UNIVERZA V LJUBLJANI
EKONOMSKA FAKULETA

SPECIALISTIČNO DELO

INTERNET IN PRAVICA DO ZASEBNOSTI

Ljubljana, avgust 2005 ROK PRIMOŽIČ

IZJAVA

Študent Rok Primožič izjavljam, da sem avtor tega specialističnega 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 specialističnega dela na fakultetnih spletnih straneh.

V Ljubljani, dne _____

Podpis: _____

KAZALO

KAZALO SLIK

KAZALO TABEL

1 UVOD

Zaradi vedno večje soodvisnosti ljudi med seboj in zaradi eksplozivnega razvoja tehnike, ki omogoča včasih komaj predstavljive posege v človekovo zasebno sfero, se pojavljajo zmeraj novi vidiki zasebnosti posameznika. Znamenita Orwellova fraza iz leta 1984, "*Veliki brat nas povsod opazuje*", dobiva nove in nepredstavljive razsežnosti.

Varovanje elektronske zasebnosti v informacijski družbi in s tem povezana specifična vprašanja elektronskega poslovanja, predstavljajo eno ključnih pravnih, sociooloških, filozofskih in etničnih vprašanj sodobne družbe. Ob vrsti pozitivnih vidikov in do pred nekaj let neslutnih možnosti, ki jih omogočata razvoj tehnologije v informacijski družbi in predvsem globalno računalniško omrežje, prinaša ta tehnološki razvoj tudi veliko nevarnost vdora v zasebnost, ki je ena izmed temeljnih človekovih pravic. Zakonodajalec takih posegov ne more zmeraj hipotetično predvideti, ne more predvideti novih oblik teh posegov in njihovih posledic, tako da za njihovo normiranje in sankcioniranje nima vedno pravega instrumentarija. Potrebno je razumeti, da je svetovni splet globalno in pravno neurejeno okolje, v katerem zakoni posamezne države veljajo le na domačem teritoriju.

Internet je postal zelo pomemben virtualni prostor, kjer se pretaka ogromno osebnih podatkov, objavljenih z dovoljenjem posameznika, dostikrat pa tudi brez njegove vednosti ali v nasprotju z njegovo voljo. Neskončne povezave in storitve, ki jih omogoča internet, so glavna privlačnost za uporabnike. Okolje je zaradi človeškega faktorja v stalnem gibanju in z novimi tehnologijami prihajajo tudi vedno nove nevarnosti. Le-te pa razkrivajo, da uporabnik ob računalniški opremi nikoli ni povsem sam ter pozivajo na previdnost ravnanja in uporabe interneta ter celotnega okolja v osebnem računalniku.

Občasni uporabniki interneta so pogosto neosveščeni oziroma podcenjujejo tveganje, ki ga uporaba interneta predstavlja s stališča varnosti elektronskih osebnih podatkov in elektronske zasebnosti. Uporabnike je nujno potrebno obveščati o prežečih nevarnostih in jim zagotoviti pravno varnost najširše uporabe interneta v domačem in mednarodnem prostoru. Področje varovanja elektronskih osebnih podatkov in elektronske zasebnosti je in bo nedvomno ena izmed najbolj aktualnih in zanimivih tem. Pri tem pa seveda ne smemo pozabiti tudi na veliko zahtevnost tega področja, saj bo potrebno vložiti velike napore za obvladovanje celotnega sistema varovanja in zaščite.

Leta 1983 je David Burnham opozoril na t.i. elektronsko sled, ki jo posamezniki puščajo za svojimi dejanji (Kovačič, 2003, str. 10). Vsakič ko se dvigne telefonska slušalka, uporabi bankomat ali plačilna kartica, gre na banko, obišče zdravnik, uporabi mobilni telefon ..., avtomatski sistemi ta dogodek zaznajo in zabeležijo. Podjetja sledijo tem aktivnostim z namenom vzorčenja in ugotavljanja preferenc. Elektronski odtis oziroma elektronska sled je torej informacija, ki se shranjuje rutinsko in kaže dejavnost nekega posameznika (Lyon, 1994, str. 59).

Vsaka organizacija oziroma ustanova zbira samo določene podatke o posameznikovih aktivnostih oziroma dejanjih. Tako na primer Zavod za zdravstveno zavarovanje zbira predvsem informacije o zdravstvenih aktivnostih, mobilni operaterji zbirajo zgodovino opravljenih klicev z osnovnim ciljem tarifiranja opravljenih pogovorov, ravno tako ponudniki stacionarne telefonije, banke potrebujejo v izogib morebitnim prihodnjim nevšečnostim popoln pregled nad gibanjem sredstev na naših bančnih računih, ponudniki internetnih storitev ves čas beležijo e-pošto oziroma dodajajo zapise o prejemnikih/pošiljateljih z namenom (varnostne) kontrole prometa in blokiranju nezaželene pošte. Osnovni smisel nadzora je samoumeven in družbeno sprejemljiv. Pojavi se vprašanje, kaj se lahko zgodi v primeru, če se začnejo te baze integrirati v enovit sistem oziroma se povezovati. S povezavo in njihovo obdelavo lahko pridemo do novih podatkov in informacij, kar je lahko za posameznika škodljivo ali celo nevarno – zaradi ogrožanja njegovih pravic (Čebulj, 1992, str. 59). Sodobne in napredne tehnologije omogočajo ravno to – zbiranje, povezovanje, urejanje in analiziranje ogromnih količin podatkov. Težko si predstavljamo kaj bi se lahko zgodilo, če bi zaradi slabe varnosti ali kakega drugega vzroka do teh podatkov prišel nek nepooblaščen subjekt. In to se seveda dogaja. Proučili bomo primer udba.net, ki kaže na ranljivost sistemov z nepredstavljivimi posledicami.

Tehnologija, ne samo, da omogoča sledenje posameznikovih aktivnosti, tudi prinaša vedno nove uporabne funkcionalnosti, ki prispevajo k lagodnosti, hkrati pa še globlje posegajo v našo zasebnost. Prihaja čas, ko bomo morali začeti izbirati med zasebnostjo in lagodnostjo, saj se slednja dva pojma izključujeta. Lep primer je uporaba mobilnih telefonov, s katerimi smo dosegljivi skoraj povsod. Po drugi strani pa operaterji beležijo čas in dolžino naših pogovorov, tip telefona, navade telefoniranja, s pomočjo metode trigonometrije pa nas tudi izsledijo.

Cilj specialističnega dela je ugotoviti, v kolikšni meri so uporabniki seznanjeni o možnostih posega v njihovo zasebnost ob uporabi interneta in hkrati preveriti, ali se zavedajo posledic, ki lahko nastanejo zaradi nepremišljenega ravnanja, nevednosti oziroma neustrezne zaščite.

Ustava Republike Slovenije in Zakon o varstvu osebnih podatkov urejujeta zakonodajno plat pravice do zasebnosti in varstva osebnih podatkov. Uporabniki interneta imamo na voljo različna strojna in programska orodja, s katerimi lahko preprečimo nepooblaščen nadzor in vpogled v našo zasebno sfero. Strokovnjaki nas preko medijev vedno pogosteje informirajo oziroma opozarjajo na nevarnosti, ki prežijo ob obisku svetovnega spleta. Ravno tako tudi oglaševalci posredno ali neposredno opozarjajo na obstoj možnosti uporabe tehnoloških orodji za standardizirano ciljanje z oglasi na spletu. Spletni vprašalniki so opremljeni z vsemi zakonsko določenimi opozorili, tako o namenu zbiranja podatkov, kot tudi o njihovi varnosti in zaupnosti. Državne institucije trdijo, da zbirajo le tiste podatke, ki jih potrebujejo in da jih varujejo skladno z zakonskimi določili.

Na prvi pogled je videti, da so vsa poglavitna področja urejena in delujejo le v korist uporabnika. Ali to pomeni, da naša pravica do informacijske zasebnosti ni ogrožena?

Tekom naloge bomo poskusili preveriti spodaj predstavljene domneve, ki bodo podale odgovor na prej zastavljeno vprašanje. Za prvi dve domnevi bi lahko rekli, da sodita v t.i. pravni vidik področja zasebnosti s poudarkom na internetu. Nadalje sledi domneva iz ekonomskega sklopa, ki zadeva ponudnike tehnologije spletnega oglaševanja. Zadnja, a zato nič manj pomembna domneva se navezuje na infrastrukturo interneta.

Raziskovalne domneve so:

1. Zakonodaja ne more slediti novim vsebinam in aktivnostim, ki jih prinaša internet.
2. Glavna sestavina zaščite informacijske zasebnosti je transparentnost uporabe zasebnih podatkov. Najboljša zaščita ni ta, da država in zasebne družbe 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.
3. Tehnološka orodja za standardizirano ciljanje z oglasi na spletu, na podlagi vedenjskih vzorcev uporabnikov interneta, nenadzorovano posegajo v zasebnost, izključno zaradi sledenja ekonomskim interesom.
4. Uporabniki svetovnega spleta moramo uporabljati rešitve, ki služijo zavarovanju različnih interesov glede zasebnosti in anonimnosti dejavnosti posameznikov ter podjeti pri uporabi internetnih storitev.

Na koncu specialističnega dela, v poglavju 6.4 bomo podali odgovore na zgornje štiri domneve.

Metoda dela, ki smo jo uporabili pri izdelavi specialističnega dela, temelji predvsem na proučevanju teoretične podlage, ki nam daje osnovo oziroma celovit pregled nad obravnavano tematiko. Praktični del bo temeljil na ugotovitvah kvalitativne raziskave, kjer bosta kot metodi zbiranja podatkov uporabljeni intervju in fokusna skupina.

Prevladujoča metoda dela temelji na analitično teoretičnem preučevanju obravnavane tematike. Delo se opira na strokovno literaturo tujih in domačih avtorjev, vire, prispevke in članke z novejšimi teoretičnimi spoznanji s področja interneta in zasebnosti. Zaradi aktualnosti izbrane tematike in vzporednega sprejemanja zakonodaje, ki obravnava proučevano področje, smo slednji posvetili dodatno pozornost. Spoznanja o zasebnosti in predvsem internetu, ki predstavljajo prakso v tujini smo poskušali prenesti v nalogo ter opozoriti na nevarnosti, ki čakajo morebiti tudi nas. Poleg izbrane literature smo vključili tudi lastno znanje, pridobljeno v praksi, na področju naprednih tehnologij in tekom študija na specialističnem programu. V nalogo so vključene tudi informacije, pridobljene v pogovoru s sodelavci, informacije pridobljene iz poslovnih poročil podjetji in internih virov podjetja.

Ugotavljanje osveščenosti uporabnikov interneta o kršenju njihovih pravic s tem, da se izvaja nadzor in zbiranje osebnih podatkov, zahteva poleg teoretičnega pristopa tudi kvalitativno in kvantitativno metodologijo. Predmet proučevanja bo seznanjenost povprečnih slovenskih uporabnikov interneta o možnostih posega v njihovo zasebnost.

Struktura specialističnega dela je zasnovana na principu “od zgoraj navzdol”, kar pomeni, da bomo od bolj splošnih tem prehajali na bolj podrobne. Po uvodu se bomo najprej v drugem

poglavju posvetili opredelitvam različnih izrazov, ki se pogosto uporabljajo pri opisovanju elektronskega okolja (na primer nova ekonomija, elektronsko poslovanje in podobno).

V tretjem poglavju bomo 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 družbo in ekonomijo oblikuje. Nadalje si bomo pogledali pasti in nevarnosti na internetu. Skozi to poglavje bomo spoznali, da problem varnosti in s tem tudi zasebnosti ni samo tehnični, pač pa je tudi družbeni problem. Nakazali bomo na zaščitne ukrepe predvsem v smislu samozaščite, s katerimi bomo predstavili varnost kot proces in ne izdelek, ki se ga da kupiti.

Predstavitev spoznanj in osvetlitev šibkih točk pri elektronskem poslovanju preko interneta ter opozorilo na potencialne nevarnosti, ki na nas prežijo ob njegovih storitvah, bo tema četrtega poglavja. Ogledali si bomo tehnologijo in metodologijo uvajanja sodobnih varnostnih mehanizmov, s katerimi se lahko le začasno onesposobi ne pa tudi prepreči vdor v zasebni informacijski sistem. Seveda bomo spoznali še druge metode, ki lahko posegajo v našo zasebnost in nakazali na nekatere rešitve. V drugem delu četrtega poglavja se bomo seznanili z opredelitvijo zasebnosti iz pravnega oziroma zakonskega zornega kota. Izpostavili bomo nekaj primerov, ki bodo podali grob pregled nad (ne)urejenostjo vprašanja virtualne zasebnosti pri nas. Poglavje bomo zaključili z predstavitvijo perspektivnosti razvoja spleta kot varnega medija za prenos elektronskih informacij, elektronskega poslovanja in drugih oblik komuniciranja po elektronski poti.

Peto poglavje bo predstavljalo osrednji del specialističnega dela. Najprej bomo na kratko predstavili smisel nadzorovanja kot proces, ki poskuša zaznati in zabeležiti dejstva oziroma aktivnosti posameznika. Spoznali bomo pobudnike in izvajalce nadzora ter njihov namen, ki bo v nadaljevanju služil kot izhodišče za preverjanje parodoksalne dvojnosti – ali ima nadzor pozitivne ali negativne učinke. Ugotovili bomo, da se država in podjetja poslužujejo nadzora z natančno določenimi cilji in slednje bomo poskusili spoznati. Ker želimo celotno delo pripraviti transparentno in objektivno, nas bo zanimalo, kaj o ugotovljenih namenih in ciljih menijo "žrtve" nadzora – uporabniki interneta. Poglavje bomo zaključili z opisom nekaterih orodij, ki lahko prispevajo k znižanju tveganja pred nepooblaščenim zbiranjem osebnih podatkov in sledljivostjo posameznika.

Šesto poglavje bo predstavljal empirični del specialističnega dela. Izvedli bomo intervju s strokovnjakom za (ne)varnost in zasebnost na internetu, nadalje bo sledil povzetek skupinske razprave, ki bo izvedena po metodologiji fokusne skupine. V sklopu študije primera bomo predstavili kritično analizo odmevnega primera objave tajnih podatkov na internetu – afera udba.net – s poudarkom na spornih odločitvah inšpektorja, ki so nastale kot odziv na nastalo situacijo. V zaključku poglavja bomo podali odgovore na štiri domneve, ki so zapisane v uvodnem poglavju. Specialistično delo bomo zaključili s sklepnim poglavjem, kjer bomo ugotovitve prejšnjih poglavij povezali s hipotezami, ki smo jih privzeli v uvodu.

2 OPREDELITVE POJMOV

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

2.1 OPREDELITVE POJMOV

Razširjenost in pomembnost elektronske tehnologije je dandanes že tako velika, 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 neprecizni. 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 specialističnem delu.

2.1.1 Nova ekonomija

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 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,

[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.

konvergenca, inovativnost, zbliževanje potrošnikov in proizvajalcev, hitrost, globalizacija ter neravnovesje in jih v nadaljevanju kratko povzemamo po avtorju ter dopolnjujemo.

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. cluster*) 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 specialističnega 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 uporabita internet in omrežja za osnovo definicije. V tem smislu se internetna ekonomija 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 specialističnem delu.

2.1.2 Elektronsko poslovanje

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 jih pa 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 podjetji (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.

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.

3 E-OKOLJE S POUDARKOM NA SLOVENSKIH RAZMERAH

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.

3.1 ELEKTRONSKA DRUŽBA IN EKONOMIJA

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 od doma, 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 specialističnega dela, je nevarnost pred vdorom v zasebno sfero posameznika.

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. Dinamiko tehnološkega napredka kaže pred natanko 40 leti zapisani t.i. Moore-ov zakon[5]: procesna moč silikonskega čipa se podvoji vsakih 18 mesecev. Podatki ta fenomen potrjujejo, hkrati pa smo bili priča hitremu naraščanjem moči procesorjev in hitremu padanju njihovih cen (Woodall, 2000, str. 5-7). V resnici Moorov zakon predvideva le podvajanje zapletenosti vezij (recimo števila tranzistorjev na procesorju) vsakih 18 mesecev in kot tak še vedno drži; vprašanje je le, koliko časa bo še veljal. Ena največjih težav, ki je preprečila pričakovano stopnjevanje hitrosti Pentiumov 4, je izgubni električni tok. Pri velikih hitrostih izgubni tok pobegne iz vezja in le greje jedro (Mesojedec, 2005, str. 126). Ali to pomeni, da se bo razvoj čipov in posledično tudi celotne informacijske tehnologije ustavil? Seveda so izdelovalci najbolj zapletenih elektronskih vezji že v preteklosti naleteli na številne ovire, a so jih vedno uspešno preskočili s takimi ali drugačnimi inženirskimi zvijačami.

3.2 ELEKTRONSKO OKOLJE V SLOVENIJI

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, carinarniški 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 po drugi strani ugotavlja, da imamo še vedno neliberaliziran trg telekomunikacijskih storitev, nepovezana omrežja za prenos podatkov in zato tudi visoke cene storitev (Ministrstvo za informacijsko družbo, 2000). Prav te pomanjkljivosti, nadalje ugotavlja

[5] Gordon Moore, soustanovitelj podjetja Intel je v nekem intervjuju, leta 1965, podal znamenito tezo o podvajanju zapletenosti računalniških vezij (Mesojedec, 2005, str. 126).

MID, upočasnjujejo razvoj elektronskega poslovanja od javne uprave pa do gospodarstva in prebivalstva. Razvojno zaostajanje, ki se kaže v relativno manjših stopnjah rasti informacijske in telekomunikacijske tehnologije, v primerjavi z drugimi srednje in vzhodno evropskimi državami, je dokumentirano tudi v ocenah EITO[6], kjer je razvidno, da Slovenija sicer ohranja mesto v evropskem povprečju, vendar zaostaja za hitro rastjo v Češki, Estoniji in Poljski (Ministrstvo za informacijsko družbo, 2000). Podatki iz iste študije kažejo, da "tranzicijske države dohitevajo in prehitevajo Slovenijo tudi v pogledu ostalih indikatorjev, kot na primer delež digitaliziranih telefonskih linij in penetracija fiksne in mobilne telefonije, v pogledu same razširjenosti Interneta pa Slovenija ohranja določeno prednost".

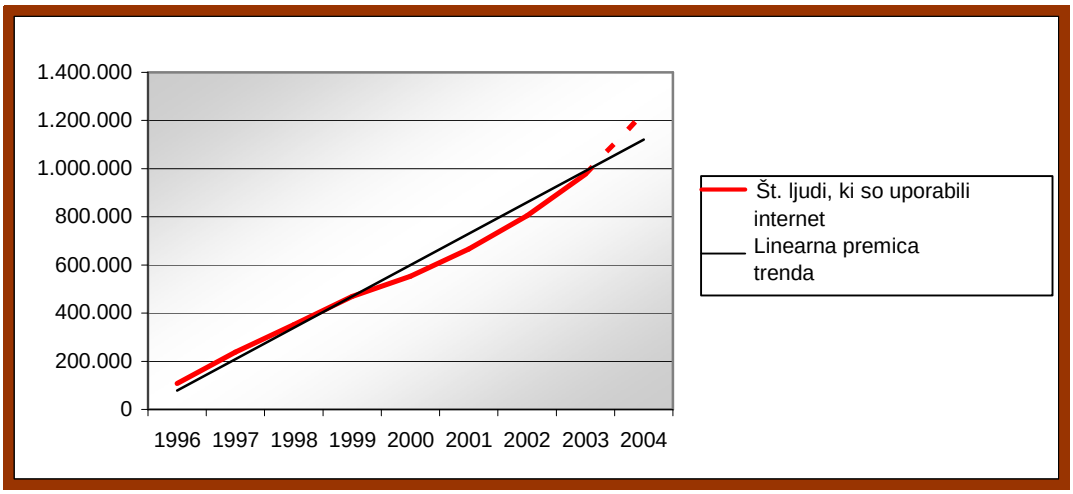
3.2.1 Prebivalstvo v elektronskem okolju

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 zato internet absorbirali zelo zgodaj, ustavlja se 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. Internet je uporabilo že preko 800 tisoč Slovencev, toda dejansko število rednih uporabnikov je manjše (Vehovar, 2000).

Število uporabnikov interneta se iz leta v leto veča. Zadnje merjenje, katerega rezultati so objavljeni na spletni strani www.ris.org kažejo, da je bilo leta 2003 že skoraj 1 milijon uporabnikov v Sloveniji. Ocene projekta RIS temeljijo na telefonskih anketah (n=3000) CATI centra. V spodnjem grafu so prikazani uporabniki, ki so že uporabili internet in jih ne smemo enačiti z aktivnimi uporabniki. Le-teh je bilo tega leta v Sloveniji dobrih 15%, kar pomeni, da je aktivnih/mesečnih uporabnikov okoli 240.000, ocena pa ima interval zaupanja širok okoli 15.000 oseb (RIS, 2003).

[6] EITO (European Information Technology Observatory) [URL: http://www.eito.com].

SLIKA 1: Uporabniki interneta v Sloveniji



Vir: Prirejeno po RIS, 2003

Na podlagi linearne funkcije trenda[7] napovedujemo, da bo v letu 2004 1.231.025 uporabnikov interneta. Pri tem predpostavljamo, da bodo različni dejavniki, ki vplivajo na število uporabnikov, tudi v letu 2004 delovali na enak način, kot so v obdobju 1996 – 2003.

Menimo, da je dobljena ocena zmotna, saj slednja ne upošteva tudi drugih dejavnikov, ki v predhodnih obdobjih niso bili toliko pomembni. Med slednje lahko uvrstimo starostno strukturo in število celotne populacije; le-ti bodo slednjo vrednost zmanjšali. Za bolj natančno oceno bi potrebovali subjektivno oceno strokovnjaka.

V starostni skupini od 10 do 75 let v Sloveniji internet uporablja že 48 odstotkov posameznikov, kar je enako povprečju v 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).

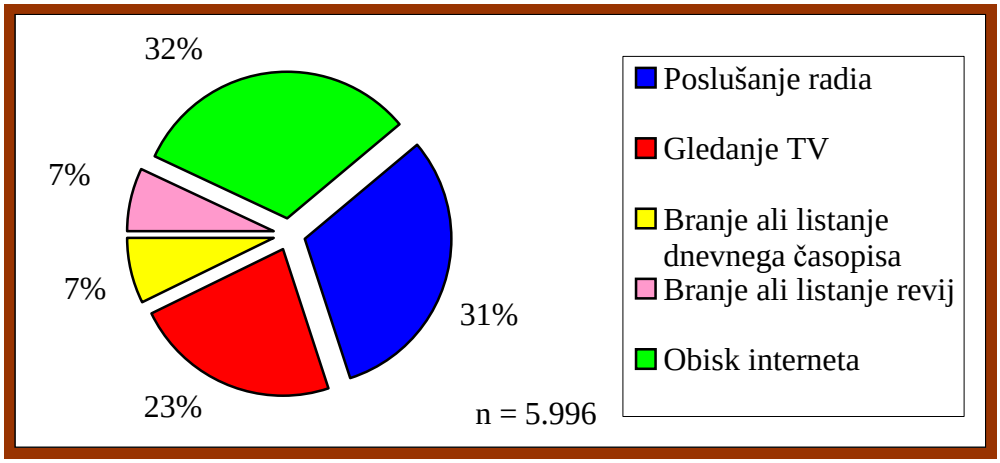
[7] $x_{t=2004} = 6$ $\quad Y'' = 520.925 + 118.350 * 6 = 1.231.025$

Ocena regresijskega koeficienta je enaka 118.350, kar pomeni, da se je število uporabnikov interneta v obdobju 1996 – 2003 vsako leto v povprečju povečalo za 118.350 uporabnikov. Ocena regresijske konstante znaša 520.925, kar pomeni, da je bilo število uporabnikov po posameznih letih različno, v povprečju pa jih je bilo 520.925 na leto.

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).

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 2: Dnevna uporaba posameznega medija



Vir: Najdi.si

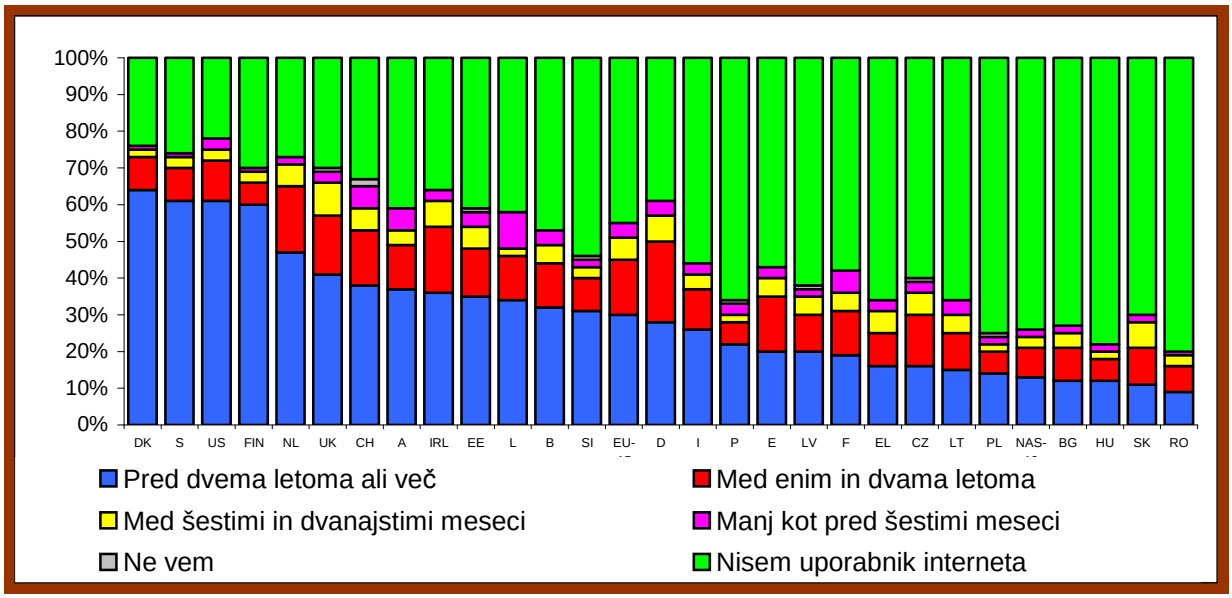
V prihodnje lahko pričakujemo, da se bo delež obiska interneta v primerjavi s pregledom oziroma poslušanjem medijev še povečeval. Vse večjo popularnost vsekakor spodbujajo vse boljši spletni informativni portali, kar povzroča izreden padec prodaje tiskanih medijev. Uporabniki pa so vse bolj pripravljeni 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. Rek, ki pravi *"Česar ne najdeš na internetu, to ne obstaja."*, vse bolj pridobiva na pomenu.

3.2.2 Izkušenost uporabnikov interneta

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.

Zanimivo si je pogledati analizo prve uporabe interneta po posameznih evropskih državah in ob tem pridobljenih izkušnjah. Najprej bi morali predstaviti skupino najrazvitejših držav, v katerih se zapazi tudi največji delež "izkušenih" uporabnikov. Kriterij izbire teh držav je naslednji: visok delež uporabnikov, katerih prva uporaba je bila pred dvema letoma ali več in da so uporabili internet vsaj enkrat v zadnjih štirih letih (tega podatka ni prikazanega na grafu). 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% 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 3: Prva uporaba interneta v izbranih evropskih državah v letu 2002



Vir: SIBIS, 2002/2003

Podatki o prvi uporabi interneta, uvrščajo Slovenijo tik nad evropskim povprečjem, saj je 31% populacije prvič uporabilo internet pred dvema letoma ali več (EU-15: 30%). Po drugi strani je delež manj izkušenih uporabnikov v Sloveniji med najnižjimi: 3,2 odstotka uporabnikov je začelo uporabljati internet med šestimi in dvanajstimi meseci ter 1,5 odstotka uporabnikov je pričelo uporabljati internet pred manj kot šestimi meseci (EU-15: 5,9 in 3,8). Nižji odstotek uporabnikov, ki so začeli uporabljati internet pred manj kot šestimi meseci, lahko opazimo le na Danskem, Finskem, Švedskem in Romuniji. V Sloveniji je prišlo do te razlike zaradi visoke penetracije uporabe interneta na začetku in pojemanja v novejšem obdobju. To opažanje tudi sovpada z razlago o relativno malem številu novih uporabnikov v zadnjih nekaj letih. Kot kaže, se populacija, ki še ni nikoli uporabila interneta, zelo težko odloči za uporabo le-tega.

Tudi v prihodnje lahko glede uporabe interneta - tako v Sloveniji kot v EU – pričakujemo zmerno rast v obsegu nekaj odstotnih točk, ki je značilna, 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.

3.3 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[8] (*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.

[8] V nadaljevanju specialističnega dela bomo besedi heker in vdiralec uporabljali kot sopomenki.

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 sledove (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*).

Povprečen uporabnik interneta je najpogosteje tudi žrtev računalniškega virusa. Gre za 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.

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). Da nam nezaželeni virusi ne bi povzročali težav, imamo na voljo več rešitev. Ena od rešitev je namestitev protivirusnega programa.

V nadaljevanju specialističnega dela se bomo posvetili predvsem elementom, ki posegajo v našo zasebnost in ne toliko ostalim nevšečnostim (virusi in črvi), ki nam načelom 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, s tem, ko v žrtvinem imenu pošilja škodljive datoteke. Vsekakor ostajajo najbolj pereč problem vohunski programi. Slednjim smo namenili podpoglavje 4.6.1.

4 ZAŠČITA OSEBNIH PODATKOV NA INTERNETU

Zasebnost[9] 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).

[9] 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).

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 specialističnem delu se bomo opredelili predvsem na informacijsko zasebnost, saj je le-ta v sodobni družbi, poleg zasebnosti komunikacij, najbolj ogrožena.

4.1 NADZOR KOT PREDPOGOJ ZA VSTOP V ČLOVEŠKO ZASEBNOST

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 manager sili delavce k povečanju produktivnosti (Lyon 1994, str. 25-26). Foucault povezuje nadzor z disciplino, disciplinski mehanizmi, ki so jih razvile sodobne družbe, 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 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 pri zagotavljanju varnosti, vzdrževanju reda in udobje. 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 komerkoli” (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.

4.1.1 Država in zasebnost

Leta 1996 so se Združene države odločile, da bodo začele zbirati podatke o vseh tujcih, ki iz takšnih in drugačnih razlogov vstopajo v njihovo državo. Naj ste poslovnež, turist ali terorist, vaši podatki bodo shranjeni v posebni biometrični podatkovni zbirki. Ko boste šli v ZDA, vas bodo fotografirali in vzeli prstne odtise, in pri vsakem naslednjem vstopu se bodo ti podatki preverjali in primerjali s podatkovno zbirko nezaželenih oseb.

Marsikdo bi Američanom v tem trenutku res pripisal, da tak projekt že izvajajo, a tudi pri njih je veliko nasprotnikov takšnega načina varovanja svojih meja. Projekt je trenutno še v idejni fazi, saj še ni izbran niti izvajalec, dviguje pa kar precej prahu, saj gre za velik poseg v človekovo zasebno sfero. Skrbi jih tudi vpliv na turizem in gospodarske povezave, strokovnjaki pa so zaskrbljeni tudi zaradi zanesljivosti takšnega sistema. Tehnologija prstnih odtisov še zdaleč ni tako dodelana, da se ne bi dogajale napake, zaradi katerih bi bilo lahko veliko osumljencev. Prve simulacije kažejo, da je lahko napak kar okoli 11 odstotkov, kar kaže na neuporabnost projekta (Moj mikro, 2004).

Prav tako kot nas skrbi, kdo gleda podatke o našem otroku (morebitne vedenjske, osebnostne ali učne težave, njegove sposobnosti, šolske ocene), smo občutljivi tudi, ko gre za podatke o našem zdravju in boleznih. Na Zavodu za zdravstveno zavarovanje Slovenije smo popisani prav vsi, ki imamo zdravstveno kartico. Kadar koli administratorka v zdravstvenem domu ali bolnišnici odčita našo kartico, lahko na njej prebere splošne podatke o imetniku (ime in priimek, datum rojstva, številko kartice), v elektronski obliki pa so zapisani še podatki o tem, kako smo zavarovani, kdo je naš osebni zdravnik, kakšne medicinsko-tehnične pripomočke imamo in ali želimo po smrti darovati katerega od svojih organov. Na zavodu pravijo, da je zdravstvena kartica miniaturni računalnik in je varovana tako, kot so varovani računalniki. Ključ za branje pametne kartice, kot ji pravijo, imajo le pooblaščeni zdravstveni delavci, ki imajo za njeno odklepanje tudi posebno profesionalno kartico in osebno kodo, ki jo poznajo le oni (Tepina, 2005, str. 14). Na kratko: na zavodu zagotavljajo, da našo zdravstveno kartico lahko berejo in vanjo pišejo le ljudje, ki imajo za to pooblastilo ali medicinsko osebje, ki skrbi za naše zdravljenje. Do podatkov, ki so na zdravstveni kartici, naj ne bi mogel nihče, ki nima pooblastila lastnika kartice. Lastnik zdravstvene dokumentacije o našem zdravstvenem stanju, boleznih, zdravilih, ki smo jih jemali ali jih jemljemo, je naš osebni zdravnik, ki ga veže prisega molčečnosti.

Ljudje smo krvavi pod kožo in radi širimo zaupne stvari, zato je najlaže priti do zaupnih zdravstvenih podatkov, če koga na ustrezni ustanovi dobro poznamo. Verjamemo, da so na sistemski ravni podatki varovani, vendar že dejstva, ki jih navaja Tepina (2005, str. 15) – v

Univerzitetnem kliničnem centru so računalniška gesla zapisana kar na listkih, ki se hranijo v bližini računalnikov in če poznaš eno geslo, vidiš celotno računalniško mrežo – zbujajo strah in dvome o varnosti naših podatkov.

Dr. Zoran Arnež iz Univerzitetnega kliničnega centra ugotavlja, da je največja varovalka za množico podatkov o bolnikih nepovezanost zdravstvenega informacijskega sistema, saj so podatki raztreseni po klinikah (Tepina, 2005, str. 14). Največji varovalki sta torej nered in zmeda, ki vladata v našem zdravstvenem sistemu.

4.2 PRAVNI VIDIKI VARSTVA OSEBNIH PODATKOV NA INTERNETU

V Sloveniji je pravica do zasebnosti zajamčena z Ustavo Republike Slovenije[10], 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 (Bogataj, 2002, str. 15). Poleg ZVOP-1 se varstva osebnih podatkov na internetu dotakne tudi Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP)[11], 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.

Slovenska Ustava elektronskih podatkov ne omenja, tako da je bilo urejanje tega področja prepuščeno ZVOP, ki je o podatkih v elektronski obliki govoril le v dveh členih in sicer:

- v 4. členu, ki določa način posredovanja (“Podatki se smejo posredovati prek telekomunikacijskih omrežij samo, če so posebej zavarovani s kriptografskimi metodami in elektronskim podpisom.”) in

[10] Ustava RS vsebuje vrsto pravic, ki se nanašajo na osebno sfero. Pri tem specialističnem 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).

[11] 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 bodo morali nemudoma odstraniti ali onemogočiti dostop do nje (Zmagaj, 2004, str.10).

- v 13. členu, ki določa obdelavo osebnih podatkov (“Strojna, sistemska in aplikativna programska oprema morajo zagotavljati, da bo obdelava osebnih podatkov skladna s pooblastili uporabnika osebnih podatkov”).

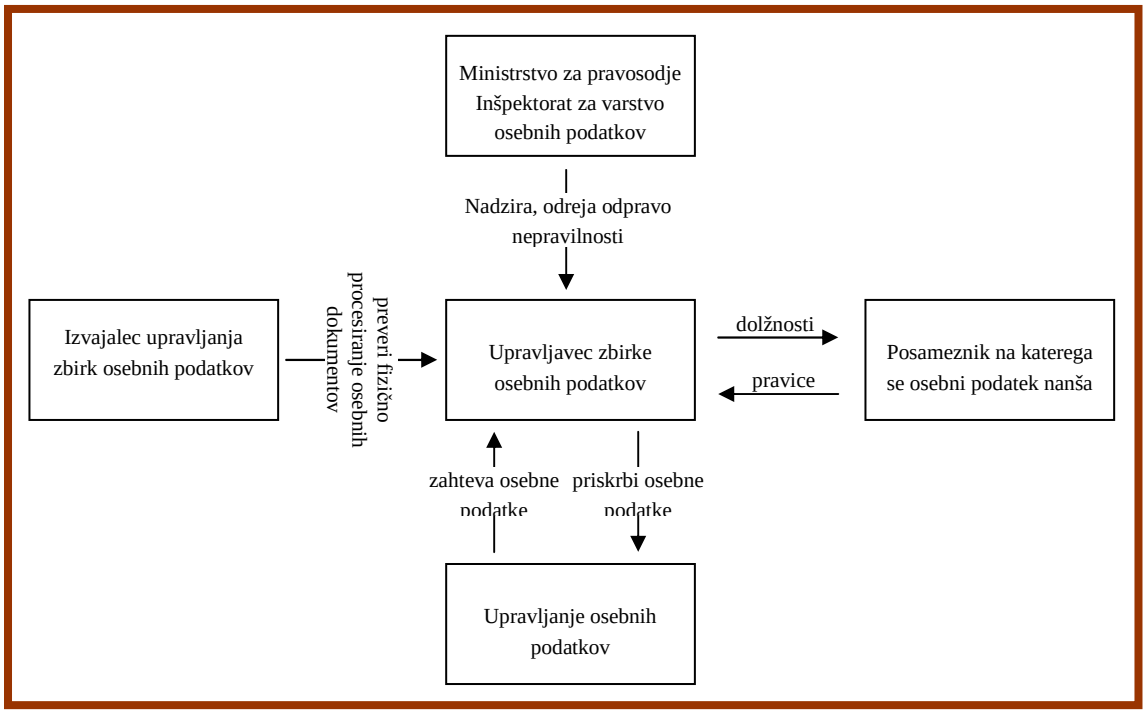
ZVOP torej ni reševal celovito področja varstva osebnih podatkov in zasebnosti v odprtih omrežjih. Za krepitev mehanizmov s tega področja je še vedno pomembno sodelovanje državnih organov s podjetji in posamezniki. Naloge državnih organov morajo biti povezane z zagotavljanjem trdnih temeljev s področja varstva osebnih podatkov in zasebnosti, predvsem z uporabo najnovejših tehnoloških rešitev in ustreznim izobraževanjem uporabnikov (Perše, 2000, str. 5).

4.2.1 Zakon o varstvu osebnih podatkov – ZVOP in ZVOP-1

Področje zasebnosti na internetu, ki je rdeča nit specialističnega dela, najpodrobneje obravnavata stari ZVOP in novi ZVOP-1. Določata, kateri podatki se lahko zbirajo in na kakšen način, kako se morajo hraniti ter komu jih je dovoljeno posredovati. 1.1.2005 je stopil v veljavo ZVOP-1, ki je poskusil zajeti vse spremembe na področju informacijske tehnologije od leta 2001 pa do danes. Obnavljanje in dopolnjevanje vsebine zakona, ki obravnava globalno, dinamično in konstantno rastoče virtualno okolje na štiri leta, je vsekakor prepočasi. Ugotavljamo, da zakonodaja ne more slediti novim vsebinam in aktivnostim, ki jih prinaša internet. Temu področju bi vsekakor morali nameniti več pozornosti, vendar ne samo na državni ravni, temveč tudi v sodelovanju z drugimi državami.

Varstvo osebnih podatkov se odvija v trikotniku med subjektom osebnih podatkov, upravljavcem zbirk osebnih podatkov in uporabnikom takih podatkov. Upravljavec osebnih podatkov ima dolžnosti predvsem do subjekta, na katerega se osebni podatki nanašajo, ta pa mu lahko dovoli (ali zavrne) določeno obdelavo, uporabo oz. posredovanje svojih osebnih podatkov. Od njega lahko zahteva, da ga mora obveščati o osebnih podatkih, ki jih vodi in se nanašajo nanj ipd. Uporabnik osebnih podatkov je oseba, ki iz kakršnegakoli razloga potrebuje osebne podatke drugih. Pridobi jih pri upravitelju zbirk osebnih podatkov, za to pa spet potrebuje ali pooblastilo s strani subjekta osebnih podatkov ali posebno zakonsko pooblastilo za vpogled v take podatke. Poleg omenjenih oseb so v proces zbiranja, shranjevanja, procesiranja in uporabe osebnih podatkov lahko vpleteni še inšpekcijsko nadzorstvo nad izvajanjem zakonov s področja osebnih podatkov (pri nas v okviru ministrstva za pravosodje), tehnične oz. informacijske službe, ki izvajajo dejansko procesiranje podatkov ter morebiti tretje države kot vir ali uporabnik takih podatkov. Tipična razmerja in subjekti zakona so predstavljeni na spodnji sliki.

SLIKA 4: Tipična razmerja in subjekti varstva osebnih pravic



Vir: Berčič et. al., 2003, str. 125

Izmed zgornjih tipičnih razmerij so najpomembnejša tista med upravljavcem zbirk osebnih podatkov in subjektom, na katere se osebni podatki nanašajo ter tista med upravljavcem zbirk osebnih podatkov in uporabnikom takih podatkov.

Kar se tiče uporabnikov zbirk osebnih podatkov, zakon za vsako zbirko osebnih podatkov določa, da je potrebno v katalogu podatkov natančno določiti uporabnike, za katere se podatki zbirajo in katerim se bodo posredovali. Določene zbirke podatkov predpisuje sam zakon (npr. centralni register prebivalstva, evidenca storilcev kaznivih dejanj itd.), hkrati pa predpisuje tudi njihove uporabnike (Berčič et. al., 2003, str. 125). Pri drugih zbirkah osebnih podatkov pa bodo morali upravljavci za zbiranje in posredovanjem takih podatkov pridobiti eksplicitna pisna dovoljenja subjektov, na katere se podatki nanašajo. Privolitev bo ravno tako morala vsebovati točno navedbo kroga uporabnikov. Pisci varnostnih politik upravljavcev zbirk osebnih podatkov bodo morali upoštevati te zahteve, če se bodo hoteli razbremeniti odgovornosti za morebitne prekrške in kazniva dejanja, ki jih podajamo v nadaljevanju.

22. člen ZVOP-1 določa, da mora upravljavec, ponavadi proti plačilu stroškov, osebne podatke posredovati uporabnikom, ki so upravičeni do dostopa za posamezno zbirko podatkov (Slika 4).

Zakon o varstvu osebnih podatkov določa naslednje:

1. Obdelava in uporaba osebnih podatkov je dovoljena edino pod pogojem, da ima upravljavec zbirke podatkov **pisno privoljenje posameznika**.
2. Osebni podatki se zbirajo **neposredno od posameznika**, v kolikor zakon ne določa drugače.
3. Osebni podatki se smejo obdelovati samo za **namen, določen s pisno privolitvijo posameznika** in se ne smejo uporabljati na način, ki ni združljiv s tem namenom.
4. Upravljavec zbirke osebnih podatkov mora za vsako zbirko osebnih podatkov zagotoviti **katalog podatkov**, kateri vsebuje podatke, določene v zakonu. Naziv zbirke osebnih podatkov, upravljavca zbirke in njegov sedež, kategorije posameznikov ter vrste osebnih podatkov, shranjenih v zbirki osebnih podatkov, mora upravljavec zbirke posredovati Ministrstvu za pravosodje najmanj 15 dni pred vzpostavitvijo zbirke osebnih podatkov.

Vir: Podjetnik, 2004

Zakon o varstvu osebnih podatkov je glede varstva osebnih podatkov precej strog, saj predpisuje denarne (in druge) kazni, ki lahko doletijo osebe, ki zbirajo in shranjujejo osebne podatke brez pooblastila in takih zbirk osebnih podatkov ne prijavijo pri ustreznih organih, ki o njih vodijo evidenco. Za najbolj resne primere zlorabe osebnih podatkov Kazenski zakonik predpisuje tudi posebno kaznivo dejanje zlorabe osebnih podatkov.

Zakon predpisuje prekrške v zvezi s pomanjkljivim varstvom oz. zlorabo osebnih podatkov, ki se lahko nanašajo na upravljavce zbirk, njihove podizvajalce, ki za njih opravljajo tehnično upravljanje zbirk ter tudi uporabnike zbirk. Upravljavci zbirk osebnih podatkov bodo morali zagotoviti, da bodo obdelovali osebne podatke samo na podlagi zakonske določbe ali privolitve posameznikov, da ne bodo obdelovali podatkov za namene, ki niso določeni v zakonu ali pisni privolitvi posameznika, da bodo pravočasno blokirali oz. zbrisali osebne podatke, ki se zbirajo za določen čas itd. (Berčič et. al., 2003, str. 126).

Za zlorabe osebnih podatkov pa bodo lahko kaznovani tudi uporabniki osebnih podatkov (če jih bodo uporabljali za namene v nasprotju z zakonom) ter tehnični izvajalci upravljanja zbirk osebnih podatkov. Ravno tako kot upravljavci, bodo tudi uporabniki morali z internimi akti in varnostnimi politikami zagotoviti pravilno ravnanje z osebnimi podatki.

Novi zakon o varstvu osebnih podatkov se od prejšnjega kaj bistveno ne razlikuje. Nova so predvsem poglavja, ki urejajo videonadzor, biometrijo ter evidenco vstopov in izstopov v prostore in iz njih.

Spremembe zakona zadevajo tudi varstvo osebnih podatkov v javnem sektorju. Podlaga sta zakon in osebna privolitev posameznika, vendar z večjim krogom izjem, kot je določeno v predhodnem zakonu. Pravice posameznika so tako razširjene. Ena temeljnih je pravica do

obveščenosti o obdelavi podatkov. V zakon so vgrajene varovalke in izjeme, kdaj osebnih podatkov ni dopustno obdelovati in uporabljati.

Podrobneje je urejeno področje videonadzora, ki določa, da mora (ali bi moral) upravljavec osebnih podatkov nadzorovano območje jasno in vidno označiti. Napisi, ki označujejo videonadzor, nas torej na to opozorijo in sami se odločimo ali bomo v tako "osvetljen" prostor vstopili in s tem tvegali, da bodo kamere posnele kaj počnemo in s kom smo ter to tudi shranile. Nekako samoumevno je, da morajo biti na primer banke, pošte, javne zgradbe, radio, televizija, šole in zdravstvene ustanove zavarovane tudi z videokamerami, manj samoumevna pa sta snemanje in nadzor v delovnih prostorih podjetij. Tepina (2005, str. 14) pravi, da zakon to dovoljuje le, če je nujno za varnost ljudi in premoženja ter če nadzor z milejšimi sredstvi ni mogoč. Za postavitev videokamer v podjetju potrebuje delodajalec soglasje sindikata, zaposleni pa morajo biti o snemanju pisno obveščeni. Snemanje v garderobah, straniščih in dvigalih je prepovedano. Biometrijske ukrepe je mogoče uporabljati le izjemoma, saj gre pri tem za ugotavljanje in primerjanje lastnosti posameznika, s katerimi se ugotavlja njegova istovetnost (prstni odtisi, šarenica, očesna mrežnica, DNK in podobno). Za varovanje ljudi in premoženja ter tudi za zagotavljanje reda v prostorih, je dovoljeno evidentirati vstope in izstope posameznikov - zaposlenih in obiskovalcev. Najpomembnejše je, kako podjetja in javne ustanove osebne podatke shranjujejo in varujejo.

Določeno zaščito zasebnosti pri uporabi telekomunikacij (tudi v internetu) nudi že omenjeni **Zakon o telekomunikacijah**. Storitve interneta so namreč telekomunikacijske storitve in torej neposredno spadajo pod predmet zakonskega urejanja telekomunikacij v širšem pomenu. To pa ne pomeni, da je zaščita v celoti ustrezna, ko govorimo o prenosu podatkov po svetovnem spletu, saj je zakon prvotno namenjen urejanju telefonskega komuniciranja in operaterjem, vendar ga je teže uporabiti pri zagotavljanju pravic in obveznosti ponudnikov internetnih storitev in predvsem upravljavcev e-poštnih strežnikov. Tako Zakon o telekomunikacijah ureja zgolj komunikacije po javnih omrežjih, kar pa pomeni, da njegove določbe ne veljajo za zaprte sisteme, npr. interne e-pošte v podjetjih in državnih ustanovah.

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, identifikacija udeležencev pri komuniciranju, varstvo osebnih podatkov ter samodejna obdelava 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[12] (Ur. l. RS. Št. 63/94, 70/94, 23/99).

4.3 PRISTOJNOST PRAVOSODNIH ORGANOV V SPORIH

Večina dogajanj po internetu se hkrati dotika pravnih ureditev v mnogih državah. Država določa, v katerih okoliščinah in na podlagi katerih dejstev bo uporabljeno njeno pravo (Ude,1996, str, 898).

Za zaprto elektronsko okolje je značilno, da je na nek način omejeno z znanimi udeleženci, ki morajo uporabljati vnaprej določene pristopne mehanizme ali pa je poslovanje omejeno na prenose med vnaprej določenimi končnimi točkami. Tudi zaprto okolje lahko uporablja omrežno infrastrukturo interneta, a zaradi tega še ne postane odprto. Med udeleženci zaprtega poslovanja veljajo vnaprej določena pravila in ni pomembno ali so jih določili večstransko ali enostransko. Tudi enostransko določeni pogoji poslovanja, ki jih druga stran sprejema, so pravni dogovor. Za lastnost zaprtega elektronskega poslovanja torej ni ključna tehnološka podlaga, temveč znana pravila igre, vključno z odgovornostjo. S tem zaprto elektronsko poslovanje vedno predstavlja pravno opredeljen prostor, čeprav sega prek državnih meja.

Dejavnosti v odprtem elektronskem prostoru niso nekaj, kar bi šlo čez državno mejo, temveč dejstva, ki se ne glede na državne meje hkrati dogajajo po celotnem svetu. Le-ta vsiljujejo posamezna pravna pravila, kajti dosedanji pojem pristojnosti je bil tesno povezan s fizično opredeljenim prostorom. Kako se bo urejala državna pristojnost v kibernetskem prostoru, je zagotovo eno ključnih razvojnih vprašanj tega medija. Sodišče naj bi vsak spor obravnavalo kot posebnost s samo njemu lastnimi dejstvi in to tako, kot je nastal. Odločitve je treba sprejemati previdno in zadržano, da novega medija ne bi po nepotrebnem ogrozili.

4.3.1 Načini reševanja sporov

Če posameznik meni, da je državni organ ali druga pravna ali fizična oseba neupravičeno posegla v njegovo pravico do zasebnosti, ki izhaja npr. iz Zakona o telekomunikacijah, Zakona o varstvu osebnih podatkov ali Zakona o elektronskem poslovanju, se lahko obrne na enega od

[12] 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.

nadzornih mehanizmov, ki jih predvidevajo omenjeni zakoni. Taki mehanizmi so npr. Inšpektorat za varstvo osebnih podatkov in Varuh človekovih pravic, poleg njiju pa so še Agencija za telekomunikacije, radiodifuzijo in pošto ter Tržni inšpektorat. Vsak zakon namreč vsebuje tudi kazenske določbe, ki predvidevajo denarne sankcije za kršitelje posameznih določb zakona.

Prizadeta oseba v sporu zaradi kršitve elektronske zasebnosti ima na voljo različne oblike pravnega varstva: ustavnosodno, civilno in kazenskopravno varstvo.

i. Ustavnosodno varstvo

Če je domnevni kršitelj državni organ, organ lokalne skupnosti ali oseba, ki je nosilec javnih pooblastil, obstaja možnost sprožitve upravnega spora po Zakonu o upravnem sporu zaradi kršitve temeljnih človekovih pravic in svoboščin.

V kolikor je posameznik neuspešno izčrpal že vsa druga pravna sredstva, lahko vloži ustavno pritožbo na ustavno sodišče ter v končni fazi tudi pritožbo na Evropsko sodišče za človekove pravice zaradi kršitve 8. člena Evropske konvencije o človekovih pravicah. Ustavno sodišče varuje temeljne pravice v okviru presoje skladnosti splošnih pravnih aktov z ustavo ali z obravnavanjem ustavnih pritožb zaradi kršitev s posamičnimi akti.

ii. Civilnopravno varstvo

Prizadeta oseba lahko sproži civilni (npr. odškodninski) spor. Za civilnopravno varstvo so pomembni zlasti tisti členi Zakona o obligacijskih razmerjih (ZOR), ki vsebujejo zahtevo, da se odstrani škodno nevarnost, zahtevo, da prenehajo kršitve pravice osebnosti in denarno odškodnino ter zadoščanje v posebnih primerih.

V zvezi z internetom je zanimiva morebitna izvedba 199. člena ZOR - objava sodbe ali popravka. Sodbo bi lahko z dovoljenjem sodišča objavil sam oškodovanec. Lahko pa se zgodi, da jo objavi tudi brez dogovora s sodiščem.

Varstvo zasebnosti poznajo tudi civilni zakoniki drugih držav. Za odškodninsko zavezo morajo obstajati splošne predpostavke: nedopustnost, odgovornost in obstoj škode.

iii. Kazenskopravno varstvo

Zasebnost je varovana tudi s kazenskopravnimi določbami. V povezavi s kazenskimi postopki so možnosti za kršitve zasebnosti izjemno velike. Ker se del javnih občil seli v elektronsko okolje, bodo v njih postale aktualne vse oblike posegov v zasebnost, ki jih je možno storiti preko občil. V hujših primerih je mogoče, da poseg v zasebnost posameznika pomeni celo kaznivo dejanje, pri čemer posameznik poda kazensko ovadbo pristojnemu državnemu tožilcu oziroma na sodišče

vloži zasebno tožbo. Kazenski zakonik navaja več kaznivih dejanj, ki inkriminira tudi posege v elektronsko pošto. Pri tem zakon žal ne ločuje med nadziranjem e-pošte v realnem času in med pregledom že dospele e-pošte. Ne glede na to je omenjeno določilo mogoče uporabiti tudi za kazenski pregon oseb, ki neupravičeno posežejo v zasebnost e-pošte.

Vse omenjene oblike pravnega varstva veljajo le na ozemlju Republike Slovenije. Če je sporno dejanje povzročila tuja pravna ali fizična oseba, npr. ponudnik internetne storitve, ki je v tujini, ima slovensko pravo malo moči. Pri tem se ponovno kažeta globalna narava interneta in z njo povezan problem pravne pristojnosti v različnih državah.

4.4 PRIJAVE, PRITOŽBE IN POBUDE POSAMEZNIKOV V ZVEZI Z VARSTVOM PODATKOV IN ZASEBNOSTI

Po podatkih Inšpektorata za varstvo osebnih podatkov je leta 2003 inšpektorat prejel in obravnaval 60 prijav, pritožb ali pobud, od tega je bilo v 19 primerih ugotovljena kršitev varstva osebnih podatkov, zaradi katere je bilo možno zoper kršitelja podati predlog za uvedbo postopka o prekršku (Bogataj, 2004, str. 13).

Iz razloga neustreznega varovanja elektronske zasebnosti so bile podane tri prijave. Poleg v poglavju 6.3 opisane afere udba.net, v kateri je nedvomno šlo za največjo do sedaj ugotovljeno zlorabo osebnih podatkov v Republiki Sloveniji, je inšpektorat v letu 2003 obravnaval še dve prijavi. Ena od prijav je bila vložena zaradi objave osebnih podatkov predsednikov društev, druga pa zaradi objave osebnih podatkov izžrebancev (Bogataj, 2004, str. 26).

Prijavo, ki je bila vložena zaradi objave osebnih podatkov predsednikov društev, je inšpektorat prejel oktobra 2003. V njej je bilo navedeno, da je na internetu nezakonito objavljen vlagateljev domači naslov. Po pregledu spletne strani je bilo tako ugotovljeno, da so na internetu dejansko objavljena osebna imena in naslovi predsednikov društev. Le-ta se po določbah 5. člena ZVOP-a lahko uporabljajo samo v primeru, če se ti strinjajo, oziroma z drugimi besedami, člani društva se morajo sami dogovoriti, katere osebne podatke o članih bodo zbirali in komu se bodo njihovi podatki posredovali. Inšpektorat je v tem primeru vlagatelju predlagal, naj se sam obrne na lastnika strežnika ter od njega zahteva, da se s spletne strani odstrani njegov naslov, oziroma naj se v društvu najprej sami dogovorijo, katere podatke bodo objavljali na spletnih straneh ter da naj se na inšpektorja ponovno obrnejo šele v primeru, če bodo njegovi podatki še naprej objavljeni kljub njegovemu nestrinjanju. Ker se po tem predlogu vlagatelj ni več oglasil, so postopek ustavili (Bogataj, 2004, str. 26-28).

V zvezi z objavo osebnih podatkov na internetu, je inšpektorat prejel tudi prijavo, v kateri je bil izražen sum, da so na internetu nezakonito objavljeni osebni podatki nagrajencev. Po pregledu spletne strani je bilo ugotovljeno, da so na spletni strani dejansko objavljeni osebni podatki 51-ih nagrajencev in sicer njihovo osebno ime, priimek, naslov, pošta, vrsta nagrade, davčna izpostava in davčna številka. V nadaljnjem postopku je bilo ugotovljeno, da zavezanec nima pisnih

privolitev za takšno obdelavo podatkov. Zavezanec bi si moral, preden na spletnih straneh objavil osebne podatke posameznega nagrajenca, od njega pridobiti podpisano izjavo, iz katere bi bilo razvidno, da le-ta zavezancu dovoljuje, da določene njegove osebne podatke objavi na spletnih straneh. Poleg tega bi moral zavezanec skladno z določbami sedmega odstavka 3. člena ZVOP-a predhodno objaviti tudi tekst, iz katerega bi bilo razvidno, za kakšne namene se bodo obdelovali in uporabljali osebni podatki nagrajencev ter koliko časa se bodo njihovi osebni podatki hranili in objavljali na spletnih straneh (Bogataj, 2004, str. 28-30).

Majhno število prijav, ki se nanašajo na elektronske medije kaže na to, da so posamezniki o možnostih zlorab na tem področju še premalo seznanjeni in se še ne zavedajo nevarnosti. Stanje se, na področju varstva osebnih podatkov v Republiki Sloveniji iz leto v leto izboljšuje, vendar še vedno prepočasi. Izboljšanje stanja se kaže že s tem, da se obdelovalci osebnih podatkov pa tudi posamezniki, vse bolj zavedajo pomena varstva osebnih podatkov. Zaradi tega število prijav in pritožb v zvezi s sumom kršitve varstva osebnih podatkov iz leta v leto narašča, še posebej pa se je v obravnavanem obdobju povečalo število zaprosil za podajo mnenj in tolmačenj, ki so jih v zvezi z varstvom osebnih podatkov na inšpektorat naslovili obdelovalci osebnih podatkov (Cvetek, 2004). Takšno povečanje po eni strani kaže na to, da se obdelovalci osebnih podatkov vse bolj zavedajo pomena varstva osebnih podatkov, po drugi strani pa takšno povečanje števila zaprosil kaže tudi na to, da se zdijo obdelovalcem osebnih podatkov nekatere določbe ZVOP-a še vedno premalo razumljive. Žal pa je to še vedno eden poglavitnih razlogov za to, da se je večina prijav in pritožb, ki jih prejme inšpektorat za varstvo osebnih podatkov, pokazala za neutemeljene.

Primer slabe zaščite zasebnih podatkov so tudi spletne strani Ekonomske fakultete oziroma portal Študent-net. Slabost se kaže predvsem v enostavnem dostopu do osebne kartoteke posameznika, z vnosom njegovega uporabniškega imena in gesla. Kritični nismo do tehnologije same, temveč do načina dodeljevanja uporabniških imen in gesel. Preprostost se kaže v enostavnem in vsem znanem sistemu dveh nizov številk. Prvi niz je vpisna številka, ki jo je moč dobiti na vsakem koraku, le sprehoditi se je potrebno, bodisi dobesedno mimo oglasne deske ali pa virtualno, saj se večina profesorjev poslužuje objave rezultatov preverjanja znanja na spletnih straneh predmeta. Geslo je mogoče na prvi pogled malo težje dobiti, ker je sestavljeno iz rojstnega datuma, vendar že nekaj klikov in malo iznajdljivosti lahko kaj kmalu obrodi sadove.

Kaj hitro bi nekdo rekel, da je geslo možno spremeniti, kar vsekakor drži. Sistem gesel temelji na predpostavki, da si bodo uporabniki ob prvi prijavi, spremenili gesla. Zanimivo bi bilo narediti analizo spremembe gesel, s pomočjo katere bi lahko ugotovili, koliko študentov še vedno uporablja prvotno dodeljena gesla. Kaj nam pomaga, da se ob prijavi povežemo s fakultetnim strežnikom preko varne povezave, če pa je v uporabi trivialen sistem administracije.

Na eni strani je ponudnik spletnega portala, ki ne namenja dovolj pozornosti varnosti, na drugi pa brezbrižni uporabniki. V kolikor se ponudnik storitve zaveda težave, bi se moral bolj potruditi za varnost, nenazadnje je on eden, študentov pa je nekaj tisoč. Sprememba sistema s strani

ponudnika bi iz tehničnega in organizacijskega vidika pomenila odpovedati se skoraj popolni avtomatizaciji in preiti na uvedbo podpornega oddelka, ki bi skrbel za dodeljevanje gesel. Druga in za fakulteto ugodnejša rešitev – dvig zavesti uporabnikov – je uresničljiva le na dolgi rok.

4.5 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 skupine[13], elektronsko poslovanje[14] in elektronsko oglaševanje. Vsaka od naštetih storitev predstavlja določeno tveganje s stališča varnosti osebnih podatkov in zasebnosti v širšem smislu.

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*, ki omogoča rutinsko, namensko pa tudi "naključno" zbiranje, hitro procesiranje, klasificiranje ter povezovanje podatkov) omogočeno avtomatsko zbiranje podatkov, objavljenih na internetu. 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 marketinška agencija in nam v elektronski predal začne pošiljati reklamna sporočila oziroma tako imenovano pošto z elektronskimi "smetmi" (*angl. junk mail*).

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.

Če 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** (poglavje 5.3.1). 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

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

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

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 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. Opozarjanje nanje je možno tudi izključiti (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).

Največ se uporabljata Tracking Cookie in RedSherrif, ki se pregledovalniku Explorer predstavita kot kolačka, s kakršnima prepoznajo uporabnika, na primer zaradi registracije.

Oglaševalske agencije, ki jim 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 novo nastale 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 trenutno 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-te 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 Macromedia-i so se že odzvali in ponudili novo nastavitev, ki ponudi možnost samodejnega brisanja objektov, ki niso del Flash predvajalnikov.

Poleg piškotov 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, vendar 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 ekonomskega okoriščanja.

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 marketinških agencij veča. Iz 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 iz 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 slednjih storitev, ki vsekakor ne smejo biti enkratne narave. Te si morajo slediti, saj že odprtje enega porta 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 opazuješ 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 ni kaj dosti za storiti, 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. Na novo sprejeti 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 podjetji, ki uporabljajo internet kot del medijskega načrta. Zaradi trenutne aktualnosti vprašanja in pomembnosti tematike, smo slednjemu namenili poglavje, ki sledi.

4.5.1 Oglaševanje na internetu

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.

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.

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 ponudnik dostopa do interneta, država dostopa, operacijski sistem, spletni iskalnik, različica 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 tudi znana pot do njega. Vsakdo se je že srečal s spletno anketo ali nagradno igro, s katero obiskovalca pozivajo, da naj jo izpolni saj bo lahko na ta način sodeloval v nagradni igri in si priboril eno od lepih 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 ne iščejo namreč 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 sklepajo, 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. In 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 spletni strani je svojim uporabnikom ponudilo izbiro med oglasi, ki se pojavljajo naključno ali oglasi, ki so bili selekcionirani glede na njihove potrebe. Na žalost je večin tistih, ki ne opozarjajo na svoje početje.

Oglaševalska podjetja niso edina, ki zbirajo naše podatke za komercialne namene. Zanimivo je, da so največji trije ponudniki brezplačne pošte 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 lokacijo, 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 zbiranje oglaševalskega denarja (Linn, 2005). Podoben primer, ki je sprožil val ogorčenja, je nova 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 iz 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).

4.6 ALI JE ZAŠČITA POTREBNA?

Analitiki in raziskovalci, specializirani za zaščito, namreč ocenjujejo, da bodo napadi virusov ter črvov, trojanskih konjev, klicalnikov in drugih hekerskih orodij letos še hujši, s težjimi morebitnimi posledicami za poslovanje. Po oceni META Group so podjetja lani porabila 8,2%

informacijskega proračuna, za zaščito od virusov in podobnih nevšečnosti, 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 lani 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[15], ki se prek e-pošte hitro širijo po celem svetu in povzročajo škodo največjega obsega. Velike škode lahko prinesejo tudi vohunski programi, ki po vdoru zbirajo podatke in jih pošiljajo na določene e-naslove v cilju 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 lahko najpogosteje zasledimo kot razlog hekarskega 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 neželena e-pošta (*angl. spam*), ki je po obsegu že dosegla "običajno" e-pošto, danes tako pomembno za poslovanje. Strokovnjaki so mnenja, da bo letošnje leto nezaželena e-pošta presegla "običajno" kar za 75%. Neželena 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.

Najbolj razširjen in za zbiratelja enostaven način zbiranja zasebnih podatkov poteka s pomočjo uporabe programov imenovanih *spyware*.

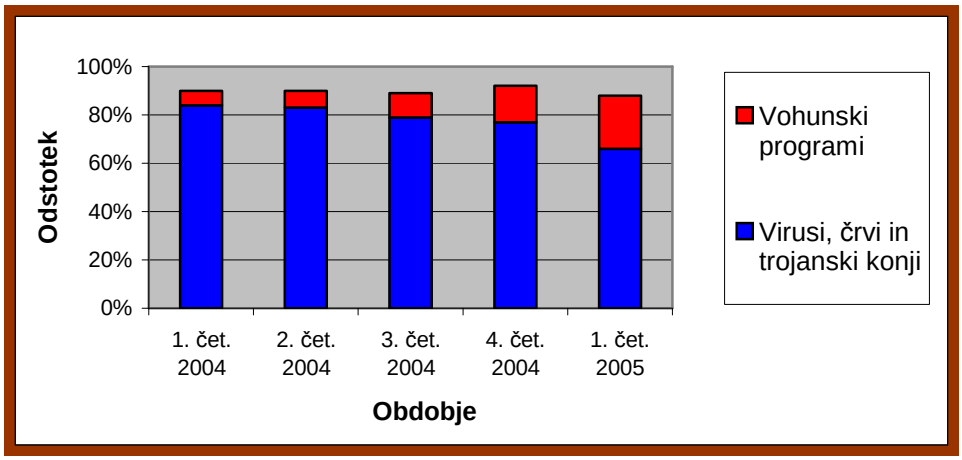
4.6.1 Vohunski programi: nadloga ali nevarnost?

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 specialističnega dela). Ti programi ne samo da vdirajo v našo zasebnost, vendar 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 (*angl. cookies*), ki jih lahko iznajdljivi avtorji uporabijo za zbiranje podatkov o navadah uporabnikov, kar je vsekakor vdor v zasebnost.

[15] 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.

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 predhodne 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 ostale nadloge.

Nekatere[16], 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 programsko rešitev.

Posledice, ki so rezultat nameščenih vohunskih programov so naslednje:

- motenje z reklamnimi sporočili,
- povzročanje sprememb v delovanju računalniku 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.

Vir: Povzeto po Djurdjič, 2004, str. 20 – 22.

[16] 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.

Vohunskih programov se marsikje lotevajo povsem brezskrbno in nepripravljeno. Med tem, ko si danes pri virusih prizadevamo, da bi bile definicije za protivirusne programe ažurne domala vsako minuto, virusno nevarnost pa danes tipično preverjamo na več različnih mestih (odjemalcih, strežnikih, internetnih prehodih), 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.

Tu so še zamaskirane (*angl. phishing sites*) strani, ki 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[17]. 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 Atni-Phishing Working Group, ki poroča, da se je število zamaskiranih strani v zadnjem letu povečalo za dobro četrtino (Ward, 2005).

Letos lahko pričakujemo, da bomo na žalost priča še več črvom, zaradi njihove vse večje sposobnosti hitrega širjenja in tudi trojanskih konjev, ki bodo še bolj sposobni nameščanja zlonamernih programov na računalnike.

4.7 NAPREDNE TEHNIČNE REŠITVE KOT PRIPOMOČEK PRED VDOROM V ZASEBNOST

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.

[17] 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).

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[18] (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

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

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.

4.8 ALI BO TERMIN "VIRTUALNA ZASEBNOST" SČASOMA IZGUBIL NA POMENU?

Strokovnjaki na področju računalniških virusov in varnostni analitiki svarijo, da se nevarnost vdorov in posegov v privatno okolje ne bo kmalu polegla, še več, stanje naj bi postajalo čedalje slabše. Hekerji imajo po novem poleg standardnih motivov (dokazovanje znanja, koristoljubje …) še nov, politični motiv. Vohunski programi postajajo vse bolj prikriti in vse bolj spretni – nekateri znajo celo prelisičiti ali celo onemogočiti programe, ki bi jih lahko zaznali! Leto 2005 tako nadaljuje grozeče trende iz preteklosti oziroma jih še poglablja. Uporabniki interneta postajajo zbegani in prestrašeni, saj več ne vedo komu gre zaupati. Vedno pogosteje se pojavljajo nove oblike vdorov v zasebnost, ki jih je nemogoče predvideti. Oglaševalska podjetja so spoznala prednosti, ki jim jih ponuja internet in slednjim se ne želijo odpovedati, še več, pripravljena so investirati veliko finančnih sredstev z namenom ohranitve sledljivosti uporabnikov. Nekatere spletne rešitve ponujajo proti plačilu vrsto spornih informacije, ki se navezujejo na posameznika. Podoben sistem je Zaba.

Spletni portali za iskanje ljudi

Že vrsto let obstajajo spletni portali preko katerih uporabniki iščejo sošolce, stare prijatelje, znance ali kogarkoli za zabavo. Podobne storitve omogoča tudi portal ZabaSearch.com in to brezplačno. ZabaSearch omogoča zelo hitro, z nekaj kliki in vnosi iskalnih kriterijev, popolnoma brezplačno in z veliko natančnostjo iskanje oseb. Zastrašujoče je to, da ima vsakdo, brez stroškov vpogled v povezane izčrpne baze javnih podatkov o vseh subjektih, ki prebivajo na območju ZDA. Gail Hillebrand iz zveze potrošnikov v San Franciscu, ZDA je zaskrbljen in zgrožen, saj ne more verjeti, kako je lahko nekdo zbral ogromno količino osebnih podatkov, jih povezal in ponudil javnosti popolnoma brezplačno (Lazarus, 2005). Predsednik ZabaSearch Robert Zakari je dejal, da za oglaševanje niso namenili niti centa (Lazarus, 2005). Spletni portal je bil postavljen 28.02.2005 in do danes je reklama od ust do ust prispevala nekaj sto tisoč obiskov dnevno.

Zakari uporablja na prvi pogled dokaj logičen argument, ki pravi, da na ta način lahko ljudje izvedo, kaj se ve o njih. Toda, ali to pomeni, da bi moral vsak državljan obiskati portal in poiskati svoje podatke ter ali ni ustaljena praksa, da se osebni podatki pojavijo v javnih zapisih le s privolitvijo osebe, na katero se ti podatki navezujejo? Sam sistem ne omogoča le izpisa osnovnih podatkov iskane osebe (ime in priimek, naslov in telefon). Pač pa je možno pridobiti tudi satelitski posnetek hiše, 5-dnevno vremensko napoved za okrožje, kjer se nahaja ciljna oseba, obširno kartoteko, ob doplačilu pa še podrobnejše podatke o zgodovini in kreditni sposobnosti.

ZabaSearch omogoča, da se posamezniki odstranijo iz baze s tem, da pošljejo preko e-pošte svoje osebne podatke (ime, datum rojstva, naslov in telefonsko številko), hkrati pa imajo zapisano v izjavi zaupnosti, da ne garantirajo, da se ne bo njihovo ime v prihodnje pojavilo v katerem drugem viru ali pa ponovno kar na portalu ZabaSearch.com. Edini izhod, ki še ostane je, da poseže oblast in uredi področje z ustrezno zakonodajo in inšpekcijskim nadzorom, ki bo spremljal izvajanje restriktivne politike na področju virtualne zasebnosti.

Radiofrekvenčna identifikacija

Predstavljajte si sledeče: Vstopili ste v trgovino z oblačili in namesto pozdrava trgovca začne na 42" plasma monitorju utripati vaše ime in računalniški glas vas nagovori: "Veseli nas, da ste ponovno prišli [vaše ime]". V nadaljevanju se pod vašim imenom izpiše seznam predhodnih nakupov ter predlogi nove kolekcije, ki vam jih je pripravil računalnik glede na vaše preference. Mogoče se sprašujete, od kod te informacije: računalnik je preko oddajnika zaznal čip, ki je nameščen na vašem puloverju, kupljenim pred nekaj meseci ravno v tej trgovini. Takoj ko ste vstopili v trgovino vas je računalnik prepoznal kot stranko. Mogoče se vse to sliši kot znanstvena fantastika, vendar vse to bo mogoče v bližnji prihodnosti z uporabo že vpeljane tehnologije, ki se imenuje radiofrekvenčna identifikacija[19] (*angl. radio frequency identification – RFID*).

V najpreprostejši obliki lahko tehnologijo radiofrekvenčne identifikacije opišemo kot sistem zelo majhnih značk - čipov (velikokrat velikosti "pike" v tisku), ki prek antene oddajajo radijski signal. Pritrdimo jih lahko na predmete (izdelke) ali bitja. Bralna naprava (čitalnik) oddaja elektromagnetno valovanje, ki ga značka brezžično prepozna, ko pride v njen domet. V kratkem času lahko bralna naprava identificira večje število značk. Prednost tehnologije je v njenem brezžičnem delovanju in dejstvu, da deluje tudi v zahtevnih okoljih, kjer se pojavljata mraz, umazanija, ali tam, kjer ni mogoča neposredna dostopnost, saj za branje ni treba, da je v vidnem polju (Vindiš, 2005).

Kot mnoge druge tehnologije je tudi radiofrekvenčna identifikacija prisotna že dolgo, približno petdeset let, a se ni uveljavila, ker še niso v celoti izpolnjeni pogoji za njeno množično uporabo. Danes, ko se s serijsko proizvodnjo nižajo cene čipov[20], ki so eden osnovnih elementov te tehnologije, internet in mobilne komunikacije pa so doživele hiter vzpon, ostaja RFID vse bolj vroča tema.

Ne samo, da je možno s pomočjo RFID tehnologije prepoznati produkt, kot to počno čitalci črtnih kod, pač pa se lahko vsak čip programira posamično. Strokovnjaki napovedujejo, da bodo baze podatkov o čipih postale zelo zanimive za tretje osebe. Brez poostrenega nadzora in dodatnih varnostnih ukrepov se lahko pripeti, da bodo nepooblaščeni uporabniki kaj hitro

[19] Najbolj znani uporabnik RFID-a so trgovine Wal-Mart. Nove tehnologije RFID poskusno uvajata tudi Tesco in Metro. Metro je s trgovino prihodnosti predstavil napredno uporabo RFID v prodaji na drobno.

[20] Gross (2004) navaja, da znaša vrednost enega čipa med 0,2 in 1 USD. Množična uporaba tehnologije RFID bo prispevala k znižanju vrednosti čipov in s tem bo postala dostopnejša tudi ostalim trgovcem.

izkoristili njihove prednosti (primer: oseba, ki bi se sprehajala po ulici bi z dovolj močnim oddajnikom zaznala kdo kaj poseduje) (Wayne, 2005). Razdalja ni ovira, saj lahko znaša slednja med čipom, ki nima lastnega napajanja in čitalcem tudi do 8 metrov (Gross, 2004).

Poznavalci tehnologije RFID se bojijo, da bodo trgovci začeli uporabljati radiofrekvenčno identifikacijo tudi za druge namene. Prodajalci bi lahko sledili svoje stranke tudi, ko bi zapustili njihovo trgovino (primer: proizvajalec športnih copatov bi lahko na neki športni prireditvi ugotovil, koliko obiskovalcev nosi njegovo znamko).

Tehnologija radiofrekvenčne identifikacije lahko zelo spremeni način, kako bomo v prihodnje poslovali, nakupovali in živeli. Drobni čipi, ki spremljajo ljudi in predmete in omogočajo številne storitve, utegnejo prodreti v vse pore našega življenja in to dobesedno. Sledenje ljudi, ki bi imeli RFID vsadek v svojem telesu, bi v urbanem okolju potekalo popolnoma avtomatizirano. ONI bi imeli, brez kakršnih koli naporov, popoln nadzor nad nami in našimi aktivnostmi. Temu bi lahko rekli popolni nadzor.

Nekatere bolnišnice so že nadomestile identifikacijske zapestnice s trakcem, v katerem se nahaja tudi RFID čip. Na ta način ne sledijo le bolnikom, temveč tudi zdravnikom in medicinski opremi, saj v vsakem trenutku poznajo natančno pozicijo iskanega predmeta oziroma človeka. Kljub temu, da je širša uporaba sistemov lociranja še daleč, so ena najbolj zainteresiranih skupin za uvedbo novosti starši. Ti bi lahko ob vsaki uri pogledali, kje se nahajajo njihovi otroci (Kavita, 2005).

Ljudje, ki nočejo biti nadzorovani oziroma prepoznavni, so že iznašli postopke, s katerimi se onesposobi čipe. Na trgu se že pojavljajo naprave, ki čipe deaktivirajo. Lahko pa se jih lotimo na bolj rudimentaren način. Delovanje slednjih se lahko zmoti, če se jih obda s folijo, popolno uničenje pa se izvede v kuhinjski mikrovalovni pečici.

Internetna telefonija

Pred leti smo bili priča, tako kot pri domala vseh novih tehnologijah, hitremu vzponu internetne telefonije (*angl. voice over IP - VoIP*), temu pa je sledilo neizbežno obdobje streznitve. Konceptualno je bilo vse slišati fantastično, zapletati pa se je začelo v podrobnostih, ki pa niso bile tako nepomembne. Predvsem so bili stroški zamenjave starih telefonskih sistemov in uvedbe novih izrazito visoki, časi povrnitve vložka pa nerealno dolgi.

Danes se zdi, da je večina teh težav za nami. Standardi so večinoma zaokroženi in že vsebovani v izdelkih, hkrati pa se je tudi sama internetna infrastruktura razvila in pridobila nove zmogljivosti, ki bolj ali manj brez težav lahko prenesejo tako pomembno (in s stališča prepustnosti požrešno) tehnologijo, kot je VoIP. Alternativ in ponudnikov je dovolj, da lahko računamo na sprejemljive, vendar še zdaleč ne nizke cene. Toda ne glede na vse to so statistike jasne. Analitske družbe pravijo, da bo več kot polovica vseh novih telefonskih sistemov

podpiralo telefonijo IP, do leta 2007 pa naj bi bil delež internetne telefonije v novo prodani opremi že 97 %. Te številke jasno kažejo, kam se usmerja globalni trg (Djurdjič, 2004).

Telefonija IP je tako kakor druge podatkovne storitve podvržena najrazličnejšim omrežnim nevarnostim, od virusov naprej. Za zdaj po svetu še ni bilo nobenega večjega vdora v sisteme VoIP, vendar tehnologija naravnost kliče hekerje. Tako kot pri vseh omrežnih storitvah bo torej treba investirati tudi v segment varnosti. Z namenom zagotovitve večje varnosti internetne telefonije in koordinacije pri vpeljavi novih standardov je bilo pred časom ustanovljeno združenje Voice over IP Security Alliance. S to pobudi naj bi se v kali izognili težavam, ki pestijo sodobna računalniška omrežja, so pa ta obenem temelj za storitve VoIP. Število sodelujočih podjetij se je hitro povzpelo čez 50, med znanimi imeni pa so McAfee, MCI, PricewaterhouseCoopers, Samsung Telecommunications America, Sprint in VeriSign (Lawson, 2005).

Nevarnosti pri VoIP storitvah se kažejo v DoS[21] (*angl. denial-of-service*) napadih, glasovnih smeteh[22] (*angl. voice spam*), vpadih v zvezo, vrinjanju besed v aktivni pogovor in neke vrste tehnikah ribarjenja (*angl. phishing*), pri katerih gre za krajo telefonske številke, ki se izpiše na virtualnem telefonu. To so le prve oblike groženj, ki nas bodo spremljale ob uporabi internetne telefonije. Nadzora nad tehnologijo VoIP se poslužuje tudi država. V lanskem letu je Zvezna komisija za komunikacije izdala odločbo, da morajo ponudniki internetne telefonije priskrbeti ustrezna stranska vrata, ki jih bo uporabljal za namene prisluškovanja ustrezen organ (Hesseldahl, 2005).

Seveda obstajajo tudi tehnike, ki pripomorejo k znižanju tveganja. Tako lahko pri glasovnih paketih uporabimo enkripcijske metode, ki bodo preprečile vpade v zvezo in dodajanje besed. Poskrbeti je potrebno za varovana omrežja in ustrezno strojno ter programsko opremo. Uporabljati je potrebno certificirane sisteme in ne take, ki bi omogočali oddajanje tudi tretjim osebam.

Zaskrbljujoče je dejstvo, da so se z internetno telefonijo pričeli ukvarjati tudi ponudniki stacionarne telefonije, ki pa nimajo izobraženega kadra na področju internetne varnosti in katerim so virusi, hekerji in črvi dokaj tuji (Greene et. al., 2004).

[21] Glavna značilnost DoS napadov je v tem, da pokušajo obremeniti naprave do take mere, da ni več sposobna normalno delovati.

[22] Predvajanje reklamnih posnetkov ali z namenom zapolnitve glasovnega nabiralnika (Voice Mail).

5 PARADOKSALNA DVOJNOST

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.

5.1 ZBIRANJE OSEBNIH PODATKOV JE 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 podeljevanjem dovoljen 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 100.000 prebivalca. Če ta podatek primerjamo z drugimi državami, lahko ugotovimo, da je ZDA veliko bolj konservativna 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 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 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 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 lanskih madridskih bombnih napadih so štiri države predlagale, da se podatki o telekomunikacijski uporabi hranijo vsaj eno leto, predlog Evropske komisije pa je bil od 6 mesecev do enega leta (Reuters, 2005).

Zadnjih nekaj let se ves svet bori proti terorističnim organizacijam, ki z množičnimi napadi ogrožajo življenja nedolžnih. Države se 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 predhodno zapisanem Friedenberg (2005) navaja primer Googla, ki ponuja brezplačno storitev Google Maps[23]. S pomočjo slednje se išče mesta ali zgradbe po njihovem naslovu oziroma po drugih kriterijih. Glede na to, da so že Googlovi posnetki iz ptičje perspektive relativno natančni, si ne moremo zamisliti kaj vse ima še država (npr. ZDA).

5.2 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 izločijo iz igre.

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

[23] http://maps.google.com

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. Kratica, ki stoji za tremi angleškimi besedami - customer (stranka, kupec, odjemalec), relationship (odnos) in management (ravnanje). V slovenščini se najpogosteje prevaja kot ravnanje odnosov s strankami. 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 njegove koristi 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 istih 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 torej, da opravijo čim manj klicev s čim učinkovitejšo prodajo (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 nami kupci. Ravnanje s strankami se že od nekdaj dogaja. Ne moremo mimo lokalnih prodajalcev, ki imajo svoje stranke preprosto v glavi; o nas vedo vse. Tega veliki trgovski sistemi ne zmorejo, si pa želijo. Ne samo, da bi nas lahko opozorili na artikle, ki jih ponavadi kupimo pa jih danes ni v vaši košari, lahko bi nam tudi poslali letak samo s tistimi izdelki, ki nas res 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-u izhajajo iz pravice do zasebnosti in načelu 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:

- 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, le to prijaviti Ministrstvu za pravosodje, posamezniku pa mora dati v podpis izjavo, s katerim da soglasje za uporabo svojih osebnih podatkov (Podjetnik, 2004).

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.

5.3 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 letošnjega leta prek svoje storitve za nadzor internetnih dejavnosti (in nevarnosti) uspelo pregledati čez dva milijona osebnih računalnikov. Dobljeni podatki so domala šokantni: v vsakem tretjem računalniku je vsaj en vohunski program, v povprečju pa imajo “okuženi” računalniki kar 28 različnih vohunskih programov (Djurdjič, 2004, str. 20).

Raziskave kažejo, da se v zadnjem času težave zaradi vohunskih programov vse bolj kopičijo. V družbi Dell so nedavno javno navedli, da že več kot 12 odstotkov vseh klicev za pomoč in podporo uporabnikov računalnikov lahko pripisujejo zgolj delovanju vohunskih programov. 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 storilnosti 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 ta hip nad vohunskimi programi precej bolj zaskrbljeni posamezniki, kakor odgovorne osebe v podjetjih, ki skrbijo za računalniško podporo. Nenavadnost tega položaja razkriva nedavna 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, ki privarčujejo tako na času kot tudi na denarju, vendarle so kljub temu jezni, če kdo poskuša v zameno za slednje vstopiti v njihovo zasebnost.

5.3.1 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 z npr. 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, vendar 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[24], TrustWise[25] in VeriSign[26] 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 namreč 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 s tem nam 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 zasebnostih 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, katerega je lastnik piškotka, 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 tako hitrejše delo. Več kot tretjina uporabnikov se jim je že bila pripravljena odreči. Brisanje piškotkov je najbolj prizadelo oglaševalsko industrijo, ki uporabljajo 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 4.5 Zasebnost na spletu: premikajoča se tarča. V računalniku se hranijo tudi podatki o straneh, ki smo jih že obiskali, t.i. (*angl. cache*), in z njimi je lahko ponovni obisk spletnih strani hitrejši. Takšen seznam se lahko izbriše.

[24] http://www.truste.org

[25] http://www.trustwise.com

[26] http://www.verisign.com

1. Pred 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 omenjen, morda nihče ne nadzira ali podjetje izpolnjuje svoje obljube.
2. 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.
3. **Preverite polja**.
   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.
4. 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, [URL:http://www.microsoft.com].

Zelo pomembno je osveščanje uporabnikov o možnih situacijah, ki pripeljejo do namestitve vohunskega programa in kakšne so posledice. Opozarjanje o nevarnostih 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 boljšo informiranost 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[27], 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 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[28] ocenjuje, da je trenutno 390 milijonov uporabnikov operacijskih sistemov Microsoft, ki še niso prešli na verzijo XP. Zavedati se moramo, da s tem, ko vedno več ljudi preizkuša alternativne iskalnike, bodo tudi hekerji postali pozorni na njih. Vincent Weafer iz Symantech, 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.

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

[28] 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 2: Kje so 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%
Poslovaje med podjetji	5%
Notranje grožnje	4%
Kraja ali poškodba podatkov	4%
Drugo	7%

Vir: KPMG, Raziskava o varnosti, 2002 v Zupan, 2004 str. 11.

Po raziskavah META Group 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).

6 KVALITATIVNA RAZISKAVA ELEKTRONSKE ZASEBNOSTI

Cilj empiričnega dela specialistične naloge je povzeti predvsem bistvene elemente in ugotovitve v zvezi z analizo področja elektronske zasebnosti, do katerih smo prišli v prejšnjih poglavjih. S pomočjo kvalitativne raziskave bomo poskusili podati celovit pogled nad elektronsko zasebnostjo v Sloveniji. Kvalitativna raziskava bo vključevala tako intervju s strokovnjakom na področju varnosti, kot tudi izvedbo fokusne skupine, s pomočjo katere bomo pridobili grob pregled nad zavedanjem uporabnikov o možnosti posega v njihovo zasebnost na internetu. Poglavje bomo zaključili s študijo primera v kateri bomo analizirali afero udba.net.

6.1 INTERVJU

S Sašo Slavnićem, vodjem razvoja in strokovnjakom na področju varnostnih sistemov iz podjetja Zaslon Telecom d.o.o., smo se pogovarjali o zasebnosti na internetu.

Saša Slavnić: “Moti me ideja, da lahko nekdo meni nekaj podtakne, jaz pa ne vem kdo je to in mu ne morem vrniti.” S tem je želel povedati, da je elektronsko okolje popolnoma drugi svet kot tradicionalno okolje. Odkar so analogne sisteme nadomestili digitalni ne moremo (in mogoče tudi ne želimo) vedeti kaj vse se dogaja okoli nas. Za nekatere aktivnosti spremljanja in

nadzorovanja bi lahko dejali, da obstajajo in se uporabljajo že desetletja (npr. prisluškovanje telefonskim pogovorom) ter da to ni nič novega. Prisluškovanje telefonskim pogovorom je postalo s pomočjo digitalnih sistemov popolnoma avtomatizirano. V preteklosti si potreboval na vsakega opazovanca enega opazovalca. Danes se lahko s pomočjo naprednih tehnoloških rešitev, ki uporabljajo funkcionalnost prepoznave govora (*angl. automatic speech recognition - ASR*) spremlja na tisoče telefonskih priključkov.

Ljudje se vedno pogosteje odločajo za kabelske televizije, vendar le malokdo ve, da se lahko preko slednjih zelo natančno določi gledanost posamezne oddaje. Nekako sprejemljivo je dejstvo, da bodo kabelski operaterji potrebovali podatke o gledanosti za načrtovanje oglaševanja in drugih aktivnosti. Kljub temu obstaja možnost, da ponudniki tovrstnih storitev zbirajo podatke o posameznikih oziroma naročniških številkah in jih hranijo v bazah. Saša pravi, da ni paranoičen, vendar ga moti.

Zanimivo se je vprašati, kdo bi rad več vedel o nas[29]. Vzemimo za primer spletni iskalnik Google, ki poleg osnovnega portala, ki je namenjen iskanju strani, ponuja tudi ogromno drugih vsebin (nekatere so bile predstavljene tekom te naloge) in sicer vse brezplačno. Saša Slavnić je prepričan, da prihodek s strani oglaševanja ne zadošča niti za nakup strojne opreme ter da za vsem tem stoji ameriška vojska. Če je to res, potem lahko zaključimo, da ZDA nadzorujejo dobršen del razvitega sveta. Tu je še dodal, da je zbiranje podatkov za ad hoc projekte oziroma namene sprejemljivo, težava pa nastopi, ko se slednji začnejo povezovati v ogromne baze podatkov.

Naslednje področje, ki smo se ga že dotaknili je internetna telefonija. Za slednjo je prepričan, da ni bila razvita z namenom olajšanja načina komunikacije, znižanja stroškov in dviga življenjskega standarda, temveč zaradi enostavnejšega nadzora. Glavni akter naj ne bi bil nihče drug kot ZDA.

Varnost in zaščita zasebnosti je pripeljala do nameščanja raznih zaščitnih sistemov in programske opreme. Lahko bi rekli, da ljudje postajajo paranoični in nezaupljivi do interneta, kar lahko povzroči nagel upad uporabnikov. Po Slavnićevih besedah nas v prihodnosti čaka neizbežno čipiranje ljudi (vsadek čipa v del telesa). Slednjemu bi se dalo izogniti z dvigom zavesti in opozarjanjem na “nevarnosti”, ki prežijo okoli nas (tudi na internetu). Ljudje, ki ne bodo pozorni na posege v njihov zasebni svet, bodo začeli jemati vse nadaljnje aktivnosti, postopke in tehnologijo kot nekaj samoumevnega in pričakovanega. Vse večji poudarek bo na znanosti, ki je bodisi posredno ali neposredno povezana z biometrijo.

[29] Akterje nadzora smo si že ogledali v poglavju 5.2.

6.2 UGOTOVITVE FOKUSNE SKUPINE

Tekom specialističnega dela smo proučili številne sekundarno zbrane podatke, ki so podali pregledno oceno trenutnega stanja na področju zasebnosti in varnosti v elektronskem okolju. Rezultati so načeloma jasni in razumljivi pa vendarle smo želeli preveriti slednje v okviru fokusne skupine, ki jo je sestavljalo 6 povprečnih uporabnikov interneta. Udeleženci so bili stari od 22 do 48 let in sicer večinoma z visokošolsko izobrazbo. Internet uporabljajo vsak dan, tako doma, kot tudi na delovnem mestu.

Vsi so bili mnenja, da se posegom v zasebnost ne posveča dovolj pozornosti. Njihovo prvo soočenje in spoznavanje tematike je potekalo preko lokalnih medijev, ko so bile predstavljene razne afere o kraji podatkov o kreditnih karticah in zlorabi bankomatov. En udeleženec, ki nadzoruje lastne poslovne prostore z videonadzornim sistemom, vse od sprejetja novega ZVOP-1, redno spremlja tudi ostala “ranljiva” področja.

Kljub temu, da se zavedajo možnosti kršenja zasebnosti z uporabo piškotkov, se slednjim ne želijo odpovedati. Osnovni razlog je ugodje, ki jim ga zagotavljajo; pa tudi, če gre le za jutranje prebiranje dnevnika Finance, pri katerem bi morali vnesti samo uporabniško ime in geslo. En udeleženec je izjavil, da vsaj enkrat mesečno briše piškotke. O alternativah, kot na primer ključki za shranjevanje gesel, še niso razmišljali, vendar se jim zdi ideja zanimiva in uporabna.

Zanimivo je, da ljudi ne skrbi in ne moti morebitno kršenje zasebnosti na internetu saj pravijo, da uporabljajo predvsem službene računalnike. Nadalje so se vsi strinjali, da jih bistveno bolj motijo tradicionalni načini poseganja v njihovo zasebno sfero kot npr. (vztrajno) telefonsko anketiranje. Prikrite metode, s katerimi se srečujejo na internetu jih ne motijo ker:

- ne vedo zanje,
- jim ne tratijo časa,
- če pa že so, naj bodo vsaj uporabne (npr. reklame).

O povezovanju baz podatkov in izdelavi dosjejev še niso ravno veliko razmišljali in tudi načrtovano prikazovanje oglasov jih ne moti. Največji in najbolj poudarjeni problem je zloraba kreditnih kartic. Večina udeležencev navaja, da ravno zaradi bojazni pred slednjim ne uporablja kartic za upravljanje spletnih nakupov. V kolikor je mogoče, se raje poslužujejo plačila po povzetju. Branje izjav o varnosti in zasebnosti je pri vseh vse prej izjema kot pravilo.

Uporaba varnostne brezplačne programske opreme jim ni tuja. Kljub temu imata le dva udeleženca nameščeno aplikacijo za odkrivanje vohunskih programov. Ravno tako imajo skoraj vsi udeleženci odprte brezplačne e-poštne račune, ki jih navajajo pri registracijah za katere menijo, da bi lahko bile sporne.

6.3 ŠTUDIJA PRIMERA – AFERA UDBA.NET

Sredi marca 2003 se je na internetu pojavila stran, na kateri je bilo mogoče prebrati skoraj milijon imen in priimkov Slovencev, skupaj s šifrantom očitanih jim kaznivih in drugih dejanj, ki naj bi jih vodila nekdanja Služba državne varnosti (SDV). Spletna stran www.udba.net naj bi vsebovala Centralno Aktivno Evidenco (CAE), posebno zbirno evidenco Republiškega sekretariata za notranje zadeve (RSNZ) Socialistične Republike Slovenije, v kateri naj bi po podatkih avtorjev strani (stran se je pojavila na nekem strežniku v Bangkoku na Tajskem), hranili podatke javne in državne varnosti o več kot milijon državljanih SR Slovenije in SFRJ ter podatke o tujcih, ki so jih obravnavali uradni organi SRS. Poleg osebnih matičnih podatkov naj bi bile v CAE še tri glavne vrste podatkov: dosjeji javne varnosti (kjer so našteti ukrepi ljudske milice in sodnikov za prekrške), dosjeji kazenskih obravnav (kjer so našteta kazniva dejanja, za katera je bil posameznik obsojen) in dosjeji državne varnosti, kjer so navedene številke dosjejev občanov iz evidence SDV s kategorijami (sodelavec SDV, bivši sodelavec SDV, nadzorovana oseba itd.).

Služba državne varnosti se je ukvarjala tako z “notranjimi” kot z “zunanjimi” sovražniki. Poleg obveščevalnih podatkov so bili v njihove evidence zajeti tudi vsi, ki so bili iz različnih razlogov evidentirani pri Upravi javne varnosti (npr. kdor je bil v evidenci Uprave javne varnosti zaradi prekrška, je bil tudi na seznamu Službe državne varnosti. Seveda pa je SDV zbirala podatke o nekaterih skupinah, ki so po njenem mnenju ogrožale stabilnost in varnost tedanje državne ureditve. Božo Repe (Repovž, 2003, str. 2) pravi, da je bilo teh kategorij več: spremljali so informbirojevce, tako imenovano meščansko opozicijo, anarholiberalce (liberalnejše člane zveze komunistov), aktivne pripadnike cerkva, v osemdesetih letih pa tudi pripadnike različnih alternativnih gibanj. Služba je spremljala tudi tiste, ki so delovali v tako imenovanih izpostavljenih poklicih.

Tu se postavi veliko zanimivih vprašanj: zakaj je država zbirala in hranila te podatke? Kateri so bili kriteriji, po katerih je bil nekdo opredeljen kot sovražen državi? Je to res že vsak, ki je storil kakšen prekršek? Kdo vse je imel dostop do teh seznamov in kako so prišli v javnost? Ali je res imela pravno podlago za tako obširen nadzor? Namen zbiranja podatkov je bil sporen z vidika varstva zasebnosti, a se v specialističnem delu ne bomo ukvarjali z njim, ampak se bomo osredotočili na problematičnost objave na internetu. Objava takšnih podatkov je problematična z vidika:

- Ustave Republike Slovenije, ki v 38. členu zagotavlja varstvo osebnih podatkov,
- Zakona o varstvu osebnih podatkov, ki v 3. členu določa, da mora biti obdelava osebnih podatkov določena z zakonom ali pisno privolitvijo posameznika,
- Slovenskega kazenskega zakonika, ki v 154. členu govori o uporabi osebnih podatkov v nasprotju z zakonom.

Na internetnem seznamu je bilo možno iskati osebe po začetnih črkah priimka (seznam vsebuje poleg imena in priimka še državljanstvo, naslov, imena staršev, poklic - torej matične podatke,

podatke o zaposlitvi, upravne podatke, podatke, ki se tičejo javne varnosti in podatke, ki se tičejo državne varnosti), našli pa smo lahko imena znanih in malo manj znanih ljudi. Po nekaterih ocenah naj bi šlo za kopije dokumentov z mikrofilmov. Zaradi nejasne kategorizacije (šifre, šifranti) je v večini primerov nemogoče sklepati, za kakšno kategorijo državljana gre, zato je dokumente možno zlorabiti. Poleg tega pa ni jasno, ali so na prvi pogled verodostojni dokumenti prirejeni ali so avtentični.

6.3.1 Sosledje dogodkov

Kmalu po objavi seznamov (17.4. in 18.4.2003) je inšpektor za varstvo osebnih podatkov štirinajstim domačim ponudnikom internetnih storitev z ustno odredbo odredil, naj v skladu z Zakonom o varstvu osebnih podatkov preprečijo vsakršen dostop ali pregledovanje te spletne strani (Makarovič, 2003a). Svojo odločitev je utemeljil z izjavo, da lahko take podatke obdelujejo le pooblaščenci po zakonu in z dovoljenjem posameznika ter, da se lahko takšni podatki odprejo šele 75 let po nastanku oziroma po 10 letih, če je oseba umrla (Kajzer, 2003, str. 1). Ustna prepoved v tem primeru ni bila upravičena, saj je taka prepoved ponavadi pisna, ustna pa samo v primeru vojnih razmer in drugih primerih, ki jih določa Zakon o upravnem postopku.

Kljub odločbi pa so lahko internetno stran še nekaj časa pregledovali internetni uporabniki zunaj slovenskih meja (pa tudi v Sloveniji, saj je bilo tehnično zelo enostavno obiti ovire), dokler ni bila vsebina umaknjena s strežnika.

Inšpektor je pri svoji odločitvi tehtal med varstvom osebnih podatkov na eni strani in svobodo izražanja, javnim delovanjem, pravico javnosti do obveščenosti in čim boljše informiranosti (kar je z 39. členom zagotovljeno v Ustavi Republike Slovenije, v 6. členu Zakona o medijih in preambuli novinarskega kodeksa) na drugi strani in dal prednost pravici do zasebnosti.

Čeprav je šlo v tem primeru za nezakonito obdelavo osebnih podatkov, so kasneje (28. 4. 2003) na inšpektoratu za varstvo osebnih podatkov odločbo o prepovedi dostopa do spletne strani www.udba.net razglasili za nično in sicer na podlagi Zakona o upravnem postopku, ki pravi, da so nične tiste odločbe, ki se jih ne da izvršiti (Bogataj et al., 2003). Tako je bil zopet omogočen dostop do omenjene spletne strani (dostop do nje pa je bil po naših izkušnjah velikokrat otežen oziroma nemogoč). V postopku se je namreč izkazalo, da izdane odločbe dejansko ni bilo mogoče izvršiti oziroma, da na takšen način ni bilo mogoče preprečiti nezakonite obdelave osebnih podatkov in s tem nezakonite in neupravičene posege v zasebnost posameznika, kar je bil dejansko poglavitni namen izdane odločbe. Izkazalo se je, da so ponudniki internet storitev v Republiki Sloveniji svojim uporabnikom sicer lahko blokirali neposreden dostop na spletni naslov http://www.udba.net, vendar pa so njihovi uporabniki do navedene spletne strani kljub temu lahko dostopali prek javnih t.i. proxy strežnikov, katerih naslovi so bili kmalu po izdaji odločbe objavljeni v medijih.

Poleg odločbe inšpektorja za varstvo osebnih podatkov so zlasti s strani policije pa tudi Ministrstva za zunanje zadeve potekale aktivnosti, da bi se sporna vsebina umaknila s spletnih strani na strežniku, ki je bil locirana v Kraljevini Tajski. A so bili tudi pri tem neuspešni, saj oseba, ki je evidenco objavila na spletnih straneh, le-te ni hotela sama odmakniti, Kraljevina Tajska pa še vedno ni sprejela zakona o varstvu osebnih podatkov, kar je pomenilo, da objava osebnih podatkov po njihovi zakonodaji ne pomeni kršitve zakona (Bogataj, 2004, str. 28).

6.3.2 Spornost sprejetih ukrepov s strani inšpektorja za varstvo osebnih podatkov

Boštjan Makarovič (2003b), ki se ukvarja s pravnimi vidiki interneta, je takole komentiral inšpektorjevo odločitev:
“Ukrep inšpektorja za varstvo osebnih podatkov v zadevi udba.net je sporen iz dveh razlogov. Prvi je strogo zakonski, saj zakon inšpektorju ne daje pristojnosti nad ponudniki internetnih storitev (ISP-ji), ker ti niso upravljavci ali obdelovalci osebnih podatkov, temveč zgolj posredniki pri prenosu (t.i. mere conduit), kar je jasno izraženo tudi v Direktivi EU 2000/31 o e-trgovini. Skladno s tem bi tovrstni ukrep lahko odredilo kvečjemu pristojno sodišče, ki bi npr. odločalo v civilnem sporu glede kršitev pravic prizadetih posameznikov. Drugi razlog je širše družbeni, saj omejevanje dostopa do tujih internetnih strani na podlagi odredbe celotni skupnosti domačih ISP-jev v demokratičnih državah ni razširjeno in lahko v skrajni fazi vodi do vzpostavitve centralnega filtrirnega (*angl. proxy*) strežnika za vso Slovenijo, kakršnega poznajo npr. na Kitajskem ali v Singapurju. Kot posledica bi internet za prebivalce Slovenije izgubil naravo globalnega okolja, saj bi si ti smeli ogledovati le tiste spletne strani, ki bi bile v celoti prilagojene domačim normam in standardom.”

Veliko polemik je primer udba.net povzročil tudi z vidika Zakona o dostopu do informacij javnega značaja. Ministrstvo za informacijsko družbo je namreč pripravilo predlog Uredbe o posredovanju informacij javnega značaja, ki pa je doživela veliko pripomb in predlogov ravno zaradi tega primera. Po mnenju nekaterih (npr. direktorja Arhiva Republike Slovenije, Vladimirja Žumerja) bi sprejem te uredbe omejil dostop do arhivov in dosjejev. Čeprav je vpogled vanje možen že od leta 1992, je zanimanje ljudi zanje naraslo ravno z njihovo objavo na internetu. Z uveljavitvijo Uredbe o posredovanju informacij javnega značaja - tako meni direktor Arhiva, naj bi bil arhiv prisiljen posegati v obstoječe dokumente (prekrivati, brisati, prečrtovati podatke). Taki dokumenti (po mnenju direktorja) nimajo niti pravne niti strokovne veljavnosti. Zagovorniki te uredbe (med njimi tudi nekdanji minister za informacijsko družbo) menijo, da se uredba ne nanaša na omenjeni primer udba.net, saj so ti dosjeji zbirka osebnih podatkov in ne gre za informacije javnega značaja - predlog se torej ne nanaša na arhivske zbirke (urejeni in varovani so po Zakonu o varstvu osebnih podatkov in Zakonu o arhivskem gradivu) (M.R., 2003).

Udba.net ni edini primer kršitve zasebnosti zaradi malomarnosti oziroma nepoučenosti državnih uradnikov v slovenskem prostoru. Pred časom je bilo moč opaziti več kot očitno kršitev zakona o varstvu osebnih podatkov na spletu. Na domači strani okrajnega sodišča Ilirska Bistrica je bil

objavljen razpis glavne obravnave, na kateri je mladoletni sin tožil očeta zaradi preživnine. Spornost se kaže v objavi polnih imen in priimkov, čeprav so obravnave, ko gre za družinske spore po zakonu tajne. V primerih, ko gre za mladoletnike bi kazalo biti še posebno pazljiv in občutljiv. Inšpektor Bogataj se je na opozorilo izgovoril češ, da prijave prizadetega niso dobili in da imajo že tako in tako preveč dela (Tepina, 2005, str. 15)!

6.4 UGOTOVITVE KVALITATIVNE RAZISKAVE

V uvodu smo zapisali štiri domneve, ki smo jih želeli preveriti tekom tega dela.

1. DOMNEVA: *Zakonodaja ne more slediti novim vsebinam in aktivnostim, ki jih prinaša internet.*

Ugotovili smo, da zakonodaja de facto ne more slediti novim vsebinam in tehnologiji, ki se pojavlja na internetu. V prid slednji trditvi govori dejstvo, da smo potrebovali štiri leta za spremembo zakona o varstvu osebnih podatkov. Nakazali smo tudi nekaj smeri razvoja novih storitev, ki v proučenih zakonih (ZVOP-1, ZEPEP in ZEK) niso niti predvidene, kaj šele omenjene. Elektronsko okolje je tako obširen medij, da bi bilo potrebno urejati zakonodajno plat na letni, če ne celo na mesečni ravni, kar pa v trenutni državi in njeni organiziranosti ni izvedljivo. Glede na to, da internet ne pozna meja, je pogoj za urejenost le-tega dobro sodelovanje med ostalimi državami sveta. Naš predlog je, da se odstopi določene kompetence centralni neodvisni organizaciji, ki bo poskrbela za splošni pravni red.

2. DOMNEVA: *Glavna sestavina zaščite informacijske zasebnosti je transparentnost uporabe zasebnih podatkov. Najboljša zaščita ni ta, da država in zasebne družbe 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.*

Prišli smo do zaključka, da se zbiranju osebnih podatkov ne bo dalo izogniti. Sedaj je potrebno vzpostaviti sistem transparentnosti, ki bo omogočal vpogled v arhive in zbirke, ki hranijo naše podatke in zagotoviti dostop do informacij; zakaj so te podatke zbrali, zakaj in kako jih hranijo in kako te informacije o nas uporabljajo. Študija primera udba.net je med drugim tudi pokazala, da podatki, ki so bili objavljeni na internetu, izhajajo iz raznih zbirk in arhivov, za katere večina prebivalcev RS ni vedela da obstajajo niti ni poznala vsebine le-teh. Od 1.1.2005 naj bi bilo drugače. ZVOP-1 v tridesetem členu jasno določa, da morajo biti informacije o zbranih podatkih dostopne posamezniku.

Sodobna zakonodaja se za zaščito zasebnosti ukvarja predvsem s transparentnostjo uporabe osebnih podatkov. Načelo transparentnosti uporabe osebnih podatkov se na internetu čedalje bolj uporablja, predvsem v obliki izjave o zasebnosti (*angl. privacy statement*), v kateri lastnik spletne strani pove, kakšni osebni podatki se zbirajo, kakšen je namen zbiranja in za kaj bodo zbrani osebni podatki uporabljeni. Ta izjava pa seveda ne zagotavlja, da bo zasebnost obiskovalca spletne strani res močno varovana, saj so mnoge izjave namenoma zapisane

dvoumno. V nekaterih je celo zapisano, da bodo zbrani podatki uporabljeni za katerekoli potrebe in namene.

3. DOMNEVA: *Tehnološka orodja za standardizirano ciljanje z oglasi na spletu, na podlagi vedenjskih vzorcev uporabnikov interneta, nenadzorovano posegajo v zasebnost, izključno zaradi sledenja ekonomskim interesom.*

Uporabnikom interneta bi bilo potrebno dati izbiro oziroma jih vsaj obvestiti, da se jim sledi. Takoj, ko bodo oglasni strežniki zapolnjeni s podatki o vedenjskih vzorcih, jih bodo lahko oglaševalska podjetja bodisi prodala, bodisi izkoristila za nadaljnje tržne aktivnosti. Vsa zbiranja in analize se ponavadi odvijajo brez vednosti in privolitve uporabnika. Saša Slavnić je v intervjuju dejal, da se je bati spletnih oglaševalcev (in ostalih upravljavcev zbirk podatkov), saj le-ti lahko dodajo v obstoječo bazo oglasnih strežnikov nekaj stolpcev, ki jih bodo zapolnili z zapisi o osebnih podatkih. Baza bi se lahko na ta način razširila, pridobila nove referenčne elemente in postala povezljiva z drugimi podatkovnimi shrambami. In tudi, če ne poznajo imen, še vedno poznajo IP naslov, geografsko lokacijo in mesta, na katerih se posamezniki najpogosteje zadržujejo. Dejstvo je, da so končni proizvodi in storitve po skoraj vseh kriterijih na svetovni ravni zelo homogeni. Eden izmed omejenih načinov boljšega pozicijoniranja proizvoda ali storitve je ravno oglaševanje. Oglaševalska podjetja bodo v prihodnje vpeljevala še bolj agresivne metode oglaševanja.

4. DOMNEVA: *Uporabniki svetovnega spleta moramo uporabljati rešitve, ki služijo zavarovanju različnih interesov glede zasebnosti in anonimnosti dejavnosti posameznikov ter podjetji pri uporabi internetnih storitev.*

Vohunskih programov in nekaterih nevarnih piškotkov se marsikje lotevajo povsem brezskrbno in nepripravljeno. Med tem, ko si danes pri virusih prizadevamo, da bi bile definicije za protivirusne programe ažurne domala vsako minuto, virusno nevarnost pa danes tipično preverjamo na več različnih mestih (odjemalcih, strežnikih, internetnih prehodih), ima le malo podjetij aktivno politiko glede vohunskih programov in podobne nesnage. Do podobnih ugotovitev smo prišli tudi na zelo majhnem reprezentativnem vzorcu v okviru fokusne skupine (poglavje 6.2), kjer so udeleženci dejali, da poznajo predvsem pozitivne lastnosti piškotkov, pred negativnimi si pa zatiskajo oči. Analitiki, ki se ukvarjajo z varnostjo v informacijskih sistemih, so zato vohunske programe in nekatere piškotke začeli postavljati med nevarnosti z največjim tveganjem, na kar bi morali biti pozorni prav vsi.

Zaradi obširne administracije posameznih programov, ki jih uporabljamo, ko brskamo po internetu so se začeli ponudniki slednjih združevati z namenom poiskati rešitev, ki bi prispevala k centralizirani nastavitvi vseh programskih (iskalniki, predvajalniki, operacijski sistemi, antivirusni programi, odstranjevalci vohunskih programov, požarne pregrade, itd.) in strojnih rešitev (usmerjevalniki, požarni zidovi, itd.), povezanih z internetom. Poznavalci razmer pravijo,

da bodo takšne agresivne taktike povečale nezaupanje med uporabniki interneta, hkrati pa povzročile drastične ukrepe, ki bodo poslabšale razmere na svetovnem spletu.

Dejstvo, da nas vedno nekdo opazuje je neizogibno. Nivo zasebnosti lahko dvignemo le sami. Če bi želeli popolnoma minimizirati možnost nadzorovanja, potem bi se morali med drugim tudi odpovedati: plačevanju s kreditnimi karticami, mobilni telefoniji, digitalnim televizijskim povezavam – IP TV, avtomatskemu cestninjenju in nenazadnje tudi uporabi interneta. Vendar glede na to, da je veliko ljudi, ki dajejo prednost hitrosti in lagodnosti napram zasebnosti, takih drastičnih ukrepov v bližnji prihodnosti ni pričakovati. Virtualna sled postaja DNA zapis vseh naših aktivnosti.

Iz vsebine predhodnih poglavij lahko zaključimo, da obstaja nevarnost posegov v zasebnost posameznika na internetu. Vsekakor bi bilo potrebno izvesti nadaljnje raziskave, s pomočjo katerih bi podrobneje proučili kje in kako pogosto se izvaja nadzor uporabnikov interneta. Rezultati fokusne skupine so pokazali da so uporabniki interneta seznanjeni z nevarnostmi, ki smo jih proučevali tekom naloge, vendar slednje obravnavajo kot nujno zlo. Zaradi majhnosti vzorca udeležencev fokusne skupine, bi bilo potrebno izvesti nadaljnje raziskave z drugimi tehnikami oziroma metodami zbiranja podatkov, ki bi lahko zajele večji reprezentativni krog uporabnikov, s pomočjo katerih bi dobili natančnejšo sliko stanja osveščenosti uporabnikov interneta v Sloveniji.

7 SKLEP

Pravica do elektronske zasebnosti predstavlja tako imenovano pravico do informacijske in komunikacijske zasebnosti, posameznikov interes, da državi ali nepovabljenim tretjim osebam ne razkrije določenih informacij in ima nadzor nad tem, katere informacije in v kakšnem obsegu bo predstavil svetu, ter da s svobodno voljo in informirano sprejme odločitve v vsakdanjem življenju.

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. Tehnološka zagotovila za varovanje elektronske zasebnosti se razvijajo skladno z razvojem sodobne informacijske in komunikacijske tehnologije. Razvoj tehnologije

poleg nevarnosti za posameznikovo zasebnost prinaša tudi nove in vedno bolj učinkovite rešitve za zavarovanje različnih interesov glede zasebnosti in anonimnosti pri uporabi internetnih storitev. Paleta teh rešitev je široka, obsega pa tako strojne kot programske rešitve.

Pravo se je izzivu informacijske tehnologije odzvalo dokaj hitro. Ukvarjati se je moralo pričeti z nevarnostmi, ki jih s seboj prinaša sodoben razvoj informacijske tehnologije. Pravico do zasebnosti in varstva osebnih podatkov pred neutemeljenimi in neupravičenimi posegi države ter drugih pravnih in fizičnih oseb, zagotavljajo vsi pomembni mednarodni dokumenti s področja varstva pravic posameznika, tudi slovenska Ustava. Čeprav ob njihovem nastanku izzivi zasebnosti in varstvu osebnih podatkov, ki sta jih prinesla razvoj tehnologije in predvsem internet še niso bili znani, ti dokumenti še vedno predstavljajo temelj varstva posameznika tako pred državnimi organi, kot pred drugimi posamezniki. Vendar pa so ob uporabi interneta in njegovih storitev potrebna tudi tehnološka in organizacijska zagotovila, oziroma sredstva za varovanje zasebnosti, saj le pravna niso dovolj.

Vse nevarnosti za vdor v elektronsko zasebnost, ki izhajajo iz uporabe sodobne informacijske in komunikacijske tehnologije pa le niso tako hude, kot se na prvi pogled zdijo. Skrb ljudi o ohranjanju elektronske zasebnosti in bojazen pred vdori, je pogosto močno pretirana in posledica (ne)znanja uporabnikov in nekaterih medijsko napihnjenih zgodb o hekerjih, pred katerimi ni varen nihče niti najbolj zaščiteni sistemi. Rešitev tega problema bi lahko bilo izobraževanje ljudi, saj se pred nevarnostmi lahko v veliki meri zavarujemo že z enostavnimi in hitro izvedljivimi varnostnimi ukrepi. Naša varnost je odvisna predvsem od našega ravnanja. Uporabniki interneta so bili še pred časom zelo odprti in pripravljeni deliti informacije o svojih preferencah in spletnih aktivnostih, kar je dokazovala tudi vedno večja uporaba kreditnih kartic pri opravljanju spletnih nakupov. Vse pogostejše kraje podatkov o kreditnih karticah so povzročile močno nazadovanje e-poslovanja. Če se ozremo globalno in dolgoročno lahko sklepamo, da bodo zlorabe kreditnih kartic vplivale na ekonomijo gospodarstev, v katerih se pojavlja kreditna kartica kot vsakdanje plačilno sredstvo. Med najbolj prizadetimi bodo ZDA.

8 LITERATURA

1. Achrol Ravi S., Kotler Philip: Marketing in the Network Economy. Journal of Marketing, vol. 63 (1999), št. 4, str. 146 – 163.
2. Batagelj Zenel: CRM te opazuje ... Ljubljana: Delo revije, Moj mikro, št. 1, 2004. str. 7-15.
3. Berčič Boštjan, Bojanec Anton, Krkoč Peter, Mrhar Peter, Patru Primož, Šinigoj Aleksander, Valenčič Iztok: Ukrepi v primeru informacijskih nesreč. Šempeter pri Gorici: Inštitut Za Informacijsko Varnost, 2003. str. 124-126.
4. Bertoncelj Brane: Psihosocialni vidiki zagotavljanja varnosti računalniško podprtega informacijskega sistema. Doktorska disertacija. Ljubljana : Fakulteta za družbene vede, 2000. 381 str.

5. Bogataj Jože: Poročilo o delu inšpektorata za varstvo osebnih podatkov v letu 2003. Ljubljana : Ministrstvo za pravosodje, inšpektorat za varstvo osebnih podatkov, 2004. str. 20-21.
6. Bogataj Jože: Poročilo o delu inšpektorata za varstvo osebnih podatkov v letu 2003. Ljubljana : Ministrstvo za pravosodje, inšpektorat za varstvo osebnih podatkov, 2004. str. 20-21.
7. Bogataj Maja, Goran Klemenčič, Boštjan Makarovič, David Pahor: Udba.net - nevarni pravni precedens. Delo. [URL:http://www.delo.si/index.php?sv_path=43,50&id =4ad801d414d127fa8a7b15681562eff004&source=Delo], 28.04.2003.
8. Borka Jerman – Blažič et al.: Elektronsko poslovanje na internetu. Ljubljana: Gospodarski vestnik, 2001. 206 str.
9. Brynjolfsson Erik, Kahin Brian (eds.): Understanding the Digital Economy. Cambridge (Massachusetts): The MIT Press, 2000. 401 str.
10. Cetin Simon: Iprom v preteklem letu posredoval 900 milijonov spletnih oglasov. Ljubljana: Iprom, [URL:http://www.iprom.si/cgi-bin/novica.cgi?id=60], 17.01.2005.
11. Choi Soon-Yong, Whinston Andrew B.: The Internet Economy: Technology and Practice. Austin (Texas): SmartEcon Publishing, 2000. 356 str.
12. Cunningham Peter, Fröschl Friedrich: Electronic Business Revolution. Berlin: Springer, 1999. 236 str.
13. Cvetek Olga: Prepovedano vse, kar v zakonu ni izrecno dovoljeno: Pogovor z v. d. glavnega inšpektorja za varstvo osebnih podatkov Jožetom Bogatajem. Delo, [URL:http://www.delo.si/index.php?sv_path=43,50&id=37eb3b4d6876ec5617720c62ef9d68e404&source=Delo], 23.8.2004.
14. Čebulj Janez: Varstvo informacijske zasebnosti v Evropi in Sloveniji. Ljubljana : Inštitut za javno upravo pri Pravni fakulteti v Ljubljani, 1992. 165 str.
15. Djurdjič Vladimir: Čas za telefonijo IP. Ljubljana : Monitor, [URL:http://www.pcmediji.infomediji.si/clanki.php?id=22], 09/2004.
16. Djurdjič Vladimir: Spyware: nadloga ali nevarnost? Sistem. Ljubljana : Monitor, 2004. str. 20-22.
17. eMarketer.com: The Mystery of Spyware, Part II, [URL:http://http://www.emarketer.com/Article.aspx?1003457], 23.6.2005.
18. Facault Michel: Nadzorovanje in kaznovanje. Ljubljana : Delavska enotnost, 1984. 324 str.
19. Friedenberg Mrk: Big Brother has arrived in Google. The Daily Collegian, [URL:http://www.bgnews.com/vnews/display.v?TARGET=printable&article_id=426f8d07c2c01], 27.04.2005.
20. Fuchs Keaton: Hecers` Playground. The Oklahoma Daily, [URL:http://www.oudaily.com/vnews/display.v?TARGET=printable&article_id=426f9e6185fb8], 27.04.2005.
21. Goldhaber Michael H.: The Attention Economy and the Net. 2nd Draft version of a talk presented at the conference on "Economics of Digital Information". Cambridge (Massachusetts), 23 – 26. januar, 1997. [URL:http://www.well.com/user/mgoldh/AtEcandNet.html].

22. Greene Tom, Hochmuth Phil: VoIP security a moving target. Network World Fusion, [URL:http://www.nwfusion.com/news/2004/102504von], 25.10.2004.
23. Gross Grant: RFID and privacy: Debate heating up in Washington. Network World Fusion, [URL:http://www.nwfusion.com/news/2004/0528rfidpriv.html], 28.05.2004.
24. Guthrie James et al.: There is no Accounting for Intellectual Capital in Australia: A review of annual reporting practices and the internal measurement of Intangibles. OECD Symposium on Measuring and Reporting of Intellectual Capital, Amsterdam, avgust 1999. 73 str. [URL: http://www.oecd.org/pdf/M00033000/M00033313.pdf].
25. Hesseldahl Arik: Big Brother Isn't Here Yet. Forbes, [URL:http://www.forbes.com/2005/05/06/cx_ah_0506diglife_print.html], 06.05.2005.
26. Jakupović Esad: Cena nezaščitenosti?. Maribor: Kapital št. 338, 2005, str. 66.
27. Janelle Chantelle: Internet users concerned with security consider alternate browsers. WorldNow, [URL:http://www.wistv.com/global/story.asp?s=3269344&ClientType=Printable], 27.04.2005.
28. Jerman-Blažič Borka, Tomaž Klobučar, Zoran Perše: Elektronsko poslovanje na internetu. Ljubljana : Gospodarski Vestnik, 2001. 206 str.
29. Kajzer Roman: To potezo smo morali narediti. Delo, št. 91: 1, 2003.
30. Kavita: Wi-Fi may become the new urban GPS. CNet, [URL:http://mobilemag.com/content/100/104/C4276], 13.07.2005.
31. 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.
32. Kim Chan W., Mauborgne Renée: Fair Process: Managing in the Knowledge Economy. Harvard Business Review, vol. 81 (2003), št. 1, str. 127 – 136.
33. Koprowski J. Gene, The Web: Search engine privacy threats. United Press International, [URL:http://www.wpherald.com/print.php?StoryID=20050427-101719-3430r], 27.04.2005.
34. Kovačič Matej: Zasebnost na internetu. Ljubljana : Mirovni inštitut, Inštitut za sodobne družbene in politične študije, Zbirka Politike, 2003. 111 str.
35. Lawson Stephen: Industry group sets out to make VoIP secure. Network World Fusion, [URL:http://www.nwfusion.com/news/2005/0329indusgroup.html], 29.03.2005.
36. Lazarus David: It's impressive, scary to see what a Zaba search can do. San Francisco Chronicle, [URL:http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/04/15/BUG6JC8U341.DTL], 15.04.2005.
37. 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], 16.3.2005.
38. Lyon David: The Electronic Eye. Cambridge : Polity Press, 1994. 270 str.
39. M.R.: Udba.net: Na vpogled le prečiščeni dosjeji?. 24ur.com, [http://24ur.com/bin/article.php?article_id=2028487], 26.8.2003.
40. Makarovič Boštjan: Afera www.udba.net. [URL:http://www.24ur.com], 25.5.2003b.
41. Makarovič Boštjan: Ali in kako lahko država pravno ureja dogajanje na internetu?. Pravna praksa, št. 18: 2003a. str. 4-6.

42. Marc Mojca: Analiza poslovanja podjetja v pogojih elektronskega poslovanja. Magistrsko delo. Ljubljana: Ekonomska fakulteta, 2003. 108 str.
43. Mark Ward: Hoe to escape the phishing nets. BBC News website, [URL:http://news.bbc.co.uk/2/hi/technology/4498939.stm], 10.05.2005.
44. Marshall Matt: New cookies much harder to crumble. Knight Ridder Newspapers, [URL: http://www.menafn.com/qn_print.asp?StoryID=CqM8oqeicq1bulunpt0Tjrvm], 27.04.2005.
45. McKeown Patrick G.: Information Technology and the Networked Economy. Fort Worth : Harcourt College Publishers, 2001. 395 str.
46. Mesojedec Uroš: Paralelizem. Ljubljana: Monitor, št. 4: 2005. str. 126.
47. Mesojedec Uroš: Požarni zidovi: Internetni varnostnik. Ljubljana: Monitor, št. 4: 2004. str. 72.
48. Moj mikro: Država in zasebnost. ZDA kot veliki brat. Ljubljana: Delo revije, št. 1, letnik 20, januar 2004.
49. Možina Damjan: Varstvo osebnih podatkov na internetu – cookie: piškotek ali Veliki brat. Pravna praksa, informatika in pravo, št. 36-37: 2000. str. 23-29.
50. Negroponte Nicholas: Being Digital. New York: First Vintage Books Edition, January 1996. 255 str.
51. Odlazek Gregor: Zasebnosti ni, prebolite že enkrat. Ljubljana: Finance, št. 78: 2003. str.16.
52. Pahor David: Bi radi zaslužili s prodajo po internetu? Podjetnik. Ljubljana: [URL:http://www.podjetnik.si/default.asp?ClanekID=210], 17.06.2003.
53. Perše Zoran: Varstvo in zaščita osebnih podatkov pri elektronskem poslovanju. Ljubljana : Pravna praksa, št. 11-12, 2000. str. 5-28.
54. Peterson Shane: Guarding Information. Government Technology, [URL:http://www.govtech.net/news/story.print.php?id=93910], 06.05.2005.
55. Petrov Sabina: Internet del medijskega načrta. Finance, Ljubljana: objavljeno 2.12.2004.
56. Podjetnik: Zbiranje osebnih podatkov. Ljubljana: Revija Podjetnik, [URL: http://www.podjetnik.si/default.asp?ClanekID=1621], 17.05.2004.
57. Raab D. Charles: Privacy, democracy, information. The Governance of Cyberspace, London : Routledge, 1997, str. 155-174.
58. Radoš Škrt: Elektronsko poslovanje med podjetji. Sistem priloga revije Monitor, Ljubljana, 1999. str. 35 – 37.
59. Repovž Gregor: Zgodovina arhivov Službe državne varnosti; SDV, 5. oddelek, arhiv. Delo, št. 91: 2003 str. 1.
60. Reuters: EU split over antiterror phone data logging rules. Reuters, [URL:http://www.computerworld.com/printthis/2005/0,4814,105120,00.html], 11.07.2005.
61. Ross Edward Alsworth: Social Control: a survey of the fundamentions of order. New York, London : The Macmillan Company, 1922. 463 str.
62. Struna Dejan: Spletno oglaševanje na osnovi vedenjskih vzorcev. Ljubljana: Iprom, [URL:http://www.iprom.si/cgi-bin/novica.cgi?id=58], 02.11.2004.
63. Surmacz Jon: Will You Pay More to Surf Safely, or Dump Internet Explorer? CXO Media, [URL:http://www.csoonline.com/talkback/092704.html], 28.04.2005.

64. Šalamon Brane: Nevarni internet. Maribor: Kapital, 09.02.2004, str. 60 - 62.
65. Tapscott Don: The Digital Economy: Promise and Peril in the Age of Networked Intelligence. New York: McGraw – Hill, 1995. 342 str.
66. Tepina Jasna: Kje vse vas vidi veliki brat. Ljubljana: Dnevnik, Nika, 2005. str. 14-15.
67. Tyson Laura D'Andrea: Old Economic Logic in the New Economy. California Management Review, vol. 41 (1999), št. 4,. str. 8 – 16.
68. 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.
69. Vagaja Aleksandra: Z identifikacijo vedenjskega vzorca uporabnika interneta do pametnih in predvsem nemotečih oglaševalskih akcij. Ljubljana: Finance, [URL:http://www.finance-on.net/print.php?id=111684&tip=1], 04.02.2005.
70. Vagaja Aleksandra: Zasebnost na spletu: Prisluškujejo nam, mar ne? Ljubljana: Finance, [URL:http://www.finance-on.net/print.php?id=100155&tip=1], 04.10.2004.
71. 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.
72. Vidmar Tone: Računalniška omrežja in storitve. Ljubljana : Atlantis, 1997. 417 str.
73. Vindiš Renato: Magična kratica: RFID. Podjetnik, [URL:http://www. podjetnik.com/ default.asp?KatID=450&ClanekID=2324], 11.04.2005.
74. Wayne Matthew: An invasion of privacy, or convenience for the consumer. The Tufts Daily, [URL:http://www.tuftsdaily.com/vnews/display.v?TARGET=printable&article_id=4271], 15.04.2005.
75. Webster Frank: Theories of the Information Society. London : Routledge, 1995. 304 str.
76. Woodall Pam: Untangling e-conomics. The Economist, vol. 356 (2000), št. 8189, 23. september, Special section str. 5 – 7.
77. WorldNow: Prying Eyes. Special report, [URL:http://www.wtol.com/global/story.asp?s=3267815&ClientType=Printable], 28.04.2005.
78. Zdovc Peter: Varna elektronska komunikacija. Ljubljana : Info SRC, glasilo, št. 33, 2002. str. 8-9.
79. Zmagaj Peter: Internetni ponudnik ne bo odgovoren za vsebino. Ljubljana : Finance, št. 59, 2004. str. 10.
80. Zupan Lucija: Prestiž ali nujnost? Sistem. Ljubljana : Monitor, 2004. str. 10-11.
81. Žurej Jurij: Deset zapovedi varstva zasebnosti v svetu interneta. Pravna praksa, informatika in pravo, št. 1: 2001. str. 38-41.

9 VIRI

1. Banisar David et al.: Privacy & Human Rights. [URL:http://www.privacy-international.org /survey/index99.html], 23.5.2000.
2. Data Protection Working Party (2000): Privacy on the Internet – An integrated EU Approach to On-line Data Protection. [URL:http://europa.eu.int/comm/internal_market/en/ dataprot/wpdocs/wpdocs_2k.htm], 20.10.2004.

3. Eurobarometer. EB60.2 – CC-EB 2004.1, [URL: http://europa.eu.int/comm/public_opinion /archives/cceb/2004/ebs_203_comp_high.pdf], 2004.
4. Kazenski zakonik Republike Slovenije (Uradni list RS, št. 63/94, 70/94, 23/99).
5. Microsoft. [URL:http://www.microsoft.com], 14.1.2005.
6. Ministrstvo za informacijsko družbo: Predstavitev Ministrstva: Zakaj Ministrstvo? Ljubljana: 2000 [URL: http://mid.gov.si/mid/mid.nsf].
7. Ministrstvo za informacijsko družbo: Slovenija v informacijski družbi. Ljubljana: 2003 [URL:http://mid.gov.si/].
8. Raba interneta v Sloveniji. [URL:http://www.ris.org], 16.4.2005.
9. SIBIS Pocket Book 2002/03. [URL:http://www.empirica.biz/sibis/files/Sibis_Pocketbook _updt.pdf], 20.12.2004.
10. Spletni portal Najdi.si. [URL:http://www.najdi.si], 18.2.2005.
11. Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/2000).
12. Ustava Republike Slovenije (Uradni list, št. 33/1991-I, 42/1997, 66/2000).
13. Wired News: Ads That Know What You Want. [URL:http://www.wired.com/news/print/0, 1294,67365,00.html], 28.4.2005.
14. Zakon o dostopu do informacij javnega značaja (Uradni list RS, št. 24-900/2003).
15. Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 57/2000, 30/2001).
16. Zakon o elektronskih komunikacijah (Uradni list RS, št. 43/2004).
17. Zakon o tajnih podatkih (Uradni list RS, št. 87/2001).
18. Zakon o telekomunikacijah (Uradni list RS, št. 30/2001).
19. Zakon o varstvu osebnih podatkov (Uradni list RS, št. 59/2001).

10 PRILOGA

10.1 KRATEK ZAPISNIK INTERVJUJA

Kraj: Ljubljana, v prostorih podjetja Zaslon Telecom d.o.o. (v nadaljevanju ZT)
Čas: 29.6.2005 ob 16:30
Prisotni: Saša Slavnić (vodja razvoja v ZT), Rok Primožič

Vsebina:

- zasebnost in internet

Ugotovitve:

- analogni sisteme zamenjujejo digitalni
- ljudje so pripravljeni namestiti veliko programov z namenom izogniti se spremljanju njihovih aktivnosti
- kabelski operaterji nas sledijo
- Google financira vojska
- nevarno ni zbiranje podatkov, temveč njihovo povezovanje in grupiranje
- prihodnost je v biometriji
- v kolikor se ne bomo zavedali posegov v našo zasebno sfero, bodo vse nadaljnje aktivnosti postale nekaj vsakdanjega in samoumevnega
- kot posledico predhodni alinei lahko skoraj zagotovo napovemo čipiranje ljudi

Dogovori:

- za morebitne dodatne informacije se vzpostavi kontakt preko e-pošte

10.2 OPOMNIK ZA FOKUSNO SKUPINO

Dne 28.6.2005 bomo organizirali fokusno skupino s šestimi udeleženci. S slednjimi se bomo pogovarjali o internetu in zasebnosti. V nadaljevanju je zapisanih nekaj bistvenih opornih točk, ki bodo služile za pravilni tok razgovora:

- Ali ste redni uporabniki interneta?
- Za kakšne namene uporabljate internet?
- Ali ste že kdaj kupovali preko spletnih trgovin?
- Ali imate kakšne pomisleke v zvezi z uporabo interneta?
- Ali ste že kdaj imeli kakšne negativne izkušnje na internetu?
- Ali menite da vam na internetu “prisluškujejo”? In če ja, kako? Ali vas to moti?
- Kaj menite o tehniki oglaševanja na podlagi vedenjskih vzorcev (prej jo razložimo)?
- Piškotki: Ali bi se jim odpovedali? Jih redno brišete?
- Ali preberete izjavo o varnosti in zasebnosti?
- Ali uporabljate opremo za odkrivanje vohunskih programov?

SLOVARČEK

anti-spayware software	programska rešitev za odstranjevanje vohunskih programov
attention economy	ekonomija pozornosti
auonimous remailer	anonimni pošiljatelj e-pošte
automatic speech recognition	avtomatska prepoznava govora
cookies	računalniški piškotki
digital economy	digitalna ekonomija
e-business	elektronsko poslovanje
e-commerce	elektronsko trgovanje
firewall	požarni zid, požarna pregrada
hacker	heker
internet economy	internetna ekonomija
internet service providers (ISP)	ponudniki internetnih storitev
IP address	IP naslov
junk mail, spam	pošta z elektronskimi “smetmi”
knowledge economy	ekonomija znanja
knowledge society	družba znanja
knowledge work	uporaba človeškega znanja
mass customization	množična proizvodnja
molecular economy	molekularna ekonomija
network economy	ekonomija omrežij
new economy	nova ekonomija
organizational learning	sposobnost organizacije za neprestano učenje
phishing sites	zamaskirane strani
privacy officer	odgovorni za varovanje podatkov
privacy statement	izjave o zasebnosti
radio frequency identification	radiofrekvenčna identifikacija
real time economy	ekonomija, ki poteka v dejanskem času
smart economy	pametna ekonomija
spam	nezaželena elektronska pošta
spyware	vohunski program
virtual identity	virtualna identiteta
voice over IP (VoIP)	internetna telefonija