UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

VAROVANJE PODATKOV IN ZASEBNOSTI NA INTERNETU

Ljubljana, maj 2006 **DARJA PRAPROTNIK**

IZJAVA

Študentka DARJA PRAPROTNIK izjavljam, da sem avtorica tega magistrskega dela, ki sem ga napisala pod mentorstvom prof. dr. BORKE JERMAN - BLAŽIČ in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne 9.5.2006

Podpis:_____

KAZALO

KAZALO SLIK

KZALO TABEL

KAZALO GRAFOV

1 UVOD

Informacijska družba predstavlja velik napredek, hkrati pa tudi vse večjo grožnjo človeku in njegovi zasebnosti. Ne obstaja nobena »on-line« aktivnost, ki bi omogočala popolno zasebnost (Kovačič, 2003, str. 40). Vendar, kot pravi Čebulj[1]: »Zasebnost posameznika ni postala ogrožena šele z uvedbo informacijskih tehnologij in računalniško vodenih zbirk osebnih podatkov, temveč jo je ta samo potencirala in privedla do tega, da so se ljudje začeli te nevarnosti veliko bolj zavedati kot v času ročno vodenih evidenc« (Čebulj, 1992, str.16). Čebulj navaja tri sestavine zasebnosti: zasebnost prostora, (možnost posameznika, da je sam), zasebnost osebnosti (svoboda misli, opredelitve, izražanja) ter informacijsko zasebnost (možnost posameznika, da ima nadzor nad informacijami o sebi). Prvi dve sestavini zasebnosti spadata med temeljne človekove pravice in v demokratični družbi nista sporni, v informacijski družbi ogrožena pa je informacijska zasebnost, ki vključuje tudi varstvo osebnih podatkov (Kovačič, 2000, str. 1021).

Z vse večjo rastjo interneta ter elektronskega poslovanja, se je bistveno povečala tudi količina podatkov dostopnih preko interneta. V prehodu na elektronsko poslovanje, elektronsko vlado, elektronsko upravo, uporabo informacijskih tehnologij v zdravstvu, zavarovalništvu, bančništvu… se zbira zmeraj več podatkov o posamezniku (državljanu), ti podatki se centralizirajo in vse več sistemov, institucij in posameznikov ima dostop do teh obsežnih zbirk. S sodobno tehnologijo je posamezne zbirke zelo enostavno združiti oziroma predelati ter jih uporabiti v druge namene, kot so bile prvotno nastavljene.

Nove tehnologije omogočajo tudi državi vse večji nadzor nad državljani. Ukrepi Evropske unije na področju zbiranja in hrambe (retencije) prometnih podatkov elektronskih komunikacij, ki predvidevajo minimalno 6 mesečno in maksimalno 24 mesečno hranjenje vseh prometnih podatkov, pomenijo samo enega izmed grobih posegov države v zasebnost državljanov. Kljub temu, da ni predvideno hranjenje vsebine, pomeni nadzor nad prometnimi podatki o vseh transakcijah in aktivnostih vseh državljanov ogrožanje zasebnosti (Working party on cooperation in criminal matters, 2005). Kovačič navaja, da država ter njene institucije potrebujejo informacije za učinkovito uravnavanje življenja posameznikov ter dobro delovanje družbe, zato jim posameznik ne more oziroma ne sme preprečiti zbiranja podatkov, pri tem pa je nujno potrebna transparentnost uporabe osebnih podatkov (Kovačič, 2000, str.1021).
Mellors je zapisal: *»Najboljša zaščita ni ta, da oni 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*« (Mellors v Kovačič, 2000, str. 1021).
Sodobne informacijsko komunikacijske tehnologije državi res omogočajo veliko stopnjo nadzora nad posamezniki, vendar pa sodobna tehnologija omogoča tudi posameznikom, da

[1] Janez Čebulj, ustavni sodnik, redni profesor na Fakulteti za upravo, avtor številnih publikacij s področja varstva podatkov in zasebnosti

zavarujejo svojo zasebnost pred vmešavanjem države ali kogarkoli drugega (Kovačič, Mehanizmi varovanja v zasebni družbi, str.24).

Korba in Song ugotavljata, da čutijo uporabniki interneta kot veliko oviro pri rabi interneta ravno zaskrbljenost glede ogroženosti njihove zasebnosti (Korba, Song 2001, str. 3).
Prav tako lahko v poslovnem svetu pomeni pomanjkanje zasebnosti – tudi pomanjkanje prodaje. Raziskave kažejo, da ljudje še zmeraj ne zaupajo dovolj internetni prodaji. Cavoukianova[2] je mnenja, da je zaupanje bolj pomembno kot karkoli drugega na internetu (Cavoukian, prosojnice, 2005).

V zadnjih letih je večina razvitih držav sicer uzakonila način ravnanja z osebnimi podatki, razvita je bila tudi tehnologija s poudarkom na zaščiti zasebnosti, vendar to še zdaleč ni zadosti za učinkovito varovanje zasebnosti. Za učinkovito varstvo zasebnosti na internetu je ključnega pomena sinergija zakonske in tehnološke ureditve ter izobraževanje in obveščanje uporabnikov internetnih storitev. Uporabniki interneta morajo biti poučeni o tem, kako se njihove osebne informacije zbirajo, uporabljajo, komu vse so podatki posredovani ter v kakšne namene. Imeti morajo pravico dostopa do osebnih podatkov ter jih v skladu z zakonom tudi popraviti, v kolikor ti podatki niso pravilni, oziroma zahtevati njihov umik. Zaščito zasebnosti razumemo kot pravico posameznika imeti nadzor nad zbiranjem, uporabo ter širjenjem njegovih osebnih podatkov, s katerimi upravljajo drugi.

Za varovanje zasebnosti se vse bolj uveljavljajo tako imenovane tehnologije za izboljšanje zasebnosti – »Privacy Enhancing Technologies« ali na kratko PETs. Tehnologije so zasnovane tako, da z minimiziranjem in eliminiranjem osebnih podatkov ščitijo informacijsko zasebnost, ne da bi se s tem izgubila oziroma zmanjšala funkcionalnost informacijskega sistema (Blarkom, 2003, str. 33). Razvoj informacijsko komunikacijskih tehnologij omogoča zmeraj več možnosti zbiranja, shranjevanja, obdelovanja ter distribucijo osebnih podatkov. Zaradi tega naraščajo tudi potencialne kršitve zasebnosti potrošnikov in državljanov. Tehnologije za zboljšanje zasebnosti pa nam pomagajo doseči osnovne norme zasebnosti pri zakoniti obdelavi podatkov (Borking, Raab, 2001, str.14).
Namen tehnologij za zaščito zasebnosti je predvsem ustvariti infrastrukturo za zaščito zasebnosti, zmanjšati (omejiti) nadzor ter omejiti zbiranje podatkov.
Na kratko lahko rečemo, da so to tehnologije, ki podpirajo nadzor uporabnikov nad lastnimi osebnimi podatki. S pomočjo uporabe tehnologij za zaščito zasebnosti lahko tudi »tradicionalna« varnostna orodja postanejo »prijazna« z vidika zasebnosti.

Z nalogo želim osvetliti problem zaščite zasebnosti ter osebnih podatkov na internetu. Predvidevam, da se uporabniki interneta premalo zavedamo oziroma premalo poznamo grožnje zasebnosti na internetu, da velikokrat brez potrebe razkrivamo svoje osebne

[2] Dr. Ann Cavoukian je kanadska pooblaščenka za varovanje zasebnosti in podatkov in ena vodilnih strokovnjakov s področja zasebnosti in varovanja podatkov.

podatke in da premalo poznamo orodja za zaščito zasebnosti na internetu. Kljub temu pa čutimo določen strah pred razkritjem osebnih podatkov ter nadzorom, ki ga nove tehnologije omogočajo.

Kot je zapisano v poročilu EU o e-Evropi, je nujno, da ljudje zaupamo internetu, če želimo rast aktivnosti na področju e-poslovanja ter dvigniti raven storitev na področju e-upravljanja, e-zdravja, e-učenja…(e Europe 2003, Progress Report, februar 2004, str. 16).

Koncept človekovih pravic in zakonodaje s področja zasebnosti v sedanji družbi pridobiva na pomenu. Zasebnost je pravica posameznika imeti osebne informacije zaščitene pred neprimernim, radovednim očesom države in zasebnih organizacij, ki skušajo uporabiti osebne informacije za komercialne namene, to je za povečanje svojega dobička.
Potrebno je najti ravnotežje v odnosu med družbo in potrebo po zasebnosti.

1.1 Metode dela

Kot metodo dela pri izdelavi naloge sem uporabila raziskovanje obstoječe literature tujih in domačih avtorjev ter virov na internetu: uporabila sem deskriptivno metodo ter analizo primarnih in sekundarnih virov. S pomočjo ankete med uporabniki interneta sem skušala ugotoviti, ali nam je zasebnost pomembna, ali smo, oziroma katere osebne podatke smo pripravljeni razkriti (mogoče v zameno za kakšno boniteto), ali se zavedamo groženj interneta ter v kolikšni meri poznamo in uporabljamo orodja za zaščito zasebnosti na internetu.
Postavila sem delovni hipotezi:

- V informacijski družbi je zasebnost ogrožena.
- Uporabnikom interneta je zasebnost na internetu pomembna, zavedajo se groženj zasebnosti na internetu, vendar premalo poznajo in uporabljajo orodja ter tehnologije za zaščito zasebnosti.

1.2 Struktura naloge

Teoretični del naloge sem razdelila na tri glavne sklope:

- zasebnost kot osnovna človekova pravica
- grožnje zasebnosti na internetu
- varovanje zasebnosti s pomočjo tehnologij za zaščito zasebnosti

Zasebnost je večplasten, večdimenzionalen pojem, ki ga ni mogoče postaviti v ozek okvir ene definicije. Skozi različna časovna obdobja se je pogled na zasebnost spreminjal, zato sem v prvem poglavju opisala razvoj zasebnosti skozi zgodovino ter moderen pogled na

zasebnost. Opisala sem dimenzije zasebnosti ter se ustavila predvsem na informacijski zasebnosti, kamor prištevamo tudi varovanje podatkov. Za boljše razumevanje informacijske zasebnosti sem v nadaljevanju opisala pojem osebni podatek, kot ga pojmujeta slovenski zakon o varovanju podatkov ter evropska direktiva o zaščiti podatkov (DPD 95/46/ES). Predstavila sem tudi dve filozofski teoriji informacijske zasebnosti: teorijo nadzora ter teorijo omejenega dostopa.

V času vsesplošne digitalizacije in informatizacije našega življenja se o varnosti podatkov, varnosti omrežij, varnem elektronskem poslovanju veliko govori, hkrati pa se pojma varnost in zasebnost pogosto zamenjujeta, oziroma smo prepričani, da je z varnostjo avtomatsko zagotovljena tudi zasebnost. Žal temu ni tako, zato sem na koncu prvega poglavja spregovorila o razlikah med pojmoma **varnost** in **zasebnost**. Kot ugotavlja Bennet, je varnost podatkov sicer nujna, vendar to še ni zadosten pogoj za zagotovitev informacijske zasebnosti (Bennet, 2001, str.9).

Pomembno vlogo za zagotovitev zasebnosti in varovanja podatkov ima prav gotovo tudi država. V drugem poglavju sem predstavila nekaj najpomembnejših zakonskih ureditev varovanja zasebnosti po svetu. Zaradi globalizacije narašča tudi mednarodna izmenjava podatkov. Sprejeti je bilo potrebno mednarodna merila, ki bi urejala pretok podatkov ter poenotila dokaj raznoliko zakonodajo. V nalogi sem predstavila nekaj teh mednarodno sprejetih meril kot so OECD principi (1980), Konvencija o zaščiti posameznika s poudarkom na avtomatski obdelavi osebnih podatkov (1981), direktiva Evropske unije DPD95/46/ES (1995). V nadaljevanju sem predstavila zakonsko osnovo zaščite podatkov v Sloveniji ter zakonodajo držav, ki imajo največ izkušenj s področja zasebnosti in varovanja podatkov: v Združenih državah Amerike, v Kanadi ter Avstraliji.

V tretjem poglavju sem se osredotočila na grožnje zasebnosti. Predstavila sem najbolj pogosto vmešavanje v našo zasebnost kot so vdori, prestrezanje podatkov, prestrezanje elektronske pošte, zbiranje in povezovanje podatkov, sledenje, uporabo piškotkov, grožnje, ki jih predstavljajo iskalniki, profiliranje, nadlegovanje z neželeno elektronsko pošto (SPAM) in rudarjenje.

V poglavju o zaščiti zasebnosti sem se osredotočila predvsem na tehnologijo za zaščito zasebnosti. Samo tehnologija sicer še ni zadosten pogoj za celovito zaščito zasebnosti, poleg tehnologije je potrebna tudi ustrezna zakonodaja, upoštevanje dobre informacijske prakse vseh udeležencev v procesu ter izobraževanje tako strokovnjakov s področja informacijskih tehnologij kot tudi uporabnikov storitev.
V nalogi sem predstavila tehnologije za zboljšanje zasebnosti (PETs) ter osnovne principe delovanja teh tehnologij kot so: anonimnost, psevdonimnost, nezdružljivost in

neopazovanost ter primere uporabe: kriptografija (PGP), steganografija, upravljavec piškotkov, zaščitnik identitete, zaupni centri, anonimni strežniki, ponovni pošiljatelji…
Podobno kot teoretični del, sem zasnovala tudi empirični del naloge – anketo med uporabniki interneta, kjer sem v prvem delu zastavila vprašanja v zvezi z zasebnostjo in osebnimi podatki, v drugem delu sem zastavila vprašanja glede groženj zasebnosti na internetu, v tretjem delu pa so anketiranci odgovarjali na vprašanja glede poznavanja in uporabe tehnologij za zaščito zasebnosti.
Z raziskavo med uporabniki interneta sem želela dokazati hipotezo, da je uporabnikom zasebnost pomembna, da se zavedajo groženj zasebnosti preko spleta ter da premalo poznajo in uporabljajo tehnologije za izboljšanje zasebnosti na internetu (PETs).

2 DEFINICIJA ZASEBNOSTI IN OSEBNIH PODATKOV

Zasebnost je osnovna človekova pravica, zaščitena z deklaracijo združenih narodov o človekovih pravicah:

»*Nikogar se ne sme nadlegovati s samovoljnim vmešavanjem v njegovo zasebno življenje, v njegovo družino, v njegovo stanovanje ali njegovo dopisovanje in tudi ne z napadi na njegovo čast in ugled. Vsakdo ima pravico do zakonskega varstva pred takšnim vmešavanjem ali takšnimi napadi.«*[3]

Zaradi širine in večdimenzionalnosti je zasebnost težko postaviti v ozke okvirje ene definicije. Skozi različna obdobja so nastajale različne definicije, ki so bile odvisne od mnogih dejavnikov: kulture, okolja, zgodovinskega dogajanja, pa tudi stopnje razvoja naroda nasploh.
Zasebnost lahko razumemo kot interdisciplinaren pojem upoštevajoč zakonski, politični in sociološki vidik.

V nadaljevanju bom predstavila zgodovinski pregled zasebnosti, moderne definicije zasebnosti, dimenzije zasebnosti s poudarkom na informacijski zasebnosti ter filozofski vidik informacijske zasebnosti.

2.1 Zgodovinski pregled zasebnosti

Že v praskupnosti je človek čutil potrebo po zasebnosti, potrebo po »biti sam, biti nemoten«. Skozi različna obdobja zgodovine je imela zasebnosti različen pomen. Sprva, v

[3] Splošna deklaracija človekovih pravic (12. člen), ki jo je razglasila Generalna skupščina združenih narodov 10. decembra 1948

manj razvitih družbah, je imela zgolj pomen fizičnega umika na lokacijo varno pred ostalimi, pred skupnostjo. Kasneje je zasebnost pridobila tudi na družbenem pomenu, v zadnjem stoletju celo kot temeljna človekova pravica.

Prve zametke zasebnosti na višji ravni najdemo v starih zapisih Korana, v Bibliji, v zapuščini zgodnje hebrejske kulture, v zakonih in kulturi klasične Grčije in Kitajske. Kot navaja Graham, je bil v družbah kot sta bili stara Grčija ali Kitajska sicer dobro razvit koncept »javno – zasebno«, vendar pa zasebnost nikoli ni bila opisana z vidika družbene politike, pojmovala se je le kot izraz lastninske pravice (Graham, 1999, str. 6).

Zaradi potrebe po utrjevanju lastne oblasti (cesarska oblast na Kitajskem, kraljevska v Evropi, katoliška cerkev...), kljub napredku in razvoju družbe, zasebnost ni pridobila veliko na pomenu. Šele v obdobju razsvetljenstva (pozno 17. stoletje) so ljudje ponovno začeli razmišljati o pravici do zasebnosti. Iz tega obdobja izhajata filozofa Locke[4] in Kant[5], ki sta s svojim delom imela velik vpliv na razmišljanje ljudi tedanjega časa. Ljudje so začeli razumevati, da so njihova izkustva pomembna in rezultat tega so bila nova spoznanja: drugače so začeli gledati na pravico do zasebnosti ter na položaj v družbi (Horniak, 2004, str. 21).

V angleškem kazenskem zakoniku se pojavi koncept: »vsakogar hiša je njegov grad«. Britanski parlamentarec William Pitt je v primeru Entick proti Carrington leta 1765 zapisal:

»The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow though it; the storms may enter; the rain may enter – but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement« [6]
(poročilo Privacy & Human Rights, 2004).

Za obdobje 18. stoletja je značilna krepitev merkantilizma[7] in buržoazije ter prevzem nadzora nad ekonomijo, ki je bil prej v rokah klera in fevdalcev. Z nadzorom nad ekonomijo si je buržoazija pridobila tudi politično moč. Za ohranitev novega položaja so

[4] John Locke (1632-1704), angleški filozof, znan po delu Second Treatise of Goverment: zanj je bila zasebnost toliko pomembna, kot človeško življenje; po njegovem je za zasebnost lastnine, zasebnost komunikacije, svobode govora, dovoljeno tudi ubijati. Tako se je zoperstavil temeljnim etičnim vrednotam tedanjega časa in s tem poudaril pomen zasebnosti (Horniak, 2004, str. 18).
[5] Immanuel Kant (1724-1804) je poudarjal, da ima človeško bitje zmožnost komuniciranja in ustvarjanja. Iz tega sledi, da če je ogrožena njegova zasebnost, je zmanjšana tudi zmožnost komunicirnja in ustvarjanja. To pomeni, da je človek avtomatsko degradiran. Kant je trdil tudi, da je človeško bitje razumsko in neodvisno, zaradi tega želi biti oseben in zaseben (Horniak, 2004, str.17)
[6] Tudi najrevnejši človek lahko v svoji koči kljubuje vsej moči Krone. Lahko je slaboten, njegova streha se lahko maje, veter lahko piha skoznjo, vihar in dež lahko vstopita – toda Kralj Anglije ne sme vstopiti; vsa njegova moč si ne sme drzniti prestopiti praga razdejanega doma
[7] Ekonomsko politična smer (16. do 18. stoletje), ki pospešuje manufakturo in zunanjo trgovino

potrebovali takšno zakonsko zaščito, ki bi varovala njihovo lastnino. To je privedlo do prve zakonske zaščite zasebnosti. Vendar ne v vseh državah hkrati in tudi ne v vseh državah enako. Te razlike se še danes odražajo v zakonodajah različnih držav (Graham, 1999, str. 9).

V 19. in še posebej v 20. stoletju se uveljavi koncept človekovih pravic. Zasebnost se sedaj razume kot osnovna človekova pravica. V demokratični družbi postane življenje posameznika sveto, nedotakljivo, razkrije se lahko samo v zakonsko upravičenih primerih.

2.2 Moderna definicija zasebnosti

»*The right to be left alone - the most comprehensive of rights, and the right most valued by all civilized men—.«*[8]
(sodnik Brandeis[9], primer Olmstead proti ZDA (1928))

Začetki modernega pogleda na zasebnost kot osebnostno in ne lastninsko pravico segajo v leto 1890, ko sta odvetnika Warren in Brandeis v reviji Harvard Law Review objavila članek Pravica do zasebnosti: pravica biti sam. V članku navajata, da bodo spremembe v tehnologiji in zakonodaji povzročile tudi spremembo narave zasebnosti. Za tedanji čas je bilo to zelo napredno in dalekovidno razmišljanje.
Novejše definicije se sicer med seboj razlikujejo, v glavnem pa vse, prav tako kot Brandeisova, bazirajo na pravici biti sam, brez nadzora in pravici sam se odločiti, katere informacije o sebi želimo razkriti in v kakšnih okoliščinah. Pojem zasebnost mora vsebovati pravico biti informiran o tem kje in kateri podatki se zbirajo o posamezniku, jih videti ter imeti možnost popraviti jih ali celo zbrisati.

Alan Westin [10] je definiral zasebnost kot:
»zahteva posameznikov, da se sami odločijo zase kdaj, kako in v kakšni obliki bodo njegovi osebni podatki posredovani drugim[11]*«* (poročilo Privacy and Human Rights, 1999).

8 »Pravica, da te pustijo samega – najbolj splošna od pravic in pravica, ki ima največjo vrednost za vsakega civiliziranega človeka«
9 Louis Dembitz Brandeis (13. november, 1856 – 3. oktober 1941) je bil ameriški odvetnik, sodnik ter pomemben zagovornik pravice do zasebnosti
10 Dr. Alan F. Westin, avtor knjige Privacy and Freedom (1967) ter mnogih drugih na temo zasebnosti; od leta 1959 je prof. za javno pravo na Kolumbijski Univerzi; je eden vodilnih ekspertov s področja informacijske zasebnosti
11 the claim of individuals...to determine for themselves when, how and to what extent information about them is communicated to others.

Podobno definicijo je postavil Schoeman (1984). Zasebnost definira kot:
»pravica določiti katere osebne podatke bomo posredovali drugim, oziroma imeti nadzor nad lastnimi osebnimi podatki« (Rezgui, Bouguettaya, Eltoweissy, 2003, str.41).

Roger Clarke[12] predlaga, definicijo zasebnosti kot
»interes posameznika, da ohrani svoj osebni prostor prost pred vmešavanjem in motenjem drugih posameznikov in organizacij.« (Clarke, Introduction to Dataveillance and Information Privacy, and Definition of Terms)

G. B. F. Niblett opredeljuje pravico do zasebnosti:
«pravica do zasebnosti - pravica posameznika, da zahteva, da se podatki in informacije o njegovih zasebnih razmerjih ne sporočajo komurkoli…«, meni, da gre pri tem za nadzor pretoka in posredovanja podatkov, ki se nanašajo nanj oziroma opisujejo njegove lastnosti (Čebulj, 1992, str.7).

2.2.1 Dimenzije zasebnosti

Zasebnost je večdimenzionalen pojem, ki mu različni avtorji pripisujejo tudi različne dimenzije. Clarke jo deli na:

Zasebnost telesa je pojmovana kot neokrnjenost posameznikovega telesa (vključuje pravico opredeliti se do obveznega cepljenja, transfuzije krvi brez soglasja, obvezne sterilizacije, obveznega dajanja telesnih tekočin in telesnih tkiv…).

Zasebnost obnašanja se nanaša predvsem na specifično (občutljivo) obnašanje kot na primer: spolne navade, politično prepričanje, versko prepričanje - povsod na zasebnem in javnem prostoru.

Zasebnost osebnega komuniciranja: posameznik ima interes po nenadzorovani komunikaciji (zahteva po dani možnosti komunicirati s komerkoli preko različnih medijev ne da bi bil nadzorovan).

Zasebnost osebnih podatkov ali informacijska zasebnost: zahteva posameznika, da podatki o njem samem (osebni podatki) niso avtomatsko na razpolago drugim osebam in organizacijam; če pa so podatki posedovani drugim, mora imeti posameznik možnost kontrole podatkov ter nadzora uporabe (Clarke, Introduction to Dataveillance and Information Privacy, and Definition of Terms).

Poročilo o človekovih pravicah[13] (13.11.2004) navaja dejstvo, da je zaščita zasebnosti pogosto videna kot linija, meja do kam lahko sega vmešavanje družbe v zadeve posameznika. Zasebnost deli na:

[12] Dr. Roger Clarke je avstralski raziskovalec s področja elektronskega poslovanja, informacijske infrastrukture, informacijske zasebnosti…je avtor številnih člankov in publikacij ter član številnih mednarodnih organizacij s področja informacijske zasebnosti.

Informacijsko zasebnost: vsebuje pravila za upravljanje zbirk osebnih podatkov kot na primer: finančne informacije, medicinske kartoteke ter zapise, ki jih upravljajo vladne agencije. Informacijska zasebnost je poznana tudi kot »varovanje podatkov«.
Telesno zasebnost: nanaša se na zaščito človekove fizične nedotakljivosti glede invazivnih posegov na telo (genetični testi, …).
Zasebnost komunikacij: pokriva varnost ter zasebnost pošte, elektronske pošte, telefonskih pogovorov ter ostale oblike komunikacij.
Prostorsko zasebnost: omejitev nadlegovanja, motenja tako v domačem kot tudi drugem okolju (delovno mesto, javni prostor). To vključuje razne raziskave, video nadzor, satelitski nadzor… (Privacy and Human Rights, 2004)

2.2.1.1 Osebni podatki

Pojem informacijska zasebnost je postal evropski koncept zaščite podatkov. Pomemben cilj politike informacijske zasebnosti je kontrola nad lastnimi osebnimi podatki. Cilj zaščite zasebnosti mora biti posameznik in ne katerakoli druga entiteta. S tega vidika je potrebno natančno definirati pojem osebni podatek.

Evropska direktiva o zaščiti podatkov (DPD 95/46/ES) navaja, da pomeni osebni podatek vsak delček informacije, ki se nanaša na točno določenega posameznika ali na posameznika, ki ga je mogoče preko te informacije identificirati (posredno ali neposredno). Neposredna identifikacija pomeni: ime in priimek, naslov, osebna številka (pri nas EMŠO), datum rojstva, nacionalnost, izobrazba, zaposlitev, zakonski stan, širše poznan psevdonim, biometrične karakteristike (prstni odtis…). Posredna identifikacija pa pomeni ostale enolično določene parametre, lastnosti ali kombinacijo, z namenom da se pridobi zadostna identifikacijska informacija,[14] na podlagi katere se lahko enolično identificira posameznik.

Slovenski zakon o varovanju osebnih podatkov definira osebni podatek kot »*katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen*.«

Če osebni podatki vsebujejo informacijo o rasni ali etični pripadnosti, politični opredelitvi, verskem prepričanju, fizičnem oziroma duševnem zdravju, spolni usmerjenosti, sumu kaznivega dejanja, govorimo o občutljivih osebnih podatkih, ki jih je potrebno še bolj učinkovito varovati.

[13] Report Privacy and Human Rights 2003, ki ga izdaja EPIC- Electronic Privacy Information Center; poroča o varovanju zasebnosti in človekovih pravic v različnih državah sveta.
[14] DPD 95/46/ES člen 2

2.2.1.2 Filozofski vidik informacijske zasebnosti

S filozofskega vidika srečamo v okviru informacijske zasebnosti dve glavni teoriji in sicer teorijo kontrole in teorijo omejenega dostopa.

Teorija nadzora (Control theory)[15] pravi, da je zasebnost posameznika pogojena z nadzorom nad njegovimi lastnimi informacijami. Torej ima nekdo zasebnost, če in edino če ima nadzor nad lastnimi podatki. Pomanjkljivost te teorije je, da praktično gledano nihče ne more imeti popolnega nadzora nad vsakim delčkom informacije o njem samem in potemtakem tudi zasebnosti ne.
S teoretičnega vidika pa je pomanjkljivost te teorije v tem, da nekdo teoretično lahko obdrži zasebnost kljub temu, da je razkril vse delčke informacije o sebi, in to samo zato, ker je to storil zavestno, ker je imel nadzor nad razkritjem informacij.
Razkritje posameznika vseh njegovih osebnih informacij ter še zmeraj imeti zasebnost se ne sklada s splošnim pojmovanjem zasebnosti (Tavani, 2000, str. 4).

Teorija omejenega dostopa (Restricted access theory)[16] definira zasebnosti kot omejitev dostopa drugim do posameznikovih podatkov. Pri tem upošteva tajnost, anonimnost in samoto. Pojem tajnost se nanaša na omejeno distribucijo osebnih podatkov, medtem ko se pojem anonimnost nanaša na zaščito pred neželenim posegom, pojem samota pa je mišljen kot fizična oddaljenost (osamitev) od drugih (Horniak, 2004, str.16).
Tavani ugotavlja, da je moč te teorije, da odpravlja zamenjavo zasebnosti z avtonomijo ter svobodo z odmaknjenostjo. Problem teorije omejenega dostopa vidi v tem, da teorija podcenjuje vlogo nadzora oziroma izbire, kar je prav tako zahteva pojma zasebnosti. Zanemari se dejstvo, da nekdo, ki ima zasebnost, lahko izbira ali bo dovolil, omejil ali celo prepovedal dostop do njemu lastnih informacij (Tavani, 2000, str. 4-6).

Bolj uspešna v razumevanju zasebnosti naj bi bila kombinacija obeh teorij, tako imenovana **Moorova teorija nadzora in omejenega dostopa**[17]**,** ki zagovarja dejstvo, da ohranja posameznik zasebnost v odnosu do drugih, če in samo če je situacija takšna, da je zaščiten pred motenjem, vmešavanjem in dostopom do informacij. Bistveno po Mooru je zagotovitev, da imajo samo »prave osebe ob pravem času« dostop do osebnih podatkov. Ljudje naj bi imeli največ mogoče nadzora nad lastnimi osebnimi podatki, potrebno pa se je osredotočiti na pravilo nujnosti ter razviti politiko zaščite zasebnosti.
Posameznik ne potrebuje absolutnega nadzora nad vsakim delčkom njemu lastne informacije (kot pri teoriji nadzora), bolj pomembno je, da ima možnost izbire. Možnost izbire pa bazira na informiranosti. Poučen posameznik se lahko odloči kdaj in v katerih situacijah bo obdržal zasebnost oziroma, bo razkril osebne podatke.

[15] Zagovarjala sta jo filozofa Fried (1970) in Rachel (1975)
[16] Zagovornica teorije je bila filozofinja Ruth Gavison (1984)
[17] Zagovarja jo filozof James Moor (1997), ki se ne strinja s Friedovo teorijo nadzora. Pravi, da danes v dobi računalništva ni mogoče imeti popolnega nadzora nad lastnimi osebnimi podatki

Zasebnost lahko bolje zaščitimo, če natančno poznamo cone zasebnosti in, če poznamo pod kakšnimi pogoji in komu bodo naše informacije posredovane (Horniak, 2004, str. 16, Tavani, 2000, str.19).

2.3 Varnost in zasebnost

V današnji dobi informatizacije in nasploh digitalizacije našega življenja se veliko govori o varnosti podatkov, o varnosti omrežij, o varnosti elektronskega poslovanja. Prepričani smo, da z zagotovitvijo varnosti poslovanja dosegamo tudi zasebnost. Žal temu ni tako. Varnost in zasebnost sta dva pojma, ki ju mnogokrat zamenjujemo, vendar ju nikakor ne moremo in ne smemo enačiti. Med njima obstajajo pomembne razlike. Kot navajata Ann Cavoukian in Mike Gurski je zasebnost usmerjena na osebo, na posameznika, medtem ko je varnost usmerjena na organizacijo, na skupnost. Varnost mora služiti zasebnosti z integriteto, verodostojnostjo, zaupnostjo – biti mora orodje za zagotovitev zasebnosti.
Varnost naj bi bila pod nadzorom računalniških strokovnjakov, zasebnost pa mora biti pod nadzorom vsakega posameznika (Cavoukian, Gurski, 2000, str.1-2).

Pomembna razlika med pojmom varnost in zasebnost v računalniški tehnologiji je v tem, da je informacija varna, če ima lastnik nadzor nad njo. Po drugi strani pa je informacija zasebna, če ima oseba na katero se informacija nanaša nadzor nad njo. Zasebnost ne pomeni samo informacije ter tveganja izgube nadzora nad njo, pomeni tudi zasebnost prostora ter zasebnost stvari, kar predstavlja pomemben vidik osebne integritete (Camp, v Horniak, 2004, str. 15).

Koncepta varnost ter zasebnost sta tesno povezana ter se pogosto prekrivata, hkrati pa je med njima tudi pomembna razlika. Predvsem prihaja do konflikta med skupinsko varnostjo ter individualno zasebnostjo (Horniak, 2004, str.15).

Pred enajstim septembrom 2001 sta bili varnost in zasebnost podobno usmerjeni. Po bombnem napadu na WTC pa se je ravnotežje porušilo. V svetu je prevladala zahteva po javni varnosti in v imenu javne varnosti se je povečal nadzor države nad državljani. Zasebnost državljanov je postala na ta način ogrožena, kljub temu, da državne agencije ravnajo z informacijami zaupno (Hinde 2002, str.18, Bainbridge, 2003, str. 1687).

Težko je najti pravo ravnovesje med pravico do zasebnosti ter dolžnostjo države, da zaščiti svoje državljane pred zunanjimi grožnjami kot so terorizem, kriminal, nesocialno obnašanje in vse druge grožnje stabilnosti v družbi.

Zbiranje osebnih podatkov za identifikacijo teroristov ali potencialnih teroristov je orodje za boj in zaščito pred terorizmom. To pa je tudi klasičen primer nasprotja med pravico

posameznika do zasebnosti in pravico države da zaščiti javni interes. Grožnje varnosti so konfliktni primeri teh dveh pravic: pravice do varnosti in pravice do zasebnosti.

Kot ugotavlja Hübnerjeva ima lahko varnost dva vidika: varnost kot tehnični pripomoček varovanja zasebnosti[18] ter varnost kot poseg v zasebnost: varnostni mehanizmi uporabljajo osebne podatke o uporabnikih in podatkovnih subjektih (prisluškovanje, detekcijski sistemi, biometrija, lokacijsko osnovano overovljenje) (Fischer-Hübner, 2001, str.105).

Bennett poudarja, da je varnost podatkov sicer nujna, vendar pa to še ni zadosten pogoj za zagotovitev informacijske zasebnosti (Bennett, 2001, str. 9).
Med varnostjo in zasebnostjo je potrebno najti pravo razmerje, ki bo vključevalo skrbno uporabo štirih dejavnikov: nujnost, učinkovitost, sorazmernost in čim manjšo uporabo zasebnostno invazivnih alternativ (Crompton, 2002, str.18).

3 PREGLED ZAKONSKE UREDITVE NA PODROČJU VAROVANJA PODATKOV IN ZASEBNOSTI

»Every one has the right to respect for his private and family life, his home and his correspondence.
There shall be no interference by a public authority with the excersise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health of morals, or for the protection of the rights and freedoms of others.[19]*«*
(8. člen Konvencije Sveta Evrope o zaščiti človekovih pravic in temeljnih svoboščin, 1950)

Hiter razvoj računalniških komunikacij, velike zmogljivosti zbiranja, shranjevanja in obdelave podatkov, medsebojno povezovanje baz podatkov ter prenos podatkov izven državnih meja, je povzročilo večjo grožnjo zasebnosti, hkrati pa tudi vse večjo skrb oziroma zavedanje državljanov glede zasebnosti kot osnovne človekove pravice.

[18] člen 17 DPD 95/46/ES zahteva od upravljavca podatkov, zagotovitev ustrezne tehnične in organizacijske ukrepe za zavarovanje osebnih podatkov pred slučajnim ali nezakonitim uničenjem ali slučajno izgubo, predelavo, nepooblaščenim posredovanjem ali dostopom, predvsem kadar obdelava vključuje prenos podatkov po omrežju, ter proti vsem drugim nezakonitim oblikam obdelave.
[19] »Vsakdo ima pravico do spoštovanja svojega zasebnega in družinskega življenja, svojega doma in dopisovanja. Javna oblast se ne sme vmešavati v izvrševanje te pravice, razen če je to določeno z zakonom in nujno v demokratični družbi zaradi državne varnosti, javne varnosti ali ekonomske blaginje države, zato da se prepreči nered ali zločin, da se zavaruje zdravje ali morala ali da se zavarujejo pravice in svoboščine drugih ljudi.«

Kot ugotavlja Webbova se je naša kontrola nad osebnimi podatki spremenila, kajti informacijska tehnologija dopušča večje količine in naraščanje občutljivosti podatkom zbranim in analiziranim tako v državnem kot tudi zasebnem sektorju (Webb, 2003, str.2).
Prav zaradi zaskrbljenosti glede vpliva informacijske tehnologije na zasebnost ter možnosti mednarodnega pretoka podatkov so se prvi zakoni v zvezi z zasebnostjo pojavili hkrati z razvojem informacijskih tehnologij v zgodnjih sedemdesetih letih v nekaterih evropskih državah. Večina teh zakonodaj je bila usmerjenih predvsem na informacijsko zasebnost. Urejale so zbiranje in ravnanje s podatki ter njihovo nadaljnje širjenje ter združevanje (Crompton, 2002, str.15).
Sprva so bile te zakonodaje zelo različne, zaradi porasta izmenjave podatkov izven državnih meja, pa je bilo potrebno sprejeti mednarodna merila, ki bi predstavljala učinkovite in poenotene okvirje zaščite podatkov in zasebnosti.

3.1 Mednarodno uveljavljeni instrumenti

Eden prvih takšnih mednarodno uveljavljenih instrumentov so bile smernice OECD[20], ki so jih članice sprejele prav z namenom, da bi bile zakonodaje (vsaj na evropski ravni) med seboj poenotene, hkrati pa tudi v pomoč državam, ki ustrezne zakonodaje še niso sprejele. Smernice, poznane kot OECD principi vsebujejo načela:

- omejitev zbiranja podatkov
- kvaliteto podatkov
- natančno določitev namena zbiranja podatkov
- omejitev uporabe podatkov
- zagotovitev varnosti podatkov
- odprtost
- individualno participacijo
- odgovornost

Kot navajajo članice v sprejetem dokumentu, mora biti zbiranje podatkov zakonito in pošteno ter z vednostjo in pristankom osebe na katero se podatki nanašajo. Osebni podatki morajo biti relevantni za namen uporabe, natančni, celoviti ter aktualni. Namen oziroma cilj zbiranja podatkov mora biti natančno določen v času zbiranja podatkov, omejiti je potrebno tudi kasnejše spreminjanje namena. Osebni podatki ne smejo biti razkriti ali kako drugače uporabljeni, kot je bilo to določeno z namenom zbiranja. Biti morajo v soglasju z osebo na katero se podatki nanašajo ali pa mora biti namen zbiranja določen z zakonom. Zagotovljena mora biti zaščita pred izgubo podatkov, neavtoriziranim dostopom, uničenjem, nepravilno rabo, predelavo ali razkritjem podatkov. Princip odprtosti zahteva,

[20] OECD - Organisation for Economic Co-operation and Development: Organizacija za ekonomsko sodelovanje in razvoj; članice so principe sprejele 23.9.1980. Sprejetje principov je narekovala potreba po zaščiti zasebnosti v zvezi z osebnimi podatki zaradi naglega razvoja avtomatskega procesiranja podatkov ter prenosa podatkov izven meja držav in kontinentov; principi so neodvisni od tehnologije.

da morajo biti na razpolago podatki o zbirkah, ki se vodijo, naravi osebnih podatkov, namenu uporabe ter upravljavcu (kontrolorju) podatkov. Posameznik mora imeti pravico do informacije ali se o njem zbirajo podatki in kateri. Zadnji princip navaja odgovornost upravljavcev (kontrolorjev) podatkov, da upoštevajo prej navedene principe.
Kmalu po sprejetju teh smernic, je podobne smernice sprejel leta 1981 tudi Svet Evrope s Konvencijo o zaščiti posameznika s poudarkom na avtomatski obdelavi osebnih podatkov ter leta 1995 še Evropska unija v znani direktivi o zaščiti podatkov (95/46/ES).

Osnovni principi, ki jih najdemo v skoraj vseh smernicah ter zakonodajah so:

- doseči poštenost in zakonitost
- informacije uporabljati samo za namen, ki je bil prvotno določen
- točnost, pomembnost in ne prekomernost glede na določen namen
- natančnost in časovna omejenost
- podatke uničiti, ko je namen izpolnjen

(Dodig-Crnkovic, Horniak, 2005, str. 4)

Do podobnih ugotovitev so prišli tudi na svetovnem kongresu neodvisnih državnih organov s področja varstva osebnih podatkov v mestu Montreux v Švici, septembra 2005. V svoji deklaraciji so izrazili ugotovitev, da gre razvoj informacijskih znanosti v smeri globalizacije informacijske izmenjave in uporabe naprednih vsiljivih tehnologij pri obdelavi podatkov; povsod po svetu je opaziti naraščanje groženj glede vseprisotnega nadzora posameznikov; izrazili so zaskrbljenost zaradi razlik v zakonski regulativi v različnih delih sveta in pomanjkanje zaščite podatkov v nekaterih državah, ki lahko spodkoplje učinek globalne zaščite podatkov.
Iz različnih mednarodnih instrumentov kot so principi OECD, principi konvencije Sveta Evrope, direktive Evropske unije 95/46/ES in drugih, so izpeljali naslednje principe:

- princip zakonitega in poštenega zbiranja in obdelovanja podatkov
- princip točnosti, natančnosti podatkov
- princip določitve namena in omejitve
- princip proporcionalnosti
- princip transparentnosti
- princip individualne participacije in zagotovitve pravice dostopa do podatkov posamezniku na katerega se podatki nanašajo
- princip ne-diskriminacije
- princip tajnosti podatkov
- princip odgovornosti
- princip neodvisnega nadzora in zakonitega sankcioniranja
- princip o primerni stopnji zaščite v primeru prekomejnega prenosa osebnih podatkov

Združene narode so pozvali, da pripravijo učinkovito zakonsko osnovo, kjer bo jasno definirana pravica do zaščite podatkov ter zasebnosti kot izterljiva človekova pravica. Vse države sveta pa pozivajo, da sprejmejo zakonodaje o zaščiti podatkov in zasebnosti, ki bodo v soglasju z osnovnimi principi.
(Deklaracija o zaščiti osebnih podatkov in zasebnosti v globaliziranem svetu: splošna pravica upoštevanja različnosti, 2005, str.1-3,)

3.1.1 Evropske direktive

Evropska unija je že leta 1995 sprejela osnovno direktivo za zaščito podatkov znano pod imenom DPD 95/46/ES, ki se nanaša na vsakršno obdelovanje osebnih podatkov ne glede na tehnologijo. Tako zapadejo pod to direktivo tudi osebni podatki, ki se pojavljajo na internetu. V svojem sedemnajstem členu direktiva nalaga upravljavcem zbirk podatkov implementacijo primerne tehnične podpore za zagotovitev osebnih podatkov, še posebej v mrežnih transakcijah.
Direktiva 95/46/ES predpisuje, da morajo biti osebni podatki obdelovani pošteno in zakonito, zbrani za točno določen in zakonit namen ter ne smejo biti nadalje obdelovani za druge namene, ki niso v skladu s prvotno določenim namenom zbiranja. Podatki morajo biti ustrezni, relevantni, ne smejo biti prekomerni glede na namen zbiranja in obdelovanja, biti morajo aktualni ter kjer je mogoče tudi datirani. Netočni in zastareli podatki morajo biti popravljeni oziroma zbrisani. Podatki so lahko shranjeni v obliki, ki dopušča identifikacijo posameznikov le toliko časa, kolikor je to potrebno za namene, za katere so bili podatki zbrani.
V skladu z direktivo se lahko osebni podatki obdelujejo samo v nedvoumnem soglasju z lastnikom podatkov, se pravi z osebo na katero se podatki nanašajo[21].
Zbiratelj podatkov mora seznaniti osebo na katero se podatki nanašajo, kateri podatki se zbirajo in za kakšen namen. Seznaniti jih mora tudi z možnostjo dostopa do podatkov ter pravico do poprave podatkov. Prenos osebnih podatkov izven držav Evropske unije je mogoč le, če država, kamor so bili podatki posredovani, zagotovi ustrezno raven varstva.

Evropski parlament je decembra 1997 sprejel še direktivo 97/66/ES, ki je prenesla načela osnovne direktive 95/46/ES v posebna pravila glede zaščite zasebnosti in osebnih podatkov na področju telekomunikacij. Ta direktiva se je nanašala predvsem na obdelavo osebnih podatkov v zvezi z javno dostopnimi telekomunikacijskimi servisi. Direktiva je zagotavljala zaupnost elektronske pošte[22], ponudnikom storitev pa je naložila obveznost, da s pomočjo tehnične in organizacijske podpore zagotovijo varno zaščito prenosa in seznanjajo uporabnike z morebitnim tveganjem. Zaradi potrebe po prilagoditvi razvoju

[21] v tuji literaturi znano kot »data subject«
[22] 5.čl. direktive: vsakdo ima pravico pošiljati elektronsko pošto drugemu, ne da bi tretja oseba to pošto prečitala

trgov in tehnologij za elektronske komunikacijske storitve, je bila ta direktiva razveljavljena in nadomeščena z julija 2002 sprejeto direktivo 2002/58/ES.

Kot je zapisano v sami direktivi 2002/58/ES, je le ta bila sprejeta zaradi razvoja digitalne tehnologije komunikacijskih omrežij, ki imajo velike zmogljivosti in zmožnosti za obdelavo osebnih podatkov. Direktivo 97/66/ES je bilo potrebno posodobiti in prilagoditi razvoju trgov in tehnologij za elektronske komunikacijske storitve, da se ne glede na uporabljeno tehnologijo zagotovi enaka raven varstva osebnih podatkov in zasebnosti uporabnikov javno razpoložljivih elektronskih komunikacijskih storitev. Internet ponuja uporabnikom nove možnosti, pa tudi nova tveganja glede njihovih osebnih podatkov in zasebnosti. Cilj direktive je čim bolj zmanjšati obdelavo osebnih podatkov in kadar je le mogoče uporabljati anonimne in psevdonimne podatke.
Osnovna načela direktive 2002/58/ES:

Zaupnost sporočil: Države morajo zagotoviti zaupnost sporočil in podatkov o prometu, ki se pošiljajo preko javnih komunikacijskih sredstev. Vsem osebam razen uporabnikom je prepovedano poslušanje, prisluškovanje, nadziranje komunikacij (sporočil) in z njimi povezane podatke o prometu brez privolitve uporabnikov, na katerega se nadzor nanaša.

Podatki o prometu: Podatki o prometu lahko dajo dobro sliko o navadah posameznika, njegovih stikih, zanimanjih, aktivnostih in zaradi tega predstavljajo občutljive podatke. Direktiva zato zahteva, da morajo biti podatki, ki jih je ponudnik storitve obdelal in shranil, zbrisani ali predelani v anonimne, potem ko niso več potrebni za namen prenosa sporočila.
Države članice pa lahko sprejmejo zakonske ukrepe, s katerimi omejijo obseg pravic in obveznosti, če je to v interesu državne varnosti.[23]

Podatki o lokaciji: Podatki o lokaciji se lahko obdelujejo šele potem, ko postanejo anonimni ali s privolitvijo posameznika na katerega se podatki nanašajo.

Nepovabljena sporočila: Uporabnikom mora biti dana možnost, da na brezplačen in enostaven način ugovarjajo uporabi elektronskega naslova za namene oglaševanja. Prepovedano je pošiljati elektronsko pošto za namene neposrednega trženja na ta način, da se skrije identiteta pošiljatelja ali brez možnosti dati zahtevo, da se taka sporočila v prihodnje ne pošiljajo več.

Uporaba vohunske programske opreme, programov za prikriti nadzor računalnika, omrežnih hroščkov ter drugih podobnih naprav, ki lahko vdrejo v uporabnikov računalnik ter resno ogrozijo njegovo zasebnost, mora biti dovoljena samo za zakonite namene, z vednostjo prizadetih uporabnikov.
Direktiva dovoljuje državam, da zakonito prestrezajo elektronska sporočila, vendar le za zaščito javne in državne varnosti ter obrambo države ter kadar je to zakonsko dovoljeno.

[23] 15. člen direktive 2002/58/ES dovoljuje državam članicam sprejetje zakonskih ukrepov, ki bi omejile pravice in obveznosti glede zaupnosti sporočil, podatkov o prometu, podatkov o lokaciji, če je to potrebno za zaščito državne varnosti, obrambe, javne varnosti…

Glede uporabe piškotkov (»cookies«) direktiva predvideva, da so to lahko zakonita in uporabna orodja za različne internetne transakcije, vendar morajo biti uporabniki seznanjeni z njihovo uporabo in imeti možnost, da jih lahko tudi zavrnejo.
Podobno kot v direktivi 95/46/ES je tudi tu navedeno, da lahko izreče posameznik svojo privolitev na kakršen koli primeren način (tudi samo tako, da pri obisku spletne strani označi rubriko s kljukico, če se s pogoji strinja.)

Po napadu na Ameriko 11. septembra 2001 se je povsod po svetu spremenil odnos do zasebnosti. Vse bolj je izražena dilema med zasebnostjo posameznikov in državno varnostjo. Tako direktiva 2002/58/ES dovoljuje državam članicam retencijo lokacijskih in prometnih podatkov preko različnih komunikacijskih sredstev: telefonije, mobilne telefonije, interneta, internetne telefonije, medtem ko direktiva 95/46/ES v 6. členu zahteva, da se podatki zbrišejo oziroma predelajo v anonimne takoj po končanem namenu za katerega so bili zbrani. Zaradi boja proti terorizmu je vse bolj glasna zahteva članic Evropske unije po večjem nadzoru nad državljani, s tem tudi po vse daljši dobi retencije prometnih in lokacijskih podatkov.
V pripravi je direktiva o retenciji podatkov obdelanih in shranjenih v povezavi z javno dostopnim elektronskim komunikacijskim servisom (komunikacijski podatki). Direktiva naj bi se nanašala na telefonijo, kratka sporočila preko mobitela (SMS, MMS), internetne protokole vključujoč: svetovni splet, elektronsko pošto, internetno telefonijo, prenos podatkov (file transfer protokol).
Ponudniki storitev naj bi omogočili retencijo podatkov 6 mesecev (z možnostjo do 36 mesecev). Dostop do ohranjenih komunikacijskih podatkov ter izmenjava naj bi bila omejena na državne ustanove pristojne za kriminalne zadeve (Working party on cooperation in criminal matters, 2005).

Direktive same po sebi niso zakon, predstavljajo le minimum zahtev oz. smernice, ki jih morajo države EU sprejeti v svojih zakonodajah.

3.2 Zakonska osnova varovanja osebnih podatkov v Sloveniji

Pravica do zasebnosti je ustavna pravica državljanov Republike Slovenije, zagotovljena v 35. členu ustave. Prav tako ustava v 38. členu opredeljuje uporabo osebnih podatkov v skladu z namenom zbiranja, pravico da se posameznik seznani z osebnimi podatki, ki se nanašajo nanj in pravico do sodnega varstva ob njihovi zlorabi.
Prvi zakon o varstvu osebnih podatkov je bil sprejet marca 1990, januarja 1992 pa je stopil v veljavo. Republika Slovenija je v letu 1993 podpisala tudi konvencijo Sveta Evrope o varstvu posameznika glede na avtomatsko obdelavo podatkov iz leta 1981. Zakon o varstvu osebnih podatkov je bil usklajen z določbami konvencije Sveta Evrope št. 108 in določbami direktive Evropske unije 95/46 ES.

V letu 2004 je bil v Sloveniji sprejet nov zakon o varstvu osebnih podatkov, ki je stopil v veljavo 1.1.2005. V zakonu so zajeta priporočila ter usmeritve mednarodno uveljavljenih smernic na področju zbiranja ter varovanja osebnih podatkov.
Pomembno je določilo, da se lahko osebni podatki obdelujejo le, če to določa zakon ali če je podana osebna privolitev posameznika. Namen obdelave mora biti določen z zakonom oziroma mora biti posameznik z njim ustrezno seznanjen. Osebni podatki se lahko zbirajo le za določene in zakonite namene ter se ne smejo nadalje obdelovati z nameni, ki so v neskladju z namenom zbiranja. Zakon določa tudi, da mora upravljavec osebnih podatkov zagotoviti, da je v vsakem trenutku možno ugotoviti komu so bili osebni podatki posredovani, kateri osebni podatki, kdaj in za kakšen namen.
V zakonu so upoštevana tudi priporočila glede posredovanja podatkov v države izven Evropske unije. Tako 63. člen določa, da je posredovanje osebnih podatkov v tretjo državo dopustno pod pogojem, da državni nadzorni organ izda odločbo, da država v katero se podatki iznašajo, zagotavlja ustrezno raven varstva osebnih podatkov.

Nenaročeno oglaševanje je v slovenski zakonodaji prepovedano z Zakonom o elektronskih komunikacijah, ki navaja, da je uporaba sistemov za opravljanje klicev na naročnikovo telefonsko številko brez človekovega posredovanja, faksimilnih naprav in elektronske pošte za namene neposrednega trženja dovoljeno samo v primeru, da naročnik predhodno soglaša s tem, oziroma če sam posreduje elektronski naslov. V tem primeru mora imeti možnost, da kadarkoli brezplačno zavrne takšno uporabo njegovega elektronskega naslova.
Decembra 2005 je bil sprejet še zakon o informacijskem pooblaščencu, ki v skladu z direktivo Evropske unije 95/46 ES skrbi za nadzor nad varstvom osebnih podatkov - Data Controler.

3.3 Varovanje podatkov in zasebnosti v Združenih državah Amerike

»*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*[24].«
(četrti amandma ameriške ustave)

V ameriški ustavi zasebnost sicer ni neposredno omenjena, vendar se prvi in četrti amandma posredno nanašata na zasebnost. Omenjena je svoboda veroizpovedi, govora,

[24] »Pravica ljudi, da so varni v njihovi osebnosti, hiši, listinah, in učinkuje tudi proti neutemeljenimi preiskavami in zaplembami, naj ne bo kršena, in nobeno opravičilo naj ne bo dano za to, toda le na osnovi verjetnega razloga, podprtega s prisego ali zagotovilom in podrobnim opisom prostora preiskave in ujetih oseb ali zaplenjenih stvari«

pisanja in zborovanja ter pravica biti varen pred nadlegovanjem, preiskovanjem brez vzroka…

Svoj prvi Zakon o zaščiti zasebnosti »Privacy Act« in Zakon o prostem dostopu do informacij »The Freedom of Information Act« so Združene države Amerike dobile že leta 1974.

»Privacy Act« se nanaša samo na zvezno vlado in njene agencije, medtem ko se zasebni sektor še zmeraj upira sprejetju takšne zakonske regulative (Raab, 2004, str.8).

Zakon temelji na načelih »poštene informacijske prakse« in zahteva od državnih organov, da zagotovijo varnost, zaupnost, integriteto ter omejeno rabo osebnih podatkov. Posamezniku omogoča videti ter kopirati datoteke, ki jih poseduje zvezna vlada v zvezi z njim, odkriti kdo drug še ima dostop do teh informacij ter zahtevati spremembo informacij, ki niso natančne ali relevantne.

Od zveznih agencij se zahteva, da v desetih dneh podajo zahtevano informacijo, seznanjati morajo javnost o vrstah zbirk, ki jih vodijo preko zveznega registra, kako uporabljajo informacije, zagotoviti morajo, da so informacije v zbirkah relevantne. Ne smejo uporabljati informacije za druge namene, kot pa so bile zbrane.

V nekaterih primerih so lahko zvezne zbirke podatkov o posameznikih dostopne tudi drugim:

- če je namen uporabe podoben kot je bil prvotni namen zbiranja informacij
- za statistične raziskave
- za zakonsko določene namene
- če je tako odločilo sodišče
- če je to nujno z medicinskega stališča

»The Freedom of Information Act«: zagotavlja državljanom dostop do vladnih zbirk, razen če razkritje vsebuje: podatke pravdanja, osebne zadeve, poslovne skrivnosti, podatke CIA, zakonsko določene aktivnosti, kršitev zasebnosti posameznika….

Agencija ima 20 dni časa, da se odloči glede zahtevanega dostopa.(URL: http://www.privacyrights.org/fs/fs11-pub.htm)

ECPA (Electronic Communication Privacy Act) Zakon o zaščiti zasebnosti elektronskih komunikacij je bil sprejet leta 1986 in prinaša ukrepe glede dostopa, uporabe, razkritja, prestrezanja in zaščito zasebnosti elektronskih komunikacij. ECPA prepoveduje nezakonit dostop in razkritje vsebine komunikacije. Zakon zahteva sodno odrejena nadzorovanja elektronskih komunikacij, oziroma pristanek vsaj enega od udeležencev komunikacije. Vendar zakon ni bil dopolnjen s prestrezanjem podatkov preko interneta, kar je omogočalo delovanjem vladnim preiskovalcem, kot je bilo na primer delovanje sistema Carnivore (Gindin, 1997).

Leta 1987 so sprejeli še **Zakon o računalniški varnosti (Computer Security Act)**, ki zahteva od državnih agencij, da označijo vse državne računalniške sisteme, ki vsebujejo občutljive osebne podatke ter načrtujejo varnost oziroma zaščito teh sistemov.

Pred enajstim septembrom 2001 je v Združenih državah veljala stroga zakonodaja, ki je ščitila širjenje informacij med različnimi agencijami. Prevladovalo je mnenje, da takšno širjenje informacij krši človekove pravice in državne agencije so se tega morale držati.
Po enajstem septembru 2001 pa je Amerika sprejela paket proti terorističnih zakonov in aktov. Predvsem «**US Patriot Act**« (2001) in »**Homeland Security Act**« (2002) povečujeta moč elektronskemu nadzoru in prestrezanju podatkov. Z zakonoma je ogrožena »online« zasebnost nedolžnih, kajti dopuščata sledenje in zapisovanje IP naslovov ter vpogled preiskovalcev v finančne in druge transakcije vseh državljanov. Takšen nadzor zmanjšuje zasebnost posameznikov na račun državne varnosti.

3.3.1 «Safe Harbor« principi

Ameriška zakonodaja glede zasebnosti (»Privacy act«) in zaščite osebnih podatkov velja samo za državne ustanove, medtem ko za podjetja zakonodaja (tako kot v evropskih in še nekaterih drugih državah) ni obvezujoča; podjetja se večinoma sprejemu takšne regulative upirajo.
Namen «Safe Harbor« principov je bil predvsem zadostiti zahtevam Evropske unije po primernem standardu zaščite podatkov glede prenosa podatkov iz držav evropske unije zahtevanih v direktivi 95/46/ES. Sprejem principov je bil nujen zaradi nemotenega pretoka podatkov med podjetji na obeh straneh Atlantika.

Principi naj bi zagotovili visoko stopnjo zaščite, ki jo zahteva evropska direktiva, pristop podjetij k njihovemu sprejemu pa je prostovoljen. Nanašajo se na:

Obveščanje: Organizacije morajo informirati posameznike o namenu za katerega zbirajo osebne podatke. Na razumljiv način morajo podati pojasnilo, kako lahko kontaktiramo z organizacijo, ki zbira podatke.

Izbiro: Organizacije morajo dati posamezniku na voljo možnost izbire ali bo, oziroma ne bo dovolil posredovanje osebnih podatkov tretji osebi ter uporabo podatkov za drug namen kot so bili le ti zbrani.

Nadaljni promet: za razkritje podatkov tretji osebi morajo organizacije upoštevati prva dva principa (obveščanje in izbira). Če posredujejo podatke naprej, jih lahko le tistim, ki zagotavljajo najmanj tako stopnjo zaščite kot jo zahtevajo ti principi.

Varnost: Organizacije, ki posredujejo osebne podatke, morajo z njimi ravnati odgovorno, zaščititi jih morajo pred izgubo, zlorabo, nedovoljenim dostopom, razkritjem, predelavo in uničenjem.

Neokrnjenost podatkov: Osebni podatki morajo biti relevantni za namen uporabe; biti morajo točni, popolni in ne smejo biti zastareli.

Dostop: Posameznik, na katerega se podatki nanašajo, mora imeti pravico dostopa do teh podatkov; omogočeno mu mora biti popravljanje, izboljšanje ali brisanje podatkov, razen v primeru, ko bi dostop povzročil ogroženost posameznika.
Uveljavljavitev: Učinkovita zaščita zasebnosti mora vsebovati mehanizme za zagotovitev skladnosti s temi principi (International Safe Harbor Privacy Principles).

Pomankljivost principov je predvsem v tem, da ni zahteve glede prekomernosti zbirk, dolžine shranjevanja, anonimnosti. Ni možnosti pritožbe neodvisnemu organu; nadaljni prenos temelji na strinjanju tretje stranke glede zaščite podatkov. (Hübner,2001 str.17)
Velika ovira uveljavljanju principov je tudi domovinski oziroma »Patriot Act«, ki v mnogih primerih razvrednoti »Safe Harbor« principe izbire, neokrnjenosti podatkov ter nadaljnega prometa. (Dhont Jan at al., 2004, str. 105, 106).

3.4 Varovanje zasebnosti v Kanadi

Prva zakonodaja Kanade na področju zasebnosti na zvezni ravni je bila vsebovana v listini o človekovih pravicah iz leta 1977 »Canadian Human Rights Act«. Na podlagi te listine so sprejeli še dva zvezna zakona o zasebnosti:
Zakon o zasebnosti (»The Privacy Act«) in Zakon o zaščiti osebnih podatkov in elektronskih dokumentih (»Personal Information Protection and Electronic Documents Act«).
»**Privacy Act**« je stopil v veljavo že leta 1983. Akt zavezuje predvsem zvezne agencije in vladne službe k spoštovanju pravice do zasebnosti z omejevanjem zbiranja osebnih podatkov, njihove uporabe ter razkritja. Posamezniku daje pravico do dostopa ter popravkov osebnih podatkov oziroma informacij o njem samem, ki jih posedujejo zvezne vladne organizacije.
Posameznik je zaščiten tudi s »**Personal Information Protection and Electronic Documents Act**« (PIPEDA), ki vsebuje niz pravil, kako lahko organizacije zasebnega sektorja zbirajo, uporabljajo ter razkrivajo osebne podatke v komercialne namene. Zakon daje posamezniku pravico dostopa do podatkov ter pravico zahtevati popravke osebnih podatkov, ki jih te organizacije zbirajo.
PIPEDA se je prvotno nanašal samo na osebne podatke o potrošnikih ali zaposlenih, ki so bili zbrani, uporabljeni ali razkriti v komercialnih aktivnostih javnega sektorja (banke, letališča, telekomunikacijske organizacije…). Danes PIPEDA vključuje tudi trgovino, tisk, storitveno dejavnost ter druge nedržavne organizacije. Ne nanaša pa se na osebne podatke o zaposlenih v teh organizacijah.

Tako kot po drugih državah, ki so sprejele zakonodajo s področja zasebnosti, je tudi v kanadski zakonodaji mogoče najti devet osnovnih principov »Fair Information Practices«, ki se nanašajo na podatke shranjene tako v papirnati kot digitalni obliki:

- pravica posameznika do dostopa do njegovih lastnih podatkov
- pravica posameznika zahtevati uničenje vseh ali del njegovih osebnih podatkov
- pravica zahtevati omejitev kroženja in širjenja informacij znotraj državnih in zasebnih organizacij
- pravica pritožiti se, če zahteva ni upoštevana ali pa je upoštevana le delno
- pravica popraviti podatke (ali zahtevati zaznamek napake, če zakonodaja ne dopušča popravljanja podatkov)
- pravica izbrisati osebne informacije, če so napačne
- pravica časovno omejiti shranjevanje podatkov (norma je 7 let)
- pravica dati dovoljenje za širjenje osebnih podatkov, če tega ni v zakonu
- pravica, da so podatki uničeni po 7 letih, razen če ni posebnega z zakonom določenega razloga za shranjevanje podatkov
- pravica pritožiti se neodvisnemu organu, če zgoraj našteti principi niso upoštevani.

Poleg teh principov vsebuje zakon še principe kot so: odgovornost, natančno določen namen, privolitev posameznika, omejitev zbiranja, omejitev uporabe, razkritja in retencije, točnost, varnost, odprtost in dostopnost (URL:http://laws.justice.gc.ca/en/P-8.6/index.html).

Po 11. septembru 2001 se je zaradi javne varnosti in boja proti terorizmu tudi v Kanadi, tako kot v večini drugih držav spremenil odnos države do zasebnosti.
V letu 2004 so bili dodani trije amandmaji: zasebnemu sektorju je dovoljeno zbirati podatke brez pristanka ali vednosti posameznikov, če to zahteva zakon. Državni preiskovalci lahko od organizacij zahtevajo podatke o posameznikih, če je to v povezavi z nacionalno varnostjo. Drugi amandma določa, da posameznik ni obveščen, če je takšna zahteva sprožena. Tretji amandma pa dopušča organizacijam zbirati nove osebne podatke po lastni izbiri, če sumijo, da bi bile informacije lahko pomembne za nacionalno varnost. Podatki so lahko razkriti varnostnim agencijam ali posebnemu industrijskemu preiskovalnemu organu (Riley, 2004, str.11-19).

3.5 Zakonska ureditev varovanja zasebnosti v Avstraliji

Za razliko od drugih držav Avstralija nima posebnega krovnega zakona oziroma listine, kot je recimo Listina o človekovih pravicah, iz katere bi lahko razvili zakonodajo o zaščiti zasebnosti z vidika človekovih pravic. Kot navaja Webbova, se ravno to pomanjkanje zakonske pravice do zasebnosti odraža tudi v zaščiti osebnih podatkov (Webb, 2003, str. 4).

Avstralija je dobila svoj zakon »**Privacy Act**« šele leta 1988, to je v času, ko so druge države sprejemale že svojo tretjo ali četrto generacijo aktov o zasebnosti (Webb, 2003 str. 7). Zakon se nanaša predvsem na področje državne uprave.
Zaradi vpliva oziroma zahtev Direktive 95/46/EC glede prenosa osebnih podatkov v tretje dežele ter pritiska informacijske industrije, ki je spoznala, da je zaščita zasebnosti vitalnega pomena za zaupanje potrošnikov novim tehnologijam, je Avstralija leta 2000 sprejela še »**Privacy Amendment (Private Sector) Act**«, ki pokriva tudi področje zasebnega sektorja. Zakon je stopil v veljavo decembra 2001.

»Privacy Act« pokriva aktivnosti državnih agencij. Zakon definira osebne podatke, občutljive osebne podatke, prav tako pa opredeljuje informacijsko zasebnost. Vsebuje enajst principov informacijske zasebnosti, ki bazirajo na osnovi smernic OECD in pokrivajo aktivnosti državnih agencij. Poleg principov o informacijski zasebnosti pa zakon vsebuje tudi deset nacionalnih principov glede varovanja zasebnosti.
Kot navaja Webbova je odločilen problem teh principov, da so usmerjeni na zapise (records) in ne na informacije.
»Privacy Amandment (Private Sector) Act« je nastal pod močnim vplivom ekonomskih interesov države za področje zasebnega (poslovnega) sektorja. Zakon dopušča možnost izbire podjetij med »Nacionalnimi principi zasebnosti« ali pa razvojem lastnega kodeksa.
Kot ugotavlja Clarke je zakon usmerjen predvsem na državo in podjetja in ne na posameznika (Webb, 2003, str. 8). Zelo nejasen je tudi glede zbiranja podatkov o zaposlenih glede njihovega zdravstvenega stanja, podrobnosti o delavčevih stikih, osebnemu dohodku, storilnosti in podobno.

Polega zakona o zaščiti zasebnosti ima Avstralija tudi Zakon o prostem dostopu do informacij: **The Freedom of Information Act (FOI Act).** Zakon je iz leta 1982 in uveljavlja pravico dostopa do uradnih dokumentov zvezne vlade, ki vsebujejo osebne podatke. Pravica do popravkov se nanaša samo na državljane Avstralije ter stalne naseljence.

Kot navaja Webbova, nastajajo razlike v občutenju zasebnosti in zaščite podatkov prebivalcev Avstralije v primerjavi z ostalimi narodi predvsem zaradi razlik v kulturnem, zgodovinskem in političnem dogajanju. Zaradi relativno mirne zgodovine, državljani Avstralije ne posvečajo toliko pozornosti zaščiti podatkov z vidika človekovih pravic, kot recimo prebivalci ostalih držav (Webb, 2003, str. 14).

4 GROŽNJE ZASEBNOSTI

Sprva je internet ponujal neomejeno priložnost svobode govora, izražanje mnenj, idej, danes pa vse bolj predstavlja neomejeno priložnost tako nadzora raznih velikih marketinških organizacij nad potrošniki kot tudi države nad državljani.

Uporabljati internet pomeni puščati digitalne sledi. Povprečen uporabnik se ponavadi niti ne zaveda kakšne sledi vse pušča za sabo, da se vse to nekje zbira, shranjuje, da ga lahko nekdo ves čas opazuje. S sestavljanjem majhnih delčkov informacij je mogoče zgraditi profil uporabnika interneta ter ga dejansko tudi identificirati v realnem svetu – brez kontrole ali so podatki pravilni ali ne lahko ostajajo ti zapisi dosegljivi še mnogo let. Danes se vse več inštitucij (tako vladnih kot velikih marketinških ustanov) ukvarja prav z zbiranjem teh informacij in izdelovanjem profilov uporabnikov interneta. Poizvedovanje po internetu se lahko zaključi s kupom neželene elektronske pošte (spamov) na posameznikov poštni predal .

Poleg čisto ekonomskih interesov poseganja v zasebnost (neželena pošta, piškotki, profiliranje uporabnikov), predstavlja posebno grožnjo zasebnosti tudi nadzor države nad internetnim prometom, ki se je po 11. septembru 2001 le še okrepil. Bombardiranje WTC je spremenilo ravnotežje v debati o zasebnosti za ali proti. Prevladala je zahteva po javni varnosti in zahteva, da vladne agencije prestrezajo elektronske komunikacije (Hinde, 2002, str. 18). Končni učinek »zahteve po javni varnosti« je vse bolj naraščajoče »vohljanje« vseh vrst: od monitoringa elektronske pošte, pa vse do retencije prometnih in komunikacijskih podatkov. Država želi imeti popoln nadzor nad državljani, hkrati pa postajajo vladne službe vse bolj skrivnostne glede njihovih aktivnostih, omejujejo informacije, ki so bile prej dostopne (Poročilo Silenced: an international report on censorship and control of the internet, 2003, str. 10).
Vse večjo grožnjo zasebnosti predstavlja tudi razvoj novih tehnologij: video nadzor, genetske podatkovne baze (biometrija), radio frekvenčna identifikacija (RFID), osebne kartice (identity card).

Razvoj informacijskih komunikacij je s tehničnega vidika zelo poenostavil dostop do podatkov, njihovega zbiranja, združevanja in obdelovanja. Povečale so se možnosti nadzora ter druge grožnje zasebnosti posameznikov.
Kot sta zapisala Kovačič in Vehovar je ogroženost zasebnosti pričela naraščati predvsem v 70.-tih letih, z razvojem informacijskih in komunikacjskih tehnologij. Po poročilu Privacy & Human Rights 1999 zasebnost danes ogrožajo trije pomembni trendi:

globalizacija: odstranjuje geografske omejitve pri pretoku podatkov (razvoj interneta)

konvergenca med tehnologijami: odstranjuje tehnološke bariere med sistemi. Moderni informacijski sistemi so vse bolj interoperabilni z drugimi sistemi; izmenjujejo in obdelujejo lahko podatke različnih oblik.

multimedialnost omogoča zlivanje in pretvorbo informacij v različne oblike (Kovačič, Vehovar, 2000, Poročilo Privacy and Human Rights 1999).

Najbolj na udaru danes je prav informacijska zasebnost in zasebnost komunikacij, zato bom v nadaljevanju naloge predstavila nekaj najbolj pogostih kršitev teh dveh dimenzij zasebnosti.

4.1 Vdori

Do vdorov v računalniške sisteme pride praviloma zaradi malomarnosti pri vzpostavitvi sistema ter slabe varnostne zaščite. Leta 1995 sta računalniška programerja Venema in Farmer objavila program SATAN (Security Administrator's Tool for Analyzing Networks) za iskanje varnostnih lukenj v računalniških sistemih. Program je bil po zagotovilih avtorjev namenjen odkrivanju in ne zlorabi varnostnih lukenj – za izboljšanje varnosti sistema. Tri leta kasneje je »hackerska« skupina »Cult of Dead Cow« izdelala trojanskega konja[25] z imenom Back Orifice.
Back Orifice je sistem za oddaljeno upravljanje z računalnikom oz. sistem, ki na žrtvinem računalniku odpre t.i. stranska vrata skozi katera je mogoče upravljati z računalnikom preko interneta, ne da bi žrtev to opazila (Kovačič, 2003 str. 56, 57).

Najbolj boleče posledice nedovoljenega dostopa do podatkov so predvsem takrat, ko so tarče sistemi, ki posedujejo občutljive osebne podatke skupine ljudi. Primer takega vdora se je zgodil leta 2000, ko je napadalec vstopil v sistem bolnišnice v Seattlu ter ukradel podatke preko 5000 pacientov (Rezgui, Bouguettaya, Eltoweissy, 2003, str. 43).

Danes je na internetu brezplačno dostopnih čedalje več orodij za nadzorovanje in vdiranje v računalniške sisteme, ki od uporabnika ne zahtevajo skoraj nobenega znanja. (Kovačič, 2003 str. 56, 57).
Študija, ki so jo pred nekaj leti opravili s skupino študentov kot napadalcev (COTS) (U. Lindquist, E. Jonsson, 1998, str. 60 –66), je dala naslednje rezultate:

- internet proizvaja ogromne količine informacij o tem kako uspešno izvesti vdor
- veliko napadalcev izvede vdor s pomočjo literature dobljene na internetu
- večina napadalcev je uspešno opravila vdor
- pri mnogih vdorih so dobili napadalci celo pravice administratorja

(Nancy R. Mead, 2004, str. 28).

[25] program, namenjen odpiranju stranskih vrat na računalniku, kraji gesel ter povzročanju druge škode; za razliko od virusov pa se ne more samodejno širiti ter okuževati drugih datotek. Primere trojanskih konjev so vsebovali celo programi, ki so jih uporabniki instalirali kot antivirusne programe, v resnici pa so vsebovali virus, ki je ukradel osebne podatke z uporabnikovega računalnika ter ga poslal nazaj k napadalcu (Rezgui, Bouguettaya, Eltoweissy, 2003, str.42).

4.2 Prestrezanje podatkov in informacij

Prestrezanje podatkov je pogosto uporabljena tehnika za spremljanje prometa. ki pa jo je težje odkriti kot vdor. Prisluškovalec namreč samo spremlja promet, tu ne gre za aktivni vdor. Prestrezanje poteka predvsem s spremljanjem prometa na usmerjevalnikih (routerjih), oziroma podatkovnih povezavah.
Tehnika je podobna telefonskemu prisluškovanju. Pri tem napadalec prestreza paketke, ki se prenašajo po internetu. Tehniko pogosto uporabljajo »hekerji« za prestrezanje gesel (pasword sniffing) (Kovačič, 2003, str. 52, 53).

4.2.1 Prestrezanje elektronske pošte

Elektronska pošta se po internetu prenaša večinoma nešifrirano, kot navaden tekst. Za napadalca ponavadi ne predstavlja prav težkega problema, saj je v nešifriranem sporočilu povsem enostavno iskanje določenih besed. Poleg tega imajo do elektronske pošte prost dostop upravitelji poštnih strežnikov (relay server), preko katerih se elektronska pošta prenaša.
Sporočilo mora biti s posredniškega, prav tako pa tudi s končnega poštnega strežnika, zbrisano takoj, ko je bilo posredovano naprej. Ohrani se lahko le nekaj tehničnih oziroma prometnih podatkov, ki se na poštnem strežniku samodejno zabeležijo in so potrebni za prenos sporočila ter zaračunavanje: velikost sporočila, elektronski naslov pošiljatelja in prejemnika, datum in čas pošiljanja…
S posebno programsko opremo je možno zbirati in shranjevati tudi ostale podatke o elektronski pošiljki: število prilog, temo, vsebino… to pa že lahko ogroža zasebnost uporabnikov.
Kot ugotavlja Kovačič, je problem elektronske pošte predvsem v tem, da je tehnično videti kot razglednica, uporabniki pa jo uporabljajo kot zaprto pisemsko pošiljko. Kot zaprto pisemsko pošiljko jo obravnava tudi zakonodaja (Kovačič, 2003, str. 55).

4.2.1.1 Nadzor elektronske pošte na delovnem mestu:

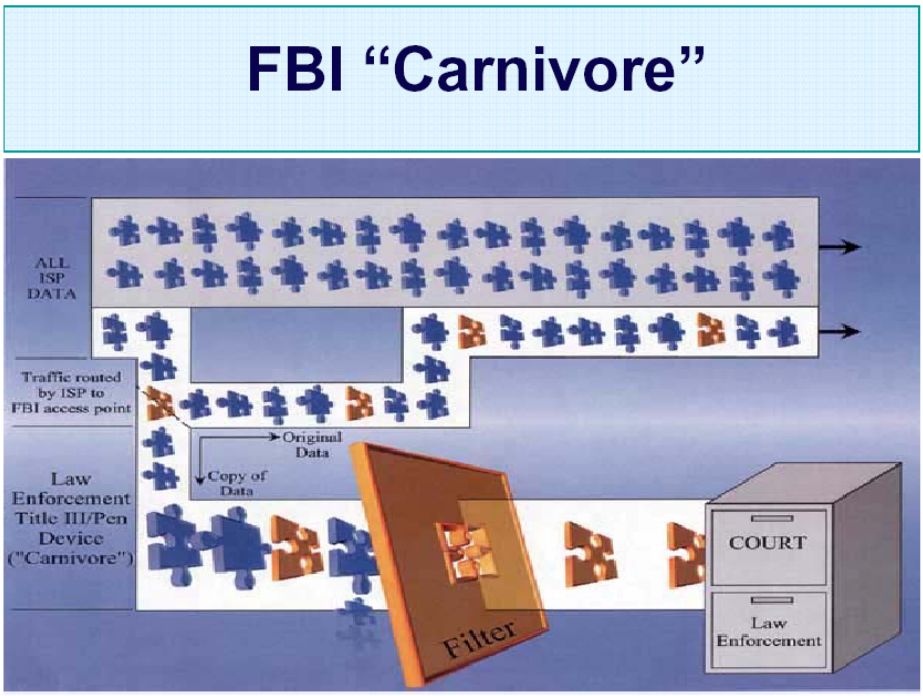
Uporaba elektronske pošte na delovnem mestu je postala nezamenljiva: velikokrat nadomešča uporabo telefona, uporabo klasične pošte, ali zgolj hojo po stopnicah. Enostavno natipkamo sporočilo ter ga odpošljemo, pri tem se nam zdi, da je sporočilo osebno, da ga bo videl le naslovnik. Pozabljamo, da temu ni tako.
Marsikateri delodajalec kontrolira elektronska sporočila. Razlogi za to so različni, večinoma zaradi nevarnosti izdajanja poslovnih skrivnosti. Zaposleni sicer čutijo ta nadzor kot invazijo na njihovo zasebnost, vendar ameriška sodna praksa v tem pogledu pritrjuje delodajalcem, češ da gre za službeno pošto in ne zasebno. V Sloveniji takšen nadzor ni

dovoljen oziroma mora biti uslužbenec predhodno seznanjen z možnostjo nadzora in se mora z njim strinjati (Kovačič, 2003, str. 55).
Elektronsko pošto je možno prečitati z različnih lokacij: z mreže, z lokalnega diska in backup trakov tudi še potem, ko je sporočilo že bilo zbrisano (Gindin, 1997).

4.2.2 Carnivore

Pri FBI so zgradili sistem za nadzor elektronskih komunikacij, ki so ga poimenovali Carnivore. Sistem je od leta 1999 pa do razkritja julija 2000 deloval v tajnosti. Namenjen je bil nadzoru elektronskih komunikacij s sodnim nalogom.
Sistem je bil nameščen na računalnik pri ponudniku internetnih storitev in je kontroliral ves promet z elektronsko pošto ter z izjemno hitrostjo prestrezal pošto s sumljivo vsebino, prav tako tudi pogovore v internetnih klepetalnicah ter zbiral datoteke, ki so jih osumljenci pobrali z interneta. Kritiki FBI očitajo, da je izkoriščal sistem za nadzor vse elektronske pošte, medtem ko zagovorniki menijo, da država potrebuje takšno orodje za zajezitev kriminala.
V preteklosti je bilo enostavno prisluškovati posamezni telefonski liniji, v obdobju elektronskih komunikacij, pa je postalo nemogoče izluščiti osumljeno elektronsko pošto, brez monitoringa vse elektronske pošte določenega ponudnika. (Horniak, 2004, str. 56, 57, Baas, prosojnica 8).
Carnivore ni več aktiven sistem, vendar kot je zapisal Declan McCullagh: »*Carnivore gone - but it's not dead*« (ZDNet News, 31. januar 2005).

Slika 1 - Arhitektura sistema Carnivore



vir: Escudero-Pascual, 2001, str. 9

4.2.3 Echelon

Prav tako kot Carnivore je bil tudi Echelon tajni sistem, ki ga je uporabljala NSA (National Security Agency) s partnerji držav na angleško govorečem področju (Kanada, Velika Britanija, Avstralija in Nova Zelandija). Gre za globalni satelitski sistem za prestrezanje zasebnih in poslovnih komunikacij in iskanje informacij, ki se nanašajo na mednarodni terorizem, promet z mamili in širjenje kopičenja uničujočega orožja. Sistem je bil razkrit leta 1998.

Razlika med Echelonom ter drugimi podobnimi sistemi je v tem, da Echelon za prestrezanje komunikacij ne potrebuje sodnega naloga. Sistem je sporen tudi zaradi načina zbiranja informacij. Poleg informacij o kriminalcih, zbira namreč še informacije o prijateljskih državah, njihovi politiki, gospodarstvu, ekonomiji…(Baase v Horniak, 2004, str. 58)

slika 2 - Morwenstow, prva postaja zgrajena za prestrezanje komercialnih satelitskih komunikacij kot del ECHELON sistema

vir: Duncan Campbell, 27.5.2001.

Poročilo evropskega parlamenta iz leta 2001 je potrdilo obstoj Echelona in priporočilo uporabnikom interneta šifriranje pomembnih elektronskih sporočil ter zavarovanje vseh komunikacijskih kanalov z uporabo visoke stopnje šifriranja. Poročilo ugotavlja, da je bil Echelon vzpostavljen za prestrezanje zasebnih in komercialnih satelitskih komunikacij in ne le vojaških, kot so sprva domnevali (Hinde, 2002, str. 17).

4.3 Zbiranje in povezovanje podatkov

Na internetu se danes zbira velikansko število osebnih podakov, večinoma brez vednosti oz. privolitve posameznika. Vse te nepovezane podatke je s sodobno tehnologijo mogoče povezovati, predelati ter tako ustvariti nove baze podatkov, ki jih uporabljajo v druge namene, kot so bili prvotno zbrani. Prav tehnologija je tisto, kar predstavlja veliko ogroženost zasebnosti na internetu.

Zmeraj več je primerov, ko podjetja ob stečaju prodajo osebne podatke svojih klientov. Leta 2002 je na primer spletna stran DrKoop.com prodala medicinske podatke svojih naročnikov drugi spletni strani vitacost.com (Rezgui, Bouguettaya, Eltoweissy, 2003, str. 42).
Nekatere spletne strani prodajajo podatke o svojih uporabnikih kljub obljubi, da tega ne bodo storile. Spletni iskalnik AskJeeves je od spletne strani ETour.com odkupil bazo z osebnimi podatki 2,2 milijona piscev novic, kljub obljubi, ki jo je dal ETour svojim uporabnikom, da osebni podatki v nobenem primeru, nikoli ne bodo posredovani naprej »tretji strani«. Baza je obsegala podatke o uporabnikovem imenu, elektronskem naslovu, starosti, spolu[26] (Hinde, 2002, str. 424).

Kot navaja Kovačič je še posebn privlačno zbiranje ter povezovanje javno dostopnih in prostovoljno posredovanih podatkov (telefonski imeniki, elektronski imeniki, elektronski načrti mest, Who is Who,…). Posebni programi (roboti, pajki, črvi) iščejo po spletnih straneh, elektronskih imenikih, forumih, novičarskih skupinah, arhivih… elektronske naslove, telefonske številke, slike in podobno, ki jih nato povezujejo z ostalimi pridobljenimi podatki.

Še lažji ter učinkovitejši način zbiranja podatkov, ki ga uporabljajo mnoge spletne strani, je pridobivanje podatkov neposredno od uporabnikov. V zameno za manjše ugodnosti, za nagradno igro, žrebanje… je marsikdo pripravljen posredovati svoje podatke. Pri tem pa ni razvidno v kakšne namene se bodo ti podatki uporabljali (Kovačič, 2003, str. 51, 52).
Neosveščenost uporabnikov interneta in podcenjeno tveganje v veliki meri še povečuje stopnjo ogroženosti. Za bolj lagodno življenje smo namreč pripravljeni razkriti marsikateri podatek, ki je lahko kasneje zlorabljen in predstavlja poseg v našo zasebnost.

[26] AskJeeves so branili nakup s tem, da US Federal Trade Commission (FTC) dovoljuje transfer podatkov o potrošnikih znotraj panoge, če so podatki uporabljeni za prvotno določen namen. Spor so rešili tako, da so o spremembi lastništva obvestili vse, na katere se podatki nanašajo ter jim dali možnost, da se izbrišejo iz baze (opt in, opt out).

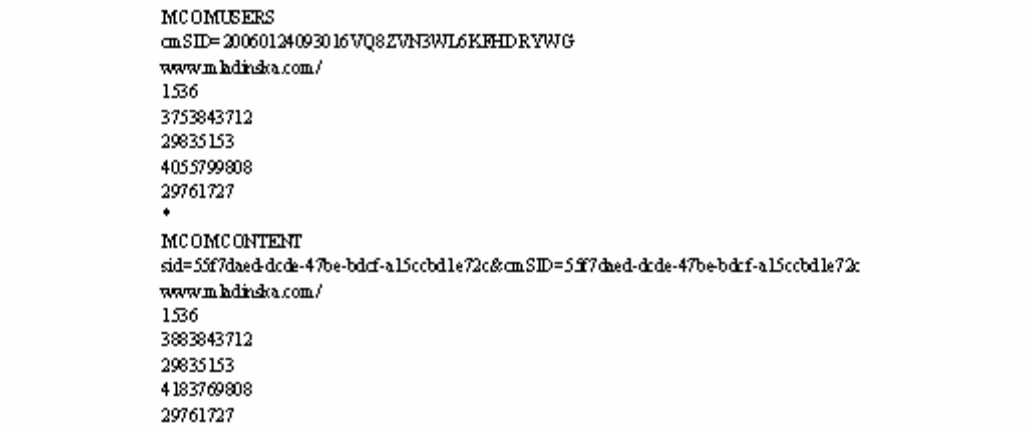
4.4 Elektronske sledi

»On – line« aktivnosti, ki bi zagotavljala absolutno zasebnost ni in tega bi se morali uporabniki internetnih storitev zavedati. Če »surfamo« z domačega naslanjača, se nam zdi, da smo sami, nevidni, da smo anonimni. Na žalost temu ni tako. Obstaja možnost sledenja vseh »on-line« aktivnosti. Ugotoviti je mogoče, katere spletne strani smo obiskali, katere datoteke smo pobrali z interneta, do katerih novičkarskih grup smo dostopali. Te informacije lahko zbirajo tako ponudniki internetnih storitev preko katerega dostopamo do interneta, kot tudi lastniki spletnih strani. Če dostopamo do interneta na delovnem mestu, se moramo zavedati, da tudi delodajalci pogosto izvajajo nadzor nad tem, katere strani obiskujemo (Privacy in Cyberspace: Rules of the Road for the Information Superhighway). Večina spletnih strani zabeleži vsak obisk: zapiše se IP naslov in naslov spletne strani, ki jo ima uporabnik nastavljeno kot trenutno, prav tako se zabeleži datum obiska. IP naslov računalnika omogoča povezovanje z drugimi sledmi, ki vsebujejo isti IP naslov. Na ta način spletni ponudniki ugotavljajo obnašanje oziroma spletne navade uporabnikov, v mnogih primerih pa lahko preko IP naslova celo enolično identificirajo aktualnega uporabnika (Rezgui, Bouguettaya, Eltoweissy, 2003, str.43).

4.5 Piškotki

Internetni piškotki (ang. cookies)[27] so majhne tekstovne datoteke, ki jih spletni strežnik pošlje spletnemu brskalniku, ta pa jih nato shrani na trdi disk uporabnikovega računalnika. Ko ponovno obiščemo spletno stran, brskalnik vrne strežniku zapisan piškotek.

Slika 3: Primer piškotka



Vir: Microsoft Internet Explorer

[27] Internetni piškotek (ang. cookie) je za podjetje Netscape leta 1994 razvil Lou Mountulli za bolj avtomatizirano interakcijo med strežnikom in uporabnikom.

V piškotku je lahko zapisana identifikacijska številka uporabnika, uporabniško ime, geslo za dostop do internetne strani, podatki o kreditnih karticah ter drugi osebni podatki, ki jih pustimo na spletni strani.

Kljub temu, da piškotki predstavljajo zelo koristno orodje na področju interaktivnih poslovnih spletnih aplikacij (elektronska trgovina, oglaševanje, bančništvo), lahko predstavljajo tudi veliko grožnjo zasebnosti uporabnika teh storitev:

Pomanjkanje varnosti (security failuers): V piškotih so pogosto shranjeni tudi občutljivi osebni podatki, ki se nezavarovani prenšajo preko spleta. Vsebina je teoretično zelo lahko dosegljiva vsakomur, ki piškotek prestreže. Prav bi bilo, da bi bila vsebina piškotka zakodirana, vendar ponavadi uporabnik na to nima vpliva.

Opazovanje (monitoring): Piškotki predstavljajo mehanizem, ki dovoljuje spletni strani zapisovanje naših internetnih aktivnosti, ponavadi brez naše vednosti ali dovoljenja. Preko identifikacijske številke lahko spletni strežnik ugotovi kaj je uporabnik počel na spletni strani, lahko pa sledi uporabniku tudi na ostale spletne strežnike.

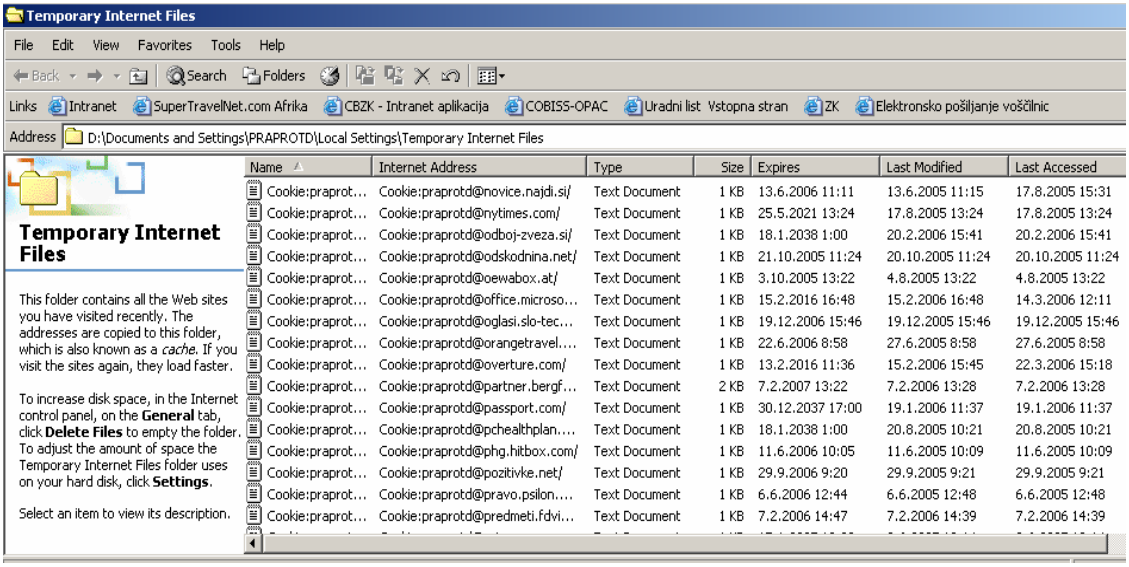
Za mnogo ljudi predstavlja takšno beleženje aktivnosti napad na njihovo zasebnost.

Razkritje podatkov (data disclosure): Komercialne spletne strani, ki si pridobivajo osebne podatke preko piškotkov, lahko te podatke izmenjujejo z drugimi spletnimi stranmi. To pomeni, da uporabnik, ki spletni strani zaupa, pusti svoje osebne podatke, le ta pa jih lahko posreduje tretji spletni strani, na kateri mogoče uporabnik sploh ni bil, niti jim ne bi zaupal svojih osebnih podatkov.

Omejen nadzor (limited control): Končni uporabnik ima žal zelo malo možnosti nadzora nad vsebino in uporabo piškotkov; za povprečnega uporabnika je to povsem nevidna tehnologija. Spletni brskalniki sicer omogočajo funkcijo izklopa piškotkov, vendar postanejo tako nekatere spletne strani neuporabne. Če pa se uporabnik odloči, da piškotek sprejme, se zgodi, da nima nadzora nad njegovo vsebino in uporabo.

Zbiranje podatkov (data collecting): Eden izmed načinov uporabe piškotkov je tudi zbiranje podatkov s pomočjo spletnega hrošča (web bug). Spletni hrošč je nevidni grafični element (velikosti enega pixla), ki omogoča ugotoviti po katerih straneh se uporabnik giblje. Na ta način je možno ugotoviti brskalne navade posameznika. Ti podatki se lahko tudi povežejo z elektronskim naslovom posameznika, pa tudi z njegovo fizično identiteto. Fizično identiteto uporabnika je mogoče ugotoviti tako, da uporabnik zaupa svoje osebne podatke neki spletni strani v omrežju, podatki pa se potem povežejo z identifikacijsko številko piškotka (Seničar, Jerman-Blažič, Klobučar, str. 4, 5, Kovačič, 2003, str. 48).

Slika 4- Primer zapisa piškotkov na disk uporabnikovega računalnika



Vir: Microsoft Internet Explorer

Tehnologijo piškotkov zakonodaja sicer dopušča, saj se lahko uporablja v povsem legitimne namene (analiziranje učinkovitosti spletnega oglaševanja, ugotavljanje istovetnosti uporabnikov storitev, olajša lahko zagotovitev nekaterih storitev informacijske družbe), vendar pod pogojem, da je uporabnik seznanjen z namenom zbiranja teh podatkov. Uporabnik mora imeti možnost izbire ali bo sodeloval ali ne (opt in oziroma opt out možnost) (Možina , 2002, str. III).

4.6 Iskalniki

Določene informacije o posameznikih, ki jih je bilo včasih težko odkriti, še težje pa povezovati, so danes preko internetnih iskalnikov lažje dostopne (Tavani, 2000, str.13).
Vsa sporočila, ki jih pošiljamo na razna javno dostopna mesta (forumi, novičarske skupine..), so dostopna vsakomur in še leta dolgo lahko ostanejo shranjena. Z iskalniki kot so na primer google, najdi.si, yahoo… bodo še naši zanamci lahko prebirali naša elektronska sporočila. Google na primer ima preko 8 bilijonov zapisanih informacij o internetnih straneh za kasnejšo uporabo, ki jih ne briše.
Kot poroča Wall Street Journal (marec 2005) so internetni »heckerji« ugotovili, da je z uporabo iskalnikov in s pomočjo tehnike poznane kot »google hacking« mogoče hitro, učinkovito in poceni pridobiti občutljive osebne podatke. Eksperti s področja varnosti so v marcu 2005 v Seatlu prikazali, kako lahko samo z uporabo iskalnika Google v manj kot eni uri pridobijo občutljive osebne podatke primerne za finančno sleparstvo za 25 milijonov ljudi. Zmagovalnemu teamu tega prikaza je uspelo odkriti celo bazo z zapisanimi »social security number« za 70 milijonov umrlih ljudi (Delaney, 2005).

Veliko skrb za zasebnost predstavljajo iskalniki ravno zaradi svoje kapacitete pridobivanja podatkov ter ohranitve vsakega sporočila poslanega v omrežje (Gindin, 1997).
Kritiki iskalnikom (predvsem Googlu) očitajo shranjevanje podatkov. Kadarkoli uporabnik vpiše iskalni niz v Google, ga ta shrani skupaj z enolično identifikacijsko številko, IP številko računalnika ter drugimi podatki pridobljenimi s pomočjo piškotkov. Ti zapisi so prava vaba za preiskovalne organe, še posebej po letu 2001 (Brandt v Ocvirk, 2003, str. 55).

4.7 Profiliranje

E-profiliranje je zapisovanje in klasificiranje obanašanja uporabnikov interneta.
Proces izgradnje podatkovne baze o aktivnostih in značilnostih uporabnikov interneta poteka preko zbiranja informacij, s sledenjem (monitoringom) s pomočjo uporabe piškotkov. Tako se pridobi vzorec obnašanja uporabnika, njegovo zanimanje in nakupovalne navade. Vse to se lahko shrani kot profil uporabnika v podatkovno bazo.
Ti podatki so večinoma neosebni, lahko pa se povežejo s podatki, ki jih prostovoljno puščamo na internetnih straneh (ime, spol, starost, izobrazba…), elektronsko pošto, IP naslovom, demografijo - tako povezani podatki lahko predstavljajo že zelo oseben profil uporabnika.
Profiliranje se uporablja predvsem za oblikovanje ponudbe in storitev spletnih strani, za osebno oglaševanje. Organizacije, ki se ukvarjajo s profiliranjem trdijo, da je to le v dobro e-uporabnika, saj mu lahko ponudijo bolj osebno prilagojene storitve.
Kljub temu pa mnogi vidijo e-profiliranje kot vdor v njihovo zasebnost, saj se zbirajo in posredujejo osebni podatki brez njihovega pristanka in v večini primerov tudi brez njihove vednosti (Seničar, Jerman-Blažič, Klobučar, 2003, str. 5-6).

Tehnologija danes omogoča organizacijam zbiranje informacij izpeljanih iz neštetih podatkovnih baz, ki jih povezujejo med sabo ter tako gradijo izčrpne profile posameznikov, ki jih nato klasificirajo v različne grupe. Eden takšnih primerov v ZDA je Claritas, ki ima posameznike grupirane v 15 grup glede na lokacijo bivališča - od visoko elitnih četrti do najbolj ubožnih mestnih predelov. Te podatke Claritas prodaja za nizko ceno 65 dolarjev za tisoč imen (Privacy and Consumer Profiling, EPIC).

Noben vidik zasebnega življenja ni preobčutljiv, da ne bi bil kategoriziran, primerjan in prodan drugim. Tako je recimo z medicinskimi informacijami, ki se prav tako zbirajo in kategorizirajo brez soglasja in brez možnosti izstopiti iz sistema.

Velikokrat res nimamo možnosti izbire, dostikrat pa povsem prostovoljno vstopamo v ta sistem. Takšen primer so različne kartice zaupanja, kjer za majhne ugodnosti prostovoljno posredujemo osebne podatke in kot navaja Kovačič iz sistema niti ne želimo izstopiti, saj nam na videz prinaša majhne popuste ali ugodnosti (Kovačič, 2003, str. 33).

4.8 Neželena elektronska pošta

Vsak dan na milijone ljudi dobiva nenaročeno komercialno elektronsko pošto (UCE)[28] popularno imenovano »spam« ali tudi »e-slama« po slovensko. Oglaševanje z nenaročeno elektronsko pošto je izredno poceni in se podjetjem splača že, če se odzove le peščica potrošnikov. Nekaterim se zdi ta način oglaševanja nemoteč, medtem ko drugi občutijo to kot nadlegovanje, ki jim povzroča velike preglavice, celo takšne, da so prisiljeni zamenjati poštni naslov.

Neželena elektronska pošta je neligitimna in nepoštena komunikacija, ki poteka v eno smer (B. in E. Whithworth, 2004, str. 40). Največja težava je, da je dejansko nemogoče odkriti pošiljatelja sporočila.

»On line« sistemi dajejo vsakomur možnost komurkoli poslati sporočilo. To pa je v nsprotju z definicijo zasebnosti po Brandeisu »pravica biti sam«. Ta pravica »ne komunicirati« vključuje pravico biti nenadlegovan, biti v tišini.

Neželena in nenaročena elektronska pošta – »spam« poleg problema zasebnosti predstavlja tudi velik ekonomski problem. Po poročilu Ferris Research (B. in E. Whithworth, 2004, str. 38) je neželena elektronska pošta stala ameriška podjetja v letu 2003 10 bilijonov dolarjev v izgubljeni produktivnosti. Po neželenem vmešavanju na omrežju neželena elektronska pošta že prekaša viruse. Kot navaja poročilo (Protecting Privacy and Fighting Spam, 2004) neželena elektronska pošta ni nepomemben pojav, kajti samo v decembru 2003 je bilo v državah EU več kot polovica prometa elektronske pošte neželene. To pa že predstavlja masovno invazijo na zasebnost, prevaro potrošnikov, nenadzorovano gibanje škodljive vsebine, velike stroške za podjetja, zmanjšano produktivnost in zaviranje rasti informacijske družbe v celoti.

B. in E. Withworth se v članku »Spam and the Social-Technical Gap« sprašujeta, kdo je lastnik naslovov elektronske pošte. Le te je mogoče izluščiti iz vsake »on line« transakcije ter jih vkomponirati v marketinške podatkovne baze. Nakup knjige preko spleta lahko na primer povzroči celo poplavo nenaročenih ponudb preko elektronske pošte. Dati nekomu pravico do informacije, še ne pomeni, dati mu vse pravice (B. in E. Whithworth, 2004, str.43).

Seigneur in Jensen v članku Privacy Recovery with disposable email addresses ugotavljata, da so najbolj občutljive tiste informacije, ki jih lahko direktno povežemo s posameznikom. Elektronski poštni naslov spada v to kategorijo: enostavno in učinkovito lahko pridemo v kontakt z naslovnikom. Ko si tretja stranka pridobi naslov brez privolitve, pomeni to kršitev zasebnosti naslova. Cena takšne kršitve zasebnosti je različna med posamezniki, celotna cena pa je zelo visoka (Seigneur in Jensen, 2003 str. 35, 36).

Kot navaja poročilo Oecd Task Force on Spam: Anti spam law enforcement »spamerji« danes pošljejo že preko bilion neželene elektronske pošte po vsem svetu, ne glede na to, ali bodo imeli od tega kakšen dobiček ali ne (neželeno elektronsko pošto pošiljajo ne glede na jezik, ne glede na razumevanje sporočila). Neželeno elektronsko pošto dobivajo članice

[28] unosolicited commercial e-mails

OECD pretežno tujega izvora (Task Force on Spam: Anti spam law enforcement, 2005, str. 6, 7)

»Spamerji« oziroma pošiljatelji neželene elektronske pošte zlahka zakrijejo svojo identiteto in lokacijo z lažnimi informacijami v glavi sporočila in s pošiljanjem sporočil preko odprtih proxi strežnikov [29] z izkoriščanjem tako imenovanih »zombie drone[30]« ali uporabo nesledljive internetne povezave. Ker je neželena elektronska pošta pretežno tujega izvora, agencije, ki se borijo proti njej, skoraj nimajo moči, tudi če jih odkrijejo.

Raziskava, ki jo je v zadnjem četrtletju 2005 opravilo podjetje Sophos je razkrila, da so največji proizvajalci e-slame Združene države Amerike s kar 24,5% deležem, sledijo ji Kitajska z 22,3% deležem, Južna Koreja z 9,7 %, Francija s 5%, Kanada z 3%, Brazilija 2,6%, Španija 2,5%, Avstrija 2,4%... poročilo prav tako navaja, da je pošta poslana večinoma preko t.i.«zombijev« in da narašča delež pošte v neangleškem jeziku (RIS, 30.1.2006, vir: Sophos, 23.1.2006).

Neželena elektronska pošta je mednarodni problem in edino skupna mednarodna »prekomejna« politika lahko razvije legalno orodje potrebno za uspešen boj proti njihovim pošiljateljem. Samo mednarodno koordinirana akcija je lahko uspešna v boju zoper neželeno elektronsko pošto.

4.9 Rudarjenje

Tradicionalno rudarjenje (ang. data mining) pomeni pridobivanje podatkov preko podatkovnih zbirk podjetij z namenom odkriti vzorce potrošniškega obnašanja. V novejšem času govorimo predvsem o spletnem rudarjenju, ki se pojavlja v dveh oblikah: rudarjenje glede na uporabnike spleta ter rudarjenje glede na spletno vsebino.
Rudarjenje pomeni niz avtomatiziranih postopkov (tehnik), ki se uporabljajo za izluščitev še nepoznanih delčkov informacij iz velikih podatkovnih baz (Cavoukian, 1998, str. 4, 5). Iz teh podatkov se odkrivajo novi vzorci in odnosi, ki se uporabljajo pri poslovnem odločanju. Rudarjenje je tako usmerjeno na avtomatizirano odkrivanje novih dejstev in relacij med podatki. Pri tem se uporablja umetna inteligenca ter inteligentne tehnike kot so živčna omrežja, matematični algoritmi, odločitvena drevesa, sklepanje…
Rudarjenje poteka v treh korakih:

- priprava podatkov, selekcioniranje, čiščenje.
- priprava podatkov z uporabo algoritmov za rudarjenje, stiskanje in transformacija podatkov za lažjo prepoznavanje pomembnih informacij.
- analiza podatkov, kjer so vrednoteni rezultati rudarjenja

[29] Proxy, vmesni strežnik, (zastopnik), ki deluje kot strežnik pri odjemalcu ter odjemalec k strežniku
[30] Računalnik, ki je »ugrabljen« s trojanskim konjem

Kot navaja Cavoukianova bo postalo rudarjenje verjetno eno največjih orodij za kapitalizacijo že obstoječih virov v poslovnem svetu, kajti informacija postaja širše dostopna, cena programske opreme pa se znižuje (Cavoukian, 1998, str.7).
Z vse večjo uporabnostjo, predstavlja rudarjenje z vidika zasebnosti tudi vse večjo nevarnost, predvsem zaradi dejavnikov kot so:

Kvaliteta podatkov: Z rastjo interneta se je tudi za rudarjenje povečala količina podatkov iz različnih virov. Več podatkovnih baz je vključenih, večje je tveganje, da so podatki zastareli ali nenatančni, težje je njihovo čiščenje; kljub temu, da se podatki prečistijo, so le ti lahko netočni, nepopolni ali zastareli. Nenatančni, zastareli ali napačni podatki lahko povzročijo tudi nenatančno ali napačno interpretacijo.

Možnost dostopa: Potrošnik nima možnosti dostopa do teh podatkov, ne more jih pregledati, popraviti ali izbrisati.

Namen uporabe: Rudarjenje predstavlja drugo rabo (ne za namen za katerega so bili podatki zbrani); nemogoče je na začetku procesa identificirati namen uporabe ter omejiti rezultate na enkratno rabo.

Odprtost in transparentnost: Rudarjenje prav gotovo ni odprta in transparentna aktivnost.

Enaka načela kot veljajo za aktivnosti zbiranja podatkov na internetu, morajo veljati tudi za zbiranje podatkov s pomočjo tehnik rudarjenja (Nissenbaum v Tavani, 1999, str.10).
Dolžnost podjetij je, da informirajo uporabnike o rudarjenju, in ne uporabnikov, da sami ugotavljajo katera »online« podjetja uporabljajo prakso rudarjenja. Uporabnikom je potrebno jasno povedati, da so informacije o njih uporabljene tudi za rudarjenje, morali bi imeti vpogled v to, kako se te informacije sestavljajo in za kaj se uporabljajo. To obveščanje bi moralo biti odprto in pošteno. Postavljena morajo biti jasno definirana pravila o načinu rudarjenja, parametrih, času trajanja, uporabi… in potrošnik mora biti z njimi seznanjen. Večina uporabnikov se verjetno ne bi odločila za rudarjenje (opt out). (Tavani, 1999, str. 20)
Kot navaja Cranorjeva je uporabnikom neprijetno ob dejstvu, da lahko računalnik predvidi njihove navade in interese. Zaskrbljeni so ob dejstvu, da lahko nekdo odkrije in prikaže napačne zaključke in rezultate. Spet drugi uporabniki pa v tem vidijo ugodnosti (direktno oglaševanje, finančne ugodnosti, popusti …) in se s takšnim načinom pridobivanja informacij strinjajo (opt in). Pomembno pri vsem tem je, da se uporabniku pove, kako se bodo podatki o njih uporabili in da se uporabnik sam odloči ali bo sodeloval ali ne (Cranor, 2003a, str.2).

V zadnjih letih uporaba rudarjenja bliskovito narašča. Uporabljajo ga različne inštitucije kot na primer banke, zavarovalnice, medicinske ustanove, industrija, trgovina, Uporabljajo ga predvsem za zmanjšanje stroškov, izboljšanje raziskav, povečanje prodaje…

Rudarjenje lahko predstavlja grožnjo zasebnosti, hkrati pa se ta tehnologija lahko uporabi tudi za identifikacijo možnih kršitev zasebnosti (Blarkom et al., 2003, str. 198).
V kontekstu državne varnosti se rudarjenje pogosto uporablja za identifikacijo aktivnosti teroristov, kot na primer transakcije denarja, komunikacije, sledenje teroristom glede na potovanje, migracije… (CRS Report: Data mining an overview, 2004, str.4).

5 ZAŠČITA ZASEBNOSTI

Razvoj informacijskih in komunikacijskih tehnologij omogoča lažje zbiranje in shranjevanje ogromnih količin podatkov, lažja je dostopnost do podatkov, olajšano je združevanje podatkovnih baz in njihovo distribuiranje – olajšan je tudi nadzor ter poseganje v našo zasebnost.
Razvoj tehnologij sicer že danes omogoča tudi zaščito zasebnosti, vendar bo v bodoče potrebno še več napora usmeriti v učinkovito varovanje zasebnosti. Kot navaja Hübnerjeva, predstavlja razvoj tehnologij za zaščito zasebnosti velik korak naprej, vendar to še ni zadosten pogoj za celovito zaščito posameznikove zasebnosti. Poleg ustrezne tehnologije je potrebno zagotoviti zaščito zasebnosti tudi:

- preko zakonske zaščite zasebnosti in podatkov, ki jo promovira vlada,
- s samozaščito upoštevajoč pošteno informacijsko prakso,
- z izobraževanjem uporabnikov in IT strokovnjakov

(Fischer- Hübner, 2001, str. 3).

Pri oblikovanju tehnologij za zaščito zasebnosti se je potrebno zavedati, da ima zasebnost interdisciplinaren pomen. Če želimo implementirati tehnologijo sprejeto tako s strani državljanov, kot tudi države in poslovnega okolja, je potrebno upoštevati zakonski, politični ter socialni vidik zasebnosti. Le tako bo tehnologija množično sprejeta. (Diaz, Preneel 2005, str.1-2).

5.1 Tehnologije za izboljšanje zasebnosti (Privacy Enhancing Technologies – PETs)

Razvoj informacijsko komunikacijskih tehnologij omogoča zmeraj več možnosti zbiranja, shranjevanja, obdelovanja in distribucijo osebnih podatkov. Temu primerno naraščajo tudi kršitve oziroma zlorabe pri poslovanju z osebnimi podatki. Pokazala se je potreba po tehnologiji, ki bi omogočala zaščito identitete uporabnika z zagotovitvijo anonimnosti, psevdonimnosti, neopazovanosti , zaščito identitete lastnika podatkov ter zaupnost in integriteto osebnih podatkov (Fischer- Hübner, 2001, str. 18).

Raziskava Palo Alto raziskovalnega centra XEROX v začetku devetdesetih je pokazala, da posameznik verjame v zaščito zasebnosti, če ima nadzor nad tem, kateri osebni podatki se zbirajo, kdo ima dostop do teh podatkov, pomembno je tudi, da dobijo povratno informacijo o tem, kdaj in katera informacija je bila pridobljena ter komu je dostopna (CEN/ISSS, 2004, str.19).

Osnovne funkcije, ki jih morajo pokrivati tehnologije za zaščito zasebnosti na internetu so:

- zaščititi pred neavtoriziranim dostopom do komunikacij ter shranjenih datotek
- avtomatsko vzpostaviti informacije o zbiratelju podatkov, politiki o zasebnosti in avtomatskem kreiranju odločitve uporabnika na osnovi teh primerov
- avtomatsko objavljati politike o zasebnosti zbiratelja podatkov
- filtrirati neželena sporočila
- preprečevati avtomatsko zbiranje podatkov s pomočjo kolačkov, spletnih hroščev, spyware programov…
- zaščititi komunikacije pred povezavo s točno določeno osebo
- podpora transakcijam, da razkrijejo minimalno osebnih podatkov

(Cranor, 2003b, str. 80).

Neposreden vpliv na razvoj tehnologij za zaščito zasebnosti je imela evropska direktiva 95/46/ES, ki v 17. členu od upravljavcev osebnih podatkov zahteva implementacijo takšnih varnostnih tehnik, ki bodo zaščitile osebne podatke pred uničenjem, izgubo, zlorabo, nedovoljenim dostopom. Uporaba teh tehnologij naj bi omogočila tako varnost podatkov kot tudi zasebnost uporabnikov. Prav tako direktiva v 6. in 7. členu zahteva, da so podatki zbrani za točno določen in zakonit namen ter ne smejo biti nadalje obdelovani za druge namene, ki niso v skladu s prvotnim. To pa je tudi osnovni motiv tehnologij za zboljšanje zasebnosti: oblikovati informacijske in komunikacijske sisteme in tehnologije tako, da bodo minimizirale zbiranje in uporabo osebnih podatkov ter preprečile njihovo nezakonito obdelovanje, ne da bi se ob tem zmanjšala funkcionalnost informacijskega sistema (CEN/ISSS, 2004, str.11).

Kot je zapisal Goldberg je namen tehnologij za izboljšanje zasebnosti povrniti zasebnost uporabnikom interneta ter izboljšati družbo skozi zaščito zasebnosti tam, kjer je bilo to prej nemogoče (Goldberg, Wagner, Brewew, 1997, str. 2).

Tehnologije za izboljšanje zasebnosti - PETs (Privacy Enhancing Technologies) ponujajo pomoč pri doseganju osnovnih norm pri zakoniti obdelavi osebnih podatkov (Borking, Raab, 2001, str.14). Eden najpomembnejših principov varovanja zasebnosti je, da se ne zbira in obdeluje nič več osebnih podatkov, kot pa je res **nujno potrebno za natančno določen namen** (Blarkom, Borking, Verhaar, 2003, str. 34).

Blarkom definira tehnologije za izboljšanje zasebnosti kot:

»Tehnologije za izboljšanje zasebnosti (PET) so sistem IKT (informacijsko komunikacijskih tehnologij) za zaščito informacijske zasebnosti z eliminiranjem ali minimiziranjem nepotrebne ali neželene obdelave osebnih podatkov, ne da bi se s tem izgubila oziroma zmanjšala funkcionalnost informacijskega sistema.«
(Blarkom, Borking, Verhaar, 2003, str. 33)

Na delovnem srečanju OECD za informacijsko varnost in zasebnost (Working party: Privacy on line, 2003, str.12) so zapisali, da so to tehnološka orodja, katerega primarni namen je pomoč pri implementaciji principov zasebnosti, kakršni so na primer principi OECD sprejeti leta 1981.

Cranorjeva meni, da tehnologije za izboljšanje zasebnosti same kot take ne morejo zaščititi podatkov pred zlorabo. Njihova moč je predvsem v sposobnosti prevzeti pobudo nad skrbjo za zasebnost in so odlično dopolnilo zakonski regulativi in samozaščiti uporabnikov. Njihova pomanjkljivost pa je predvsem v okornosti večine od teh orodij. Uporabnost teh tehnologij bi se bistveno povečala z izboljšavo in poenostavitvijo uporabniškega vmesnika ter vgradnjo v ostala orodja. Tehnologija mora biti zasnovana tako, da uporabniku ne bi bilo potrebno storiti ničesar, da bi si že s klikom na gumb zagotovil ustrezno zaščito zasebnosti (Cranor, 2003b, str.80-83).

5.1.1 Osnovni principi delovanja PET

Fischer Hübnerjeva navaja štiri osnovne principe delovanja tehnologij za izboljšanje zasebnosti:

Anonimnost zagotavlja uporabniku uporabo podatkov ali storitev, ne da bi moral razkriti svojo identiteto. Anonimnost zagotavlja zaščito uporabnikove identitete (ISO15408).

Ločimo anonimnost pošiljatelja: uporabnik je anonimen v vlogi pošiljatelja sporočila in anonimnost prejemnika: uporabnik je anonimen v vlogi prejemnika sporočila

Psevdonimnost zagotavlja uporabniku uporabo podatkov ali storitev, ne da bi moral razkriti svojo identiteto, vendar pa je še zmeraj odgovoren za to uporabo (ISO 15408). Psevdonim predstavlja identifikator subjekta, psevdonimnost pa je uporaba psevdonimov kot identifikatorjev. Biti psevdonimen predstavlja stanje uporabe psevdonima kot identifikatorja.

Nezdružljivost zagotavlja, da lahko uporabnik uporablja različne vire ali usluge ne da bi bilo mogoče te različne rabe med seboj združiti (ISO 15408).

Neopazovanost zagotavlja uporabniku, da lahko uporablja različne vire ali usluge, ne da bi ga nekdo tretji pri tem opazoval (ISO 15408) (Fischer- Hübner, 2001, str. 21 – 24, CEN/ISSS, 2004, str. 7-9).

5.1.1.1 Anonimnost

Anonimnost je pomembna oblika zaščite zasebnosti. Kot navaja Goldberg se anonimnost ne uporablja zgolj zaradi anonimnosti kot take, temveč kot orodje za dosego ciljev zaščite zasebnosti. Dolga leta so ljudje opravljali svoje aktivnosti »offline«, in pri tem bili anonimni, zato tudi sedaj v dobi interneta pričakujejo podobno oziroma večjo raven anonimnosti in s tem zasebnosti.
Goldberg je definiral anonimnost kot: »*Anonimnost je zasebnost identitete.«*
Razdelil jo je na

- stalno anonimnost (ali psevdonimnost), ki ni povezana z uporabnikovo fizično identiteto
- enkratno anonimnost, ki traja samo v času enkratne internetne uporabe

Koncept anonimnosti je v možnosti povezovanja: nekdo lahko pošlje sporočila, ki se lahko vsa med seboj povežejo, toda ne more se jih povezati s fizično identiteto pošiljatelja.
Pri uporabi enkratne anonimnosti za vsako sporočilo posebej, pa le ta ne moremo povezati med sabo, niti jih ne moremo povezati s fizično identiteto pošiljatelja (Goldberg, Wagner, Brewer, 1997, str. 4, 5).

Anonimnost pomeni biti neidentificiran znotraj niza subjektov (anonimni niz). To pomeni, da za anonimnost potrebujemo niz subjektov, ki nas pokriva. Večji je anonimni niz, večjo anonimnost nam zagotavlja. Anonimnost potrebuje sodelovanje množice ljudi – večja je, boljše je. V tem pogledu je anonimnost socialna kategorija (potreba sodelovanja družbe za skupno delovanje) (Diaz, Preneel 2005, str.3).

Veliko je priložnosti zakonite uporabe internetne anonimnosti, seveda pa ponujajo tehnike za dosego anonimnosti na internetu tudi ogromno možnosti zlorab, kot je na primer nedovoljeno kopiranje ali pošiljanje neželene elektronske pošte.

Znana je karikatura objavljena v New Yorker magazinu (5.7.1993):

Slika 5- Anonimnost na internetu: «Na internetu nihče ne ve, da si pes…«

vir: New Yorker magazin (5.7.1993)

5.2 Vrste tehnologij za izboljšanje zasebnosti

Tehnologije za izboljšanje zasebnosti - PET se lahko uporabljajo za zaščito ali zmanjšanje identifikacije ali za zaščito pred nezakonitim obdelovanjem osebnih podatkov. To ni ena vrsta tehnologije, temveč se lahko pojavlja v različnih oblikah in velikostih in v različnih fazah obdelave podatkov:

- Implementacija PET v fazi zbiranja podatkov (PET so v tej fazi lahko zelo učinkovite ter pozitivno vplivajo na ostale faze)
- V fazi obdelave in shranjevanja podatkov se kaže učinkovitost PET v zaščiti pred nezakonitim združevanjem podatkov. (Uporaba zaščitnika identitete – Identity Protector).
- V tretji fazi (distribucija podatkov) je učinkovita uporaba PKI, šifriranja, uporaba psevdo identitete ter ostalih arhitektur za zmanjšanje pretoka podatkov (CEN/ISSS, 2004, str. 18-19).

Goldberg razvršča PET v štiri večje skupine in sicer:

- **produkti za osebno rabo:** to so produkti, namenjeni posamezniku oziroma enemu uporabniku, neodvisno od zunanjih partnerjev oziroma drugih uporabnikov sistema. V to skupino prišteva »spam filtre«, upravljavce piškotkov ter podjetniške sisteme za upravljanje na področju zasebnosti.

- **centralni vmesnik:** te tehnologije tečejo centralno na serverju ter združujejo zahteve uporabnikov. Takšen primer je Anonymizer.
- **distribuiran vmesnik:** primer te vrste tehnologije je Remailer, Crowds, Freedom Network. Deluje na principu sodelovanja večih vmesnikov. So bolj zanesljivi kot posamični vmesniki, vendar je tudi cena delovanja mnogo višja.
- **zahtevana podpora:** ta kategorija vsebuje tehnologije, ki zahtevajo sodelovanje še nekih drugih strežnikov za dosego zasebne transakcije (tako imenovane tretje stranke). Primer uporabe je e-cash (Goldberg, 2002, str. 9).

Simone Fischer Hübner deli PET glede na osnovne principe delovanja na različnih ravneh:

1. PET za zaščito uporabnikove identitete z anonimnostjo, psevdonimnostjo, nezdružljivostjo ter nezmožnostjo opazovanja uporabnikov

- Zaščita na komunikacijski ravni
  (DC net, MIX nets MIX nets aplikacije: Anonymous Remailer, Onion Routing, Freedom network, Crowds)
- Zaščita na sistemski ravni
  (Anonimni dostop z avtorizacijo SPKI certifikat)
- Zaščita na aplikacijski ravni
  (Slepi digitalni podpis, Ecash, Anonimni plačilni protokoli)

2. PET za zaščito identitete uporabnika, ki so mu podatki posredovani, z uporabo anonimnosti ter psevdonimnosti podatkov

- Anonimizacija in psevdonimizacija osebnih podatkov
- Inferenčna (sklepna) kontrola statističnih baz podatkov

3. PET za zaščito osebnih podatkov ter uveljavitev zakonskih določil
(P3P, modeli za nadzor dostopa)

(Fischer- Hübner, 2001, str. 28 – 38).

Zaradi medsebojne prepletenosti tehnologij za povečanje zasebnosti, jih je težko enolično klasificirati. Različni avtorji jih, kot smo videli zgoraj, delijo po različnih kriterijih. V nadaljevanju naloge bom predstavila nekaj izmed poznanih mehanizmov in tehnologij, ki sem jih razdelila v tri sklope:

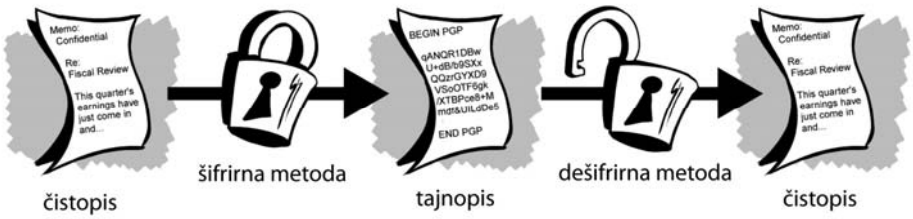
- mehanizmi za zaščito podatkov (kriptografija, steganografija,)
- zaščita zasebnosti z zagotovitvijo anonimnosti in psevdonimnosti (zaščitnik identitete, zaupni centri, anonimni strežnik, ponovni pošiljatelj, slepi podpis, Freenet, Crowds)
- zašita zasebnosti s privolitvijo (P3P, Upravitelj piškotkov)

5.2.1 Tehnologije za zaščito podatkov

5.2.1.1 Kriptografija (šifriranje)

»Kryptos logos« pomeni po grško skrita beseda. Kriptologija je veda, ki vključuje dva pojma: kriptografijo in kriptoanalizo. Kriptografija predstavlja pretvorbo podatkov v tajno – nečitljivo obliko s pomočjo kriptografskega algoritma. Nasprotni proces kriptografije oziroma šifriranju pa je kriptoanaliza, to je dešifriranje oziroma razkritje šifriranih podatkov, za kar pa je potrebno poznati kriptografski ključ (Kovačič, 2003, str. 64).
Kriptografija je ena izmed najbolj znanih in učinkovitih tehnik zaščite podatkov in zasebnosti. Zagotavlja zaupnost med udeleženci, ki želijo med sabo komunicirati.
Sporočilo, ki ga pošiljatelj želi poslati, s pomočjo šifrirne metode zakrije (zašifrira) ter nato pošlje šifriran tekst. Če tak šifriran tekst prestreže napadalec, mu ne pove nič, teksta ne more dešifrirati, lahko samo spremlja promet. Prejemnik prejme šifriran tekst ter ga s pomočjo dešifrirne metode dešifrira ter tako dobi sporočilo, ki mu ga je poslal pošiljatelj.

Slika 6- Šifriranje in dešifriranje

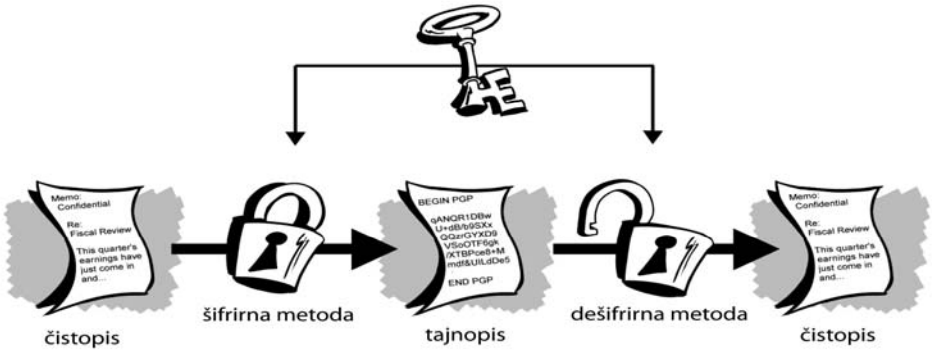


vir: An Introduction to Cryptography, str.11

Pri šifriranju in dešifriranju je pomemben postopek šifriranja imenovan tudi kriptografski algoritem ter šifrirni ključi, ki določajo delovanje algoritma.
V preteklosti je bil algoritem tajen, zato uporaba šifrirnih ključev ni bila potrebna. Za dešifriranje je bilo dovolj poznavanje algoritma. Modernejši algoritmi pa so večinoma javni, zato je nujna uporaba šifrinih ključev, ki pa morajo ostati tajni.
Postopek za šifriranje in dešifriranje ter množica vseh ključev sestavljajo skupaj z možnimi tajnopisi in podatki, ki jih lahko zaščitimo, kriptografski sistem (kriptosistem).
Glede na šifrirni in dešifrirni ključ ločimo simetrične in asimetrične kriptosisteme.
V simetričnih kriptosistemih uporabljamo za šifriranje in dešifriranje isti ključ, medtem ko sta pri asimetričnih sistemih ključa različna.
Problem uporabe simetrične kriptografije v javnih omrežjih je izmenjava ključa. Vsak prejemnik šifriranega sporočila mora pri sebi imeti ključ s katerim je bilo sporočilo zaščiteno, da lahko sporočilo dešifrira. Zato si morajo udeleženci v komunikaciji pred prvo vzpostavitvijo zveze ključe izmenjati, najbolje osebno, če želijo skrivnost ohraniti zase. V današnjem času pa je tak postopek skoraj nemogoč, zato se simetrični algoritmi

uporabljajo le v manjših zaključenih skupinah ali pa v kombinaciji z drugimi algoritmi, ki omogočajo varno izmenjavo ključev (Jerman-Blažič, 2002, str. 102, 103).

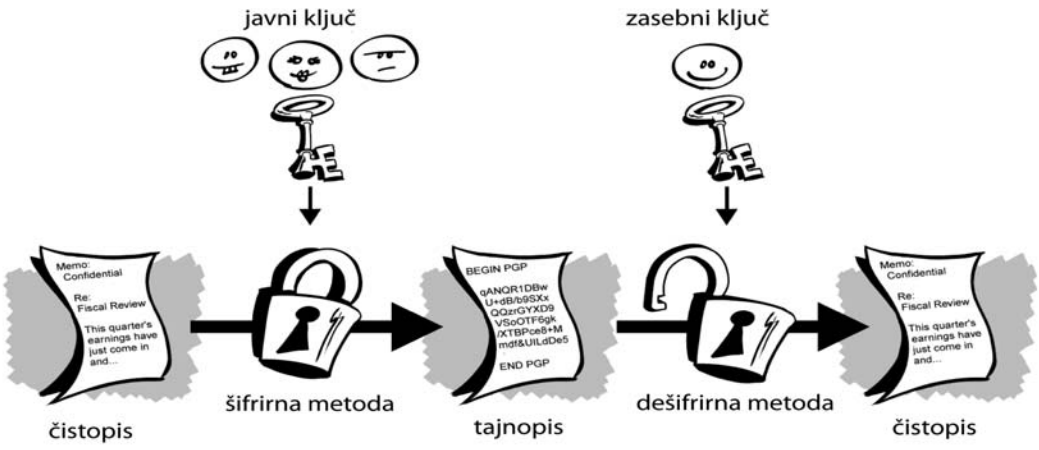
Slika 7- Simetrčna metoda šifriranja



vir: An Introduction to Cryptography, str.13

Eden pomembnejših mejnikov v razvoju kriptografskih algoritmov predstavlja leto 1976, ko je inženir Sun Microsystemsa Whitfield Diffie skupaj z Martinom Hellmanom z Stanfordske univerze razvil asimetrično šifrirno shemo imenovano tudi sistem javnih ključev (Horniak, 2004, str. 37).
Pri tem sistemu ključa za šifriranje in dešifriranje nista več enaka, pošiljatelj in prejemnik imata vsak svoj par ključev: javnega, ki je javno objavljen in zasebnega, ki ga obdržita v tajnosti. Prednost te metode je v tem, da ni več potrebnih »tajnih kanalov« za distribucijo ključev.

Slika 8 - Asimetrčna metoda šifriranja



vir: An Introduction to Cryptography, str.15

Kmalu po razvoju sistema javnih ključev so razvili kodirni algoritem imenovan RSA[31], ki je dolgo časa veljal skoraj za nezlomljivega[32]. Za pošiljanje šifriranega sporočila potrebuje pošiljatelj prejemnikov javni ključ in svoj zasebni ključ, prejemnik pa potrebuje pošiljateljev javni ključ in svoj zasebni ključ[33]. Ključa sta med seboj povezana v posebnem matematičnem razmerju, ki omogoča, da oseba, ki sporočilo pošilja le-to zašifrira s svojim tajnim in naslovnikovim javnim ključem. Tako šifrirano sporočilo pa lahko prebere samo naslovnik s svojim tajnim in pošiljateljevim javnim ključem (Kovačič, 2003, str.65).

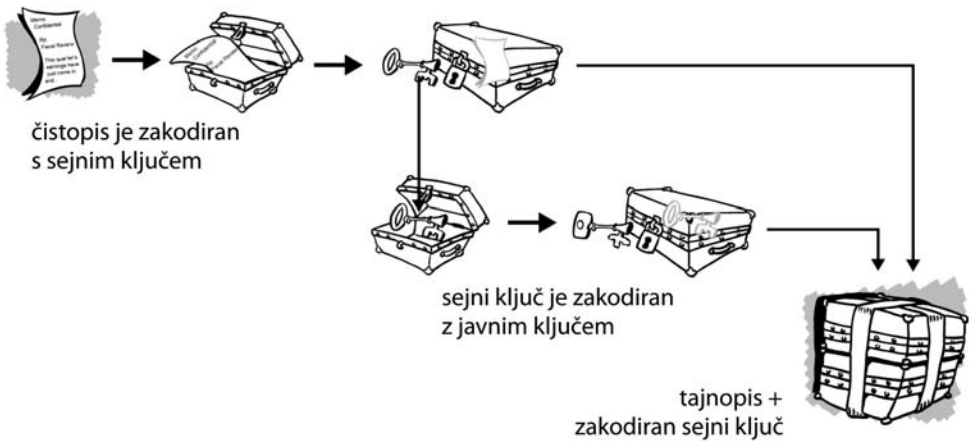
5.2.1.1.1 PGP (Prety Good Privacy)

PGP[34] je program za kodiranje vsebine datotek in elektronskih sporočil. Je hibridni kriptosistem, ki pri kodiranju uporablja kombinacijo simetričnega kodiranja ter kodiranje z javnim ključem. Bazira na obstoječih standardiziranih algoritmih kot so RSA, IDEA in MD5.
RSA algoritem je implementiran v kodiranje z javnim ključem, temelji na dejstvu, da je enostavno pomnožiti dve veliki praštevili, ter težko ti dve števili izluščiti iz produkta.

Primer delovanja programa PGP
Kadar uporabnik želi šifrirati sporočilo s pomočjo programa PGP, ga le ta najprej zgosti (s pomočjo MD5). Zgoščevanje oziroma stiskanje podatkov je pomembno predvsem za povečanje moči šifriranja, hkrati pa nam prihrani čas in prostor na disku.
PGP nato kreira enkratni tajni ključ, imenovan sejni ključ. To je naključno število, zgenerirano iz naključnega premika miške ter tipkanja preko tipkovnice. Sejni ključ nato z varnim in hitrim simetričnim šifrirnim algoritmom (IDEA) zakodira čistopis (plaintext) in nastane tajnopis (ciphertext).
Ko so podatki enkrat šifrirani, se sejni ključ zakodira s prejemnikovim javnim ključem in se skupaj s tajnopisom pošlje prejemniku.

[31] RSA je dobil ime po svojih ustvarjalcih: Ronald **R**ivest, Adi **S**hamir, Leonard **A**dleman
[32] Leta 1999 je eden izmed razvijalcev RSA- Shamir razbil 512 bitni RSA ključ.(Horniak, 2004, str.39)
[33] Javni ključi se nahajajo na javno dostopnih mestih, ena izmed možnosti so spletne strani
[34] program je leta 1991 razvil Phil Zimmerman in ga javno objavil. Zaradi tega je imel težave z FBI (v ZDA je prepovedan izvoz kriptografskih metod, ki se pojmujejo kot vojaška tehnologija). Leta 1996 so obtožbe proti njemu umaknili. Program so izvozili iz ZDA na ta način, da so programske stavke PGP natisnili v knjigi, programerji po svetu pa so jih nato pretipkali nazaj v elektronsko obliko.
V Sloveniji uporaba kriptografije ni prepovedana, tako kot v nekaterih drugih državah.

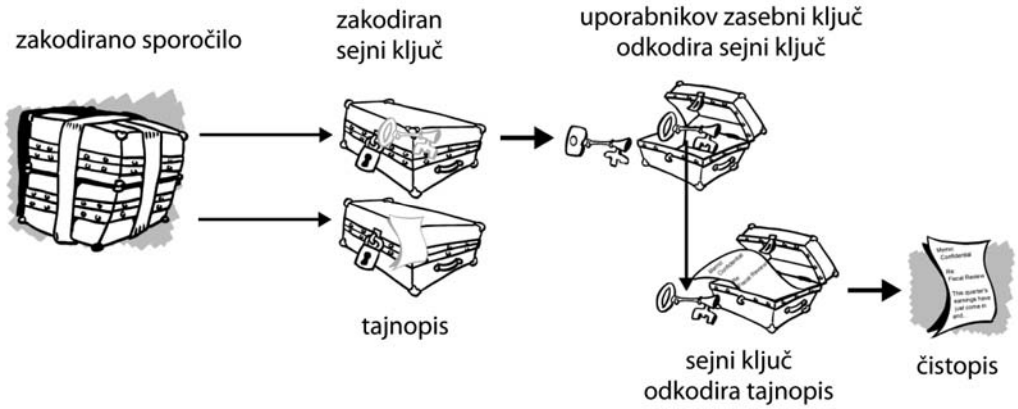
Slika 9 - Primer delovanja PGP – kodiranje



vir: An Introduction to Cryptography, str.16

Odkodiranje poteka v obratni smeri. Prejemnikova kopija programa PGP uporabi svoj zasebni ključ s katerim odkodira sejni ključ. S sejnim ključem pa nato odkodira simetrično zakodiran tajnopis.

Slika 10 - Primer delovanja PGP – odkodiranje



Vir: An Introduction to Cryptography, str.17

Metoda šifriranja s PGP izkorišča prednosti dveh šifrirnih metod: pripravnost asimetrične metode uporabe javnih ključev ter hitrost simetrične metode s katero je zakodiran čistopis. Simetrična metoda je približno 1000 krat hitrejša kot metoda z uporabo javnih ključev. Uporaba javnih klučev pa rešuje problem distribucije ključev (An Introduction to Cryptography, 1999, str. 16, 17).

5.2.1.2 Steganografija

Steganografija je prav tako kot kriptografija zelo stara veda, poznana že iz antične Grčije in pomeni »zakrito pisanje« Gre za sklop metod za skrivanje informacij v druge informacije. Sprva je bila steganografija le slab približek kriptografiji. Danes pa vse bolj pridobiva na popularnosti, predvsem zaradi možnosti skrivanja raznovrstnih informacij npr. zaščita avtorskih pravic, nevidno kodiranje, zapis serijskih številk…

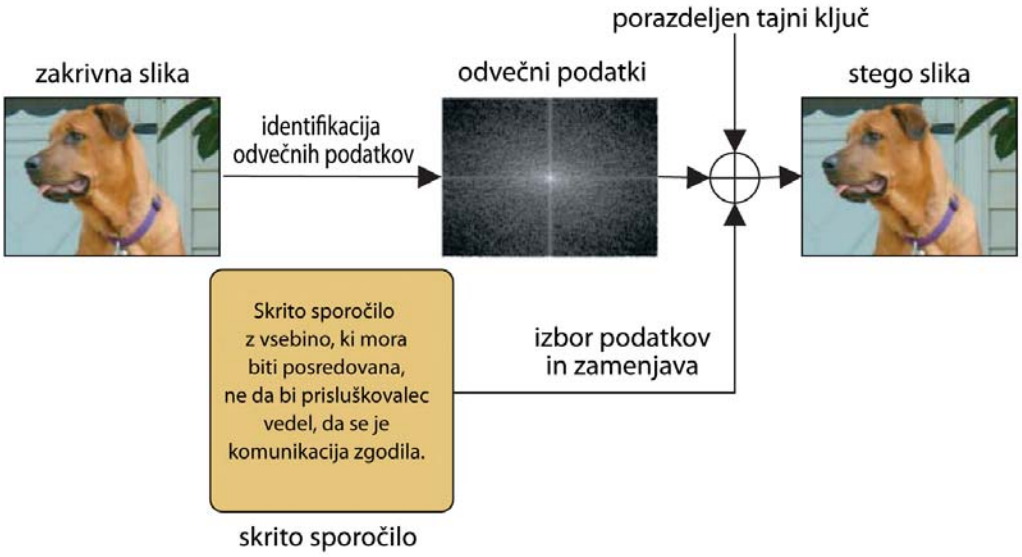
Definicija steganografije se glasi: *metoda oddajanja sporočila znotraj nekega drugega sporočila (nosilca) na tak način, da je obstoj skritega sporočila neprepoznaven .*
Primeri takšnih nosilcev skritih sporočil so slike, audio, video ali tekstovne datoteke…

Obstajata dve varianti steganografskih sistemov glede na namen uporabe:

- puščanje prstnih odtisov (fingerprinting) : skrivanje informacij v datoteke, kjer izkoriščajo prazen prostor v datotekah (skrivanje serijskih številk)
- digitalni vodni tisk: uporablja se za vstavljanje informacij o licenci, lastništvu, avtorskih pravicah…

Tajnost steganografskega procesa je odvisna od tajnosti steganografskega ključa.

Slika 11 - Primer uporabe steganografije



Vir: Provos, Honeyman, 2003, str. 33

Steganografske metode delujejo na principu izkoriščanja praznega prostora v datotekah ali na nosilcih digitalnih zapisov:

- skrivanje podatkov v slikovne datoteke s pomočjo navideznega povečanja števila barv;
- skrivanje podatkov v zvočne datoteke z za človeško uho neopaznim popačenjem digitalne oblike zvoka;

- skrivanje podatkov na neuporabljene sektorje disket in CDjev;
- skrivanje podatkov v HTML datoteke;
- skrivanje podatkov v ASCII datoteke (s pomočjo zamika kazalca za začetek datoteke);
- s pomočjo programa, ki binarno datoteko pretvori v nesmiseln tekst, ta pa je statistično podoben tekstu v poljubnem naravnem jeziku (imeti moramo slovar za ta jezik)

(Fischer- Hübner, 2001, str. 150–161, URL:
http://www.ljudmila.org/matej/privacy/kripto/stego.html)

Razvoj šifrirnih tehnik, ki zagotavljajo zasebnost izmenjanih sporočil, je prav gotovo najboljša obramba pred grožnjami informacijske družbe, vendar pa kriptografija ne more skriti informacije o naslovu. Mrežni operater ali domnevni napadalec lahko prebereta in zbirata uporabnikove interakcije, iz katerih se lahko izpelje uporabnikov profil. Če je kriptografija osnova digitalne zasebnosti, potem je anonimnost komunikacij njegova trdna podlaga – brez anonimnosti bi bila tudi kriptografija zelo šibka podlaga zasebnosti sporočil (Agrawal, Kesdogan, 2003, str. 27).

5.2.1.3 Zaščitnik identitete

Zaščitnik identitete (ang. Identity Protector) je del sistema tehnologij za zaščito zasebnosti, ki nadzoruje izmenjavo uporabnikove identitete znotraj informacijskega sistema.
Ponuja naslednje možnosti:

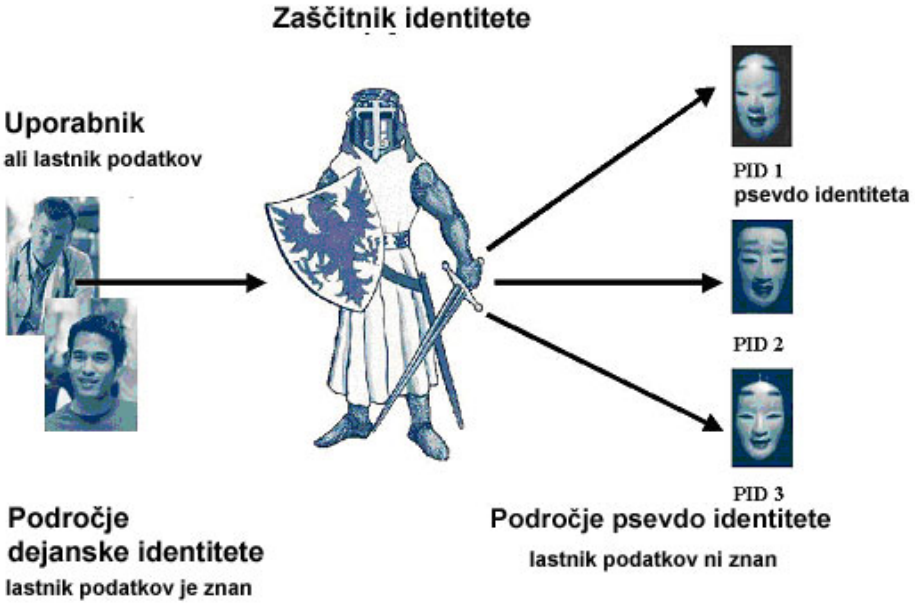
- daje poročila in kontrolo, ko je identiteta odkrita
- generira psevdo identitete
- prevaja psevdo identitete v pravo identiteto uporabnika in obratno
- prevaja psevdo identitete v druge psevdo identitete
- bori se proti zlorabam

Pomembna funkcija zaščitnika identitete je predvsem pretvorba uporabnikove identitete v eno ali več psevdo identitet. Psevdo identiteta je alternativna (digitalna) identiteta, ki jo uporabnik pridobi z vstopom v sistem (Blarkom, Borking, Verhaar, 2003, str. 34).
Namestitev zaščitnika osebnosti ustvari najmanj dve različni področji znotraj podatkovnega sistema: eno je področje, kjer je identiteta uporabnika poznana oziroma dostopna (področje dejanske identitete) in najmanj eno področje psevdo identitete (kjer dejanska identiteta ni poznana oziroma dostopna).
Namen psevdo identitete je zaščititi uporabnika pred identifikacijo na osnovi predhodno pridobljenih osebnih podatkov in obratno, doseči, da osebni podatki niso pridobljeni na osnovi pridobljene identitete.

Zaščitnik identitete je lahko integriran v informacijski sistem v različnih oblikah:

- kot ločeno delovanje znotraj podatkovnega sistema
- ločen podatkovni sistem nadzorovan s strani uporabnika (na primer pametne kartice za biometrično identifikacijo)
- podatkovni sistem nadzorovan s strani zaupnih centrov (Trust Center, Trusted Third Party)

Slika 12 - Zaščitnik identitete



Vir: Blarkom, Borking, Verhaar, 2003 str. 37

Ker je zaščitnik identitete pod nadzorom uporabnika, lahko le ta poljubno dovoljuje razkritje svoje prave identitete nekaterim internetnim ponudnikom, drugim pa ne. Uporabnik tako lahko uporablja storitve in izvaja transakcije anonimno (z uporabo psevdo identitete). Ponudnik internetne storitve lahko sledi in zapisuje internetne aktivnosti le uporabnika s psevdo identitetami in ne uporabnika z dejansko identiteto. S tem je ponudnikom storitev onemogočeno profiliranje dejanskih uporabnikov storitev.
Ponudnik storitve mora v nekaterih primerih imeti nadzor nad avtorizacijo, zato mora biti poučen o uporabnikovi pravi identiteti. Ker predstavlja zaščitnik identitete vmesni člen med uporabnikom in ponudnikom, mu morata obe strani zaupati. Zaščitnik osebnosti je narejen tako,da preprečuje prevare in nepravilno uporabo; ščiti uporabnikovo anonimnost, vendar jo lahko v določenih okoliščinah tudi razkrije, kot na primer internetnemu posredniku ali državnim organom.

Tehnike uporabljene za implementacijo zaščitnika identitete so lahko digitalni podpis, slepi digitalni podpis, digitalni psevdonim in zaupni centri (Seničar, Jerman-Blažič, Klobučar, 2003, str. 9, 10, Song, Korba, 2001, str. 7).

5.2.1.4 Zaupni centri

Naloga zaupnih centrov (ang. Trust Centres) je vzpostaviti varen servis znotraj celotne informacijske strukture, na način, da mu bodo zaupale vse vpletene strani: tako uporabniki kot tudi ponudniki storitev. Primerjamo ga lahko z notarjem: nevtralno, nevpleteno telo. Uporabnik mora zaupati, da bo ostala relacija med dejansko identiteto in psevdonimom tajna. V primeru zakonitega razkritja identitete, mora biti uporabnik nemudoma obveščen o tem, kdo in zakaj bo razkril njegovo identiteto. Ponudnik pa mora zaupati zaupnemu centru, da bo uporabnikova dejanska identiteta v posameznih, dogovorjenih primerih razkrita.
Glavne naloge zaupnih centrov so upravljanje s ključi (generiranje, shranjevanje, distribucija ključev), izdaja ter upravljanje s certifikati, naloga pooblaščenca (zaupnika) ter servisne funkcije (posredovanje informacij kot je seznam ključev, časovnih žigov, informacije o overovljenjih, opozarja na varnostno kritične dogodke…).

Zaupni centri morajo biti nevtralni in neodvisni ter ne smejo biti ogroženi zaradi nasprotja interesov (Seničar, Jerman-Blažič, Klobučar, 2003, str. 8, 9).

5.2.1.5 Anonimni strežniki

Prej smo omenili, da je bistvenega pomena uporabe interneta anonimnost, ki jo lahko dosežemo z uporabo različnih tehnik. Ena izmed njih je anonimni strežnik.
Anonimni strežniki omogočajo uporabnikom anonimni dostop do internetnih strani. Strežnik predstavlja neke vrste pregrado med računalnikom in internetom. Princip delovanja je enostaven: sklene se pogodba z organizacijo, ki ji zaupamo (zaupati ji morajo tako internetni uporabniki kot tudi komercialne organizacije).
Zahteva, ki jo pošljemo v internet, gre preko anonimnega strežnika, ki jo transformira tako, da končna destinacija ne more določiti izvora - zahteva, ki je prispela do končne destinacije vsebuje samo IP naslov anonimnega strežnika, uporabnikovega pa ne.
V skupino anonimnih strežnikov kahko prištevamo tudi proxi strežnike in požarne zidove, ki prav tako predstavljajo neke vrste pregrado med računalnikom in internetom. Komunikacija je dovoljena samo pod določenimi pogoji. Proxi strežnik je lahko nastavljen za blokiranje kolačkov, neželeno pošto…, požarni zidovi pa onemogočajo nedovoljen dostop do računalnika (Rezgui, Bougettaya, Eltoweissy, 2003. str. 45, Seničar, Jerman-Blažič, Klobučar, 2003, str.11, 12).

Eno izmed najstarejših podjetij s ponudbo storitve anonimnega strežnika je Anonymizer, ki obstaja že od leta 1995. Pri uporabi njihovih anonimnih strežnikov je IP naslov končnega uporabnika skrit, tako je onemogočeno logiranje spletnih strani, sledenje oglaševalcev, hekerskih napadov, monitoringa s strani ponudnikov internetnih storitev ali delodajalcev, filtrirajo se piškotki, spletni hrošči, virusi ter ostale grožnje zasebnosti, kot so kraje identitete, neželeno oglaševanje ...
Podjetje nezadržno raste, od leta 2001 je tudi dobičkonosno; imajo preko 100.000 predplačniških uporabnikov; preko milijon mesečnih uporabnikov ter od leta 1995 preko štiri bilijone zaščitenih pogledov spletnih strani (URL: http://www.anonymizer.com).
Anonimne strežnike ponujajo tudi druga podjetja kot so: Lucent Personal Web Assistant, iPrivacy, Websecure…

5.2.1.6 Ponovni pošiljatelj

Ponovni pošiljatelji (ang. re-mailer) so programi, ki sprejemajo elektronska sporočila od pošiljateljev ter jih po preoblikovanju pošiljajo naprej prejemnikom, tako da le ta ne more ugotoviti identitete pošiljatelja. Uporabniki pošiljajo sporočila preko »remailerja«, ki sporočilu odreže identifikacijske informacije ter ga opremi s psevdonimom. Za prejemnika elektronskega sporočila ostane pošiljateljev elektronski naslov neznan, ni pa neznan za operaterja ponovnega pošiljatelja.
Odgovor prejme pošiljatelj prav tako preko »remailerja«. Stopnja zasebnosti je odvisna od zaupanja, ki ga imamo do servisa ter njihove varnostne tehnike.
Za boljšo zaščito anonimnosti lahko uporabniki sporočilo zakodirajo ter ga pošljejo preko verige ponovnih pošiljateljev.
Novejša različica »re-mail« tehnologije je t.i. Mixmaster, ki omogoča zaščito pred prisluškovanjem ter pred napadi pri odgovoru na pošto (Seničar, Jerman-Blažič, Klobučar, 2003, str.12, Goldberg, 2002, str. 4).

5.2.1.7 Slepi digitalni podpis

Ena izmed različic digitalnega podpisa, ki zagotavlja uporabnikovo anonimnost, je slepi digitalni podpis[35] (ang. blind digital signature). Razlika med navadnim digitalnim podpisom in slepim digitalnim podpisom ni v samem podpisu, temveč v dokumentu, ki je bil podpisan. Ko nekdo podpiše dokument z digitalnim podpisom, pozna vsebino dokumenta, ko pa nekdo podpiše dokument s slepim digitalnim podpisom, vsebine dokumenta ne pozna, oziroma pozna samo del vsebine. Podpisniki so v tem primeru posebne agencije ali notariati, ki za vsebino dokumenta ne odgovarjajo.
Slepi podpis deluje na ta način: uporabnik prinese dokument notariatu; pri tem ne želi, da bi kdor koli vključno z notarjem poznal vsebino dokumenta. Dokument je obdan z ovojem,

[35] njegov ustvarjalec je David Chaum, 1990

del dokumenta pa je viden. Na vidni del dokumenta da notar pečat, ki dokazuje avtentičnost dokumenta. Kadar se uporablja digitalni podpis, zamenjajo ovoj in pečat šifrirne tehnike. Uporabnik šifrira digitalni dokument, ta dokument pa potem s svojim digitalnim podpisom podpiše notar. Podpis zagotavlja avtentičnost dokumenta.
Slepi digitalni podpis se uporablja v plačilnem sistemu poznanem kot elektronski denar (Ecash), kot časovni žig (timestamping)… (Hes, Borking, 2000, str. 32, Seničar, Jerman-Blažič, Klobučar, 2003, str. 8).

5.2.1.8 Omrežje Freenet

Kot navajajo avtorji sistema[36] je za digitalno dobo značilno pomanjkanje zasebnosti na internetu, porast cenzure, grožnja svobodi izražanja. Pretok osebnih informacij postaja predmet opazovanja in nadzorovanja, različne državne in zasebne institucije želijo preprečiti dostop do spornih informacij ter uničiti določen material. Ti trendi ne zadevajo samo političnih oporečnikov, temveč vse drugače misleče (s sledenjem internetnih aktivnosti, prebiranjem elektronske pošte) (Clarke at al., 2002, str. 40).

Projekt »Freenet« predstavlja distribuiran informacijski sistem narejen zato, da ohrani zasebnost informacij. Sistem deluje kot lokacijsko neodvisen distribuiran datotečni sistem preko številnih osebnih računalnikov, ki dajejo na razpolago proste kapacitete diska za anonimno shranjevanje in povpraševanje ter tako kreirajo virtualni datotečni sistem.
Glavni cilji sistema so:

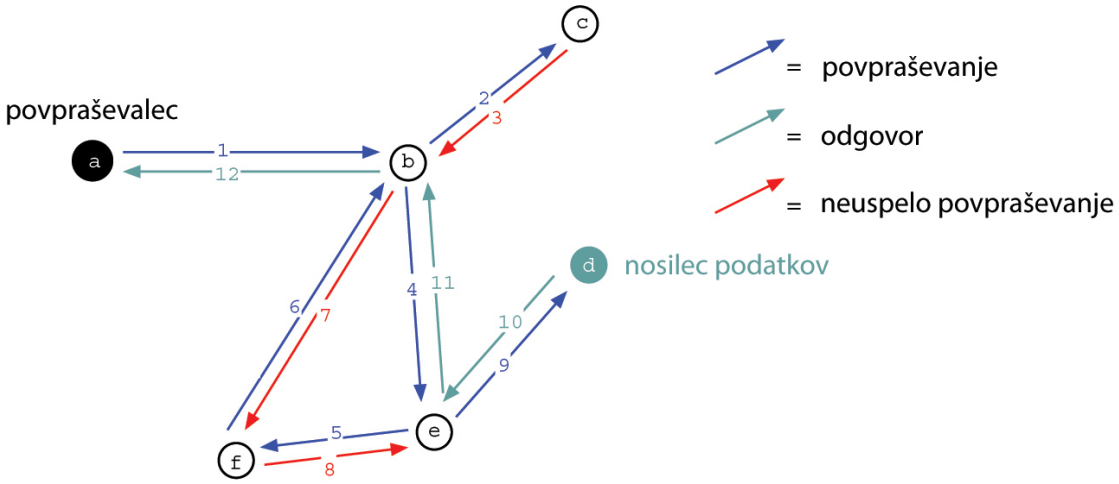
- anonimnost za producenta, uporabnika ter nosilca informacije
- onemogočen nepooblaščen dostop do informacij
- učinkovito dinamično shranjevanje ter usmerjanje informacij
- decentralizacija vseh mrežnih funkcij

Arhitektura sistema Freenet uporablja prilagodljivo P2P[37] mrežno relacijo vozlišč (vključenih računalnikov). Vsako vozlišče upravlja z lastnim lokalnim podatkovnim skladiščem, ki pa je na razpolago tudi omrežju. Če želi nekdo dodati novo datoteko, pošlje omrežju sporočilo, ki vsebuje datoteko ter ustrezen lokalno neodvisen identifikator[38], ki sproži shranjevanje datoteke na računalnik oziroma na več računalnikov v vozliščih (nodes). V času življenske dobe datoteke, se le ta večkrat prestavlja ali preslikava na druga vozlišča. Če želi uporabnik prečitati datoteko, pošlje zahtevo z vsebovanim identifikatorjem v omrežje in ko zahteva prispe na vozlišče, kjer se datoteka nahaja, pošlje vozlišče podatke nazaj do odjemalca (request originator).

[36] Avtorji sistema freenet so Ian Clarke, Oskar Sandberg, Scott Miller, Matthew Toseland, Steven Starr
[37] P2P: peer to peer internet omrežje, ki omogoča skupini uporabnikov povezavo in direkten dostop do povezanih računalnikov. Komunikacija ni podrejena kot v primeru strežnik – odjemalec.
[38] GUIDE: global unique identifier (globalni univerzalni identifikator)

Primarni namen Freeneta je zagotoviti zaščito anonimnosti povpraševalcev ter vsebine povpraševanj. Zasebnost je ohranjena z uporabo različice mix-net sheme za dosego anonimnosti komunikacije. Namesto direktno od pošiljatelja k prejemniku, sporočilo potuje skozi verigo vozlišč, v katerem je vsak link posebej šifriran, vse dokler sporočilo ne doseže končnega prejemnika. Vsako vozlišče pozna samo svojega neposrednega soseda v verigi, zato je lahko končna točka kjerkoli v omrežju vozlišč, ki neprenehoma izmenjujejo nečitljiva sporočila. Niti vozlišče neposredno za pošiljateljem ne more vedeti ali je njegov predhodnik resnični pošiljatelj (originator) ali samo prenaša sporočilo z drugega vozlišča. Prav tako za naslednje vozlišče ne more vedeti ali je to že pravi prejemnik (recipient originator) ali pa bo poslal sporočilo naprej.
Takšna ureditev ne ščiti samo producenta ter uporabnika informacije (na začetku verige), temveč tudi nosilca informacije (na koncu verige) (Clarke at al., 2002 str. 40-45).

Slika 13 - Povpraševanje v sistemu Freenet



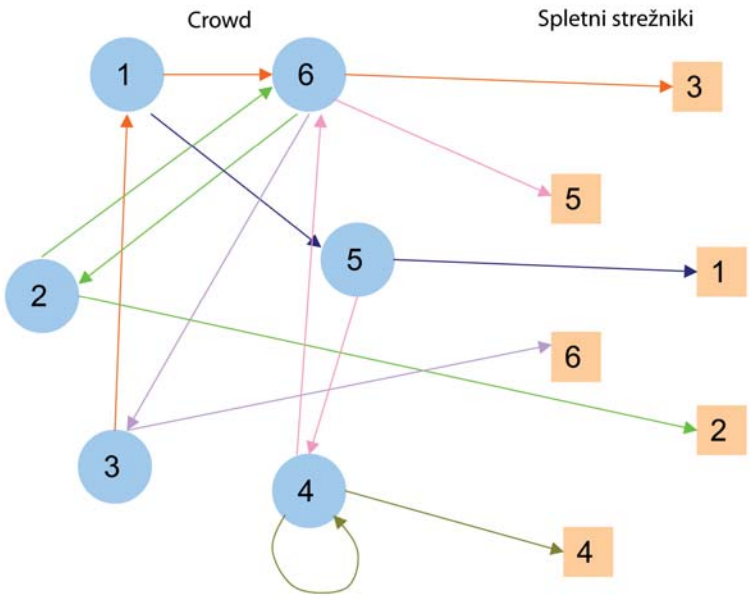
Vir: Clarke at. al, 2002, str. 44

Kot je zapisal Clarke, je Freenet sistem, ki omogoča nastajanje in ohranitev informacij na internetu, ne da bi nas skrbela cenzura. Omogoča prost pretok podatkov, svobodno širjenje misli, idej in mnenj. »Edina pot do demokracije je, da se vladam onemogoči kontrola nad državljani. Dokler bo vse kar vidimo in slišimo filtrirano, ne bomo resnično svobodni« (Clarke, The Philosophy behind Freenet). V svoji filozofiji se Clarke dotika tudi problema zaščite intelektualnih in avtorskih pravic (copyright). Jedro problema zaščite intelektualne pravice vidi v uveljavljanju zahteve po monitoringu komunikacij. Če je nadzorovano vse kar kdo reče, svobode govora ni. To pa je razlog, da Freenet onemogoči uveljavitev zakona o zaščiti intelektualne lastnine (URL: http://freenet.sourceforge.net/).

5.2.1.9 Sistem Crowds

Sistem Crowds[39] pomaga zagotoviti zasebnost dostopa do spleta, ne da bi lahko spletne strani ugotovile, s katerega računalnika smo dostopali. Bazira na ideji, da so ljudje lahko anonimni, če se skrijejo v množici, to pomeni: skriti svojo aktivnosti znotraj aktivnosti drugih udeležencev. Udeležencem sistema tako ni potrebno zaupati še neki tretji stranki, ki bi mu zagotavljala anonimnost.
Vsak uporabnik kontaktira z osrednjim strežnikom ter sprejme participacijski list »crowd«. Uporabnik nato prenaša svoje povpraševanje preko naključno izbranega vozlišča v sistemu crowd. Na osnovi prejetja zahteve vsakega vozlišča se naključno žreba žeton in odloči, ali gre povpraševanje še naprej skozi množico (crowd) ali pa se pošlje končnemu prejemniku. Odgovor je poslan nazaj uporabniku preko poti ustanovljene z zahtevo skozi množico »crowd«. (Reiter, Rubin, 1998, str. 73, 74, Seničar, Jerman-Blažič, Klobučar, 2003, str. 12, 13.)

Slika 14 - Delovanje sistema Crowds



Vir: Reiter, Rubin, 1998, str. 74

Prednost sistema je v tem, da tako zunanji opazovalec kot član množice (crowds) ter končni strežnik ne morejo ugotoviti pobudnika povpraševanja, njegova identiteta ostane skrita. Povsem nemočen pa je sistem v primeru, da uporabnik sam razkrije osebne podatke, kot na primer pri izpolnjevanju raznih obrazcev za registracijo, ki nezaščiteni potujejo skozi množico (Reiter, Rubin, 1998, str. 68).

[39] sistem sta razvila Reiter in Rubin sodelavca AT&T Laboratorija

5.2.2 Tehnologije za zaščito zasebnosti s privolitvijo

5.2.2.1 Platforma P3P

Tehnologija P3P[40] (ang. Platform for privacy preferences) je bila razvita kot industrijski standard za dosego večje avtomatske zaščite zasebnosti uporabnikov interneta. P3P predstavlja standardiziran niz vprašanj, ki pokrivajo vse glavne vidike zasebnostne politike spletnih strani. Uporabnikom omogoča vpogled nad zbiranjem osebnih podatkov na obiskani spletni strani ter primerjavo z lastnim naborom zahtev glede zasebnosti. P3P omogoča pretvorbo dokumenta o zasebnostni politiki spletne strani v standardiziran strojno čitljiv zapis - XML[41], ki se avtomatsko prečita in primerja z zahtevami, ki jih ima uporabnik glede zasebnosti (www.w3.org). P3P ne predpostavlja standardov zasebnosti, kot so recimo OECD principi, namesto tega predlaga izčrpen izbor zasebnostnih zahtev, med katerimi si naredi uporabnik lasten izbor o zasebnosti zbiranja in uporabe osebnih podatkov. Če zasebnostna politika spletne strani ustreza zahtevam uporabnika, je dostop do strani uspešen, v nasprotnem primeru P3P opozori uporabnika na razhajanje glede zasebnostnih preferenc (Prety poor privacy, 2000).
Takšen sistem komunikacije omogoča uporabniku brskanje po spletu in samodejno pridobivanje informacij o politiki zasebnosti spletnih strani, ne da bi bilo potrebno na vsaki strani posebej najprej poiskati politiko zasebnosti ter jo analizirati. Politike zasebnosti za spletne strani pišejo odvetniki, ki jim je glavni cilj zaščita lastnikov spletnih strani, ne pa obvešanje uporabnikov o zbiranju in uporabi osebnih podatkov. (Kercevan, 2003, str.40). Kot navaja Cranorjeva je eden pomembnih ciljev P3P seznanitev uporabnika glede politike zasebnosti spletne strani, ne da bi mu bilo treba čitati obsežne potlitike na vsaki obiskani spletni strani. Prav tako se spletne strani bolj trudijo izboljšati politiko zasebnosti, če je le ta prikazana skozi uporabo P3P (Cranor, 2003, str.55).

V poročilu »Prety poor privacy« ugotavljajo problematiko v zvezi z uporabo protokola P3P v tem, da prihaja do podobne situacije kot pri piškotkih: če zavračaš piškotke v celoti, potem skoraj ni več strani, ki bi jo lahko obiskal. Podobno je pri nastavitvah P3P. Uporabniki, ki so zelo zaskrbljeni glede svoje zasebnosti in si nastavijo P3P na visoko stopnjo zaščite ter blokirajo strani, ki tem zahtevam ne ustrezajo, potem skoraj ni strani, ki bi jo lahko obiskali. Da se uporabnik izogne takšnim situacijam, si nastavi stopnjo zaščite na minimum, s tem mu je omogočen dostop do vseh strani, vprašljivo pa postane varovanje zasebnosti.
Platforma P3P omogoča komunikacijo spletne strani z uporabniki glede njihove politike varovanja zasebnosti, toda to še ni zagotovilo, da bodo spletne strani tej politiki zasebnosti res tudi sledile (Cranor, 2003b, str. 81).

[40] platforma za zagotovitev zasebnosti; razvil jo je W3C – World Wide Web Consortium; neprofitna organizacija ustanovljena 1994, skrbi za razvoj spleta in postavitev standardov ter tehničnih priporočil
[41] XML (Extensible Markup Language): standard za zapis strukturiranih dokumentov na spletu

5.2.2.2 Upravitelj piškotkov

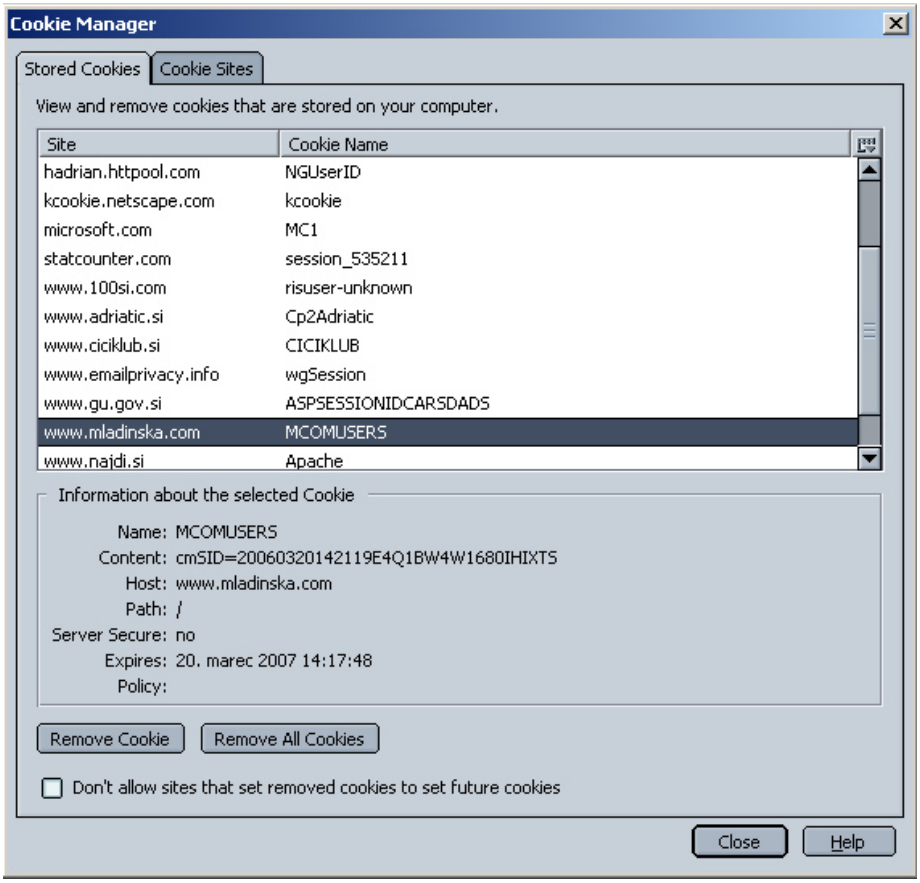
Tehnologija piškotkov omogoča določeno stopnjo identifikacije obiskovalcev spletne strani. Kot je omenjeno že v prejšnjem poglavju so piškotki (ang. cookies) majhne datoteke shranjene na uporabnikovem računalniku (praviloma brez vednosti uporabnika), namenjeni identifikaciji uporabnika. V datoteki so zapisani podatki o naslovu računalnika, življenska doba piškotka, identifikacijska številka, pogosto pa vsebuje tudi podatke, ki se nanašajo na uporabnika: ime, čas obiska strani, gesla… Piškotki omogočajo prikrito spremljanje uporabnika na internetu, podatke pa potem s pridom uporabljajo spletni oglaševalci za direktni marketing[42] (Možina, 2000, str. II).
Piškotki lahko vsebujejo tudi občutljive osebne podatke in zaradi tega predstavljajo grožnjo zasebnosti. Grožnje ne predstavlja samo sledenje uporabniku ter ugotavljanje njegovih navad, nevarnost predstavlja tudi prestrezanje piškotkov ter vdor v uporabnikov računalnik. Uporabnik ponavadi nima pregleda nad stopnjo ter načinom zaščite piškotkov pri samem prenosu ter shranjevanju (Seničar, Jerman.Blažič, Klobučar, 2003, str.11, Kercevan str. 28, 29).
Eden izmed načinov nadzora nad piškotki je upravljanje piškotkov (ang. Cookie management). To so orodja, ki omogočajo:

- rutinsko brisanje piškotkov s trdega diska
- onemogočanje elektronskih piškotkov (preprečevanje shranjevanja piškotkov na uporabnikov računalnik
- selektivno sprejemanje piškotkov (omogoča izbiro sprejemanja ali zavračanja piškotkov)
- pregled datotek elektronskih piškotkov (omogoča pregled nad shranjenimi piškotki in shranjeno vsebino)
- pregled spletnih strani, ki so postavile piškotke
- pregled časa trajanja posameznih piškotkov

Upravitelji elektronskih piškotkov (ang. cookies managers) omogočajo večji nadzor uporabnika nad piškotki ter njihovo vsebino, omogočajo mu lastno izbiro ali bo piškotek sprejel ali ne. Odpira pa se problem dostopa do spletne strani. V preveliki vnemi zavračanja piškotkov se nam kaj kmalu lahko zgodi, da bo izbor spletnih mest, kamor bomo lahko dostopali brez sprejema piškotka, zelo omejen.

[42] tako imenovani One-to-One Marketing – oblika neposrednega trženja, prilagojena profilu posameznika

Slika 15 - Upravitelj piškotkov



Vir: Netscape, ver. 7.1

5.3 Razvoj tehnologij za zboljšanje zasebnosti (PET) v Evropi

V okviru evropskega raziskovalnega programa se odvija mnogo projektov na temo zasebnosti in tehnologije. Ti projekti predstavljajo kažipot oziroma smernice za nadaljne delo ter implementacijo tehnologij v vsakdanjo rabo.
Primeri takšnih projektov so GUIDES, PRIDEH, PISA, PAMPAS, RAPID in drugi.

GUIDES (Smernice za e-poslovanje na podlagi direktive 95/46/ES)
Primarni cilj projekta je razvoj smernic s področja zaščite podatkov v pomoč evropskemu e-poslovanju. Smernice pokrivajo področje zakonodaje in tehnologije (predvsem opozarjajo na nevarnosti glede zasebnosti http protokola, spletnih hroščev, piškotkov, e-profiliranja).
Opozarjajo na naraščanje pretoka podatkov med podjetji; politike zasebnosti niso vedno najbolj jasne, uporabljajo jih predvsem velika podjetja, medtem ko majhna in srednja ne.

Za varnost podatkov priporočajo »on line« podjetjem uporabo varnostnih orodij, nadzor dostopov (identifikacija, avtentičnost), uporabo gesel, digitalnih potrdil, omejitev dostopov do podatkov, spremljanje in analizo dostopov…(GUIDES Project – Final Report)

PRIDEH: **(Privacy Enhancement in Data Management in E-Health) – Povečanje zasebnosti pri upravljanju s podatki na področju E-zdravja**

S projektom so pričeli zaradi vse pogostejših kršitev zasebnosti med samim pretokom podatkov ter naraščajoče potrebe po aktualnih podatkih za podporo medicinskim evidencam in odločanju v medicini. Osebni podatki so še posebej v zdravstvu pogosto občutljive narave. Različne aplikacije uporabljajo identiteto kot ključ za združevanje podatkov iz različnih virov, ne da bi dejansko to identiteto tudi potrebovali.

PRIDEH raziskuje možnosti vpeljave tehnologij za povečanje zasebnosti na področju zdravstva, ki bi tveganje glede kršenja zasebnosti zmanjšala na minimum. Eden izmed ciljev projekta je uporabiti identiteto samo takrat, ko je to res nujno potrebno. To naj bi dosegli s pomočjo tehnologij za zboljšanje zasebnosti, ki omogočajo varen in sprejemljiv način rokovanja s podatki, brez tveganja glede kršenja zasebnosti, a z vsemi prednostmi združevanja in sledenja informacijam, ki prihajajo iz različnih virov. Projekt se opira na Zaupne centre imenovane tudi psevdonimizacijski servisi, ki zagotavljajo varnost operacij ter varnost vseh ključev in metod znotraj procesa (URL: http://www.prideh.custodix.com).

Slika 16 - Uporaba PET za izboljšanje zasebnosti v zdravstvu

Vir**:** URL: http://www.prideh.custodix.com

PISA (Privacy Incorporated Software Agent)

Cilj tega projekta je razvoj elektronskega posrednika za zaščito uporabnikove zasebnosti. To vključuje filter imenovan zaščitnik identitete (Identitiy Protector), ki bi odstranjeval vse nepotrebne povezave do uporabnikovih osebnih identifikacijskih podatkov (URL: http://www.pet-pisa.nl).

PAMPAS (Pioneering Advanced Mobile Privacy and Security)
Pričel se je leta 2002 z namenom prepoznati vidike mobilne zasebnosti in varnosti ter postaviti okvirje za nadaljne raziskave. Namen PAMPAS je zagotoviti mobilnim servisom in sistemom varnost in zasebnost. Postaviti model za anonimnost in psevdonimnost, ki bi vsebovala mrežne protokole za zagotovitev različne stopnje zaščite (Crowds in Onion routing protokoli) ter razvoj internetnih orodij za anonimizacijo mobilnih mrež (URL: http//www.pampas.eu.org).

RAPID (Roadmap for Advanced Research in Privacy and Identitiy Management)
Cilj projekta je bil odkriti in konstruirati tehnološke, zakonske in metodološke osnove za rešitev problema zaščite zasebnosti kot je zagotoviti:

- anonimnost: uporabo virov in servisov ne da bi bila razkrita uporabnikova identiteta
- psevdonimnost: uporabo virov in servisov ne da bi bila razkrita uporabnikova identiteta, še zmeraj pa bi bil odgovoren za to rabo
- nepovezljivost: omogoča uporabniku različne nezdružljive rabe servisov in virov
- neopazovanost: zagotavlja, da uporabnik lahko uporablja vire in servise ne da bi ga pri tem kdo drug (tretja stran) opazoval.

(RAPID, Final Report, 2003, str. 13)

PRIME (Privacy and Identity Management for Europe)
Projekt se je začel v letu 2004 in bo trajal do leta 2008. Prikazati želi, kako lahko tehnologije za zboljšanje zasebnosti (PET) učinkovito zapolnijo vse večjo vrzel, ki nastaja na področju varovanja zasebnosti in osebnih podatkov med zakonodajo in dejansko prakso. Raziskuje digitalno upravljanje identitet (digital identity management) in zasebnost v informacijski družbi.
Projekt je usmerjen na uporabnike, razviti želi rešitve, ki bi posameznikom omogočile nadzor njihove zasebne sfere ter upravljanja z njihovimi identitetami (URL: http://www.prime-project.eu.org/).

6 POMEN ZASEBNOSTI MED SLOVENSKIMI UPORABNIKI INTERNETA

6.1 Opredelitev problema in cilj raziskave

Z vse večjo rastjo interneta, elektronskega poslovanja in razvojem informacijsko komunikacijskih tehnologij, se je bistveno povečala tudi količina podatkov dostopnih preko interneta. Na vsakem koraku je prisotna digitalizacija našega življenja: prehod na e-poslovanje, e-upravo, e-vlado, e-bančništvo, e-zdravstvo… skorajda ni več področja, kjer

ne bi bila prisotna »e« komponenta. Zbira se zmeraj več podatkov o posamezniku (državljanu), sodobne informacijsko komunikacijske tehnologije omogočajo enostavno združevanje, obdelovanje ter distribucijo podatkov. Vse več sistemov, institucij ter posameznikov ima dostop do teh (tudi osebnih) podatkov, s tem pa naraščajo potencialne kršitve zasebnosti potrošnikov in državljanov. Zmeraj več možnosti kršitev je tudi zaradi bliskovitega naraščanja uporabnikov interneta. Po podatkih RIS[43] je bilo v Sloveniji oktobra 2005 že 500.000 dnevnih, 700.000 tedenskih ter 840.000 mesečnih uporabnikov interneta.

Z raziskavo o pojmovanju zasebnosti ter varovanju osebnih podatkov med slovenskimi uporabniki interneta sem želela ugotoviti, ali je uporabnikom interneta v Sloveniji zasebnost pomembna, so pripravljeni razkriti svoje osebne podatke, ali se zavedajo groženj interneta ter v kolikšni meri poznajo in uporabljajo orodja za zaščito zasebnosti na internetu.

Na začetku naloge sem predstavila delovno hipotezo, ki sem jo s to raziskavo želela tudi dokazati:

> *Uporabnikom interneta je zasebnost na internetu pomembna, zavedajo se groženj zasebnosti na internetu, vendar pa premalo poznajo in uporabljajo orodja ter tehnologije za zaščito zasebnosti.*

6.2 Metodologija

V empiričnem delu raziskave sem izvedla anketo med uporabniki interneta starejšimi od 15 let. Uporabila sem dva načina anketiranja in sicer:

- anketiranje preko natisnjene ankete
- anketiranje preko interneta

Anketo so uporabniki izpolnjevali sami, brez pomoči anketarja. Prednost takega načina je, da ni vpliva anketarja, anketiranci ostanejo anonimni; slabost pa je predvsem v večji možnosti nepopolnih odgovorov, kajti ni dodatnega pojasnjevanja in pomoči anketarja.
Anketiranje preko interneta sem izvedla tako, da sem najprej preko elektronske pošte razposlala vabilo k sodelovanju ter povezavo na spletno stran, kjer je bil shranjen anketni vprašalnik. Anketiranci so prav tako sami izpolnjevali vprašalnik.

Anketa je potekala od 7. do 21. februarja 2006. V tem času sem dobila vrnjenih 112 izpolnjenih vprašalnikov, 76 (67,8%) v tiskani obliki ter 36 (32,2%) v elektronski obliki.

[43] Raba interneta v Sloveniji je akademski neprofitni projekt Centra za metodologijo in informatiko Fakultete za družbene vede v Ljubljani. Poteka od leta 1996 in proučuje družboslovne vidike informacijske tehnologije, predvsem interneta in mobilne telefonije (URL: http://www.ris.org)

6.3 Sestava vprašalnika

Anketni vprašalnik (priloga 1) je obsegal 28 vprašanj, ki sem jih razdelila v štiri sklope. Pripravila sem vprašanja zaprtega tipa in sicer tako, da so bila čim krajša in razumljiva, brez nepotrebnih tujk in strokovnih izrazov.
Vprašalnik sem zasnovala podobno kot samo magistrsko delo:

- vprašanja v zvezi z zasebnostjo in osebnimi podatki
- vprašanja glede groženj zasebnosti
- vprašanja glede uporabe tehnologij za izboljšanje zasebnosti na internetu
- splošni podatki o anketirancu

V prvem sklopu vprašanj v zvezi z zasebnostjo, sem želela izvedeti ali nam je zasebnost pomembna, ali smo pripravljeni razkriti osebne podatke in katere. Koliko poznamo zakonodajo v zvezi z zasebnostjo ter kaj menimo o nekaterih določilih iz zakonodaje.
V drugem sklopu, ki se nanaša na grožnje zasebnosti, sem želela ugotoviti ali poznamo grožnje zasebnosti preko interneta in če smo glede tega zaskrbljeni.
V tretjem sklopu sem zastavila nekaj vprašanj v zvezi s poznavanjem in uporabo orodij za izboljšanje zasebnosti na internetu. Želela sem ugotoviti ali so uporabniki interneta poučeni o obstoju orodij, v koliki meri jih uporabljajo, oziroma zakaj jih ne uporabljajo. V zvezi z vse večjim nadzorom oblasti zaradi preprečevanja terorizma (direktiva, ki jo je sprejela Evropska unija v zvezi z ohranitvijo (retencijo) prometnih podatkov), me je zanimalo ali se uporabnikom interneta zdi potrebno, da smo nadzorovani.
Z zadnjim, četrtim sklopom vprašanj, sem od anketirancev želela pridobiti nekaj splošnih podatkov kot so: starost, spol, izobrazba ter čas, ki ga tedensko porabijo na internetu.

Anketni vprašalnik sem pred začetkom izvedbe še testirala na skupini anketirancev, ki so podali svoje mnenje o vprašanjih. Vsebinskih pripomb na vprašanja niso imeli, odpraviti je bilo potrebno le nekaj nejasnosti glede možnih odgovorov.

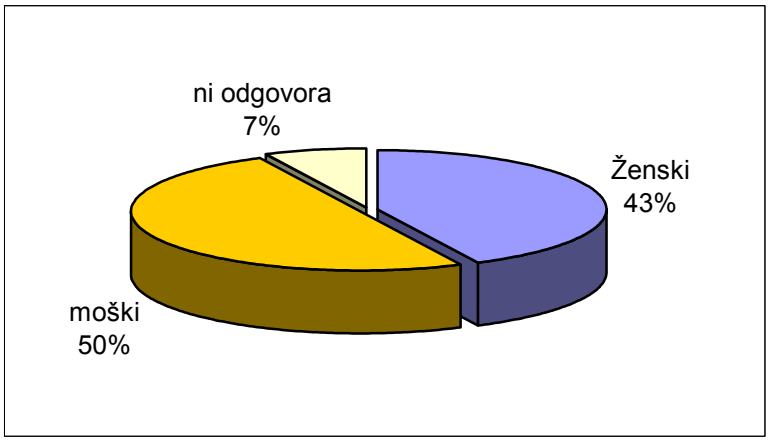
Pridobljene podatke je bilo potrebno še računalniško obdelati, analizirati ter prikazati rezultate v primernih tabelah in grafih.

6.4 Interpretacija pridobljenih rezultatov

6.4.1 Sodelujoči v anketi (demografski podatki):

V anketi je sodelovalo 47 žensk in 56 moških, 9 anketirancev ni podalo odgovora o spolu.

graf 1: Struktura anketirancev po spolu



vir: anketa, Splošni podatki o anketirancu

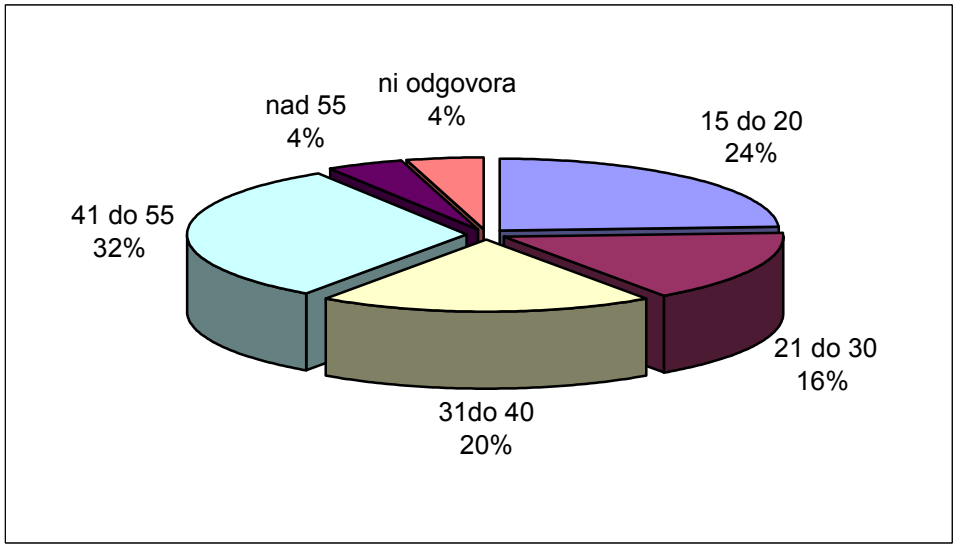
Sodelovali so uporabniki interneta stari nad 15 let, ki sem jih razdelila v pet skupin.

tabela 1: starostna struktura anketirancev

starost (leta)	frekvenca	odstotek
15 do 20	27	24,11
21 do 30	18	16,07
31 do 40	22	19,64
41 do 55	35	31,25
nad 55	5	4,46
ni odgovora	5	4,46
skupaj	112	100,00

vir: anketa, Splošni podatki o anketirancu

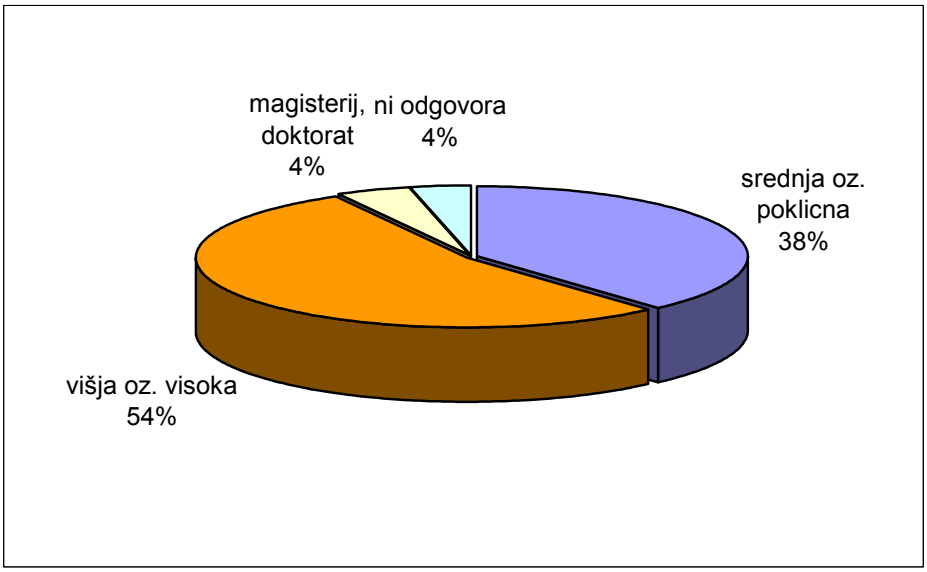
graf 2: Starostna struktura anketirancev



vir: anketa, Splošni podatki o anketirancu

Po izobrazbeni strukturi sem anketirance razdelila v 3 skupine in sicer:
dokončana poklicna ali srednješolska izobrazba (38%), višja oziroma visokošolska izobrazba (54%), magisterij oziroma doktorat (4%). Na vprašanje o izobrazbi ni želelo odgovoriti 4% anketirancev.

graf 3: Izobrazbena struktura anketirancev

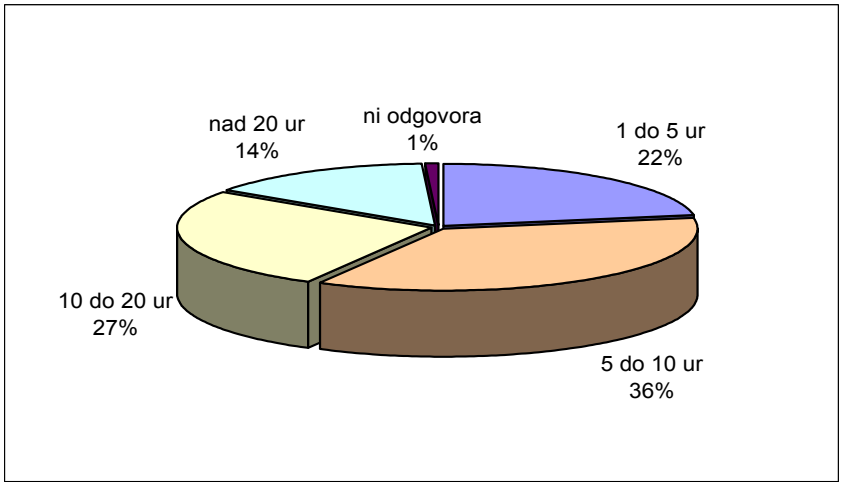


vir: anketa, Splošni podatki o anketirancu

V sklopu splošnih vprašanj o anketirancih je bilo tudi vprašanje, koliko časa porabijo za brskanje po spletu. Na vprašanje sta odgovorila 102 anketiranca.

Iz grafičnega prikaza je razvidno, da je največ uporabnikov (36%) na spletu od 5 do 10 ur tedensko, 27% uporabnikov jih preživi na spletu od 10 do 20 ur (to pomeni 2 do 3 ure dnevno), 14 % uporabnikov pa preživi na spletu več kot 20 ur. Do 5 ur tedensko porabi za obiskovanje spletnih strani 22 % anketirancev.

graf 4: Čas, ki ga anketiranci preživijo na spletu



vir: anketa, Splošni podatki o anketirancu

Iz manjkajočih odgovorov pri demografskih podatkih lahko sklepamo, da določen odstotek uporabnikov interneta ne želi posredovati nikakršnih osebnih podatkov kljub zagotovilu o anonimnosti. Manjkajoči podatki so bili predvsem pri internetnih vprašalnikih.

6.4.2 Zasebnost in osebni podatki

V prvem delu ankete, so bila vprašanja glede pojmovanja zasebnosti, informiranosti o zakonodaji ter pravicah, ki jih imajo uporabniki interneta glede varovanja zasebnosti, o občutljivosti osebnih podatkov oziroma o pripravljenosti uporabnikov storitev do razkritja osebnih podatkov.

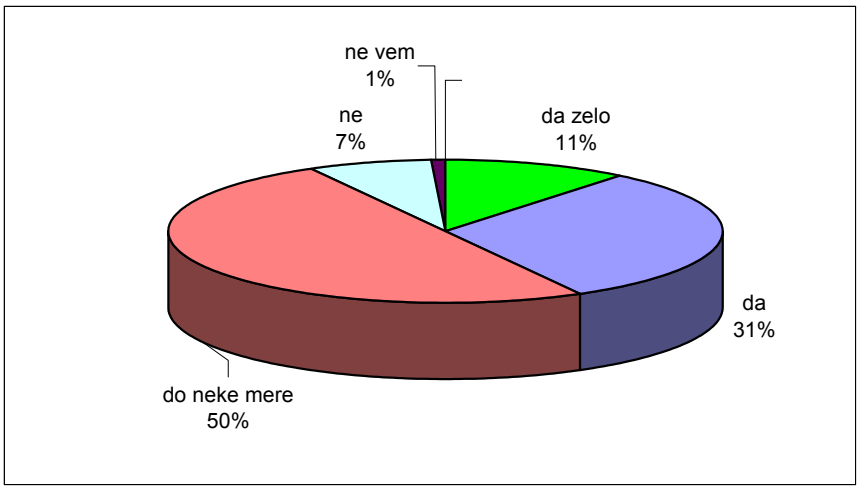
Na vprašanje o zaskrbljenosti glede varovanja zasebnosti je odgovorilo 112 anketirancev. Največ (50%) jih je odgovorilo, da so zaskrbljeni »*do neke mere*«. Z odgovorom »*da zelo*« in »*da*« je skupaj odgovorilo 41% in le 7 % anketirancev je odgovorilo, da glede varovanja zasebnosti niso zaskrbljeni.

tabela 2: Zaskrbljenost uporabnikov interneta glede varovanja zasebnosti

	frekvenca	odstotek	kumulativni odstotek
da zelo	12	10,71	10,71
da	35	31,25	41,96
do neke mere	56	50,00	91,96
ne	8	7,14	99,11
ne vem	1	0,89	100,00
skupaj	112	100,00	

vir: anketa, vprašanje 1

graf 5: Zaskrbljenost uporabnikov interneta glede varovanja zasebnosti



vir: anketa, vprašanje 1

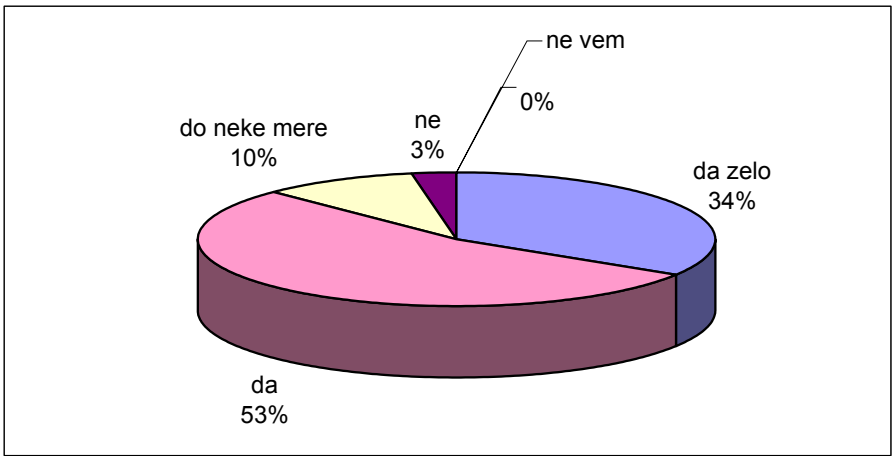
Glede na dobljene rezultate lahko rečemo, da so uporabniki interneta zaskrbljeni glede varovanja zasebnosti. Zelo pomembno se jim tudi zdi, da vedo kateri osebni podatki se zbirajo o njih. Na vprašanje: »*Se vam zdi pomembno, da veste kateri vaši osebni podatki se zbirajo in v kakšen namen«* je kar 87, 5% anketirancev odgovorilo, da se jim zdi pomembno oziroma zelo pomembno, da vedo kateri njihovi osebni podatki se zbirajo in v kakšen namen, 9.8 % jih je odgovorilo , da jim je to pomembno do neke mere, samo 2.7 % pa jih je odgovorilo, da jim ni pomembno, če vedo v kakšne namene ter kateri podatki se zbirajo.

tabela 3: Pomembnost obveščenosti uporabnikov glede zbiranja osebnih podatkov

	frekvenca	odstotek	kumulativni odstotek
da zelo	38	33,93	33,93
da	60	53,57	87,50
do neke mere	11	9,82	97,32
ne	3	2,68	100,00
ne vem	0	0,00	
skupaj	112	100,00	

vir: anketa, vprašanje 2

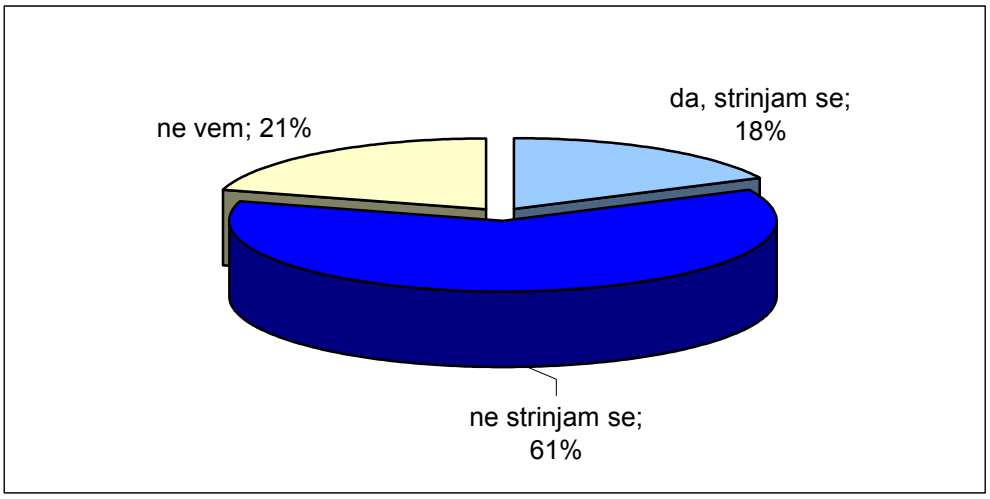
graf 6: Pomembnost obveščenosti uporabnikov glede zbiranja osebnih podatkov



vir: anketa, vprašanje 2

V borbi za kupca pridobiva veliko podjetij v marketinške namene podatke iz različnih javnih imenikov ter drugih javno dostopnih evidenc. Uporabnikom interneta sem zastavila vprašanje, če se strinjajo, da podjetja pridobivajo osebne podatke iz javnih imenikov. Večina anketirancev (61%) se s takim načinom zbiranja podatkov ne strinja, 18% se jih strinja, 21% pa se jih glede pridobivanja podatkov iz javnih imenikov ni opredelilo.

graf 7: Strinjanje s pridobivanjem podatkov iz javnih imenikov za marketinške namene

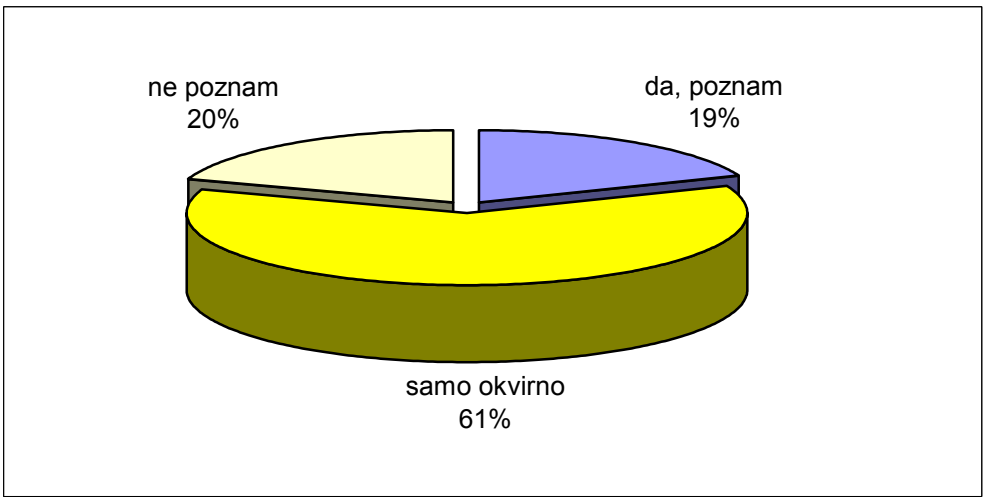


vir: anketa, vprašanje 3

Osebni podatki se brez soglasja osebe na katero se ti podatki nanašajo ne smejo zbirati. 79,5% anketirancev je odgovorilo, da vedo, da se podatki brez njihovega soglasja ne smejo zbirati, 20,5% anketirancev pa je odgovorilo, da s tem niso seznanjeni.

Podoben odstotek anketirancev je tudi seznanjeno z zakonodajo s področja varovanja zasebnosti in osebnih podatkov. Na vprašanje, če poznajo zakonodajo, je 61% vprašanih odgovorilo, da jo poznajo samo okvirno, 19% je odgovorilo, da zakonodajo poznajo in 20% vprašanih zakonodaje ne pozna.

graf 8: Poznavanje zakonodaje s področja varovanja zasebnosti in osebnih podatkov

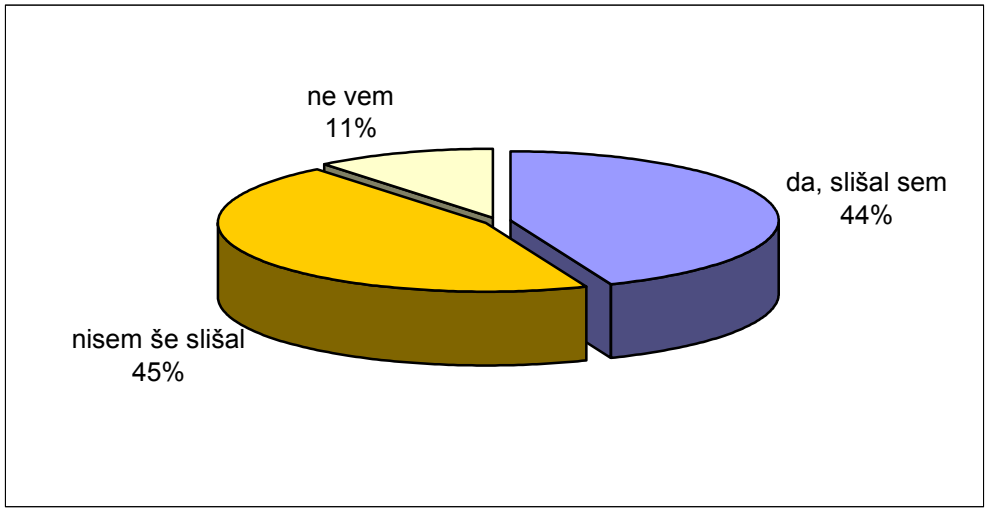


vir: anketa, vprašanje 5

Po Zakonu o varstvu osebnih podatkov[44] ima vsakdo pravico do vpogleda v osebne zbirke, ki jih določena institucija vodi o njem. Upravljavec osebnih podatkov mora na zahtevo posameznika omogočiti mu vpogled v katalog zbirke podatkov, potrditi ali se podatki o njem zbirajo ali ne, omogočiti mu vpogled v osebne podatke, ki se nanašajo nanj. Če so podatki netočni, nepopolni, neažurni, ali nezakonito pridobljeni, jih mora upravljavec na zahtevo osebe na katero se podatki nanašajo popraviti, blokirati ali izbrisati. 43,8% vprašanih je za to pravico že slišalo, 45,5% za to še ni slišalo, 10,7% pa je odgovorilo, da ne vedo ali so o tem že kaj slišali.

Pravico do vpogleda v osebne podatke, ki jih nekdo vodi o njem je izkoristilo samo 5,4% vprašanih.

graf 9: Informiranost o pravici do vpogleda v osebne zbirke



vir: anketa, vprašanje 6

Spletne strani od uporabnikov mnogokrat zahtevajo izpolnjevanje raznih obrazcev, kjer je potrebno posredovati tudi osebne podatke. Anketiranci so bili vprašani, ali so, zato da pridejo do neke internetne vsebine, pripravljeni razkriti svoje osebne podatke.

[44] Uradni list RS št. 86/2004 z dne 5.8.2004, v veljavo je stopil 1.1.2005

tabela 4: Pripravljenost razkriti lastne osebne podatke

	vedno		*včasih*		*nikoli*		
	N	**%**	**N**	**%**	**N**	**%**	**Veljavni odgovori**
ime, priimek	36	32,14	67	59,82	9	8,04	112
naslov	26	23,21	75	66,96	11	9,82	112
rojstne podatke	17	15,32	75	67,57	19	17,12	111
EMŠO	6	5,45	45	40,91	59	53,64	110
elektronski naslov	32	28,83	65	58,56	14	12,61	111
telefonsko številko	12	12,50	54	56,25	30	31,25	96
številko bančnega računa	0	0,00	11	9,91	100	90,09	111
številko kreditne kartice	1	0,89	11	9,82	100	89,29	112
izobrazbo	26	23,42	76	68,47	9	8,11	111
zaposlitev	19	17,12	81	72,97	11	13,58	111
narodnost, veroizpoved	20	17,86	49	43,75	43	38,39	112
podatke o svojem zdravju	3	2,73	30	27,27	77	68,75	110

vir: anketa, vprašanje 8

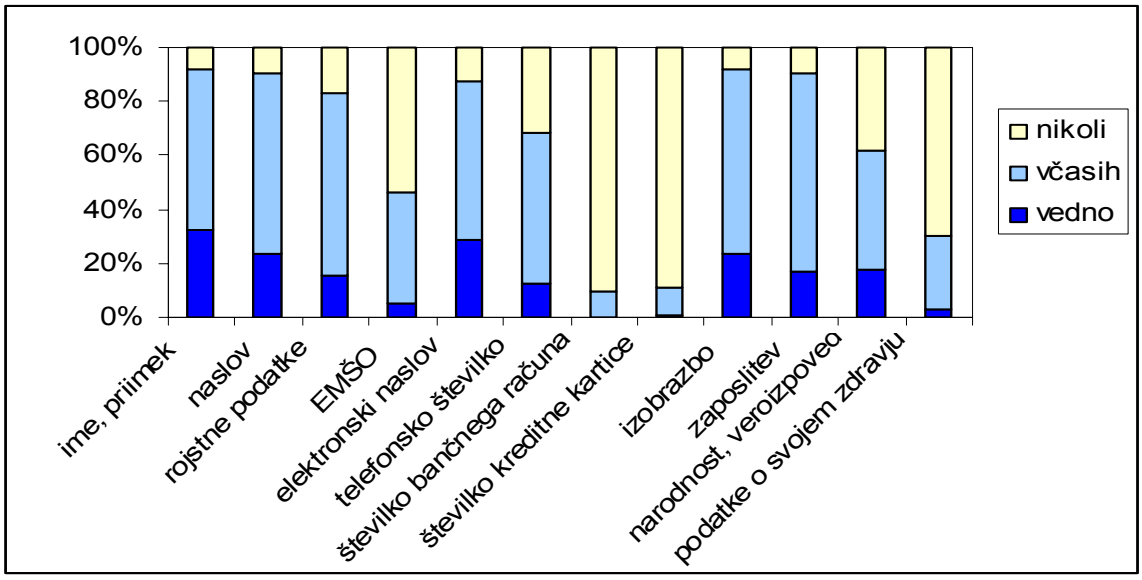
Iz pridobljenih podatkov je razvidno, da najtežje izdamo številko bančnega računa (90% je odgovorilo, da številke bančnega računa nikoli ne povedo), podoben odstotek je pri številki kreditne kartice (89% je odgovorilo z nikoli), sledijo podatki o zdravju (z nikoli ne izdam podatkov o svojem zdravju je odgovorilo 69 %), uporabniki interneta skrbno varujejo tudi svojo matično številko (EMŠO) – 54% jih je odgovorilo z »nikoli«. Narodnost, veroizpoved nikoli ne pove 38% vprašanih in telefonske številke nikoli ne izda 31% vprašanih.

Pri odgovoru »vedno« se je največ vprašanih opredelilo za podatek o imenu in priimku (32%), 8% vprašanih pa imena nikoli ne izda. Da vedno povedo svoj elektronski naslov je odgovorilo (29%) vprašanih, ter nikoli – 13% vprašanih. Pri odgovoru »vedno« sledi, izobrazba in naslov (23%), nikoli ne izda teh podatkov: naslov 10% ter izobrazbo 9% vprašanih.

Slovenski uporabniki interneta dokaj skrbno čuvajo osebne podatke, ter jih ne posredujejo zmeraj in vsakomur. Najlažje zaupajo elektronski naslov ter ime in priimek, najbolj skrbno pa varujejo podatke o bančnem računu (nihče ni odgovoril, z odgovorom »vedno«),

številko kreditne kartice (pod 1%) in podatke o svojem zdravju (le 2% uporabnikov brez oklevanja zaupa te podatke).
Iz tabele je razvidno, da je bila največja frekvenca odgovorov pod kategorijo »*včasih*«, kar kaže na to, da tehtamo ali bomo podatke zaupali ali ne, torej jih ne zaupamo zmeraj in vsakomur. Najmanjši odstotek je pri razkritju številke bančnega računa, kreditne kartice (10%) ter podatkov o zdravju (27%).

graf 10: Pripravljenost razkriti osebne podatke



vir: anketa, vprašanje 8

Kljub temu, da se zavedamo pomena zasebnosti, da želimo imeti nadzor nad osebnimi podatki, pa vendarle velikokrat čisto prostovoljno posredujemo svoje podatke različnim marketinškim in drugim organizacijam.

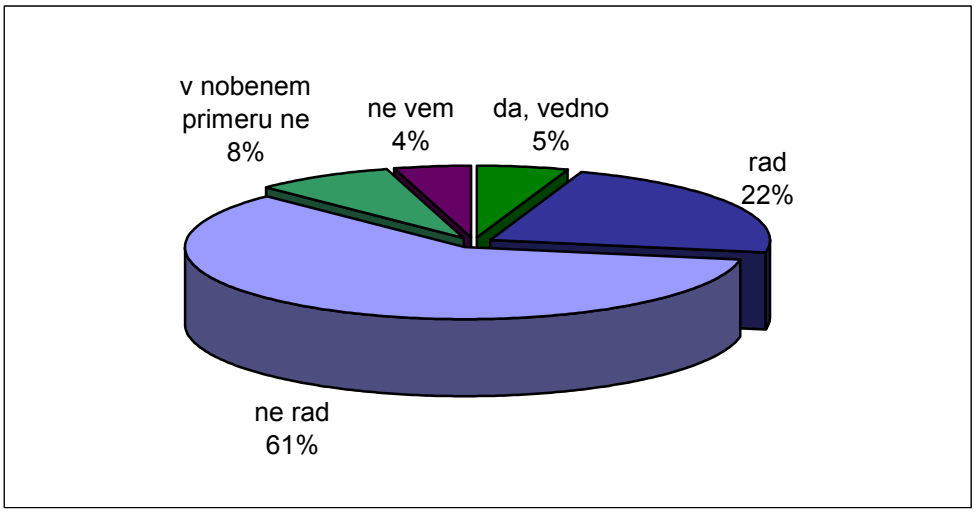
tabela 5: Ali smo pripravljeni posredovati osebne podatke za določene bonitete

	frekvenca	odstotek	kumulativni odstotek
da, vedno	6	5,36	5,36
rad	25	22,32	27,68
ne rad	67	59,82	87,50
v nobenem primeru ne	9	8,04	95,54
ne vem	5	4,46	100,00
skupaj	112	100,00	

vir: anketa, vprašanje 9

V zameno za posredovanje osebnih podatkov mnoge organizacije ponujajo različne bonitete, kot so popusti, nagradne točke, žrebanje nagrad, kartice zaupanja in podobno. Na vprašanje *ali ste pripravljeni razkriti osebne podatke za določene bonitete (nagradne točke, popusti, kartice zaupanja,…)* je samo 8% vprašanih odgovorilo z *«v nobenem primeru ne«,* 4% vprašanih ne vedo oziroma niso želeli povedati, ali so pripravljeni posredovati osebne podatke za določene ugodnosti, 60% jih je odgovorilo z »ne rad«, 22% radi posredujejo osebne podatke, če za to kaj prejmejo in 5% vprašanih to zelo radi naredijo.

graf 11: Ali smo pripravljeni posredovati osebne podatke za določene bonitete



vir: anketa, vprašanje 9

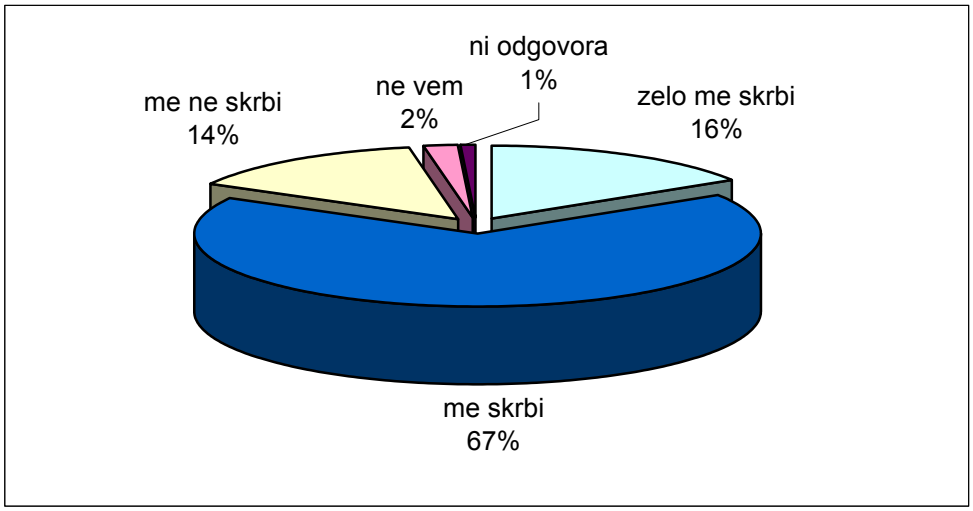
Osebni podatki, ki jih puščamo na internetu ob uporabi različnih spletnih storitev, se lahko uporabijo za pošiljanje reklamnih sporočil, lahko se prodajo trgovinam, zavarovalnicam ali so predani državnim organom.
Na vprašanje ali so uporabniki interneta glede tega zaskrbljeni, je 83% vprašanih odgovorilo »*me skrbi*« oziroma »*zelo me skrbi*«, samo 14% pa je takšnih, ki glede tega niso zaskrbljeni.

tabela 6: Zaskrbljenost glede namena uporabe osebnih podatkov na internetu

	frekvenca	odstotek	kumulativni odstotek
zelo me skrbi	18	16,07	16,07
me skrbi	75	66,96	83,03
me ne skrbi	16	14,29	97,32
ne vem	2	1,79	99,11
ni odgovora	1	0,89	100,00
	112	100,00	

vir: anketa, vprašanje 10

graf 12: Zaskrbljenost glede namena uporabe osebnih podatkov na internetu



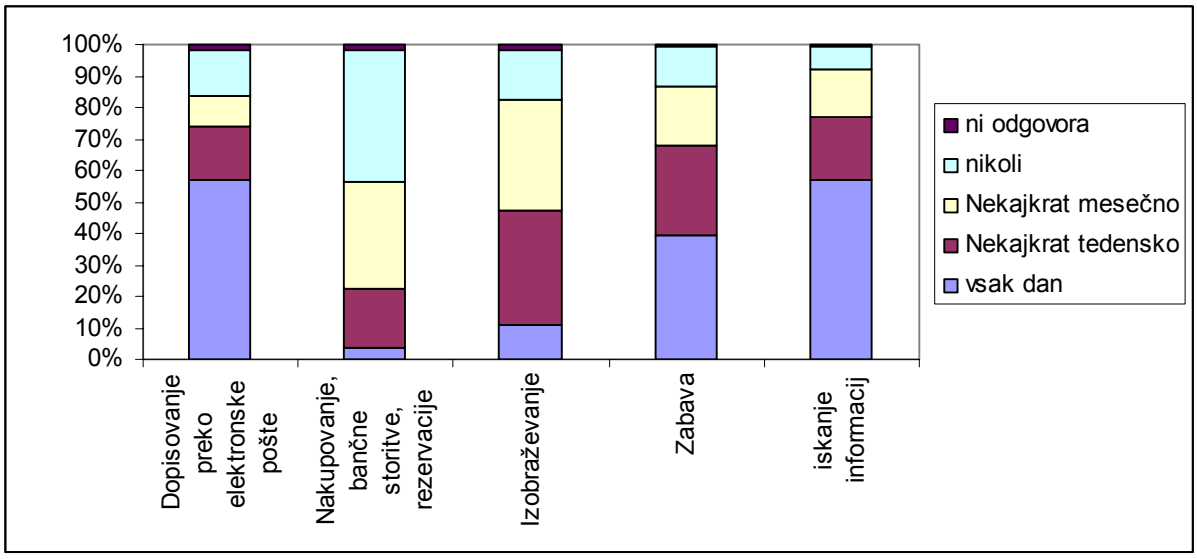
vir: anketa, vprašanje 10

Kljub temu, da so pri vprašanju o posredovanju osebnih podatkov za določene bonitete vprašani odgovorili, da posredujejo podatke (87%) v zameno za ugodnosti, pa so skoraj v enakem odstotku (83%) izrazili zaskrbljenost glede namena uporabe teh podatkov.

6.4.3 Grožnje zasebnosti

V sklopu vprašanj glede groženj zasebnosti, sem uporabnike interneta najprej vprašala v kakšne namene in kako pogosto uporabljajo internet.

graf 13: Namen in pogostost uporabe interneta



vir: anketa, vprašanje 11

tabela 7: Namen in pogostost uporabe interneta

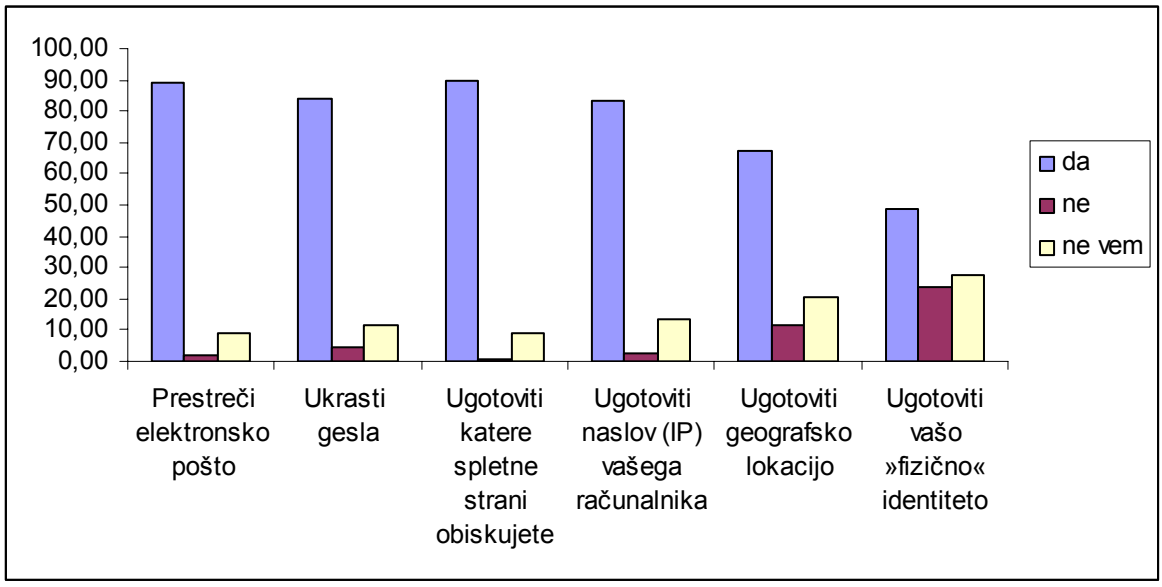
	vsak dan		*nekajkrat tedensko*		*nekajkrat mesečno*		*nikoli*			
	N	**%**	**N**	**%**	**N**	**%**	**N**	**%**	**veljavni odgovori**	**ni odgovora**
dopisovanje preko elektronske pošte	64	58,18	19	17,27	11	10,00	16	14,55	110	2
nakupovanjebančne storitve, rezervacije	4	3,64	21	19,09	38	34,55	47	42,73	110	2
izobraževanje	12	10,91	41	37,27	39	35,45	18	14,00	110	2
zabava	44	39,64	32	28,83	21	18,92	14	12,61	111	1
iskanje informacij	64	57,66	22	19,82	17	15,32	8	7,21	111	1

vir: anketa, vprašanje 11

Iz tabele in grafičnega prikaza je razvidno, da je najbolj pogosto uporabljena internetna storitev uporaba spleta za iskanje informacij. Vsak dan uporablja internet za iskanje informacij 58 % vprašanih, nekajkrat tedensko pa 20%. Elektronsko pošto vsak dan uporablja prav tako 58% vprašanih ter 17% nekajkrat tedensko. Najmanj pogosto vprašani uporabljajo internet za nakupovanje oziroma bančne storitve (vsak dan samo 4 % vprašanih, 19% nekajkrat tedensko, 42% vprašanih pa nikoli ne uporablja interneta za nakupovanje, bančne storitve oziroma rezervacije).

O tem, da je možno preko interneta prestreči elektronsko pošto, ukrasti gesla, številke kreditnih kartic, ugotoviti katere spletne strani obiskujemo, ugotoviti naslov (IP) računalnika, ugotoviti celo geografsko lokacijo ter fizično identiteto uporabnika, so vprašani zelo dobro poučeni.

graf 14: Grožnje zasebnosti preko interneta



vir: anketa, vprašanje 12

Iz grafa je razvidno, da večina vprašanih (nad 80%) pozna grožnje kot so prestrezanje elektronske pošte, kraja gesel ter številk kreditnih kartic, vedo, da je možno ugotoviti katere spletne strani obiskujejo ter IP njihovega računalnika. 67% vprašanih meni tudi, da se da ugotoviti geografsko lokacijo uporabnika interneta. Najmanj verjetno se zdi vprašanim, da se preko interneta lahko ugotovi »fizična« identiteta uporabnika: 47% jih meni, da se identiteta uporabnika da ugotoviti, 23% jih meni, da to ni mogoče, 28% pa ne vedo ali je to možno, ali ne.

Na vprašanje ali so ob uporabi interneta že kdaj začutili neželen poseg v njihovo zasebnost, je pozitivno odgovorilo 28% vprašanih, 54% neželenega posega v zasebnost na internetu še ni občutilo, 18% pa tega ne ve.

V spodnji tabeli so prikazani odgovori na vprašanje v koliki meri so uporabniki interneta zaskrbljeni glede različnih groženj zasebnosti.

tabela 8: Prikaz stopnje zaskrbljenosti glede različnih groženj zasebnosti

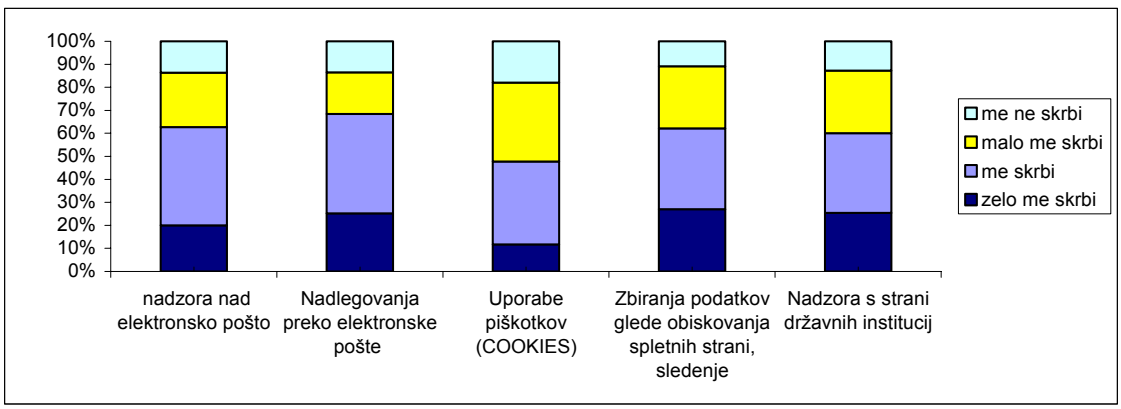
	zelo me skrbi		me skrbi		malo me skrbi		me ne skrbi		
	N	%	N	%	N	%	N	%	Veljavni odgovori
prestrezanja elektronske pošte oz. nadzora nad elektronsko pošto	22	20	47	42,73	26	23,64	15	13,64	110
nadlegovanja preko elektronske pošte (neželena elektronska pošta-SPAM)	28	25,23	48	43,24	20	18,02	15	13,51	111
uporabe piškotkov (COOKIES)	13	11,71	40	36,04	38	34,23	20	18,02	111
zbiranja podatkov glede obiskovanja spletnih strani, sledenje	30	27,03	39	35,14	30	27,03	12	10,81	111
nadzora s strani državnih institucij	28	25,45	38	34,55	30	27,27	14	12,73	110

vir: anketa, vprašanje 14

Raziskava je pokazala, da je preko 80% vprašanih zaskrbljenih zaradi različnih groženj oziroma nadzora, ki ga omogoča internet. V povprečju je samo13,7% odgovorilo, da jih ne skrbijo posamezne grožnje zasebnosti na internetu. Najmanj so zaskrbljeni zaradi uporabe kolačkov (18%).

Največ odgovorov »*zelo me skrbi*« in »*me skrbi*« so označili pri nadlegovanju preko elektronske pošte (68%), pri prestrezanju elektronske pošte (63%), pri zbiranju podatkov glede obiskovanja spletnih strani (62%) ter nadzoru s strani državnih institucij (60%).

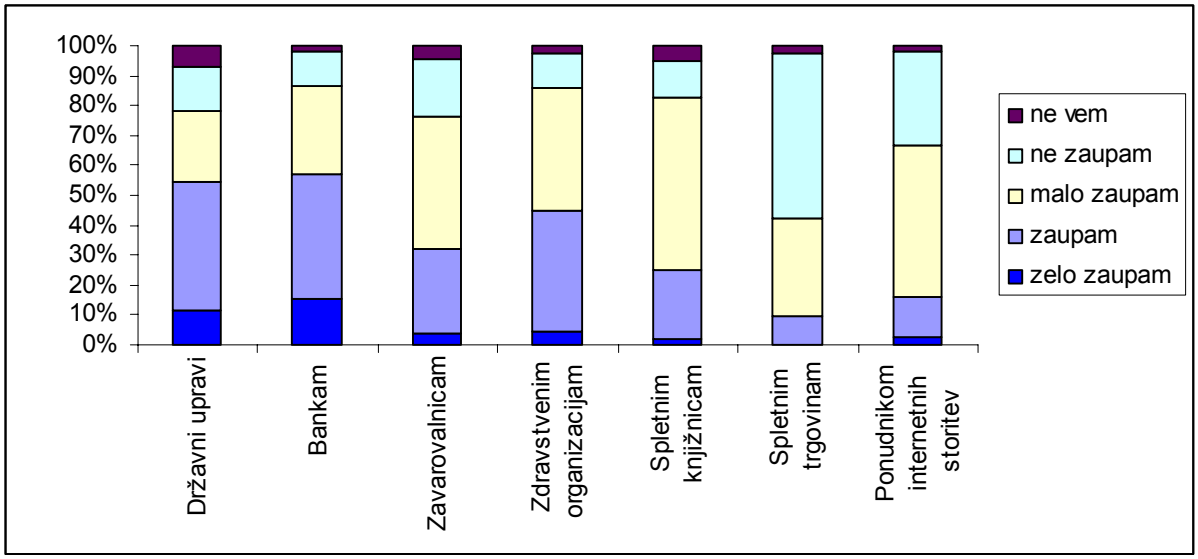
graf 15: Prikaz zaskrbljenosti glede različnih groženj zasebnosti



vir: anketa, vprašanje 14

Katerim organizacijam uporabniki interneta najbolj zaupajo je razvidno iz spodnjega grafičnega prikaza:

graf 16: Prikaz zaupanja različnim organizacijam glede varovanja podatkov na internetu



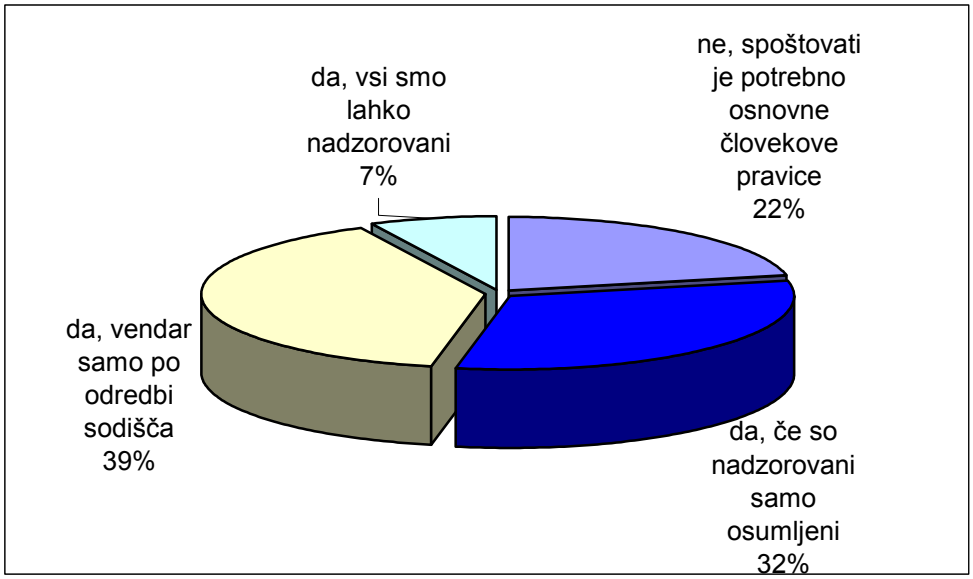
vir: anketa, vprašanje 15

Najbolj zaupanja vredne so po mnenju anketirancev banke (»zelo zaupam« in »zaupam« so odgovorili v 57%), državni upravi zaupa (55%), sledijo zdravstvene organizacije (45%) in zavarovalnice (4% »zelo zaupam« in 28% jih je odgovorilo z »zaupam«).

Najmanj zaupanja vredne so po mnenju anketiranih spletne trgovine (nihče od vprašanih jim ne »zelo zaupa«, le 10% pa jim »zaupa«. Spletne trgovine so dobile tudi največ odgovorov »ne zaupam« in sicer kar 55% vprašanih jim ne zaupa. Malo več zaupanja so deležni ponudniki internetnih storitev: 3% vprašanih jim »zelo zaupa«, 13% jim »zaupa«, 51% jim »malo zaupa« in 31% vprašanih jim »ne zaupa«.

Po 11. septembru 2001 se je zaradi preprečevanja terorizma »v imenu javne varnosti« v vseh državah povečal tudi nadzor »države nad državljani«. Evropska unija je sprejela direktivo v zvezi z ohranitvijo prometnih podatkov (elektronska pošta, telefon, mobilni telefon…), v potne liste se vpisujejo biometrične lastnosti, povečuje se video nadzor…
V zvezi z vse večjim nadzorom oblasti zaradi preprečevanja terorizma, me je v raziskavi zanimalo ali se uporabnikom interneta zdi potrebno, da smo za povečanje varnosti v tolikšni meri nadzorovani.

graf 17: Potrebnost nadzora »države nad državljani« po mnenju uporabnikov interneta



vir: anketa, vprašanje 16

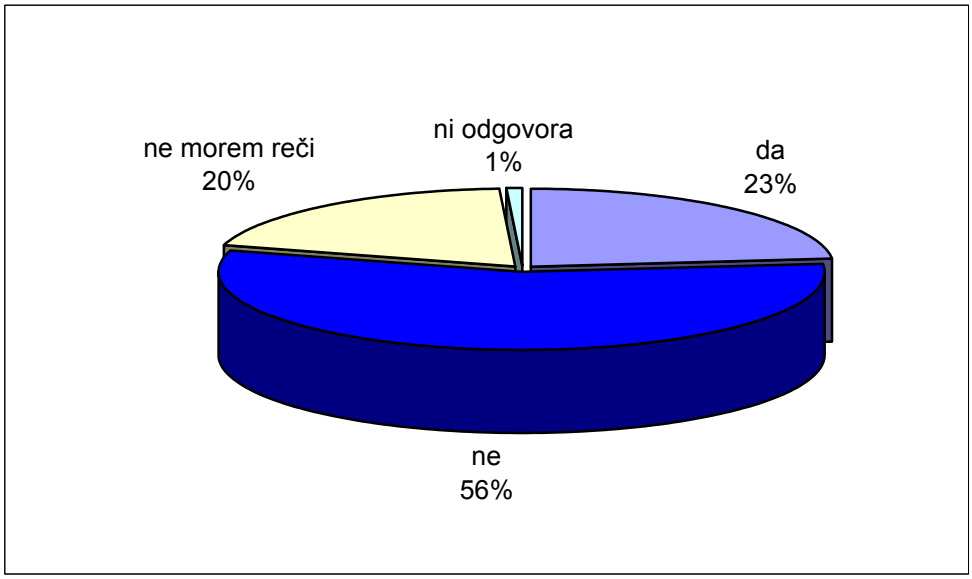
Največ vprašanih (40%) meni, da je nadzor sicer potreben, vendar samo po odredbi sodišča; 31% jih meni, da so lahko nadzorovani samo osumljeni; 21% vprašanih pa meni, da nadzor ni potreben, temveč je potrebno spoštovati človekove pravice. Brez omejitev smo lahko vsi nadzorovani meni 7% vprašanih, 1% pa jih na vprašanje ni odgovorilo.

6.4.4 Poznavanje in uporaba tehnologij za zaščito zasebnosti

Da omejimo nadzor ter zaščitimo našo zasebnost, lahko mnogo pripomoremo tudi uporabniki interneta sami s poznavanjem in uporabo orodij oziroma tehnologij za izboljšanje zasebnosti na internetu.
V raziskavi sem želela ugotoviti, ali poznamo in uporabljamo ustrezna orodja oziroma tehnologije za zaščito zasebnosti

Najprej me je zanimalo, če uporabniki interneta poznajo spletne objave o »Politiki podjetja glede varovanja zasebnosti in osebnih podatkov«.
Več kot polovica vprašanih (56%) je odgovorila, da spletnih objav o Politiki podjetja o zasebnosti ne poznajo, 20% pa je odgovorilo, da tega ne vedo.
Po anketi sodeč pozna spletne objave o »Politiko podjetja o varovanju zasebnosti« 23% uporabnikov interneta.

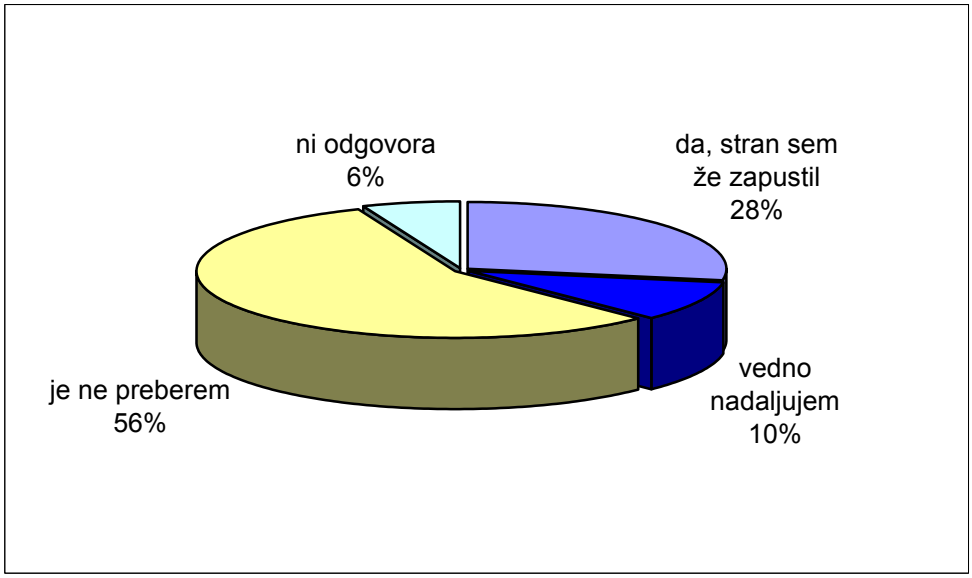
graf 18: Poznavanje spletne objave o Politiki podjetja glede zasebnosti



vir: anketa, vprašanje 17

Zaradi nestrinjanja s pogoji glede varovanja zasebnosti je 28% tistih, ki preberejo izjavo o zasebnosti spletno stran že kdaj zapustilo, 10% jih vedno nadaljuje, 56% vprašanih pa »Politike« oziroma izjave o zasebnosti ne prebere.

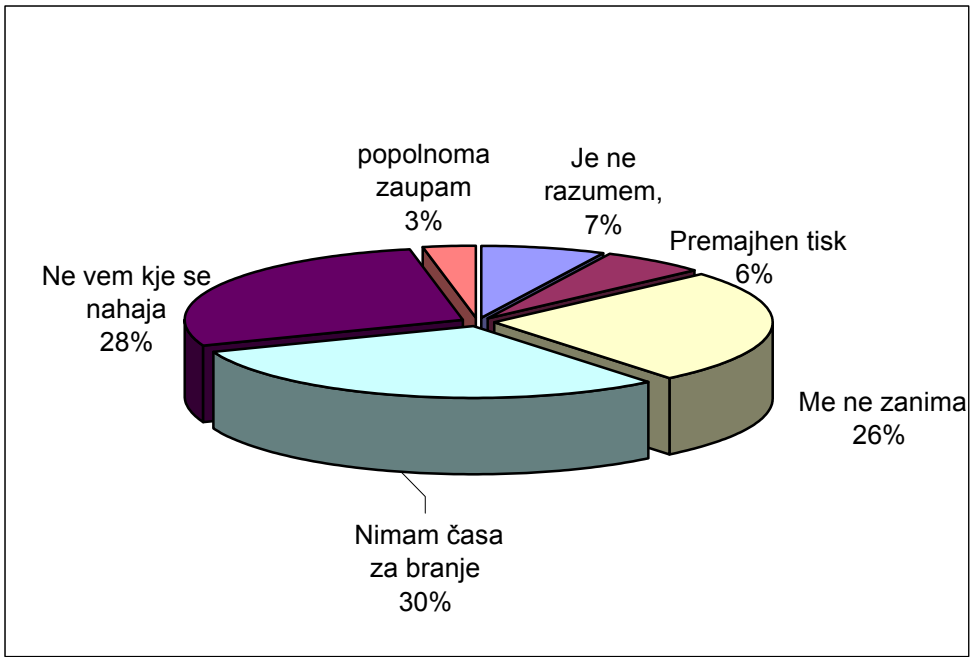
graf 19: Strinjanje s Politiko podjetja glede varovanja zasebnosti



vir: anketa, vprašanje 18

Na vprašanje zakaj uporabniki ne preberejo objav o varovanju zasebnosti na spletu, je bil najpogostejši odgovor, da nimajo časa za branje (30%), sledi odgovor, da ne vedo, kje se »Politika« nahaja (28%), 26% jih ne zanima, 7% jih je odgovorilo, da je ne razumejo, je nejasna, 6% je odgovorilo, da je ne preberejo zaradi premajhnega tiska, samo 3% pa so odgovorili, da strani popolnoma zaupajo.

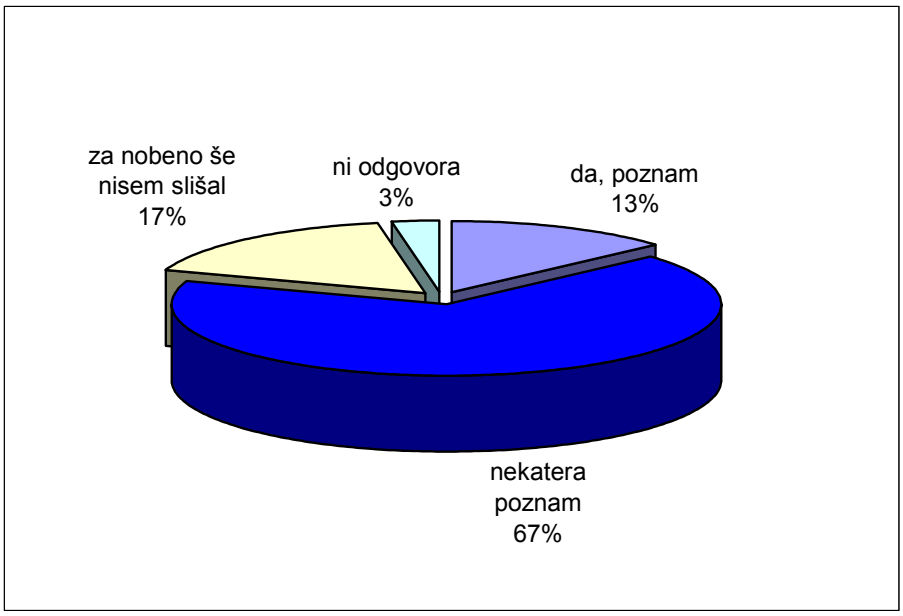
graf 20: Razlogi, da uporabniki ne berejo Politike o varovanju zasebnosti



vir: anketa, vprašanje 19

Glede poznavanja orodij oz. tehnologij za izboljšanje zasebnosti na internetu, je samo 13% vprašanih je odgovorilo, da ta orodja poznajo.
67% vprašanih je odgovorilo, da poznajo nekatera orodja, oziroma so zanje že slišali.
Za nobeno orodje še niso slišali, je odgovorilo 17% vprašanih, 3% pa na vprašanje ni dalo odgovora.

graf 21: Poznavanje orodij oziroma tehnologij za zaščito zasebnosti

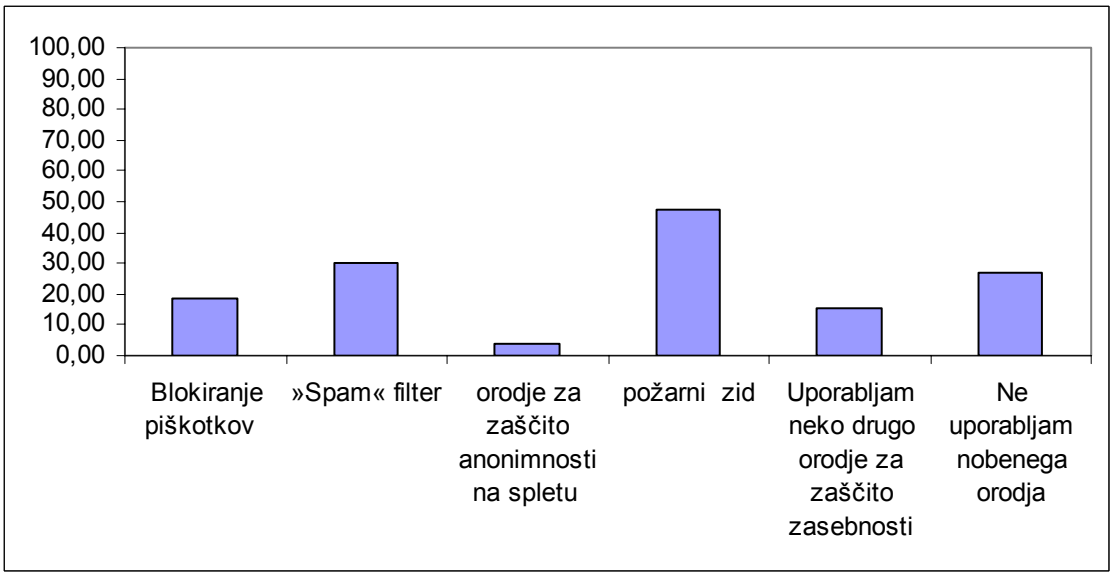


vir: anketa, vprašanje 20

Na vprašanje ali uporabljajo katero od orodij za zaščito zasebnosti na internetu, je 73% vprašanih odgovorilo, da uporabljajo vsaj eno orodje, 27% uporabnikov pa ne uporablja nobene zaščite.

Največ anketirancev uporablja požarni zid (47%), filter za preprečevanje neželene pošte (»spam filter«) uporablja 30% vprašanih, blokiranje piškotkov uporablja 19% vprašanih, orodje za zaščito anonimnosti uporablja 6% vprašanih, 15% pa jih je odgovorilo, da uporabljajo neko drugo orodje za zaščito zasebnosti.

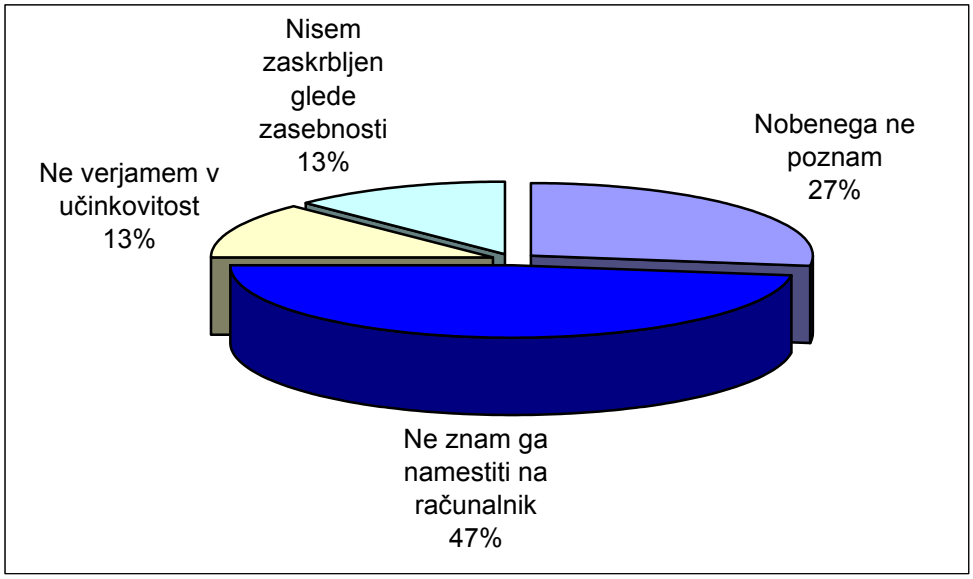
graf 22: Prikaz uporabe orodij za zaščito zasebnosti v odstotkih



vir: anketa, vprašanje 21

Na vprašanje zakaj ne uporabljajo nobenega orodja (odgovarjali so samo tisti, ki ne uporabljajo ničesar), je bil najpogostejši odgovor, da ga ne znajo namestit na računalnik (48%), da nobenega ne poznajo je odgovorilo 27% vprašanih, 13% jih ne verjame v učinkovitost orodij za zaščito zasebnosti, 13% pa je odgovorilo, da niso zaskrbljeni glede zasebnosti.

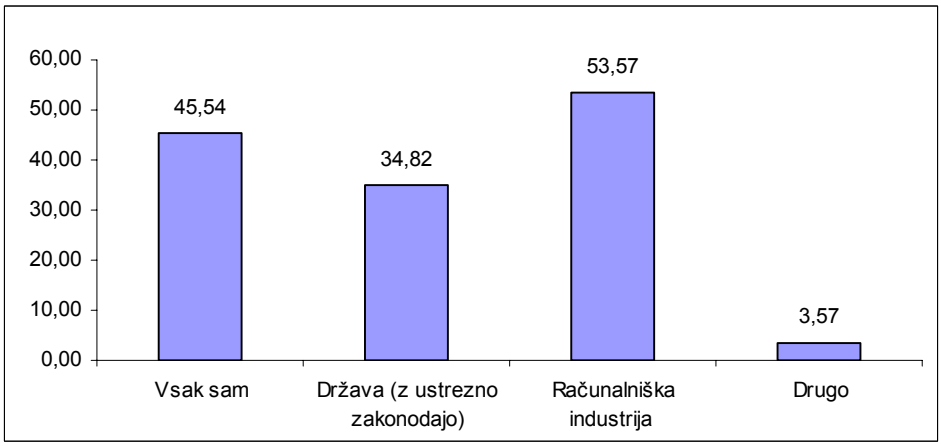
graf 23: Razlogi za »ne uporabo« orodij za zaščito zasebnosti



vir: anketa, vprašanje 22

Na vprašanje kdo je odgovoren za izboljšanje zaščite zasebnosti, so vprašani največkrat odgovorili, da je to računalniška industrija z ustrezno programsko podporo (54%). Da je tudi vsak sam odgovoren za zaščito lastne zasebnosti so menili v 46%, 35% vprašanih pa je menilo, da mora za zaščito zasebnosti svojih državljanov poskrbeti država z ustrezno zakonodajo. 4% so odgovorili, da je še nekdo drug odgovoren za zaščito zasebnosti na internetu (po mnenju vprašanih naj bi to bil tudi ponudnik internetnih storitev).

graf 24: Kdo je po mnenju uporabnikov interneta odgovoren za zaščito zasebnosti



vir: anketa, vprašanje 23

6.5 Ugotovitve raziskave:

Iz raziskave lahko povzamemo, da je slovenskim uporabnikom interneta zasebnost pomembna. Ne izražajo sicer neke panične zaskrbljenosti glede varovanja zasebnosti, saj jih je polovica odgovorila, da so do neke mere zaskrbljeni glede varovanja zasebnosti, 42 odstotkov vprašanih je glede varovanja zasebnosti zaskrbljenih, le 7 odstotkov vprašanih pa je odgovorilo, da jih zasebnost ne skrbi. Večina želi vedeti, kaj kdo o njih zbira in zakaj bo podatke uporabil. Kar 87 odstotkov vprašanih je odgovorilo, da jim je pomembno, da vedo, kateri njihovi podatki se zbirajo in v kakšen namen in samo 3 odstotkom vprašanih to ni pomembno. V primerjavo navajamo podatke iz raziskave HarrisInteractive raziskovalnega centra, ki so jo opravili marca 2003. Rezultati so pokazali, da se 69 odstotkom Američanov zdi zelo pomembno, da imajo nadzor nad zbiranjem podatkov, 24 odstotkom je to pomembno do neke mere, medtem ko jih 7 odstotkov ne zanima, katere podatke o njih zbirajo (Taylor, 2003).

Zakonodajo o varovanju podatkov uporabniki interneta poznajo samo okvirno, vendar se zavedajo svojih osnovnih pravic. 79 odstotkov uporabnikov ve, da lahko organizacije zbirajo osebne podatke samo z njihovim pristankom. Osebnih podatkov na internetu ne razkrijejo radi. Najbolj čuvajo številke kreditnih kartic, bančnega računa, podatke o svojem zdravju, EMŠO, največkrat pa razkrijejo ime in priimek ter elektronski naslov. Po raziskavi sodeč, v zameno za kakšno ugodnost, vse prepogosto puščamo svoje podatke. Samo 8 odstotkov vprašanih nikoli ne posreduje svojih osebnih podatkov v zameno za kakšno boniteto, 28 odstotkov vprašanih to radi storijo, večina vprašanih (60 odstotkov) pa tega sicer ne počnejo radi, vendar včasih tudi razkrijejo svoje osebne podatke v zameno za kakšno nagrado. Do podobnih ugotovitev so prišli tudi v raziskavi »Online« zasebnost Američanov, ki so jo opravili na Univerzi v Pensilvaniji, junija 2003, kjer so ugotovili, da 21 odstotkov Američanov rado zamenja podatke za kakšno ugodnost, 16 odstotkov pa posreduje svoje podatke samo proti plačilu (Turow, 2003).
Kljub temu, da slovenski uporabniki interneta dokaj radi puščajo svoje podatke na internetu (predvsem, če v zameno kaj dobijo), so glede kasnejše rabe teh podatkov zaskrbljeni. Kar 83 odstotkov uporabnikov je odgovorilo, da so zaskrbljeni glede možnosti posredovanja njihovih podatkov v reklamne namene, zavarovalnicam, državnim ustanovam… V raziskavi Eurobarometer 46.1 leta 1996, je 72 odstotkov Evropejcev izrazilo zaskrbljenost glede posredovanja njihovih osebnih podatkov tretjim osebam.

Slovenski uporabniki interneta so zelo dobro poučeni glede groženj zasebnosti, ki jih prinaša internet. Da je možno prestreči elektronsko pošto, ukrasti gesla, številke kreditnih kartic, ugotoviti katere spletne strani obiskujejo, ugotoviti IP naslov računalnika, ve preko 80 odstotkov uporabnikov. Malo manj verjetno se jim zdi, da je možno ugotoviti geografsko lokacijo uporabnika. Zaskrbljujoče pa je dejstvo, da se zdi uporabnikom interneta zelo malo verjetno, da je možno preko spleta ugotoviti celo njihovo fizično identiteto. Rezultati kažejo na slabo poučenost uporabnikov o delovanju interneta.

Najbolj zaupanja vredne organizacije so po mnenju uporabnikov interneta banke, državna uprava ter zdravstvene organizacije, najmanj pa spletne trgovine in ponudniki spletnih storitev. Bankam zaupa 57 odstotkov uporabnikov, spletnim trgovinam pa le 10.

Uporabniki interneta se zavedajo nevarnosti nadzora države nad državljani zaradi zagotovitve javne varnosti. Dve tretjini vprašanih meni, da je potrebno spoštovati osnovne človekove pravice ter nadzorovati osumljence samo po odredbi sodišča.

Za zagotovitev zasebnosti lahko največ storijo uporabniki sami z večjo osveščenostjo. Kar 56 odstotkov vprašanih je odgovorilo, da izjave o varovanju zasebnosti, ki jih objavljajo spletne strani, ne preberejo. Najpogostejši razlog za »nebranje« je po navedbah vprašanih pomanjkanje časa, 28 odstotkov jih ne ve, kje imajo spletne strani objavljene svoje »zasebnostne izjave«, ali pa jih to sploh ne zanima, le 3 odstotki vprašanih pa je odgovorilo, da spletni strani popolnoma zaupajo.

Tehnologije in mehanizme za izboljšanje zasebnosti na internetu uporabniki interneta slabo poznajo. Samo 13 odstotkov vprašanih je odgovorilo, da poznajo orodja za zboljšanje zasebnosti, dve tretjini vprašanih je odgovorilo, da poznajo nekatera izmed orodij.
Največ uporabnikov uporablja požarni zid (47 odstotkov), filter za preprečevanje neželene pošte uporablja 30 odstotkov vprašanih, piškotke jih blokira 19 odstotkov, anonimnosti pa se poslužuje le 6 odstotkov uporabnikov interneta. Raziskava »Online« zasebnost Američanov, iz junija 2003, je pokazala, da Američani v večji meri uporabljajo orodja za zaščito zasebnosti, kot Slovenci: 65 odstotkov jih blokira piškotke, 43 odstotkov jih uporablja filtre za preprečevanje neželene pošte, 17 odstotkov pa jih uporablja orodja za dosego anonimnosti (Turow, 2003).

Odgovornost za zaščito zasebnosti je več kot polovica uporabnikov prepustila računalniški industriji. Skoraj polovica uporabnikov pa meni, da je tudi vsak sam odgovoren za zaščito lastne zasebnosti. Država je tista, ki mora poskrbeti za zasebnost uporabnikov interneta z ustrezno zakonodajo, meni dobra tretjina vprašanih.

Raziskava potrjuje hipotezo, ki sem jo postavila na začetku naloge, da je uporabnikom interneta zasebnost pomembna, zavedajo se groženj interneta, vendar pa premalo poznajo in uporabljajo tehnologije in mehanizme za zaščito zasebnosti.

7 SKLEP

Internet postaja nepogrešljiv del vsakdana, posega v vse sfere našega življenja, tako zasebnega kot poslovnega. Nepregledno število e-projektov se izvaja doma in v svetu, s tem pa nezadržno naraščajo tudi potencialne kršitve zasebnosti potrošnikov in državljanov.

Da se lahko uspešno spoprimemo s problemom ogroženosti zasebnosti, je potrebno najprej ugotoviti, kaj pravzaprav je zasebnost in kaj jo ogroža.
Večina modernih definicij ugotavlja, da je zasebnost osnovna človekova pravica. Pomeni pravico vsakogar, da ostane sam, če tako želi, da se sam odločiti komu in katere podatke o sebi bo posredoval, da bo imel nadzor nad zbiranjem in obdelavo njemu lastnih osebnih podatkov in da bo lahko te podatke popravil ali zbrisal, če bo to želel.
Za zagotovitev zasebnosti je pomembno predvsem **biti informiran in sam se odločiti.**

Globalizacija in integracija informacijsko komunikacijskih tehnologij v vsakodnevno življenje prinašata mnogo ugodnosti in priložnosti, hkrati pa tudi veliko tveganje za našo zasebnost in osebne podatke. Internet omogoča zbiranje velikanskega števila podatkov, tudi osebnih. S sodobnimi tehnologijami lahko nepovezane podatke združujejo, predelujejo ter ustvarjajo povsem nove baze podatkov, ki jih uporabljajo v druge namene, kot pa so bili prvotno zbrani. Večinoma se to dogaja brez vednosti in privolitve posameznika, na katerega se podatki nanašajo.
Zbiranje in povezovanje podatkov, sledenje, video nadzor, profiliranje, rudarjenje, nadlegovanje preko elektronske pošte, uporaba biometričnih metod in radio frekvenčnih identifikacijskih tehnologij (RFID) so grožnje, ki jih moramo spoznati, se z njimi soočiti ter jih sprejeti kot neizbežno dejstvo, šele nato se jih bomo lahko tudi uspešno ubranili.

Različne mednarodne institucije si prizadevajo zajeziti val poseganja v zasebnost ljudi in zaščititi potrošnike in državljane pred nedovoljenimi posegi v zasebnost. Pomembno vlogo pri tem imajo tudi države s svojo politiko ter ustrezno zakonodajo glede človekovih pravic in varovanja podatkov. Zakonodaja mora uravnotežiti dva interesa: prost pretok podatkov (informacij) na eni strani ter spoštovanje zasebnosti posameznika na drugi strani.
Z razvojem informacijskih tehnologij so se tako pojavili tudi prvi zakoni v zvezi z zaščito zasebnosti. Zaradi globalizacije informacijske izmenjave pa je pomemben razvoj mednarodnih meril oziroma principov varovanja podatkov in zasebnosti.
Direktiva Evropske unije o zaščiti podatkov DPD 95/46/ES zahteva od upravljavcev osebnih podatkov implementacijo takšne tehnologije, ki bo zaščitila osebne podatke pred uničenjem, izgubo, zlorabo in nedovoljenim dostopom. Pri tem je potrebno razlikovati pojma varnost in zasebnost, ki ju mnogokrat kar enačimo. Res je, da sta varnost in zasebnost dostikrat povezana, se prekrivata, velikokrat pa prihaja tudi do nasprotij - predvsem pri pojmovanju skupinske varnosti in individualne zasebnosti. Za dosego skupinske varnosti je lahko ogrožena zasebnost posameznika. To se dogaja predvsem po

11. septembru 2001, ko se je v imenu javne varnosti povečal in se še povečuje nadzor države nad državljani.
Pri kreiranju novih tehnologij je potrebno pozornost usmeriti ne le na varnost podatkov, temveč tudi na varovanje zasebnosti in zaupnost podatkov. To vrsto tehnologij imenujemo tehnologije za izboljšanje zasebnosti ali krajše PET.
S pomočjo te tehnologije naj bi vpeljali osnovne principe zasebnosti v zakonito obdelavo podatkov. PET predstavljajo velik potencial v zaščiti zasebnosti, vendar le v sodelovanju z osveščanjem in izobraževanjem uporabnikov in IT strokovnjakov, promoviranjem ter ustrezno zakonodajo.
Kot so zapisali na CEN/ISSS Data protection and privacy workshop, ni edini problem kako kreirati tehnologije, da bodo resnično varovale zasebnost, kot take jih morajo prepoznati in sprejeti tudi uporabniki. Postati morajo uporabniku prijazne in enostavne za uporabo. Kajti poleg zakonodaje, smo tudi sami dolžni poskrbeti za našo zasebnost. To bomo dosegli predvsem z večjo osveščenostjo ter uporabo tehnologij za izboljšanje zasebnosti.

Programi in orodja za zaščito zasebnosti niso ravno popularni med uporabniki interneta. Iz raziskave je razvidno, da se jih le ti ne poslužujejo prav pogosto. Uporabljajo predvsem orodja za blokiranje kolačkov, filtre neželene pošte ter požarne zidove, medtem ko so tehnologije za dosego anonimnosti na spletu povsem neznane. Temu je v veliki meri krivo tako nepoznavanje orodij, kot tudi njihova okorelost. Orodja za izboljšanje zaščite zasebnosti bi morala biti bolj prilagojena potrebam povprečnega uporabnika. Z enostavnim pritiskom na gumb bi morali doseči anonimnost ter tako zaščititi svojo zasebnost. Tehnologije je potrebno vključiti v ostale aplikacije na način, da uporabniku ne bo potrebno storiti ničesar, da se ne bo niti zavedal, da uporablja programe za zaščito zasebnosti, hkrati pa mora biti storitev brezplačna ter tako dostopna širši javnosti. Vsakomur je potrebno omogočiti, anonimno brskanje po spletu, iskanje občutljivih informacij, anonimnost dostopa do različnih storitev...
Zavzeti je potrebno takšne ukrepe oziroma spremeniti mišljenje pri načrtovanju novih sistemov, da bodo le ti zagotovili učinkovito in zmogljivo rabo brez razkritja uporabnikove identitete. Identiteta ni nujno potrebna za vse korake znotraj podatkovnega sistema, mnogokrat je za dobro delovanje sistema povsem nepomembna. V primeru, ko pa je identiteta uporabnika, potrošnika ali državljana potrebna, jo moramo ustrezno zaščititi.

Seveda tehnološki napredek oziroma razvoj tehnologij in ustrezna zakonodaja še nista zadosten pogoj za zaščito naše zasebnosti. Zelo pomembna je tudi poučenost in osveščenost uporabnikov storitev, le tako bodo tudi uporabniki sami pripomogli k boljši zaščiti zasebnosti ter manjšemu nadzoru.

Uporabniki interneta velikokrat čisto zavestno in prostovoljno izdajajo svoje osebne podatke. Včasih res nimajo izbire - če želijo priti do določene vsebine, se pač odločijo za razkritje - velikokrat pa razkrijejo podatke zgolj za kakšno majhno ugodnost, kakšno nagrado ali popust pri nakupu.

Svoje podatke uporabniki razkrivajo tudi nehote, neprostovoljno. Do tega prihaja predvsem s sodelovanjem v različnih forumih in spletnih klepetalnicah, kjer se uporabniki niti ne zavedajo, da izdajajo tudi osebne podatke, ki se nekje beležijo in lahko ostanejo zapisani in dostopni še mnoga leta.
Uporabniki so različni, nekateri bi za najmanjšo ugodnost takoj razkrili svoje ime, svoj elektronski naslov, skoraj vse osebne podatke, spet drugi želijo anonimnost, uporabljajo ponovne pošiljatelje, blokirajo kolačke.
Pomembno je, da so uporabniki obveščeni, da vedo kaj kdo o njih zbira, zakaj in kaj počne s temi podatki in imeti morajo možnost izbire: bodo podatke razkrili »opt in« ali pa bodo iz sistema iztopili »opt out«.

Na podlagi večletnih raziskav iz tujine je razvidno, da skrb oziroma zavest o varovanju zasebnosti med uporabniki spleta narašča. Tudi raziskava, ki sem jo opravila v okviru empiričnega dela naloge, je pokazala, da je slovenskim uporabnikom interneta zasebnost pomembna, vedeti želijo kaj kdo o njih zbira in zakaj uporablja njihove osebne podatke, zavedajo se groženj zasebnosti, vendar zelo malo uporabljajo ustrezno zaščito. Zavestno ne razkrivajo prav radi svojih podatkov, predvsem skrbno varujejo podatke o kreditnih karticah, bančnih računih, matični številki ter podatke o zdravju. Največkrat pa posredujejo svoje ime ter elektronski naslov.
Izjav o zasebnosti, ki jo objavljajo ponudniki storitev na svojih straneh, slovenski uporabniki skoraj ne berejo. Večina odgovorov zakaj spletne izjave o varovanju zasebnosti ne berejo, je bil, da nimajo časa za branje, veliko pa jih niti ne ve, kje se spletne izjave nahajajo. Politika podjetij glede varovanja zasebnosti je ponavadi skrita nekje na robu, zapisana je nerazumljivo in z drobnim tiskom. Podjetja bi morala jasno in razvidno označiti na spletni strani svojo politiko glede varovanja zasebnosti uporabnikov. Vsebino izjav bi z mednarodnimi instrumenti morali poenotiti ter doseči, da bi jih tudi spoštovali. Spletne izjave o varovanju zasebnosti bi morale vsebovale:

- katere osebne podatke zbirajo in v kakšen namen
- kdo ima dostop do teh podatkov in komu so razkriti
- kako so varovani
- koliko časa jih obdržijo
- osebo, ki je odgovorna za ravnanje s podatki in dajanje informacij

Raziskava je pokazala tudi, da uporabniki najmanj zaupajo spletnim trgovinam, komaj 10 odstotkov uporabnikov je odgovorilo, da jim »*zaupa*«, nihče pa jim ne »*zelo zaupa*«. Najbolj zaupanja so uporabniki izkazali bankam ter državnim ustanovam, vendar tudi njim zaupa komaj polovica uporabnikov.
Problem elektronskega poslovanja je prav gotovo tudi v zaupanju uporabnikov do elektronskih storitev. Zaupanje bomo dosegli le z jasno in razumljivo politiko varovanja osebnih podatkov in s tem zasebnosti uporabnikov.

Kot sem zapisala že na začetku: internet in sodobne komunikacijske tehnologije prinašajo mnogo prednosti in ugodnosti v vsakodnevno življenje, hkrati pa nam prinašajo tudi mnogo pasti, ki se jih bomo ognili le z dobro poučenostjo in osveščenostjo. Seznaniti se moramo z nevarnostmi, ki nam pretijo ter z možnostmi kako se jih ubraniti. Tradicionalne varnostne tehnike niso dovolj za zagotovitev zasebnosti. Potrebna je večja promocija mehanizmov za zaščito zasebnosti od zakonodaje do ustreznih tehnologij (PET), ki jih je potrebno upoštevati že ob načrtovanju novih informacijskih sistemov.

8 LITERATURA IN VIRI

8.1 Literatura

1. Agrawal Dakshi, Kesdogan Dogan: Measuring Anonymity: The Disclosure Attack. New York: IEEE Security&Privacy, November/December 2003. str. 27 – 34
2. An Introduction to cryptography. Palo Alto: PGP Corporation, 2003. 74 str.
3. Bainbridge William Sims: Privacy and Property on the Net: Research Questions. Science, New York:302, December 2003. str. 1686 – 1687
4. Bennett J. Colin: What Governmen Should Know about Privacy. Victoria: Department of Political Science University of Victoria, 2001. 24 str.
5. Blarkom et. al.: Handbook of Privacy and Privacy-Enhancing Technologies. The case of Intelligent Software Agents. Haag: PISA Consortium, 2003. 372 str.
6. Borking J., Raab C.: Laws, PETs and Other Technologies for Privacy Protection. The Journal of Information. Law and Technology, Coventry, februar 2001. 16 str.
7. Borking John: The PET story: Privacy Enhancing Technology online and offline. Sydney: 25. konferenca komisarjev za varovanje podatkov in zasebnosti, 2003. 33 str.
8. Cavoukian Ann, Gurski Mike: Managing privacy a challange in designing today`s systems. Toronto: Municipal Interface, 2000. 3 str.
9. Clarke Roger: Introduction to Dataveillance and Information Privacy, and Definitions of Terms. [URL http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html], 21.10.2005
10. Clarke Ian, et al.: Protecting Free Expression Online with Freenet. New York: Institute of Electrical and Electronics Engineers, 2002. str. 40 – 49
11. Cranor Lorrie Faith: Privacy Tools Overview. New Jersey: AT&T Labs-Research, 2000. 13 str.
12. Cranor Lorrie Faith: P3P: Making Privacy Policies More Useful, IEEE Security & Privacy, New York, November/December 2003, str. 50 – 54
13. Cranor Lorrie Faith: »I didn`t buy it for myself«.Washington: ACM Workshop on Privacy in the Electronic Society (WPES), 2003. 16 str.
14. Cranor Lorrie Faith: The role of Privacy Enhancing Technologies. Considering Consumer Privacy. Washington: Center for democracy and technology, 2003. str. 80 - 83
15. Crompton Malcom: Under the Gaze, Privacy Identity and New Technology. Sydney: International Association of Lawyers, 75th Anniversary Congress, 2002. 27 str.
16. Cavoukian Ann: Data Mining: Staking a Claim on your Privacy. Toronto: The Information and privacy commissioner Ontario,1998. 25 str.
17. Čebulj Janez: Varstvo informacijske zasebnosti v Evropi in Sloveniji. Ljubljana: Inštitut za javno upravo pri Pravni fakulteti v Ljubljani, 1992. 74 str.
18. Dhont Jan at al.: Safe Harbour Decision Implementation Study. Namur: European Commission, Internal Market, 2004. 263 str.
19. Diaz Claudia, Preneel Bart: Accountable Anonymous Communication Infrastructure. Leuven-Heverlee, Belgium: Dept. Electrical Engineering – ESAT/COSIC, 2005. 20 str.

20. Dodig – Crnkovič Gordana, Horniak Virginia: Good to Have Someone Watching Us from a Distance: Privacy vs. Security at the Workplace. Enschede: theSixth International Conference of Computer Ethics CEPE, 2005. 10 str.
21. Gindin Susan: Lost and Found in Cyberspace: Informational Privacy in the Age of Internet. San Diego: Law Review, 34, 1997. [URL:http//www.info-law.com/lost.html]
22. Goldberg Ian, Wagner David, Brewer Eric: Privacy-Enhancing Technologies for the Internet. Berkeley: University of California, 1997. 16 str.
23. Goldberg Ian: Privacy –Enhancing Technologies for the Internet, II: Five years later. San Francisco: Workshop on Privacy Enhancing Technologies, 2002. 17 str.
24. Graham Ian: Putting Privacy in Context: An overview of the Concept of Privacy and of Current Technologies. Toronto: Centre for Academic Technology Information Commons University of Toronto, 1999. 19 str.
25. Horniak Virginia, Privacy of Communication – Ethics and Technology. Master thesis. Vasteras: Department of Computer Science and Engineering Malardalen University, 2004. 67 str.
26. Hinde Stephen: 2001: A Privacy Odyssey Revisited. Computer&Security, 1, 2002, str. 16 – 34
27. Hinde Stephen: The perils of privacy. Computer&Security, 5, 2002, str. 424 – 432
28. Huizenga Jan: Roadmap for Advanced Research in Privacy and Identity Management, Deliverable RD 3.0, Overall Roadmap 'Privacy and Identity Management' Final Report, 2003. 61 str.
29. Jerman Blažič Borka at al.:Elektronsko poslovanje na internetu. Ljubljana: Gospodarski vestnik, 2001. 206 str.
30. Kovačič Matej: Zasebnost v informacijski družbi. Teorija in praksa, Ljubljana, 37, (2000), 6, str.1019-1034
31. Kovačič Matej: Zasebnost na internetu. Ljubljana: Mirovni inštitut, Inštitut za sodobne družbene in politične študije, 2003. 111 str.
32. Kovačič Matej: Mehanizmi varovanja v zasebni družbi. [URL: http://www.ljudmila.org/matej/zasebnost/zasebnost.html], 27.8.2004
33.Kercan Vojko: Sistemi in metode za zagotovitev zasebnosti na internetu. Diplomsko delo. Ljubljana: Ekonomska fakulteta, 2003. 66 str.
34. Mead Nancy R.: Who is Liable for insecure Sysems? IEEE, Computer, julij 2004. str. 27 – 33
35. Možina Damjan: Se Evropa odreka zasebnosti v korist varnosti. Pravna praksa 21 (2002), št. 43, priloga Informatika in pravo, (1/2002). str. III – V
36. Ocvirk Vasja: Veliki brat ali grešni kozel. Moj mikro, Ljubljana, november 2003. str. 54 – 58
37. Provos Niels, Honeyman Peter: Hide and Seek: An Introduction to Steganography. IEEE Security & Privacy, New York, maj/junij 2003. str. 32 – 44.

38. Raab Charles D.: The future of privacy protection. Cyber Trust & Crime Prevention Project. Edinburgh University, 2004. 22 str.
39. Riley Thomas B.: Security vs. Privacy: A comparative analysis of Canada, The United Kingdom, and The United States. Ottawa: Riley Information Services Inc., 2004. 43 str.
40. Reiter K. Michael, Aviel D. Rubin: Crowds: Anonimity for Web Transactions. ACM Transactions on Information and System Security, New York, November 1998. str. 66-92
41. Rezgui Abdelmounaam, Bouguettaya Athman, Eltoweissy Mohamed: Privacy on the web: Facts, Challenges and Solutions. IEEE Security&Privacy, November/December 2003. str. 40 – 49
42. Seigneur Jean Marc, Damsgaard Jensen Cristian: Privacy Recovery with Disposable Email Addresses. IEEE Security&Privacy, New York, November/December 2003. str. 35 – 39
43. Seničar Vanja, Jerman Blažič Borka, Klobučar Tomaž: Privacy Enhancing Technologies - approaches and development. Ljubljana: Laboratory for Open Systems and Networks, Inštitut Jožef Štefan, 2003. 19 str.
44. Song, R., Korba, L.: Anonymous Internet Infrastructure Based on PISA Agents. Ottawa: National Research Council of Canada, 2001. 23 str.
45. Tavani , Herman T.: Privacy and the Internet. B.k.: 2000. 23 str. [URL: http://www.bc.edu/bc_org/avp/law/st_org/iptf/commentary/content/2000041901.html]
46. Whitworth Brian, Whitworth Elizabeth: Spam and the Social-Technical Gap. IEEE, Computer, October 2004. str. 38 – 45
47. Webb Philippa: A Comparative Analysis of Data Protection Laws in Australia and Germany. Journal of Information. Law and Technology, Coventry, december 2003. 22 str.

8.2 Viri

1. Anonymizer. [URL: http://www.anonymizer.com/],12.1.2006
2. Cavoukian Ann: Preserving Privacy and Security. Toronto: prosojnice, 2005. [URL: http://www.ipc.on.ca/docs/2005-03-01-ImperialOil.ppt], 14.10.2005
3. CEN/ISSS Data protection and privacy workshop: Final version of CWA for Public Enqury-Work area C2: Technology Impact Analysis, October 2004. 35 str.
4. Clarke Ian: The Philosophy behind Freenet. [URL:http://www.freenet.sourceforge.net/index.php?page=philosophy], 6.10.2005
5. CRS Report: Data mining an overview. B.k. 2004. 16. str. [URL: http://www.fas.org/sgp/crs/intel/RL31798.pdf], 6.10.2005
6. Delaney Kevin J.: Identity Theft Made Easier. Wall Street Journal on line, March 29. 2005. [URL: http://online.wsj.com/article/0,,SB111205677536691444-search.html?collection=wsjie%2F30day&vql_string=Identity+Theft%3Cin%3E%28article%2Dbody%29]

7. Direktiva 95/46/ES Evropskega parlamenta in sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov. Luksemburg, 24. oktobra 1995
8. Direktiva 97/66/ES Evropskega parlamenta in sveta o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij. (Official Journal of the European Communities L 24/1 30.1.98)
9. Direktiva 2002/58/ES Evropskega parlamenta in Sveta o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij. Bruselj, 12. julija 2002. (Official Journal L 201, 31/07/2002 P.0037 – 0047)
10. EPIC.[URL: http://www.epic.org/privacy], 8.11.2004
11. EPIC. Privacy and Consumer Profiling.
[URL: http://www.epic.org/privacy/profiling/], 10.2.2006
12. Escudero – Pascual Alberto: Analysis of Carnivore »Lawful Interception System to fight Crime. Kista: Institutet for Informationteknologi, 2001, 24 str.
13. Eurobarometer 46.1. Koln. Zentralarchiv fur Empirische Sozialforschung an der Universitat zu Koln, 2000. 387 str
14. e- europe 2003, Final Progress Report, European Ministerial Conference on the Information Society. Budapest, Februar, 2004. 47str.
15. Fischer-Hübner Simone: Privacy Enhancing Technologies. 2001, Karlstad: Department of Computer Science, Karlstad University, prosojnice, 2001. 147 str.
16. Fox Susannah: Trust and privacy online: Why Americans want to rewrite the rules. Washington: The Pew Internet & American Life Project, 2000. 29 str.
17. International Safe Harbor Privacy Principles.
[URL: http://ita.doc.gov/td/ecom/shprin.html],19.4.1999
18. GUIDES Project: Final Report. Joint Research Centre-PricewaterhouseCooopers. April 2002. 10 str.
19. Kovačič Matej, Vehovar Vasja: Slovenski uporabniki interneta in zasebnost. [URL: http://www.ljudmila.org/matej/privacy/vsebina/odnos.html], 18.4.2005
20. McCullagh Declan: »Carnivore gone - but it's not dead«. ZDNet News, 31. januar 2005
21. New Yorker magazin. New York, 5.7.1993.
22. PAMPAS [URL http://www.pampas.eu.org], 21.6.2005
23. Pretty Poor Privacy:An Assessment of P3P and Internet Privacy. [URL: http://www.epic.org/Reports/prettypoorprivacy.html], 23.3.2006
24. PRIME Privacy and Identity Management for Europe. [URL: http://www.prime-project.eu.org/], 19.5.2005
25. Privacy Act 1988: Canberra. Office of Legislative Drafting and Publishing, Attorney-General's Department. [URL: http://www.privacy.gov.au/act/], november 2005
26.Privacy and Human Rights Report 1999. [URL: http://www.privacy.org/pi/survey/]
27. Privacy and Human Rights Report, 2004. [URL:
http://www.privacyinternational/survey/]

28. Privacy in Cyberspace: Rules of the Road for the Information Superhighway. [URL: http://www.privacyrights.org/fs/fs18-cyb.htm], 8.6.2005
29. Privacy Incorporate Software Agent (PISA). [URL:http://petpisa.openspace.nl/pisa_org/pisa/pisa_project_aim.html]. 20.6.2005
30.Protecting Privacy and Fighting Spam, [URL: http://europa.eu.int/information_society/doc/factsheets/024-privacy-and-spam-en.pdf], 3.2.2006
31. Raba interneta v Sloveniji. [URL: http://www.ris.org/main/rubrika3/readrub3.php?sid=170&m2w=Tuje%20raziskave%20-%20arhiv], 30.1.2006
32. Silenced: an international report on censorship and control of the internet. Privacy International and GreenNet Education Trust, 2003, 23 str. [URL: http://www.privacyinternational.org/survey/censorship/Silenced.pdf]
33. Special Eurobarometer: Data protection, december 2003. [URL: http://europa.eu.int/comm/public_opinion/archives/ebs/ebs_196_data_protection.pdf]
34. Steganografija ali kako nevidno kodirati sporočila. [URL: http://www.ljudmila.org/matej/privacy/kripto/stego.html], 15.1.2006
35. Task Force on Spam: Anti spam law enforcement report. Pariz: OECD, 2005. 32 str.
36. The protection of personal data and privacy in a globalised world: a universal right respecting diversities. Montreux: september 2005. [URL:http//www.datenschutz-berlin.de/doc/int/iwgdpt/tc_en.htm]
37. Taylor Humphrey: Most People Are »Privacy Pragmatists« Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits., HarrisInteractiv, Inc., marec 2003. [URL:http://www.harrisinteractive.com/harris_poll/printerfriend/index.asp?PID=365]
38. The Free Network Project. [URL:http://freenet.sourceforge.net/], 14.5.2005
39. Turow Joseph: Americans and Online Privacy:The System is Broken. Philadelphia: Annenberg Public Policy Center of the University of Pennsylvania, 2003. 37 str.
40. [URL: http://www.privacyrights.org/fs/fs11-pub.htm], 16.9.2005
41. [URL: http://laws.justice.gc.ca/en/P-8.6/index.html], 16.9.2005
42. Working party on cooperation in criminal matters. Brussels: Council of the European union, 24. February 2005. 11 str.
43. Working party: Privacy online: policy and practical guidance. Paris: OECD, 21. Jan. 2003. 20 str.
44. Zakon o varstvu osebnih podatkov (Uradni list RS, št.86/2004)
45. Zakon o elektronskih komunikacijah (Uradni list RS, št.43/2004)

9 SLOVAR KRATIC IN TUJIH IZRAZOV

Biometrija		zbiranje, obdelovanje in shranjevanje podatkov o posameznikovih fizičnih lastnostih za potrebe identifikacije
Blind digital signature		slepi digitalni podpis
Carnivore		sistem za nadzor elektronskih komunikacij
Chattroom		spletna klepetalnica
Ciphertext		tajnopis
Cookie		piškotek
Cookie manager		upravitelj piškotkov
Data Controler		informacijski pooblaščenec; skrbi za nadzor nad varovanjem osebnih podatkov
Data mining		podatkovno rudarjenje
DPD	**D**ata **P**rotection **D**irective	direktiva Evropske unije o zaščiti osebnih podatkov
Ecash		elektronski denar
Echelon		satelitski sistem za prestrezanje zasebnih in poslovnih elektronskih komunikacij
ECPA	**E**lectronic **C**ommunication **P**rivacy **A**ct	zakon za zaščito zasebnosti elektronskih komunikacij v ZDA
EPIC	**E**lectronic **P**rivacy **I**nformation **C**enter	center za zaščito zasebnosti elektronskih informacij
GUIDE	**G**lobal **U**nique **IDE**ntifier	globalni univerzalni identifikator
GUIDES		smernice evropske unije za e-poslovanje na podlagi direktive 95/46/ES
Identity Card		identifikacijska kartica
Identity Protector		zaščitnik identitete
IKT		**I**nformacijsko **K**omunikacijske **T**ehnologije
IP naslov		naslov računalnika s katerim se predstavi v omrežju; lahko je stalni ali dinamični.
Node		vozlišče; računalnik vključen v omrežje
One-to-One Marketing		oblika neposrednega trženja, prilagojena profilu posameznika
OECD	**O**rganization for **E**conomic **C**ooperation and **D**evelopment	Organizacija za ekonomsko sodelovanje in razvoj
Originator		Pošiljatelj
P2P	peer to peer	internetno omrežje, ki omogoča skupini uporabnikov povezavo in direkten dostop do povezanih računalnikov
P3P	**P**latform for **p**rivacy **p**references	platforma za zagotovitev zasebnosti

PAMPAS	**P**ioneering **A**dvanced **M**obile **P**rivacy **a**nd **S**ecurity	
Pasword sniffing		prestrezanje gesel
PET	**P**rivacy **E**nhancing **T**echnologie	tehnologije za zboljšanje zasebnosti
PIPEDA	**P**ersonal **I**nformation **P**rotection and **E**lectronic **D**ocuments **A**ct	zakon o zaščiti osebnih podatkov in elektronskih dokumentov
PISA	**P**rivacy **I**ncorporated **S**oftware **A**gent	
PGP	**p**retty **g**ood **p**rivacy	program za kodiranje vsebine datotek in elektronskih sporočil
Plaintext		Čistopis
PRIDEH	**Pr**ivacy Enhancement in **D**ata Management in **E-H**ealth	projekt Evropske unije za povečanje zasebnosti pri upravljanju s podatki na področju E-zdravja
PRIME	**Pr**ivacy and **I**dentity **M**anagement for **E**urope	projekt Evropske unije
RAPID	**R**oadmap for **A**dvanced Research in **P**rivacy and **Id**entitiy Management	Projekt Evropske unije
Relay server		poštni strežnik
Request originator		Odjemalec
Retencija podatkov		zbiranje in hramba podatkov
RIS	**R**aba **I**nterneta v **S**loveniji	akademski neprofitni projekt Centra za metodologijo in informatiko Fakultete za družbene vede v Ljubljani
RFID	**R**adio **F**requency **ID**entification	radio frekvenčna identifikacija
RSA		algoritem, ki je dobil ime po svojih ustvarjalcih: Ronald Rivest, Adi Shamir, Leonard Adleman
Safe Harbor principi		smernice sprejete v ZDA, ki naj bi zagotovile visoko stopnjo zaščite v skladu z evropsko direktivo; pristop podjetij k njihovemu sprejemu je prostovoljen
SATAN	**S**ecurity **A**dministrator's **T**ool for **A**nalyzing **N**etworks	program za iskanje varnostnih lukenj v omrežju
Timestamping		časovni žig
Trust Center		zaupni center

UCE	**U**nosolicited **C**ommercial **E**-mails	nenaročena komercialna elektronska pošta
W3C	**W**orld **W**ide **W**eb **C**onsortium	neprofitna organizacija ustanovljena 1994, skrbi za razvoj spleta in postavitev standardov ter tehničnih priporočil
XML	e**X**tensible **M**arkup **L**anguage	standard za zapis strukturiranih dokumentov na spletu

PRILOGE

Priloga 1: Vprašalnik

I. Zasebnost, osebni podatki

1. Različne javne in zasebne organizacije zbirajo osebne podatke o nas. Ali ste zaradi tega zaskrbljeni glede varovanja vaše zasebnosti?
□ da zelo □ da □ do neke mere □ ne □ ne vem

2. Se vam zdi pomembno, da veste kateri vaši osebni podatki se zbirajo in v kakšen namen?
□ da zelo □ da □ do neke mere □ ne □ ne vem

3. Ali se strinjate, da lahko podjetja v marketinške namene zbirajo podatke iz različnih javnih imenikov (telefonskih…)
□ da, strinjam se □ ne strinjam se □ ne morem reči

4. Ali veste, da se vaši osebni podatki ne smejo zbirati brez vašega soglasja.
□ da, vem □ ne vem

5. Poznate zakonodajo v zvezi z zaščito zasebnosti oz. osebnih podatkov
□ da, poznam □ samo okvirno □ ne poznam

6. Ste že slišali, da imate pravico do vpogleda v osebne zbirke, ki jih posamezna organizacija zbira o vas, da lahko te podatke popravite oz. zbrišete, če so bili pridobljeni nezakonito.
□ da, slišal sem □ ne, nisem še slišal □ ne vem

7. Ste to pravico že kdaj izkoristili.
□ da □ ne

8. Spletne strani velikokrat zahtevajo od nas izpolnjevanje določenih obrazcev, kjer moramo posredovati tudi osebne podatke. Ali ste pripravljeni razkriti katere od spodaj naštetih osebnih podatkov?

	vedno	včasih	nikoli
ime, priimek			
naslov			
rojstne podatke			
EMŠO			
elektronski naslov			
telefonsko številko			
številko bančnega računa			
številko kreditne kartice			
izobrazbo			
zaposlitev			
narodnost, veroizpoved			
podatke o svojem zdravju			

9. Ali ste pripravljeni razkriti osebne podatke za določene bonitete (nagradne točke, popusti, kartice zaupanja,…)

□ da, vedno □ rad □ ne rad □ v nobenem primeru ne □ ne vem

10. Osebni podatki, ki jih puščamo na internetu ob uporabi različnih spletnih storitev, se lahko uporabijo za pošiljanje reklamnih sporočil, lahko se prodajo trgovinam, zavarovalnicam ali so predani državnim organom. Ali ste glede tega zaskrbljeni:

□ zelo me skrbi □ malo me skrbi □ me ne skrbi □ ne vem

II. Grožnje zasebnosti

11. V kakšne namene in kako pogosto uporabljate internet

	Vsak dan	Nekajkrat tedensko	Nekajkrat mesečno	Nikoli
Dopisovanje preko elektronske pošte				
Nakupovanje, bančne storitve, rezervacije				
Izobraževanje				
Zabava				
Brskanje kar tako				

12. Ali menite, da je možno preko interneta:

	Da	Ne	Ne vem
Prestreči elektronsko pošto			
Ukrasti gesla, številke kreditnih kartic			
Ugotoviti katere spletne strani obiskujete			
Ugotoviti naslov (IP) vašega računalnika			
Ugotoviti kje se nahajate (geografsko lokacijo)			
Ugotoviti vašo »fizično« identiteto			

13. Ali ste ob uporabi interneta že kdaj začutili neželjen poseg v vašo zasebnost

□ da □ ne □ ne vem

14. V kolikšni meri ste zaskrbljeni glede:

	zelo me skrbi	me skrbi	malo me skrbi	me ne skrbi
Prestrezanja elektronske pošte oz. nadzora nad elektronsko pošto				
Nadlegovanja preko elektronske pošte (neželjena elektronska pošta- SPAM)				
Uporabe piškotkov (COOKIES)				
Zbiranja podatkov glede obiskovanja spletnih strani, sledenje				
Nadzora s strani državnih institucij				

15. Koliko zaupate spodaj naštetim organizacijam glede varovanja zasebnosti na internetu:

	zelo zaupam	zaupam	malo zaupam	ne zaupam	ne vem
Državni upravi					
Bankam					
Zavarovalnicam					
Zdravstvenim organizacijam					
Spletnim knjižnicam					
Spletnim trgovinam					
Ponudnikom internetnih storitev					

16. Zaradi preprečevanja terorizma je v zadnjem času vse več nadzora države nad državljani. Ali se vam zdi to potrebno?

- *ne, spoštovati je potrebno osnovne človekove pravice*
- *da, če so nadzorovani samo osumljeni*
- *da, vendar samo po odredbi sodišča*
- *da, vsi smo lahko nadzorovani*

III. Uporaba tehnologij za izboljšanje zasebnosti na internetu

17. Ste kdaj videli oziroma prebrali spletne objave o »Politiki podjetja ali oglaševalca o varovanju podatkov«?
 da ne ne morem reči

18. Če »Politiko podjetja o varovanju podatkov« preberete, ali se kdaj niste strinjali s pogoji in ste stran zapustili?
 da, stran sem že zapustil ne, vedno nadaljujem je ne preberem

19.Če »Politike podjetja o varovanju podatkov« ne preberete, zakaj ne? (odgovorite samo če »Politike« ne preberete)

- *Je ne razumem, je nejasna*
- *Premajhen tisk*
- *Me ne zanima*
- *Nimam časa za branje*
- *Ne vem kje se nahaja*
- *Spletni strani popolnoma zaupa*

20. Ali poznate orodja oz. tehnologije za izboljšanje zaščite vaše zasebnosti na internetu kot so na primer šifriranje, upravitelj piškotkov, zaščitnik identitete, anonimni strežniki, ponovni pošiljatelj, P3P?

□ da poznam □ nekatera poznam □ za nobeno še nisem slišal

21. Ali morda uporabljate katero od spodaj naštetih orodij za izboljšanje zasebnosti

- □ *Blokiranje piškotkov*
- □ *»Spam« filter*
- □ *orodje za zaščito anonimnosti na spletu*
- □ *požarni zid*
- □ *Uporabljam neko drugo orodje za zaščito zasebnosti*
- □ *Ne uporabljam nobenega orordja*

22. Če ne uporabljate nobenega orodja, zakaj ne? (odgovorite samo, če ne uporabljate nobenega orodja za zaščito zasebnosti)

- □ *Nobenega ne poznam*
- □ *Ne znam ga namestiti na računalnik*
- □ *Ne verjamem v učinkovitost*
- □ *Nisem zaskrbljen glede zasebnosti*
- □

23. Kdo je po vašem mnenju odgovoren za izboljšanje zasebnosti na internetu

- □ *Vsak sam*
- □ *Država (z ustrezno zakonodajo)*
- □ *Računalniška industrija (ustrezna programska podpora)*
- □ *Drugo*_____

IV. Splošni podatki o anketirancu

Starost:

□ 15 do 20 □ 21 do 30 □ 31do 40 □ 41 do 55 □ nad 55

Spol:

□ Ženski □ moški

Stopnja izobrazbe:

□ Srednja oz. poklicna □ višja oz. visoka □ magisterij oz. doktorat

Koliko ur tedensko uporabljate internet?

□ 1 do 5 □ 5 do 10 □ 10 do 20 □ nad 20

Za sodelovanje se vam najlepše zahvaljujem!

Priloga 2: FREKVENČNE TABELE

Splošni podatki o anketirancih:

Spol anketirancev

	frekvenca	Odstotek
Ženski	48	42,86
Moški	56	50,00
ni odgovora	8	7,14
Skupaj	112	100,00

Izobrazba anketirancev

	frekvenca	odstotek
srednja oz. poklicna	43	38,39
višja oz. visoka	60	53,57
magisterij, doktorat	5	4,46
ni odgovora	4	3,57
skupaj	112	100,00

Čas, ki ga anketiranci tedensko preživijo na spletu

	frekvenca	odstotek
1 do 5 ur	25	22,32
5 do 10 ur	40	35,71
10 do 20 ur	30	26,79
nad 20 ur	16	14,29
ni odgovora	1	0,89
skupaj	112	100,00

Vprašanje št. 3: Strinjanje s pridobivanjem podatkov iz javnih imenikov:

	frekvenca	odstotek
da	20	17,86
ne	69	61,61
ne vem	23	20,54
skupaj	112	100,00

Vprašanje št 4: Ali veste, da se podatki ne smejo zbirati brez soglasja?

	frekvenca	odstotek
Da, vem	89	79,46
Ne vem	23	20,54
skupaj	112	100,00

Vprašanje št. 5: Poznavanje zakonodaje s področja zasebnosti in varovanja podatkov

	frekvenca	odstotek
Da, poznam	21	18,75
samo okvirno	69	61,61
Ne poznam	22	19,64
skupaj	112	100,00

Vprašanje št. 6: Informiranost o pravici do vpogleda v osebne zbirke:

	frekvenca	Odstotek
Da, slišal sem	49	43,75
nisem še slišal	51	45,54
Ne vem	12	10,71
skupaj	112	100,00

Vprašanje št. 12: Grožnje zasebnosti preko interneta:

	frekvenca				odstotek		
	da	ne	ne vem	ni odgovora	da	ne	ne vem
Prestreči elektronsko pošto	98	2	10	2	89,09	1,82	9,09
Ukrasti gesla	93	5	13	1	83,78	4,50	11,71
Ugotoviti katere spletne strani obiskujete	99	1	10	2	90,00	0,91	9,09
Ugotoviti naslov (IP) vašega računalnika	92	3	15	2	83,64	2,73	13,64
Ugotoviti geografsko lokacijo	75	13	23	1	67,57	11,71	20,72
Ugotoviti vašo »fizično« identiteto	14	23	27	14	48,98	23,47	27,55

Vprašanje št. 13: Ali ste ob uporabi interneta že kdaj začutili neželen poseg v zasebnost?

	frekvenca	odstotek
da	31	27,68
ne	60	53,57
ne vem	20	17,86
ni odgovora	1	0,89
skupaj	112	100,00

Vprašanje št. 15: Katerim organizacijam uporabniki interneta zaupajo:

	frekvenca					odstotek				
	zelo zaupam	zaupam	malo zaupam	ne zaupam	ne vem	zelo zaupam	zaupam	malo zaupam	ne zaupam	ne vem
Državni upravi	13	47	26	16	8	11,82	42,73	23,64	14,55	7,27
Bankam	17	47	33	13	2	15,18	41,96	29,46	11,61	1,79
Zavarovalnicam	4	31	48	21	5	3,67	28,44	44,04	19,27	4,59
Zdravstvenim organizacijam	5	45	45	13	3	4,50	40,54	40,54	11,71	2,70
Spletnim knjižnicam	2	26	64	13	6	1,80	23,42	57,66	11,71	5,41
Spletnim trgovinam	0	11	36	61	3	0,00	9,91	32,43	54,95	2,70
Ponudnikom internetnih storitev	3	14	55	34	2	2,78	12,96	50,93	31,48	1,85

Vprašanje št. 16: Ali je potreben nadzor države nad državljani:

	frekvenca	odstotek
ne, spoštovati je potrebno osnovne človekove pravice	24	21,43
da, če so nadzorovani samo osumljeni	35	31,25
da, vendar samo po odredbi sodišča	44	39,29
da, vsi smo lahko nadzorovani	8	7,14
ni odgovora	1	0,89
skupaj	112	100,00

Vprašanje št. 17: Poznavanje spletne strani, kjer so objavljene izjave o politiki podjetja glede varovanja zasebnosti:

	frekvenca	odstotek
Da	26	23,21
Ne	63	56,25
Ne morem reči	22	19,64
ni odgovora	1	0,89
skupaj	112	100,00

Vprašanje št. 18:Ali se kdaj niste strinjali s pogoji glede varovanja zasebnosti in ste stran zapustili:

	frekvenca	odstotek
Da, stran sem že zapustil	31	27,68
vedno nadaljujem	11	9,82
je ne preberem	63	56,25
ni odgovora	7	6,25
skupaj	112	100,00

Vprašanje št. 19: Zakaj ne preberete politike o varovanju zasebnosti:

	frekvenca	odstotek
Je ne razumem, je nejasna	7	7,22
premajhen tisk	6	6,19
Me ne zanima	25	25,77
nimam časa za branje	29	29,90
ne vem kje se nahaja	27	27,84
spletni strani popolnoma zaupam	3	3,09
skupaj	97	100,00

Vprašanje št. 20: Poznavanje orodij za izboljšanje varovanja zasebnosti:

	frekvenca	odstotek
Da, poznam	15	13,39
nekatera poznam	75	66,96
Za nobeno še nisem slišal	19	16,96
ni odgovora	3	2,68
Skupaj	112	100,00

Vprašanje št. 21: Ali uporabljate katero od spodaj naštetih orodij

	frekvenca	odstotek
blokiranje piškotkov	21	18,75
»spam« filter	34	30,36
orodje za zaščito anonimnosti na spletu	4	3,57
požarni zid	53	47,32
uporabljam neko drugo orodje za zaščito zasebnosti	17	15,18
ne uporabljam nobenega orodja	30	26,79

Vprašanje št. 22: Zakaj ne uporabljate nobenega orodja

	frekvenca	odstotek
nobenega ne poznam	13	27,08
ne znam ga namestiti na računalnik	23	47,92
ne verjamem v učinkovitost	6	12,50
nisem zaskrbljen glede zasebnosti	6	12,50

Vprašanje št. 23: Kdo je po mnenju anketirancev odgovoren za izboljšanje zasebnosti na internetu:

	frekvenca	odstotki
Vsak sam	51	45,54
Država (z ustrezno zakonodajo)	39	34,82
Računalniška industrija	60	53,57
Drugo	4	3,57