorici : 2003. str. 124–126.
12. Berčič Boštjan: SPAM na sodišču. Sistem, Ljubljana : Monitor, oktober 2006. str. 8–10.
13. Bergstein Heather, Estelami Hooman: A survey of emerging technologies for pricing newto-the-world products. Journal of Product & Brand Management, št. 11, Santa Barbara : 2002. str. 303–319.
14. Bertoncelj Brane: Psihosocialni vidiki zagotavljanja varnosti računalniško podprtega informacijskega sistema. Doktorska disertacija. Ljubljana : Fakulteta za družbene vede, 2000. 381 str.
15. Bitting Elijah, Ghorbani A. Ali: Protecting e-commerce agents from defamation. Electronic Commerce Research and Applications, Vol. 3, 2004. str. 21–38.
16. Bračun Franc: Zaupanje v elektronsko plačevanje: raziskava v praksi. Organizacija 36 (3), Kranj : Moderna organizacija, marec 2003. str. 152–161.
17. Bračun Franc: Zaupanje v sistem elektronskega poslovanja: teoretični model dejavnikov zaupanja v plačevanje prek interneta. Organizacija 35 (3), Kranj : Moderna organizacija, marec 2002. str. 144–151.

18. Brynjolfsson Erik, Kahin Brian (eds.): Understanding the Digital Economy. Massachusetts : Cambridge, The MIT Press, 2000. 401 str.
19. Cetin Simon: Iprom v preteklem letu posredoval 900 milijonov spletnih oglasov. Ljubljana : Iprom, [URL:http://www.iprom.si/cgi-bin/novica.cgi?id=60], objavljeno: 17. 01. 2005.
20. Cheskin Research: E-commerce Trust Study. [URL:http://www.cheskin.com/p/ar.asp?mlid=7&arid=40&art=0], 2000.
21. Choi Soon-Yong, Whinston Andrew B.: The Internet Economy: Technology and Practice. Austin (Texas): SmartEcon Publishing, 2000. 356 str.
22. Churchill A. Gilbert, Jr.: Marketing Research. Methodological Foundations. Fifth Edition. Dryden : The Dryden Press, 1991. 1070 str.
23. Compagno Cristiana: Il management della qualità: dagli standard al knowledge management. Torino : UTET libreria, 1999.
24. Consumers Union: A Matter of Trust: What Users Want from Web Sites. Results of National Survey of Internet Users for Consumer WebWatch. Consumers Union, San Francisco, CA : [URL:http://www.consumerwebwatch.org/news/report1.pdf], 2002.
25. Culnan J. Mary, Armstrong K Pamela: Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. Organization Science, Vol. 10, No. 1, 1999. str. 104–115.
26. Cunningham Peter, Fröschl Friedrich: Electronic Business Revolution. Berlin : Springer, 1999. 236 str.
27. Čebulj Janez: Varstvo informacijske zasebnosti v Evropi in Sloveniji. Ljubljana : Inštitut za javno upravo pri Pravni fakulteti v Ljubljani, 1992. 165 str.
28. De Vos Henk, Wielers Rudi: Calculativeness, trust and the reciprocy complex. Nooteboom Bart, Six Frederique, ur., The Trust Process in organization. Cheltenham. UK, Northampton : Edward Elgar, 2003. str. 75–104.
29. Djurdjič Vladimir: Spyware: nadloga ali nevarnost? Sistem. Ljubljana : Monitor, 2004. str. 20–22.
30. Doney M. Patricia, Cannon P. Joseph: An examination of the nature of trust in the buyer-seller relationship. Journal of Marketing, Vol. 51, 1997. str. 35–51.
31. Dong-Her Shih, Hsiu-Sen Chiang, Chun-Yuan Chan, Lin Binshan: Internet security: malicious e-mails detection and protection. Industrial Management & Data Systems, Vol. 104, No. 7, 2004. str. 613–623.
32. Eckel George, Steen William: Intranet Working. Indianapolis, USA : New Riders Publishing, 1996. 472 str.
33. eMarketer.com: The Mystery of Spyware, Part II, [URL:http://www.emarketer.com/Article.aspx?1003457], 23. 7. 2006.
34. Facault Michel: Nadzorovanje in kaznovanje. Ljubljana : Delavska enotnost, 1984. 324 str.
35. Forcht A. Karen: Computer security management. Cambridge : International Thomson publishing company, 1994. 486 str.
36. Friedenberg Mrk: Big Brother has arrived in Google. The Daily Collegian, [URL:http://www.bgnews.com/home/index.cfm?event=displayArticlePrinterFriendly&uStory_id=e47fadb8-74a1-4af5-8244-10a4a3d85657], objavljeno: 27. 04. 2005.

37. Fuchs Keaton: Hecers` Playground. The Oklahoma Daily, [URL:http://www.oudaily.com/vnews/display.v?TARGET=printable&article_id=426f9e6185fb8], 27. 07. 2006.
38. Fung Raymond, Lee Matthew: EC-trust (trust in electronic commerce): Exploring the antecedent factors. 5th Americas Conference on Information Systems, Milwaukee : Avgust 1999. Vol. 13-15, str. 517–519.
39. Ganesan Shanaker: Determinants of long-term orientation in buyer-seller relationship. Journal of Marketing, Vol. 58, 1994. str. 1–19.
40. Gartner: Gartner's Top Predictions for IT Organizations and Users, 2007 and Beyond. [URL:http://www.gartner.com/DisplayDocument?ref=g_search&id=498768&subref=simplesearch], objavljeno: 1. 12. 2006, 25 str.
41. Gefen David, Karahanna Elena, Straub W. Detmar: Trust and TAM in online shopping: an integrated model, MIS Quarterly, Vol. 27, No. 1, 2003.
42. Gefen David: E-commerce: the role of familiarity and trust, Omega 28, No. 6, 2000. str. 725–737.
43. Goldhaber Michael H.: The Attention Economy and the Net. 2nd Draft version of a talk presented at the conference on "Economics of Digital Information". Massachusetts : Cambridge, 23–26. januar, 1997. [URL:http://www.well.com/user/mgoldh/AtEcandNet.html].
44. Goldman Arieh: The shopping style explanation for store loyalty. Journal of Retailing, Vol. 53, 1978. str. 33–46.
45. Gordon A. Lawrence, Loeb P. Martin, Lucyshyn William, Richardson Robert: Computer Crime and Security Survey. San Francisco : Computer Security Institute Publications, 2004.
46. Greene Tim: Forum warns of hidden DDoS legal liability. Network World, [URL:http://www.nwfusion.com/archive/2000/108677_10-02-2000.html], 2000.
47. Griffin Jill: Customer loyalty: how to earn it, how to keep it. San Francisco: Jossey-Bass Publishers, 1995. 272 str.
48. Grizold Anton: Varnostna paradigma v mednarodnih odnosih. Človek, država in vojna. Ljubljana : Fakulteta za družbene vede, 2001. str. 83–161.
49. Gundlach Gregory, Murphy E. Patric: Ethical and legal foundations of relational marketing exchanges. Journal of Marketing, Vol. 57, 1993. str. 35–46.
50. Harris Interactive: Privacy On and Off the Internet: What Consumers Want. [URL:http://www.aicpa.org/download/webtrust/priv_rpt_21mar02.pdf], 2002.
51. Hayden Michael: National information assurance glossary, Committee on national Security Systems, NSA, [URL:http://www.cnss.gov/ Assets/pdf/cnssi_4009.pdf], 2003.
52. Henderson David: David Cancel at Open Data 2007 - Your ISP may be selling your web clicks. Blog, [URL:http://www.blogs.dhenderson.com/David_Henderson/?p=244], objavljeno: 15. 3. 2007.
53. Hesseldahl Arik: Big Brother Isn't Here Yet. Forbes, [URL:http://www.forbes.com/technology/2005/05/06/cx_ah_0506diglife.html], objavljeno: 06. 05. 2005.
54. Hill Niegel, Brierley John, MacDougall Rob: How to measure customer satisfaction. Great Britain : MPG Books Ltd, 2004. 151 str.

55. Hoffman L. Donna, Novak P. Thomas, Marcos Peralta: Building consumer trust online. Communications of the ACM, Vol. 42, No. 4, [URL:http://sloan.ucr.edu/blog/uploads/papers/Building%20Consumer%20Trust%20in%20Online%20Environments%20%20The%20Case%20for%20Information%20Privacy%20%5BHoffman,%20Novak,%20Marcos%20Peralta%20-%201998%5D.pdf], 1999. str. 80–85.
56. Houle J. Kevin, Weaver M. George: Trends in Denial of Service Attack Technology v 1.0. New York : CERT Coordination Center, 2001. 21 str.
57. Houston A. Douglas: Trust in the networked economy: doing business on web time. Business Horizons, Vol. 44, No. 2, 2001. str. 38–44.
58. Hudoklin Alenka, Stadler Alenka: Varno elektronsko trgovanje s pomočjo kreditnih kartic. Organizacija 30, Kranj : Moderna organizacija, 1997. str. 288–293.
59. Jakupović Esad: Cena nezaščitenosti? Maribor : Kapital št. 338, 2005. str. 66.
60. Janelle Chantelle: Internet users concerned with security consider alternate browsers. WorldNow, [URL:http://www.wistv.com/global/story.asp?s=3269344&ClientType=Printable], objavljeno: 27. 04. 2005.
61. Jarvenpaa L. Sirkka, Knoll Kathleen, Leidner E. Dorothy: Is anybody out there? The implication of trust in global virtual teams. Journal of Management Information Systems (JMIS) Vol. 14, No. 4, 1998. str. 29–64.
62. Jelušič Ljubica: Legitimnost sodobnega vojaštva. Knjižna zbirka Teorija in praksa, Ljubljana : Fakulteta za družbene vede, 1997.
63. Jerman-Blažič Borka, Tomaž Klobučar, Zoran Perše: Elektronsko poslovanje na internetu. Ljubljana : Gospodarski Vestnik, 2001. 206 str.
64. Kavran Darko: Puresight - Zaščita otrok in poslovnega okolja pred neprimernimi spletnimi vsebinami. Real security info, Revija za računalniško varnost. št. 3, 2004. str. 23–24.
65. Kim Chan W., Mauborgne Renée: Fair Process: Managing in the Knowledge Economy. Harvard Business Review, vol. 81, No. 1, 2003. str. 127–136.
66. Kolsaker Ailsa, Payne Claira: Engendering trust in e-commerce: a study of gender-based concerns. Marketing Intelligence & Planning, Vol. 20, No. 4, 2002. str. 206–214.
67. Koprowski J. Gene, The Web: Search engine privacy threats. United Press International, [URL:http://www.wpherald.com/print.php?StoryID=20050427-101719-3430r], objavljeno: 27. 04. 2005.
68. Kostanjšek Eva, Batagelj Zenel: Nekateri vidiki merjenja zadovoljstva potrošnikov. CATI Center-telefonsko raziskovanje. [URL:http://www.crm-forum.com/library/art/art-110/art-110.html], 2000.
69. Kotler Philip: Marketing management – trženjsko upravljanje: analiza, načrtovanje, izvajanje in nadzor. Ljubljana : Slovenska knjiga, 1996. 832 str.
70. Koufaris Marios, Hampton-Sousa William: Customer trust online. Examining the role of the experience with the web site. CIS working papers series [URL:http://cisnet.baruch.cuny.edu/papers/cis200205.htm], 2002.
71. Kovač Jure, Jesenko Manca: Instrumentalni pomen zaupanja v organizaciji. Zaupanje v in med organizacijami (združbami). Ljubljana : Fakulteta za organizacijske vede, Ekonomska fakulteta, Zveza organizatorjev Slovenije, 2004. str. 41–47.

72. Kovačič Matej: Zasebnost na internetu. Ljubljana : Mirovni inštitut, Inštitut za sodobne družbene in politične študije, Zbirka Politike, 2003. 111 str.
73. Kumar Vineet, Aaker A. David, Day S. George: Essentials of Marketing Research. New York : John Wiley & Sons, 1999. 623 str.
74. Lane Christel: Theories and Issues in the Study of Trust. Lane Christel, Trust within and between organizations: Conceptual Issues and Empirical Applications. Oxford : Oxford University Press, 1998. 334 str.
75. Larzelere E. Robert, Huston L. Ted: The dyadic trust scale: toward understanding interpersonal trust in close relationships. Journal of Marriage and the Family, 1980. str. 595–604.
76. Lavrenčič Marko: Etičnost trženja z digitalnimi tehnologijami. Diplomsko delo. Ljubljana : Fakulteta za družbene vede, 2004. str. 4.
77. Lawrence Elaine, Corbitt Brain: Internet Commerce: Digital Models for Business (2nd edition). New York : John Wiley & Sons, 2000. 360 str.
78. Layder Derek: Understanding social theory. London : Sage Publications, 1994. 230 str.
79. Lee Geun Ho: Do electronic marketplaces lower the price of goods? Communications of the ACM, Vol. 41, No. 1, 1998. str. 73–80.
80. Lenhart Amanda: Who's not online: 57 per cent of those without Internet access say that thay do not plan to log on. Pew Internet and American Life Project, [URL:http:// www.pewinternet.org/pdfs/Pew_Those_Not_Online_Report.pdf], 2000.
81. Linn Allison: Microsoft to Launch Paid Search Technology. [URL:http://story.news.yahoo.com/news?tmpl=story&cid=528&e=1&u=/ap/20050316/ap_on_bi_ge/microsoft_paid_search], objavljeno: 16. 3. 2005.
82. Liu Chang, Arnett P. Kirk: Raising a red flag on global WWW privacy policies. Journal of Computer Information Systems, XXXXIII (1), 2002. str. 117–127.
83. Lyman Jay: Symantec report puts corporations, consumers in crosshairs. Technewsworld, [URL:http://www.technewsworld.com/perl/story/33142.html], 2003.
84. Lyon David: The Electronic Eye. Cambridge : Polity Press, 1994. 270 str.
85. Marc Mojca: Analiza poslovanja podjetja v pogojih elektronskega poslovanja. Magistrsko delo. Ljubljana : Ekonomska fakulteta, 2003. 108 str.
86. Marshall Edward M.: Building Trust at the Speed of Change: The Power of the Relationship-Based Corporation. New York : Amacom, 2000. 224 str.
87. Marshall Matt: New cookies much harder to crumble. Knight Ridder Newspapers, [URL:http://www.menafn.com/qn_print.asp?StoryID=CqM8oqeicq1bulunpt0Tjrvm], objavljeno: 27. 04. 2005.
88. Mavsar Mitja: Internet – tehnologija zaupanja. Izpitna naloga. Ljubljana : Fakulteta za družbene vede, 2003, str. 3.
89. Mayer Janez: Zaupanje kot pogoj za ustvarjalno sodelovanje, Zaupanje v in med organizacijami (združbami). Kranj : Fakulteta za organizacijske vede, Ekonomska fakulteta, Zveza organizatorjev Slovenije, 2004. str. 57–63.
90. McDaniel George: IBM Dictionary of computing, New York : McGraw-Hill, 1994. 758 str.

91. McKeown Patrick G.: Information Technology and the Networked Economy. Fort Worth : Harcourt College Publishers, 2001. 395 str.
92. Mcllroy Andrea, Barnett Shirley: Building customer relationship: do discount cards work? Managing Service Quality, Emerald Group Publishing Limited, Vol. 6, 2000. str. 347-355.
93. Možina Damjan: Varstvo osebnih podatkov na internetu – cookie: piškotek ali Veliki brat. Pravna praksa, informatika in pravo, št. 36–37, Ljubljana : Gospodarski vestnik, 2000. str. 23–29.
94. Možina Stane: Zaupanje v teamih in organizaciji. Zaupanje v in med organizacijami (združbami). Kranj : Fakulteta za organizacijske vede, Ekonomska fakulteta, Zveza organizatorjev Slovenije, 2004. str. 65–71.
95. Murphy B. Gregory in Blessinger A. Ashley: Perceptions of no-name recognition business to consumer e-commerce trustworthiness: the effectiveness of potential influence tactics. Journal of High Technology Management Research, Vol. 14, No. 1, 2003. str. 71–92.
96. Negroponte Nicholas: Being Digital. New York : First Vintage Books Edition, January 1996. 255 str.
97. Nielsen Jakob: Trust or Bust: Communicating Trustworthiness in Web Design. [URL:http://www.useit.com/alertbox/990307.html], 1999.
98. Nitke Marla: IAB/PwC release fourth-quarterd and fy 2006 internet ad revenue figures. [URL:http://www.iab.net/news/pr_2007_03_07.asp], objavljeno: 7. 3. 2007.
99. Odlazek Gregor: Zasebnosti ni, prebolite že enkrat. Ljubljana : Finance, št. 78, 2003. str.16.
100. Odlyzko Andrew: Economics, Psychology and Sociology of Security. Digital Security Center, University of Minnesota. [URL:http://www.dtc.umn.edu/~odlyzko/doc/econ.psych.security.pdf], 10. 11. 2006.
101. Pahor David: Bi radi zaslužili s prodajo po internetu? Podjetnik. Ljubljana : [URL:http://www.podjetnik.si/default.asp?ClanekID=210], objavljeno: 17. 06. 2003.
102. Pečovnik Marko: Zaupanje, organizacija in socialni kapital. Diplomsko delo. Ljubljana : Univerza v Ljubljani, Fakulteta za družbene vede, 2001. 66 str.
103. Pepelnjak Ivan, Bradeško Marjan: Varnost računalniških sistemov in elektronskih transakcij. Zbornik, Banke in tveganja. Portorož : Zveza ekonomistov Slovenije, 1997. str. 155–165.
104. Perše Zoran: Varstvo in zaščita osebnih podatkov pri elektronskem poslovanju. Ljubljana : Pravna praksa, št. 11–12, 2000. str. 5–28.
105. Peterson Shane: Guarding Information. Government Technology, [URL:http://www.govtech.net/news/story.print.php?id=93910], objavljeno: 06. 05. 2005.
106. Petrov Sabina: Internet del medijskega načrta. Finance, št. 236, Ljubljana : Časnik Finance objavljeno v tiskani izdaji: 2. 12. 2004.
107. Primožič Rok: Internet in pravica do zasebnosti. Specialistično delo. Ljubljana : Ekonomska fakulteta, 2005. 67 str.
108. Raab D. Charles: Privacy, democracy, information. The Governance of Cyberspace, London : Routledge, 1997. str. 155–174.

109. Radoš Škrt: Elektronsko poslovanje med podjetji. Sistem priloga revije Monitor, Ljubljana : 1999. str. 35–37.
110. Reuters: EU split over antiterror phone data logging rules. Reuters, [URL:http://www.computerworld.com/printthis/2005/0,4814,105120,00.html], objavljeno: 11. 07 .2005.
111. Rojšek Iča, Žabkar Vesna: Metode trženjskega raziskovanja: vodič po predmetu dodatek. Ljubljana : Ekonomska fakulteta, 1997. 34 str.
112. Ross Edward Alsworth: Social Control: a survey of the fundations of order. New York, London : The Macmillan Company, 1969. 463 str.
113. Rozman Rudi, Kovač Jure, Koletnik Franc: Management. Ljubljana : Gospodarski vestnik, 1993. 312 str.
114. Sahay Barrett: Understanding trust in supply chain relationships. Industrial Management & Data Systems, Vol. 103, No. 8, 2003. str. 553 – 563.
115. Sirdeshmukh Deepak, Singh Jagdip, Sabol Barry: Consumer trust, value, and loyalty in relational exchanges. Journal of Marketing, Vol. 66, No. 1, 2002. str. 15–37.
116. Sitkin B. Sim, Roth L. Nancy: Explaining the limited effectiveness of legalistic remedies for trust/distrust. Organization Science, Vol. 4, 1993. str. 367–392.
117. So W.C. May, Wong T.N. Danny, Sculli Domenic: Factors Affecting intentions to purchase via the internet. Industrial Management & Data Systems. Hong Kong : Faculty of Engineering, Vol. 105, No. 9, 2005. str. 1225–1244.
118. Stallings William: Network and Internetwork Security: Principles and Practice. New Jersey : Prentice Hall, 1995. 462 str.
119. Stone Merlin, Woodcock Neil, Machtynger Liz: Customer Relationship Marketing. London : Kogan Page, 2000. 190 str.
120. Struna Dejan: Spletno oglaševanje na osnovi vedenjskih vzorcev. Ljubljana : Iprom, [URL:http://www.iprom.si/cgi-bin/novica.cgi?id=58], objavljeno: 02. 11. 2004.
121. Surmacz Jon: Will You Pay More to Surf Safely, or Dump Internet Explorer? CXO Media, [URL:http://www.csoonline.com/talkback/092704.html], objavljeno: 28. 04. 2005.
122. Svete Uroš: Varnostne implikacije uporabe informacijsko-komunikacijske tehnologije. Doktorska disertacija, Ljubljana : Fakulteta za družbene vede, 2005.
123. Šalamon Brane: Nevarni internet. Maribor : Kapital, 09.02.2004, str. 60–62.
124. Šinigoj Aleksander, Turk Tomaž: Sodobno elektronsko poslovanje – varnostni vidiki. Dnevi slovenske informatike Portorož 1999. Zbornik posvetovanja. Ljubljana : Slovensko društvo informatika, 1999. str. 457–466.
125. Tapscott Don: The Digital Economy: Promise and Peril in the Age of Networked Intelligence. New York : McGraw – Hill, 1995. 342 str.
126. Taylor Nelson Sofres Interactive: Global Ecommerce Report 2002. [URL:http://www.tnsinfo.com/common/corporate/images/tns/GER2002FullReport.zip], 2002.
127. Tull Donald S., Hawkins Del I.: Marketing research. Measurement&Method. Sixth Edition. Caledonia : Carlisle Communications, 1993. 863 str.
128. Tyson Laura D'Andrea: Old Economic Logic in the New Economy. California Management Review, Vol. 41, No. 4, 1999. str. 8–16.

129. Ude Lojze: Pravno varstvo osebnih podatkov kot element pravice do zasebnosti: Ustavne podlage za varstvo zasebnosti in osebnih podatkov. Ljubljana : Podjetje in delo: revija za gospodarsko, delovno in socialno pravo, št. 5–6, 1996. str. 894–902.
130. UNDP - United Nations Development programme: Human development report. New York : [URL:http://hdr.undp.org/reports/global /1994/en/pdf/hdr_1994_ch2.pdf], 1994.
131. Vagaja Aleksandra: Z identifikacijo vedenjskega vzorca uporabnika interneta do pametnih in predvsem nemotečih oglaševalskih akcij. Finance, Ljubljana : Časnik Finance, [URL:http://www.finance-on.net/print.php?id=111684&tip=1], objavljeno: 04. 02. 2005.
132. Vagaja Aleksandra: Zasebnost na spletu: Prisluškujejo nam, mar ne? Finance, Ljubljana : Časnik Finance, [URL:http://www.finance-on.net/print.php?id=100155&tip=1], objavljeno: 04. 10. 2004.
133. Vehovar Vasja: Je slovenski trg za internet premajhen? Ljubljana : Fakulteta za družbene vede, 2000. [URL:http://www.ris.org/si/ris2000/novice/200000619.htm], 06. 07. 2001.
134. Verčič Dejan, Razpet Aleš, Samo Dekleva in Mitja Šlenc: International public relations and the Internet: Diffusion and Linkages. Journal of Communication Management, december 2000.
135. Vesel Patrick, Žabkar Vesna: Program zvestobe kupcev na primeru poslovnega sistema Mercator. Akademija MM-Slovenska znanstvena revija za trženje, VI / 10, 2003. str. 41–49.
136. Vidmar Tone: Računalniška omrežja in storitve. Ljubljana : Atlantis, 1997. 417 str.
137. Wang Huaiqing, Lee K. O. Matthew, Wang Chen: Consumer privacy concerns about internet marketing, Communications of the ACM, Vol. 41, 1998. str. 63–70.
138. Webster Frank: Theories of the Information Society. London : Routledge, 1995. 304 str.
139. Whitney O. John: The Trust Factor: Liberating Profits and Restoring Corporate Vitality. New York : McGraw-Hill, Inc., 1994. 235 str.
140. WorldNow: Prying Eyes. Special report, [URL:http://www.wtol.com/global/story.asp?s=3267815&ClientType=Printable], objavljeno: 28. 04. 2005.
141. Yousafzai Y. Shumaila, Pallister G. John, Foxall R. Gordon: A proposed model of e-trust for electronic banking, Technovation, Vol. 23, 2003. str. 847–860.
142. Zdovc Peter: Varna elektronska komunikacija. Ljubljana : Info SRC, glasilo št. 33, 2002. str. 8–9.
143. Zmagaj Peter: Internetni ponudnik ne bo odgovoren za vsebino. Ljubljana : Finance, št. 59, 2004. str. 10.
144. Zupan Lucija: Prestiž ali nujnost? Sistem. Ljubljana : Monitor, 2004. str. 10–11.
145. Žurej Jurij: Deset zapovedi varstva zasebnosti v svetu interneta. Pravna praksa, informatika in pravo, št. 1, Ljubljana : Gospodarski vestnik, 2001. str. 38–41.

VIRI

1. Banisar David, Davies Simon: Privacy & Human Rights. 1999, [URL:http://www.privacy-international.org/survey/index99.html], 23. 7. 2006.
2. CIB, Profile of the Internet Shopper. Study of Consumer Internet Barometer, CIB, [URL:http://www.conference-board.org/pdf_free/CIBpp.ppt], 2003.
3. Data Protection Working Party: Privacy on the Internet – An integrated EU Approach to On-line Data Protection. 2000, [URL:http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf], 20. 11. 2006.
4. Eurobarometer: Illegal and harmful content on the internet. EB60.2 – CC-EB 2004.1, 2004, [URL:http://ec.europa.eu/public_opinion/archives/ebs/ebs_203_comp_high.pdf], 18. 11. 2006.
5. European Commission: Issues relating to Business and Consumer E-commerce. Special Eurobarometer 60.0/ Wave 201, European Opinion Research Group, 2004.
6. FTC Report to Congress: Privacy online: fair information practices in the electronic marketplace. 2000, [URL:http://www.ftc.gov/os/2000/05/index.htm#22], 10. 10. 2006.
7. Informacijski pooblaščenec: [URL:http://www.ip-rs.si/], 10. 01. 2006.
8. Kazenski zakonik Republike Slovenije (Uradni list RS, št. 63/1994, 70/1994, 23/1999, 60/1999, 40/2004, 37/2005 in 17/2006).
9. Kovačič Matej: On-line slovarček statističnih pojmov. [URL:http://www.ljudmila.org/matej/statistika/mva.html], 2001.
10. Microsoft: [URL:http://www.microsoft.com], 19. 11. 2006.
11. Ministrstvo za informacijsko družbo: Predstavitev Ministrstva: Zakaj Ministrstvo? Ljubljana : 2000 [URL:http://mid.gov.si/mid/mid.nsf], 21. 11. 2006.
12. Ministrstvo za informacijsko družbo: Republika Slovenija v informacijski družbi. Ljubljana : 2003 [URL:http://mid.gov.si/], 5. 12. 2006.
13. Ministrstvo za visoko šolstvo, znanost in tehnologijo: Strategija razvoja informacijske družbe v Republiki Sloveniji si2010. Ljubljana : 2007 [URL:http://www.mvzt.gov.si/fileadmin/mvzt.gov.si/pageuploads/pdf/informacijska_druzba/Strategija_si2010.pdf], 9. 8. 2007.
14. RIS, Internat in slovanska država, Center za metodologijo in informatiko, Fakulteta za družbene vede, Ljubljana : [URL:http://www.ris.org/uploadi/editor/1180437233 InternetInSlovenskaDrzava2006.pdf], 10. 08. 2007.
15. SIBIS Pocket Book 2002/03: [URL:http://www.empirica.biz/sibis/files/Sibis_Pocketbook _updt.pdf], 20. 12. 2006.
16. Spletni portal Najdi.si: [URL:http://www.najdi.si], 17. 11. 2006.
17. Taylor Nelson Sofres Interactive: Global Ecommerce Report 2002. 2002, [URL:http://www.tnsinfo.com/common/corporate/images/tns/GER2002FullReport.zip], 17. 7. 2006.
18. Ustava Republike Slovenije (Uradni list, št. 33/1991-I, 42/1997, 66/2000, 24/2003, 69/2004 in 68/2006).

19. Wired News: Ads That Know What You Want. [URL:http://www.wired.com/news/print/0, 1294,67365,00.html], 28. 8. 2006.
20. Zakon o elektronskem poslovanju in elektronskem podpisu, ZEPEP (Uradni list RS, št. 57/2000, 30/2001).
21. Zakon o elektronskem poslovanju na trgu, ZEPT (Uradni list RS, št. 61/2006).
22. Zakon o elektronskih komunikacijah, ZEKom (Uradni list RS, št. 43/2004 in 86/2004).
23. Zakon o telekomunikacijah, ZTel (Uradni list RS, št. 30/2001 in 110/2002-ZGO-1).
24. Zakon o varstvu osebnih podatkov, ZVOP (Uradni list RS, št. 59/2001).
25. Zakon o varstvu osebnih podatkov, ZVOP-1 (Uradni list RS, št. 86/2004 in 113/2005).
26. Zakon o varstvu potrošnikov, ZVPot (Uradni list RS, št. 20/1998, 23/1999, 110/2002 in 51/2004).

PRILOGE

PRILOGA 1: SPLETNI VPRAŠALNIK

Spoštovani!

Sem Rok Primožič, podiplomski študent magistrskega programa na Ekonomski fakulteti v Ljubljani. Vabim vas, da sodelujete v raziskavi, ki proučuje pomen zasebnosti, varnosti in zaupanja na internetu. Rezultati raziskave bodo uporabljeni v magistrski nalogi katero pripravljam pod mentorstvom dr. Tanje Dmitrović in dr. Jurija Jakliča.

Ker je vaše mnenje zelo pomembno, bom zelo vesel, če si boste lahko vzeli 10 minut časa in izpolnili anketo.

Za morebitne težave pri izpolnjevanju ankete, vam bom v pomoč na telefonski številki: 01 563 43 30 in na elektronskem naslovu rok.primozic@zaslon-telecom.si.

Začeli bomo z nekaj splošnimi vprašanji o internetu.

(1=sploh ne, 2=ne, 3=niti ne niti sem, 4=sem, 5=zelo sem)	
Ali ste zaskrbljeni glede varnosti na internetu?	1 2 3 4 5
Ali ste zaskrbljeni glede varnosti pri opravljanju spletnega nakupa ali elektronskega bančništva?	1 2 3 4 5
Kaj je za vas bolj pomembno: praktičnost ali zasebnost?	Praktičnost zasebnost
Ali ste pripravljeni uporabiti vašo kreditno kartico za plačilo spletnega nakupa?	da ne
O: da -> naslednje vprašanje	
O: ne -> Zakaj ne?	*tekst*
Kako pogosto ste uporabili internet, v zadnjih šestih mesecih, za spletne nakupe?	vsak dan / vsaj 1x na teden / vsaj 1x na mesec / manj kot enkrat na mesec / nikoli

Vpišite naslov spletne strani, ki jo pogosto uporabljate in je od vas zahtevala osebne podatke (ime, priimek, e-naslov, …).	*tekst*

Vprašanja, ki sledijo, se nanašajo na spletno stran, katere ime ste navedli v predhodnem vprašanju.

Na lestvici 1-5 označite kakšno je vaše stališče do varnosti na spletni strani *(vpisali ste jo zgoraj)*, kjer 1 pomeni »sploh se ne strinjam«, 5 pa »popolnoma se strinjam«.

(1=sploh se ne strinjam, 2=ne strinjam se, 3=niti se ne strinjam niti se strinjam, 4=strinjam se, 5=popolnoma se strinjam)	
Upravljavci spletne strani *(vpisali ste jo zgoraj)* imajo orodja s katerimi zagotavljajo varen vnos in prenos podatkov s strani uporabnikov.	1 2 3 4 5
Upravljavci spletne strani *(vpisali ste jo zgoraj)* kažejo veliko skrb za varnost vseh transakcij.	1 2 3 4 5
Upravljavci spletne strani *(vpisali ste jo zgoraj)* imajo na voljo dovolj tehnične opreme s pomočjo katere bodo zagotovili, da drugi nepooblaščeni subjekti ne bodo imeli dostopa do osebnih podatkov.	1 2 3 4 5
Menim, da je spletna stan *(vpisali ste jo zgoraj)*, ko se povežem nanjo, avtentična.	1 2 3 4 5
Upravljavci spletne strani *(vpisali ste jo zgoraj)* posedujejo dovolj tehničnih sredstev s pomočjo katerih bodo zagotovili, da podatki, ki jih pošiljam, ne bodo prestreženi s strani tretjih oseb.	1 2 3 4 5
Predani osebni podatki ne bodo spremenjeni s strani tretjih oseb.	1 2 3 4 5

Sledijo vprašanja o zasebnosti na internetu. Prosim, da ponovno označite, v kolišni meri se strinjate z naslednjimi trditvami.

(1=sploh se ne strinjam, 2=ne strinjam se, 3=niti se ne strinjam niti se strinjam, 4=strinjam se, 5=popolnoma se strinjam)	
Upravljavci spletne strani *(vpisali ste jo zgoraj)* obveščajo uporabnike o vrsti osebnih podatkov, ki se bodo zbirali in hranili.	1 2 3 4 5
Upravljavci spletne strani *(vpisali ste jo zgoraj)* so pojasnili pomen zbiranja osebnih podatkov.	1 2 3 4 5
Upravljavci spletne strani *(vpisali ste jo zgoraj)* so razložili namen uporabe osebnih podatkov.	1 2 3 4 5
Zbrani osebni podatki ne bodo predani brez mojega dovoljenja tretjim osebam.	1 2 3 4 5
Upravljavci spletne strani *(vpisali ste jo zgoraj)* se trudijo zagotoviti in ohraniti točne podatke o meni.	1 2 3 4 5
Upravljavci spletne strani *(vpisali ste jo zgoraj)* so mi ponudili možnost preklica predaje osebnih podatkov tretjim osebam.	1 2 3 4 5
Upravljavci spletne strani *(vpisali ste jo zgoraj)* imajo postopke s pomočjo katerih preverjajo in popravljajo morebitne nepravilne podatke o posameznikih.	1 2 3 4 5
Upravljavci spletne strani ne pošiljajo brez naslovnikovega dovoljenja reklamnih sporočil preko elektronske pošte.	1 2 3 4 5
Menim, da se upravljavci spletne strani *(vpisali ste jo zgoraj)* trudijo ohraniti moje osebne podatke izven dosega nepooblaščenih posameznikov.	1 2 3 4 5

Naslednji sklop vprašanj obravanava vaše zaupanje do spletne strani *(vpisali ste jo zgoraj)*.

(1=sploh se ne strinjam, 2=ne strinjam se, 3=niti se ne strinjam niti se strinjam, 4=strinjam se, 5=popolnoma se strinjam)	
Menim, da upravljavci spletne strani *(vpisali ste jo zgoraj)* izpolnijo zadane obveze.	1 2 3 4 5
Menim, da lahko zaupam izjavi o varovanju zasebnosti, ki jo navajajo upravljavci spletne strani *(vpisali ste jo zgoraj)*.	1 2 3 4 5
Menim, da se upravljavci spletne strani zavzemajo za sedanja in prihodnja zanimanja svojih uporabnikov.	1 2 3 4 5
Menim, da upravljavci spletne strani *(vpisali ste jo zgoraj)* ne bi namerno naredili nečesa, kar bi uporabnikom povzročilo škodo.	1 2 3 4 5
Menim, da zasnova spletne strani in ponudba upoštevata potrebe in želje njenih uporabnikov.	1 2 3 4 5
Menim, da so upravljavci spletne strani *(vpisali ste jo zgoraj)* dovzetni za potrebe uporabnikov.	1 2 3 4 5
Menim, da imajo upravljavci spletne strani *(vpisali ste jo zgoraj)* dovolj razpoložljivih sredstev za nadaljnji razvoj.	1 2 3 4 5
Menim, da spletna stran *(vpisali ste jo zgoraj)* pozna svoje uporabnike toliko dobro, da lahko prilagodi ponudbo storitev oziroma produktov njihovim potrebam.	1 2 3 4 5

Za konec sledi samo še nekaj trditev, ki obravnavako zvestobo do spletne strani in za katere želim, da mi poveste, v kolikšni meri se z njimi strinjate.

(1=sploh se ne strinjam, 2=ne strinjam se, 3=niti se ne strinjam niti se strinjam, 4=strinjam se, 5=popolnoma se strinjam)	
Spletno stran *(vpisali ste jo zgoraj)* obiskujem bolj pogosto, kot druge spletne strani s podobno vsebino.	1 2 3 4 5
Imam pozitivno mnenje o slednji spletni strani in sem ga tudi pripravljen deliti z drugimi.	1 2 3 4 5
Spletno stran *(vpisali ste jo zgoraj)* nameravam obiskati ponovno.	1 2 3 4 5
To je spletna stran na kateri se zadržim najdlje časa v primerjavi z drugimi stranmi s podobno vsebino.	1 2 3 4 5
To je moja najljubša spletna stran v primerjavi z drugimi stranmi s podobno vsebino.	1 2 3 4 5

To je skoraj vse. Za analize bi potrebovali še nekaj podatkov o vas, ki bodo seveda ostali anonimni.

Demografski podatki	
Spol	moški ženski
Starost	do 17 / 17-20 / 21 – 25 / 26 – 30 / 31 – 35 / 36 –

	40 / 41 – 45 / 46 – 50 / več kot 50
Dokončana izobrazba	osnovnošolska ali manj / srednješolska, poklicna / višješolska, visokošolska, univerzitetna / magisterij, doktorat

Pošlji anketo Začni znova

Zahvaljujem se za vašo pozornost in pripravljenost za sodelovanje.

PRILOGA 2: OPISNE STATISTIKE

Tabela 1: Opisne statistike za Q1 in Q2

ID	Trditev	Aritmetična sredina	Standardni odklon	Koeficient asimetrije	Koeficient sploščenosti
Q1	Ali ste zaskrbljeni glede varnosti na internetu?	3,38	0,968	-0,357	-0,157
Q2	Ali ste zaskrbljeni glede varnosti pri opravljanju spletnega nakupa ali elektronskega bančništva?	3,68	1,131	-0,605	-0,469

Vir: Anketa, 2007.

Tabela 2: Frekvence in odstotni deleži za 3. vprašanje (Kaj je za vas bolj pomembno: praktičnost ali zasebnost?)

Odgovor	Frekvenca	Odstotni delež
praktičnost	166	41,5
zasebnost	234	58,5
Skupaj	400	100

Vir: Anketa, 2007.

Tabela 3: Frekvence in odstotni deleži za 4. vprašanje (Ali ste pripravljeni uporabiti vašo kreditno kartico za plačilo spletnega nakupa?)

Odgovor	Frekvenca	Odstotni delež
da	228	57
ne	172	43
Skupaj	400	100

Vir: Anketa, 2007.

Peto vprašanje (Zakaj ne? oziroma Zakaj niste pripravljeni uporabiti vašo kreditno kartico za plačilo spletnega nakupa?), ki je postalo aktivno le v kolikor je anketiranec na predhodnega odgovoril nikalno, nisem uporabil v analizi. S slednjim podvprašanje sem želel pridobiti seznam vzrokov izogibanja spletnim nakupom.

Tabela 4: Frekvence in odstotni deleži za 6. vprašanje (Kako pogosto ste uporabili internet, v zadnjih šestih mesecih, za spletne nakupe?)

Odgovor	Frekvenca	Odstotni delež
vsak dan	15	3,8
vsaj enkrat na teden	16	4
vsaj enkrat na mesec	97	24,3
manj kot enkrat na mesec	151	37,8
nikoli	121	30,3
Skupaj	400	100

Vir: Anketa, 2007.

Sedmo vprašanje (Vpišite naslov spletne strani, ki jo pogosto uporabljate in je od vas zahtevala osebne podatke (ime, priimek, e-naslov, …) tudi nisem uporabil v analizi. Postavil sem ga kot

pomožno vprašanje, da bi si skozi celotno reševanje vprašalnika lažje zapomnili, za katero spletno stran odgovarjajo na vprašanja.

Tabela 5: Opisne statistike za postavljene trditve oz. spremenljivke konstrukta varnosti

ID	Trditev	Aritmetična sredina	Standardni odklon	Koeficient asimetrije	Koeficient sploščenosti
Q8	Upravljavci spletne strani (vpisali ste jo zgoraj) imajo orodja s katerimi zagotavljajo varen vnos in prenos podatkov s strani uporabnikov.	3,85	0,893	-0,836	1,066
Q9	Upravljavci spletne strani (vpisali ste jo zgoraj) kažejo veliko skrb za varnost vseh transakcij.	3,83	0,917	-0,586	0,226
Q10	Upravljavci spletne strani (vpisali ste jo zgoraj) imajo na voljo dovolj tehnične opreme s pomočjo katere bodo zagotovili, da drugi nepooblaščeni subjekti ne bodo imeli dostopa do osebnih podatkov.	3,66	0,942	-0,454	0,174
Q11	Menim, da je spletna stan (vpisali ste jo zgoraj), ko se povežem nanjo, avtentična.	4,11	0,845	-0,911	1,069
Q12	Upravljavci spletne strani (vpisali ste jo zgoraj) posedujejo dovolj tehničnih sredstev s pomočjo katerih bodo zagotovili, da podatki, ki jih pošiljam, ne bodo prestreženi s strani tretjih oseb.	3,61	0,98	-0,512	0,176
Q13	Predani osebni podatki ne bodo spremenjeni s strani tretjih oseb.	3,71	0,972	-0,523	0,07

Vir: Anketa, 2007.

Tabela 6: Opisne statistike za postavljene trditve oz. spremenljivke konstrukta zasebnosti

ID	Trditev	Aritmetična sredina	Standardni odklon	Koeficient asimetrije	Koeficient sploščenosti
Q14	Upravljavci spletne strani (vpisali ste jo zgoraj) obveščajo uporabnike o vrsti osebnih podatkov, ki se bodo zbirali in hranili.	3,6	1,154	-0,743	-0,176
Q15	Upravljavci spletne strani (vpisali ste jo zgoraj) so pojasnili pomen zbiranja osebnih podatkov.	3,74	1,102	-0,791	-0,074
Q16	Upravljavci spletne strani (vpisali ste jo zgoraj) so razložili namen uporabe osebnih podatkov.	3,77	1,068	-0,79	0,018
Q17	Zbrani osebni podatki ne bodo bili predani brez mojega dovoljenja tretjim osebam.	3,62	1,138	-0,554	-0,415
Q18	Upravljavci spletne strani (vpisali ste jo zgoraj) se trudijo zagotoviti in ohraniti točne podatke o meni.	3,79	0,992	-0,677	0,148

Nadaljevanje tabele 6:

ID	Trditev	Aritmetična sredina	Standardni odklon	Koeficient asimetrije	Koeficient sploščenosti
Q19	Upravljavci spletne strani (vpisali ste jo zgoraj) so mi ponudili možnost preklica predaje osebnih podatkov tretjim osebam.	3,03	1,35	-0,056	-1,128
Q20	Upravljavci spletne strani (vpisali ste jo zgoraj) imajo postopke s pomočjo katerih preverjajo in popravljajo morebitne nepravilne podatke o posameznikih.	3,1	1,025	-0,001	-0,206
Q21	Upravljavci spletne strani ne pošiljajo brez naslovnikovega dovoljenja reklamnih sporočil preko elektronske pošte.	3,92	1,135	-0,984	0,223
Q22	Menim, da se upravljavci spletne strani (vpisali ste jo zgoraj) trudijo ohraniti moje osebne podatke izven dosega nepooblaščenih posameznikov.	3,98	0,902	-0,665	0,196

Vir: Anketa, 2007.

Tabela 7: Opisne statistike za postavljene trditve oz. spremenljivke konstrukta zaupanja

ID	Trditev	Aritmetična sredina	Standardni odklon	Koeficient asimetrije	Koeficient sploščenosti
Q23	Menim, da upravljavci spletne strani (vpisali ste jo zgoraj) izpolnijo zadane obveze.	4	0,836	-0,874	1,166
Q24	Menim, da lahko zaupam izjavi o varovanju zasebnosti, ki jo navajajo upravljavci spletne strani (vpisali ste jo zgoraj).	3,89	0,882	-0,758	0,562
Q25	Menim, da se upravljavci spletne strani zavzemajo za sedanja in prihodnja zanimanja svojih uporabnikov.	4	0,893	-1,041	1,568
Q26	Menim, da upravljavci spletne strani (vpisali ste jo zgoraj) ne bi namerno naredili nečesa, kar bi uporabnikom povzročilo škodo.	4,15	0,817	-0,985	1,347
Q27	Menim, da zasnova spletne strani in ponudba upoštevata potrebe in želje njenih uporabnikov.	3,98	0,827	-1,063	1,959
Q28	Menim, da so upravljavci spletne strani (vpisali ste jo zgoraj) dovzetni za potrebe uporabnikov.	3,97	0,872	-0,989	1,437

Nadaljevanje tabele 7:

ID	Trditev	Aritmetična sredina	Standardni odklon	Koeficient asimetrije	Koeficient sploščenosti
Q29	Menim, da imajo upravljavci spletne strani (vpisali ste jo zgoraj) dovolj razpoložljivih sredstev za nadaljnji razvoj.	4,07	0,833	-0,78	0,751
Q30	Menim, da spletna stran (vpisali ste jo zgoraj) pozna svoje uporabnike toliko dobro, da lahko prilagodi ponudbo storitev oziroma produktov njihovim potrebam.	3,88	0,943	-0,762	0,489

Vir: Anketa, 2007.

Tabela 8: Opisne statistike za postavljene trditve oz. spremenljivke konstrukta zvestobe

ID	Trditev	Aritmetična sredina	Standardni odklon	Koeficient asimetrije	Koeficient sploščenosti
Q31	Spletno stran (vpisali ste jo zgoraj) obiskujem bolj pogosto, kot druge spletne strani s podobno vsebino.	3,72	1,166	-0,743	-0,254
Q32	Imam pozitivno mnenje o slednji spletni strani in sem ga tudi pripravljen deliti z drugimi.	3,92	0,939	-0,919	0,808
Q33	Spletno stran (vpisali ste jo zgoraj) nameravam obiskati ponovno.	4,35	0,806	-1,672	3,991
Q34	To je spletna stran na kateri se zadržim najdlje časa v primerjavi z drugimi stranmi s podobno vsebino.	3,44	1,277	-0,406	-0,903
Q35	To je moja najljubša spletna stran v primerjavi z drugimi stranmi s podobno vsebino.	3,31	1,274	-0,29	-0,909

Vir: Anketa, 2007.

Tabela 9: Frekvence in odstotni deleži za 36. vprašanje (Spol)

Odgovor	Frekvenca	Odstotni delež
moški	214	53,5
ženski	186	46,5
Skupaj	400	100

Vir: Anketa, 2007.

Tabela 10: Frekvence in odstotni deleži za 37. vprašanje (Starost)

Odgovor	Frekvenca	Odstotni delež
do 25 let	27	6,8
26 do 30 let	78	19,5
31 do 35 let	79	19,8
36 do 40 let	70	17,5
41 do 45 let	54	13,5
46 do 50 let	45	11,3
več kot 50 let	47	11,8
Skupaj	400	100

Vir: Anketa, 2007.

Tabela 11: Frekvence in odstotni deleži za 38. vprašanje (Dokončana izobrazba)

Odgovor	Frekvenca	Odstotni delež
osnovnošolska, srednješolska, poklicna	94	23,5
višješolska, visokošolska, univerzitetna	261	65,3
Magisterij, doktorat	45	11,3
Skupaj	400	100

Vir: Anketa, 2007.

PRILOGA 3: REZULTATI ANALIZE GLAVNIH KOMPONENT ZA KONCEPT VARNOSTI

Tabela 12: KMO test ustreznosti

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0,89
Bartlett's Test of Sphericity	Approx. Chi-Square	1699,117
	Df	15
	Sig.	0

Vir: Anketa, 2007.

Tabela 13: Komunalitete

Vprašanja	Začetne vrednosti	Vrednosti po estrakciji
Q8 Upravljavci spletne strani (vpisali ste jo zgoraj) imajo orodja s katerimi zagotavljajo varen vnos in prenos podatkov s strani uporabnikov.	1	0,752
Q9 Upravljavci spletne strani (vpisali ste jo zgoraj) kažejo veliko skrb za varnost vseh transakcij.	1	0,753
Q10 Upravljavci spletne strani (vpisali ste jo zgoraj) imajo na voljo dovolj tehnične opreme s pomočjo katere bodo zagotovili, da drugi nepooblaščeni subjekti ne bodo imeli dostopa do osebnih podatkov.	1	0,773
Q11 Menim, da je spletna stan (vpisali ste jo zgoraj), ko se povežem nanjo, avtentična.	1	0,504
Q12 Upravljavci spletne strani (vpisali ste jo zgoraj) posedujejo dovolj tehničnih sredstev s pomočjo katerih bodo zagotovili, da podatki, ki jih pošiljam, ne bodo prestreženi s strani tretjih oseb.	1	0,776
Q13 Predani osebni podatki ne bodo spremenjeni s strani tretjih oseb.	1	0,697

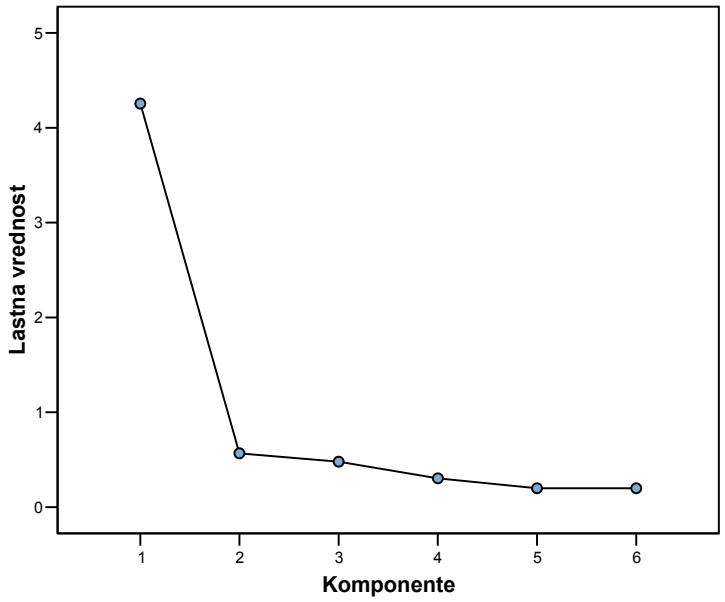
Vir: Anketa, 2007.

Tabela 14: Delež pojasnjene variance

Vprašanja	Skupaj	% variance	Kumulativa	Skupaj	% variance po ekstrakciji	Kumulativa po ekstrakciji
1	4,256	70,926	70,926	4,256	70,926	70,926
2	0,567	9,447	80,373			
3	0,479	7,978	88,351			
4	0,303	5,044	93,395			
5	0,198	3,304	96,699			
6	0,198	3,301	100			

Vir: Anketa, 2007.

Slika 1: Scree diagram



Vir: Anketa, 2007.

Tabela 15: Vrednost komponentnih uteži

Vprašanja	Komponenta varnost
Q8 Upravljavci spletne strani (vpisali ste jo zgoraj) imajo orodja s katerimi zagotavljajo varen vnos in prenos podatkov s strani uporabnikov.	0,867
Q9 Upravljavci spletne strani (vpisali ste jo zgoraj) kažejo veliko skrb za varnost vseh transakcij.	0,868
Q10 Upravljavci spletne strani (vpisali ste jo zgoraj) imajo na voljo dovolj tehnične opreme s pomočjo katere bodo zagotovili, da drugi nepooblaščeni subjekti ne bodo imeli dostopa do osebnih podatkov.	0,879
Q11 Menim, da je spletna stan (vpisali ste jo zgoraj), ko se povežem nanjo, avtentična.	0,71
Q12 Upravljavci spletne strani (vpisali ste jo zgoraj) posedujejo dovolj tehničnih sredstev s pomočjo katerih bodo zagotovili, da podatki, ki jih pošiljam, ne bodo prestreženi s strani tretjih oseb.	0,881
Q13 Predani osebni podatki ne bodo spremenjeni s strani tretjih oseb.	0,835

Vir: Anketa, 2007.

PRILOGA 4: REZULTATI ANALIZE GLAVNIH KOMPONENT ZA KONCEPT ZASEBNOSTI

Tabela 16: KMO test ustreznosti

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0,872
Bartlett's Test of Sphericity	Approx. Chi-Square	2035,263
	df	36
	Sig.	0

Vir: Anketa, 2007.

Tabela 17: Komunalitete

Vprašanja	Začetne vrednosti	Vrednosti po estrakciji
Q14 Upravljavci spletne strani (vpisali ste jo zgoraj) obveščajo uporabnike o vrsti osebnih podatkov, ki se bodo zbirali in hranili.	1	0,764
Q15 Upravljavci spletne strani (vpisali ste jo zgoraj) so pojasnili pomen zbiranja osebnih podatkov.	1	0,907
Q16 Upravljavci spletne strani (vpisali ste jo zgoraj) so razložili namen uporabe osebnih podatkov.	1	0,892
Q17 Zbrani osebni podatki ne bodo bili predani brez mojega dovoljenja tretjim osebam.	1	0,606
Q18 Upravljavci spletne strani (vpisali ste jo zgoraj) se trudijo zagotoviti in ohraniti točne podatke o meni.	1	0,639
Q19 Upravljavci spletne strani (vpisali ste jo zgoraj) so mi ponudili možnost preklica predaje osebnih podatkov tretjim osebam.	1	0,706
Q20 Upravljavci spletne strani (vpisali ste jo zgoraj) imajo postopke s pomočjo katerih preverjajo in popravljajo morebitne nepravilne podatke o posameznikih.	1	0,697
Q21 Upravljavci spletne strani ne pošiljajo brez naslovnikovega dovoljenja reklamnih sporočil preko elektronske pošte.	1	0,761
Q22 Menim, da se upravljavci spletne strani (vpisali ste jo zgoraj) trudijo ohraniti moje osebne podatke izven dosega nepooblaščenih posameznikov.	1	0,81

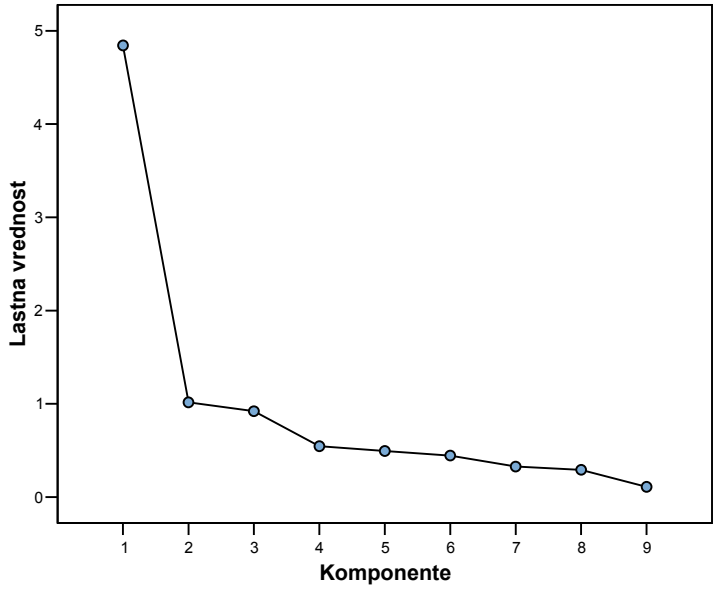
Vir: Anketa, 2007.

Tabela 18: Delež pojasnjene variance

Vprašanja	Skupaj	% variance	Kumulativa	Skupaj	% variance po ekstrakciji	Kumulativa po ekstrakciji
1	4,844	53,818	53,818	4,844	53,818	53,818
2	1,017	11,296	65,114	1,017	11,296	65,114
3	0,922	10,241	75,355	0,922	10,241	75,355
4	0,546	6,071	81,426			
5	0,495	5,503	86,928			
6	0,446	4,951	91,879			
7	0,328	3,64	95,519			
8	0,293	3,254	98,773			
9	0,11	1,227	100			

Vir: Anketa, 2007.

Slika 2: Scree diagram



Vir: Anketa, 2007.

Tabela 19: Vrednost komponentnih uteži – rotacija oblimin

Vprašanja	Seznanjenost	Varnost	Možnost izbire
Q15 Upravljavci spletne strani (vpisali ste jo zgoraj) so pojasnili pomen zbiranja osebnih podatkov.	0,962		
Q16 Upravljavci spletne strani (vpisali ste jo zgoraj) so razložili namen uporabe osebnih podatkov.	0,96		
Q14 Upravljavci spletne strani (vpisali ste jo zgoraj) obveščajo uporabnike o vrsti osebnih podatkov, ki se bodo zbirali in hranili.	0,838		
Q22 Menim, da se upravljavci spletne strani (vpisali ste jo zgoraj) trudijo ohraniti moje osebne podatke izven dosega nepooblaščenih posameznikov.		0,889	
Q21 Upravljavci spletne strani ne pošiljajo brez naslovnikovega dovoljenja reklamnih sporočil preko elektronske pošte.		0,879	
Q17 Zbrani osebni podatki ne bodo bili predani brez mojega dovoljenja tretjim osebam.		0,495	0,341
Q18 Upravljavci spletne strani (vpisali ste jo zgoraj) se trudijo zagotoviti in ohraniti točne podatke o meni.		0,474	0,454
Q20 Upravljavci spletne strani (vpisali ste jo zgoraj) imajo postopke s pomočjo katerih preverjajo in popravljajo morebitne nepravilne podatke o posameznikih.			0,84
Q19 Upravljavci spletne strani (vpisali ste jo zgoraj) so mi ponudili možnost preklica predaje osebnih podatkov tretjim osebam.			0,798

Vir: Anketa, 2007.

PRILOGA 5: REZULTATI ANALIZE GLAVNIH KOMPONENT ZA KONCEPT ZAUPANJA

Tabela 20: KMO test ustreznosti

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0,906
Bartlett's Test of Sphericity	Approx. Chi-Square	2248,463
	df	28
	Sig.	0

Vir: Anketa, 2007.

Tabela 21: Komunalitete

Vprašanja	Začetne vrednosti	Vrednosti po estrakciji
Q23 Menim, da upravljavci spletne strani (vpisali ste jo zgoraj) izpolnijo zadane obveze.	1	0,718
Q24 Menim, da lahko zaupam izjavi o varovanju zasebnosti, ki jo navajajo upravljavci spletne strani (vpisali ste jo zgoraj).	1	0,671
Q25 Menim, da se upravljavci spletne strani zavzemajo za sedanja in prihodnja zanimanja svojih uporabnikov.	1	0,651
Q26 Menim, da upravljavci spletne strani (vpisali ste jo zgoraj) ne bi namerno naredili nečesa, kar bi uporabnikom povzročilo škodo.	1	0,616
Q27 Menim, da zasnova spletne strani in ponudba upoštevata potrebe in želje njenih uporabnikov.	1	0,723
Q28 Menim, da so upravljavci spletne strani (vpisali ste jo zgoraj) dovzetni za potrebe uporabnikov.	1	0,708
Q29 Menim, da imajo upravljavci spletne strani (vpisali ste jo zgoraj) dovolj razpoložljivih sredstev za nadaljnji razvoj.	1	0,544
Q30 Menim, da spletna stran (vpisali ste jo zgoraj) pozna svoje uporabnike toliko dobro, da lahko prilagodi ponudbo storitev oziroma produktov njihovim potrebam.	1	0,589

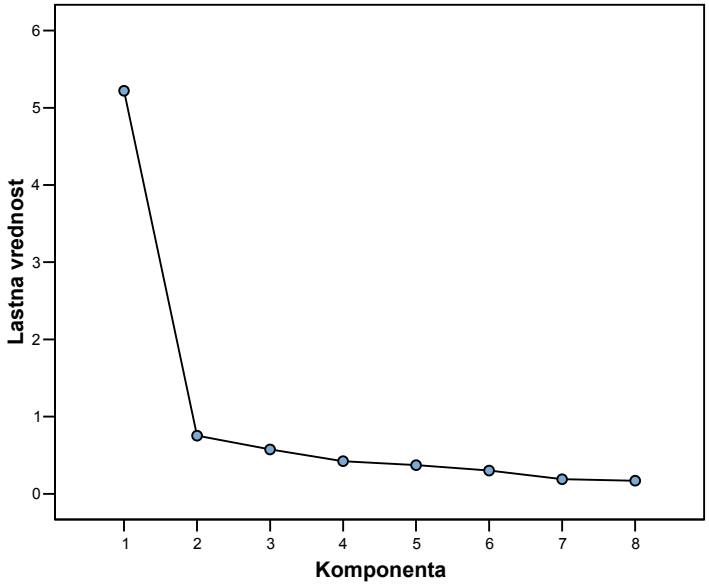
Vir: Anketa, 2007.

Tabela 22: Delež pojasnjene variance

Vprašanja	Skupaj	% variance	Kumulativa	Skupaj	% variance po ekstrakciji	Kumulativa po ekstrakciji
1	5,22	65,251	65,251	5,22	65,251	65,251
2	0,754	9,421	74,672			
3	0,575	7,185	81,857			
4	0,422	5,271	87,128			
5	0,371	4,64	91,767			
6	0,301	3,762	95,529			
7	0,189	2,358	97,887			
8	0,169	2,113	100			

Vir: Anketa, 2007.

Slika 3: Scree diagram



Vir: Anketa, 2007.

Tabela 23: Vrednost komponentnih uteži

Vprašanja	Komponenta zaupanja
Q23 Menim, da upravljavci spletne strani (vpisali ste jo zgoraj) izpolnijo zadane obveze.	0,847
Q24 Menim, da lahko zaupam izjavi o varovanju zasebnosti, ki jo navajajo upravljavci spletne strani (vpisali ste jo zgoraj).	0,819
Q25 Menim, da se upravljavci spletne strani zavzemajo za sedanja in prihodnja zanimanja svojih uporabnikov.	0,807
Q26 Menim, da upravljavci spletne strani (vpisali ste jo zgoraj) ne bi namerno naredili nečesa, kar bi uporabnikom povzročilo škodo.	0,785
Q27 Menim, da zasnova spletne strani in ponudba upoštevata potrebe in želje njenih uporabnikov.	0,85
Q28 Menim, da so upravljavci spletne strani (vpisali ste jo zgoraj) dovzetni za potrebe uporabnikov.	0,841
Q29 Menim, da imajo upravljavci spletne strani (vpisali ste jo zgoraj) dovolj razpoložljivih sredstev za nadaljnji razvoj.	0,738
Q30 Menim, da spletna stran (vpisali ste jo zgoraj) pozna svoje uporabnike toliko dobro, da lahko prilagodi ponudbo storitev oziroma produktov njihovim potrebam.	0,767

Vir: Anketa, 2007.

PRILOGA 6: REZULTATI ANALIZE GLAVNIH KOMPONENT ZA KONCEPT ZVESTOBE

Tabela 24: KMO test ustreznosti

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0,826
Bartlett's Test of Sphericity	Approx. Chi-Square	1100,334
	Df	10
	Sig.	0

Vir: Anketa, 2007.

Tabela 25: Komunalitete

Vprašanja	Začetne vrednosti	Vrednosti po estrakciji
Q31 Spletno stran (vpisali ste jo zgoraj) obiskujem bolj pogosto, kot druge spletne strani s podobno vsebino.	1	0,709
Q32 Imam pozitivno mnenje o slednji spletni strani in sem ga tudi pripravljen deliti z drugimi.	1	0,628
Q33 Spletno stran (vpisali ste jo zgoraj) nameravam obiskati ponovno.	1	0,574
Q34 To je spletna stran na kateri se zadržim najdlje časa v primerjavi z drugimi stranmi s podobno vsebino.	1	0,764
Q35 To je moja najljubša spletna stran v primerjavi z drugimi stranmi s podobno vsebino.	1	0,728

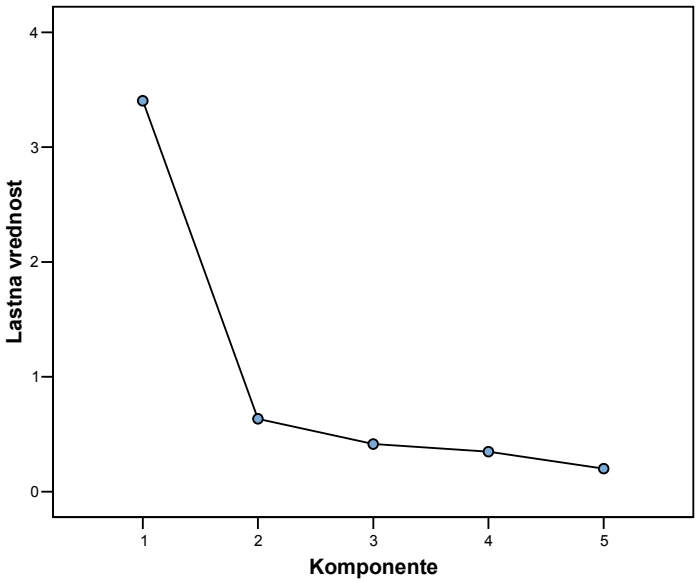
Vir: Anketa, 2007.

Tabela 26: Delež pojasnjene variance

Vprašanja	Skupaj	% variance	Kumulativa	Skupaj	% variance po ekstrakciji	Kumulativa po ekstrakciji
1	3,403	68,066	68,066	3,403	68,066	68,066
2	0,634	12,677	80,743			
3	0,414	8,289	89,032			
4	0,348	6,961	95,993			
5	0,2	4,007	100			

Vir: Anketa, 2007.

Slika 4: Scree diagram



Vir: Anketa, 2007.

Tabela 27: Vrednost komponentnih uteži

Vprašanja	Komponenta zvestobe
Q31 Spletno stran (vpisali ste jo zgoraj) obiskujem bolj pogosto, kot druge spletne strani s podobno vsebino.	0,842
Q32 Imam pozitivno mnenje o slednji spletni strani in sem ga tudi pripravljen deliti z drugimi.	0,793
Q33 Spletno stran (vpisali ste jo zgoraj) nameravam obiskati ponovno.	0,758
Q34 To je spletna stran na kateri se zadržim najdlje časa v primerjavi z drugimi stranmi s podobno vsebino.	0,874
Q35 To je moja najljubša spletna stran v primerjavi z drugimi stranmi s podobno vsebino.	0,853

Vir: Anketa, 2007.

PRILOGA 7: PROUČEVANE SPREMENLJIVKE S PRIPADAJOČIMI TRDITVAMI

TRDITEV	PROUČEVANA SPREMEN-LJIVKA	CRON-BACH ALFA	KMO in Barletov test		USTRE-ZNOST
			KMO	P	
Q8 Upravljavci spletne strani (vpisali ste jo zgoraj) imajo orodja s katerimi zagotavljajo varen vnos in prenos podatkov s strani uporabnikov.	VARNOST	0,917	0,89	0,000	✓
Q9 Upravljavci spletne strani (vpisali ste jo zgoraj) kažejo veliko skrb za varnost vseh transakcij.					
Q10 Upravljavci spletne strani (vpisali ste jo zgoraj) imajo na voljo dovolj tehnične opreme s pomočjo katere bodo zagotovili, da drugi nepooblaščeni subjekti ne bodo imeli dostopa do osebnih podatkov.					
Q11 Menim, da je spletna stan (vpisali ste jo zgoraj), ko se povežem nanjo, avtentična.					
Q12 Upravljavci spletne strani (vpisali ste jo zgoraj) posedujejo dovolj tehničnih sredstev s pomočjo katerih bodo zagotovili, da podatki, ki jih pošiljam, ne bodo prestreženi s strani tretjih oseb.					
Q13 Predani osebni podatki ne bodo spremenjeni s strani tretjih oseb.					
Q14 Upravljavci spletne strani (vpisali ste jo zgoraj) obveščajo uporabnike o vrsti osebnih podatkov, ki se bodo zbirali in hranili.	ZASEBNOST SEZNANJENOST	0,913	0,872	0,000	✓
Q15 Upravljavci spletne strani (vpisali ste jo zgoraj) so pojasnili pomen zbiranja osebnih podatkov.					
Q16 Upravljavci spletne strani (vpisali ste jo zgoraj) so razložili namen uporabe osebnih podatkov.					
Q17 Zbrani osebni podatki ne bodo bili predani brez mojega dovoljenja tretjim osebam.	ZASEBNOST VARNOST	0,813			
Q18 Upravljavci spletne strani (vpisali ste jo zgoraj) se trudijo zagotoviti in ohraniti točne podatke o meni.					
Q21 Upravljavci spletne strani ne pošiljajo brez naslovnikovega dovoljenja reklamnih sporočil preko elektronske pošte.					
Q22 Menim, da se upravljavci spletne strani (vpisali ste jo zgoraj) trudijo ohraniti moje osebne podatke izven dosega nepooblaščenih posameznikov.					

Q19 Upravljavci spletne strani (vpisali ste jo zgoraj) so mi ponudili možnost preklica predaje osebnih podatkov tretjim osebam.	ZASEBNOST VARNOST	0,647			
Q20 Upravljavci spletne strani (vpisali ste jo zgoraj) imajo postopke s pomočjo katerih preverjajo in popravljajo morebitne nepravilne podatke o posameznikih.					
Q23 Menim, da upravljavci spletne strani (vpisali ste jo zgoraj) izpolnijo zadane obveze.	ZAUPANJE	0,923	0,906	0,000	✓
Q24 Menim, da lahko zaupam izjavi o varovanju zasebnosti, ki jo navajajo upravljavci spletne strani (vpisali ste jo zgoraj).					
Q25 Menim, da se upravljavci spletne strani zavzemajo za sedanja in prihodnja zanimanja svojih uporabnikov.					
Q26 Menim, da upravljavci spletne strani (vpisali ste jo zgoraj) ne bi namerno naredili nečesa, kar bi uporabnikom povzročilo škodo.					
Q27 Menim, da zasnova spletne strani in ponudba upoštevata potrebe in želje njenih uporabnikov.					
Q28 Menim, da so upravljavci spletne strani (vpisali ste jo zgoraj) dovzetni za potrebe uporabnikov.					
Q29 Menim, da imajo upravljavci spletne strani (vpisali ste jo zgoraj) dovolj razpoložljivih sredstev za nadaljnji razvoj.					
Q30 Menim, da spletna stran (vpisali ste jo zgoraj) pozna svoje uporabnike toliko dobro, da lahko prilagodi ponudbo storitev oziroma produktov njihovim potrebam.					
Q31 Spletno stran (vpisali ste jo zgoraj) obiskujem bolj pogosto, kot druge spletne strani s podobno vsebino.	ZVESTOBA	0,878	0,826	0,000	✓
Q32 Imam pozitivno mnenje o slednji spletni strani in sem ga tudi pripravljen deliti z drugimi.					
Q33 Spletno stran (vpisali ste jo zgoraj) nameravam obiskati ponovno.					
Q34 To je spletna stran na kateri se zadržim najdlje časa v primerjavi z drugimi stranmi s podobno vsebino.					
Q35 To je moja najljubša spletna stran v primerjavi z drugimi stranmi s podobno vsebino.					

Legenda: ✓ konstrukt je ustrezen ✘ konstrukt ni ustrezen

Vir: Anketa, 2007.

PRILOGA 8: KORELACIJSKA MATRIKA

		Kako pogosto ste uporabili internet, v zadnjih šestih mesecih, za spletne nakupe?	Zasebnost - seznanjenost	Zasebnost - pričakovano varovanje zasebnosti	Zasebnost - dodatno varovanje zasebnosti	Varnost	Zaupanje	Zvestoba
Uporaba interneta za spletne nakupe	Pearson Correlation	1	,102(*)	,203(**)	,138(**)	,302(**)	,238(**)	,150(**)
	Sig. (2-tailed)	.	0,041	0	0,006	0	0	0,003
Zasebnost – seznanjenost	Pearson Correlation	,102(*)	1	,622(**)	,531(**)	,518(**)	,559(**)	,324(**)
	Sig. (2-tailed)	0,041	.	0	0	0	0	0
Zasebnost - pričakovano varovanje zasebnosti	Pearson Correlation	,203(**)	,622(**)	1	,541(**)	,678(**)	,758(**)	,416(**)
	Sig. (2-tailed)	0	0	.	0	0	0	0
Zasebnost – dodatno varovanje zasebnosti	Pearson Correlation	,138(**)	,531(**)	,541(**)	1	,468(**)	,467(**)	,286(**)
	Sig. (2-tailed)	0,006	0	0	.	0	0	0
Varnost	Pearson Correlation	,302(**)	,518(**)	,678(**)	,468(**)	1	,716(**)	,442(**)
	Sig. (2-tailed)	0	0	0	0	.	0	0
Zaupanje	Pearson Correlation	,238(**)	,559(**)	,758(**)	,467(**)	,716(**)	1	,536(**)
	Sig. (2-tailed)	0	0	0	0	0	.	0
Zvestoba	Pearson Correlation	,150(**)	,324(**)	,416(**)	,286(**)	,442(**)	,536(**)	1
	Sig. (2-tailed)	0,003	0	0	0	0	0	.
*** Correlation is significant at the 0.01 level (2-tailed).*								
** Correlation is significant at the 0.05 level (2-tailed).*								

Vir: Anketa, 2007.

PRILOGA 9: REGRESIJSKA ANALIZA: VPLIV IZKUŠENJ NA VARNOST

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,302(a)	0,091	0,089	0,74372

ANOVA(b)

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	22,11	1	22,11	39,974	,000(a)
	Residual	220,14	398	0,553		
	Total	242,25	399			

Coefficients(a)

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3,296	0,087		38,018	0
	Kako pogosto ste uporabili internet, v zadnjih šestih mesecih, za spletne nakupe?	0,232	0,037	0,302	6,322	0

PRILOGA 10: REGRESIJSKA ANALIZA: VPLIV VARNOSTI NA ZAUPANJE

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,716(a)	0,513	0,512	0,48635

ANOVA(b)

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	99,261	1	99,261	419,65	,000(a)
	Residual	94,14	398	0,237		
	Total	193,401	399			

Coefficients(a)

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1,566	0,121		12,945	0
	Varnost	0,64	0,031	0,716	20,485	0

PRILOGA 11: REGRESIJSKA ANALIZA: VPLIV ZASEBNOSTI NA ZAUPANJA

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,767(a)	0,588	0,585	0,44863

ANOVA(b)

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	113,699	3	37,9	188,31	,000(a)
	Residual	79,702	396	0,201		
	Total	193,401	399			

Coefficients(a)

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1,497	0,108		13,915	0
	Zasebnost – seznanjenost	0,088	0,029	0,129	2,984	0,003
	Zasebnost – varovanje zasebnosti	0,543	0,036	0,653	15,038	0
	Zasebnost – možnost izbire	0,031	0,027	0,045	1,132	0,258

PRILOGA 12: REGRESIJSKA ANALIZA: VPLIV ZAUPANJA NA ZVESTOBO

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,536(a)	0,288	0,286	0,76807

ANOVA(b)

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	94,862	1	94,862	160,8	,000(a)
	Residual	234,795	398	0,59		
	Total	329,658	399			

Coefficients(a)

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	0,951	0,224		4,249	0
	Zaupanje	0,7	0,055	0,536	12,681	0

PRILOGA 13: REGRESIJSKA ANALIZA: VPLIV VARNOSTI NA ZVESTOBO

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,442(a)	0,195	0,193	0,8165

ANOVA(b)

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	64,319	1	64,319	96,477	,000(a)
	Residual	265,338	398	0,667		
	Total	329,658	399			

Coefficients(a)

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1,794	0,203		8,834	0
	Varnost	0,515	0,052	0,442	9,822	0

PRILOGA 14: REGRESIJSKA ANALIZA: VPLIV IZKUŠENJ NA ZASEBNOST

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,171(a)	0,029	0,027	0,80059

ANOVA(b)

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	7,703	1	7,703	12,018	,001(a)
	Residual	255,096	398	0,641		
	Total	262,799	399			

Coefficients(a)

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3,24	0,093		34,709	0
	Kako pogosto ste uporabili internet, v zadnjih šestih mesecih, za spletne nakupe?	0,137	0,04	0,171	3,467	0,001

PRILOGA 15: REGRESIJSKA ANALIZA: VPLIV ZASEBNOSTI IN VARNOSTI NA ZAUPANJE

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,809(a)	0,655	0,651	0,41122

ANOVA(b)

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	126,607	4	31,652	187,18	,000(a)
	Residual	66,794	395	0,169		
	Total	193,401	399			

Coefficients(a)

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1,093	0,109		10,028	0
	Zasebnost – seznanjenost	0,057	0,027	0,084	2,12	0,035
	Zasebnost – varovanje zasebnosti	0,381	0,038	0,459	10,053	0
	Zasebnost – možnost izbire	0,004	0,025	0,006	0,16	0,873
	Varnost	0,321	0,037	0,359	8,737	0

PRILOGA 16: REGRESIJSKA ANALIZA: VPLIV VARNOSTI IN ZAUPANJA NA ZVESTOBO

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,543(a)	0,295	0,291	0,76538

ANOVA(b)

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	97,094	2	48,547	82,873	,000(a)
	Residual	232,563	397	0,586		
	Total	329,658	399			

Coefficients(a)

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	0,87	0,227		3,834	0
	Zaupanje	0,59	0,079	0,452	7,48	0
	Varnost	0,138	0,07	0,118	1,952	0,052