Univerza v Mariboru
Fakulteta za varnostne vede

DIPLOMSKO DELO

Zasebnost in internet

Maja Žbogar

Julij, 2009

Mentor: dr. Igor Belič

ZAHVALA

Najlepše se zahvaljujem svojemu mentorju za pomoč pri izdelavi diplomske naloge. Prav tako se zahvaljujem tudi vsem, ki me poznajo.

Kazalo

Kazalo grafov

Povzetek

Internet je v svojih začetkih veljal za kraj neomejene svobode in anonimnosti. Kasneje se je izkazalo se je da temu ni tako. Rastoče število uporabnikov interneta in možnih načinov zlorab, je seboj prineslo vse večjo zaskrbljenost glede ogrožanja zasebnosti in zlorabe osebnih podatkov. Tako se mnogo uporabnikov čedalje bolj zaskrbljeno sprašuje kaj se utegne zgoditi z njihovo zasebnostjo. Diplomska naloga obravnava problem zasebnosti v internetnem okolju. V prvem delu se ukvarja z vprašanjem definicije zasebnosti in išče možne razloge, zakaj različni avtorji zasebnost razumejo na različne načine. Predstavljeni so izsledki nekaterih raziskav o stališčih in dejanskih praksah uporabnikov za varovanje zasebnosti. Diplomska naloga analizira in primerja normativno ureditev tega področja v Evropi in v ZDA. Na kratko je predstavljen Safe Harbour sporazum. Identificiranih je nekaj prednosti in slabosti državne regulacije in samoregulacije. V naslednjem delu pa obravnava vire ogrožanja. Loti se problema elektronske pošte in s tem povezanim problemom zasebnosti na delovnem mestu. Kot velik problem je predstavljeno tudi zbiranje in obdelovanje osebnih podatkov s strani komercialnega sektorja. Izpostavljen je problem profiliranja uporabnikov in personalizacije storitev ter sporni načini pridobivanja soglasja. Med drugimi viri ogrožanja zasebnosti so predstavljeni še prikrita programska oprema, DRM ali tehnike upravljanja dostopa do digitalnih vsebin in nezaželena elektronska pošta. V zadnjem delu pa so podani izsledki raziskave med slovenskimi uporabniki interneta o njihovem zavedanju zasebnosti pri delu v spletnem okolju.

Ključne besede:

Internet, zasebnost, delovno mesto, nezaželena elektronska pošta, viri ogrožanja

Privacy and internet

Summary

Internet used to be regarded as a place of infinite freedom and anonymity. Later it turned out to be, that this was not the case. Ever growing number of users and new ways of how to invade people's privacy, are causing concerns about threats to people's privacy and abuse of their personal information. Many of today's users are raising a serious question as to what is going to happen to their privacy. This degree work tries to present the problem of privacy on the World Wide Web. The first section deals with the question of how to define the concept of privacy and tries to identify some of the possible reasons why different authors understand the concept of privacy in different ways. This degree paper also compares different legal organisation of this field in the USA and Europe. It also presents the safe harbour agreement and identifies some shortcomings and benefits of both the state regulation and the self regulation. It also covers some of the research findings about beliefs and actual praxis among users in regards to privacy. The next section deals with threats to privacy. It presents the problem of email surveillance in connection to workplace privacy. Another growing concern is the issue of gathering and analysing personal information undertaken by the private sector. It presents the problem of consumer profiling, personalization of services and controversial ways of acquiring people's permission. Among other threats it also presents covert software like spyware, DRM or digital rights management and spam. Final part of this degree work consists of a research done among Slovenian internet users. It presents findings about people's level of concern about their privacy while surfing the World Wide Web.

Key words:

Internet, privacy, workplace, spam, threats

1. Uvod

Diplomska naloga obravnava problem zasebnosti na internetu. Internet je v svojih začetkih veljal za kraj neomejene svobode in anonimnosti. Kasneje se je izkazalo se je da temu ni tako. Rastoče število uporabnikov interneta in možnih načinov zlorab, je seboj prineslo vse večjo zaskrbljenost glede ogrožanja zasebnosti in zlorabe osebnih podatkov. Eden izmed problemov je, da ima veliko število uporabnikov pomanjkljivo računalniško znanje in so se zato nezmožni učinkovito zaščititi pred velikim številom virov ogrožanja. Pokazala se je potreba po zakonski regulaciji. Različne države so se tega področja lotile urejati na različen načine. Velika razlika je opazna zlasti med ameriškim in evropskim modelom regulacije. Tovrstna teritorializirana normativna ureditev pa pomeni dodatni problem, saj je internet po svoji naravi globalen prostor in ne pozna državnih meja.

Predstavljen je problem zasebnosti v spletnem okolju. Opisani so nekateri viri ogrožanja. Primerjali smo zakonodajno ureditev tega področja v ZDA in v Evropi. V zadnjem empiričnem delu pa smo tudi raziskali mnenja uporabnikov o zasebnosti v internetnem okolju in interpretirati dobljene rezultate

Izhajamo iz predpostavke, da je velik delež uporabnikov interneta zaskrbljenih glede zasebnosti in da jih večina meni, da je njihova zasebnost v spletnem okolju ogrožena. Kljub temu se jih veliko ne zaveda virov ogrožanja in ne pozna dovolj dobro zaščitnih tehnologij za varovanje svoje pravice do zasebnosti. Domnevali smo tudi, da so uporabniki dostikrat v zameno za prejemanje drobnih ugodnosti pripravljeni različnim spletni stranem zaupati svoje osebne podatke.

Kot metodo dela smo uporabili študiranje strokovne literature tujih in domačih avtorjev. Na ta način smo osvetlili problem zasebnosti v svetovnem spletu s teoretične plati. V empiričnem delu diplomske naloge smo izvedli anketo med uporabniki o zavedanju konceptov varnosti in zasebnosti pri delu v spletnem okolju. Na ta način smo poskušali ugotoviti, kateri so najpogostejši ukrepi za varovanje informacijske zasebnosti. Dobljene podatke smo statistično analizirali, grafično prikazali in interpretirali dobljene rezultate.

V diplomski nalogi obravnavamo problem zasebnosti v svetovnem spletu. V prvem poglavju so predstavljene različne definicije pravice do zasebnosti. To poglavje pa poskuša tudi odgovoriti na vprašanje, kaj je razlog za pomanjkanje konsenza in množico različnih opredelitev zasebnosti. Tretje poglavje predstavi ugotovitve raziskav s področja pravice do zasebnosti in išče odgovor na vprašanje, zakaj različne raziskave prihajajo do različnih zaključkov. Četrto poglavje s pomočjo doktrine razumnega pričakovanja zasebnosti pojasnjuje, kdaj gre za vdor v zasebnost. Peto poglavje primerja zakonodajo na področju pravice do zasebnosti v Evropi in ZDA. Šesto poglavje poskuša identificirati in predstaviti različne vire ogrožanja zasebnosti na spletu. Sedmo poglavje se ukvarja z razvojem tega področja v prihodnost. V zadnjem poglavju pa so predstavljeni izsledki empirične raziskave med slovenskimi uporabniki interneta in njihovem zavedanju pravice do zasebnosti na internetu.

2. Pravica do zasebnosti

Zgodovinsko gledano se je pravica do zasebnosti v obliki kot jo poznamo danes, razvila šele s pojavom kapitalizma. Po mnenju nekaterih pa kapitalizem in množična tržna usmerjenost, ta »ideal, čedalje bolj spodjedata in ob pomoči tehnološkega napredka tudi ožita območje zasebnosti« (Kovačič, 2006, str. 38). Pravica do zasebnosti v današnji družbi pa je izredno težko opredeljiv pojem.

2.1. Kaj sploh je zasebnost?

Pravico do zasebnosti je težko natančno in nedvomno definirati. Tako obstaja mnogo različnih definicij. V nadaljevanju bomo izpostavili nekaj izmed njih.

2.1.1. Zasebnost kot pravica biti sam (right to be left alone)

Zasebnost kot »right to be left alone«, se je prvič pojavila v članku Warrena in Brandeisa. Ob svojem nastanku je bila odziv na konflikt med vsiljivimi mediji in posamezniki, ko so slednji zahtevali kontrolo nad svojim imenom in videzom (Baruh, 2007). Ta definicija zasebnosti po mnenju nekaterih poudarja aspekt zaščite misli ter čustev in pravico, da lahko vsak posameznik zasleduje svoje interese (Coleman, 2006). Tako dojemanje pravice do zasebnosti je danes dokaj značilno. Vendar pa ima v ZDA to posebnost, da jo nekateri dojemajo kot »okoliščino v kateri ni dostopa do neobjavljenih informacij do o drugem« (Kovačič, 2006, str. 43). Problem takega »poudarjanja objavljenosti osebnih informacij (v smislu javne objave) pa je v tem, da po tem razumevanju pravice do zasebnosti, zbiranje osebnih podatkov, ki so v različnih dosjejih, če le ti niso javno dostopni (npr. Medicinske kartoteke, potrošniški profil itd.), ne pomeni kršitve zasebnosti« (Kovačič, 2006, str. 43).

2.1.2. Zasebnost kot pravica do komunikacijske zasebnosti

Pravica do zasebnosti pa ni le pravica do tega, da se posameznika pusti pri miru. Pravica do komunikacijske zasebnosti je močno povezana z informacijsko zasebnostjo in posamezniku omogoča, da vzpostavlja in vzdržuje stike z drugimi (Kovačič, 2003). Pravica do komunikacijske zasebnosti je v Sloveniji zavarovana s 37. členom ustave. Ta pravica pomeni, »varstvo posameznikovega interesa, da se država ali nepovabljeni tretji ne seznanijo z vsebino sporočila, ki ga posreduje preko kateregakoli sredstva, ki omogoča izmenjavo oziroma posredovanje informacij na daljavo« (Klemenčič, 2005, str. 43). Klemenčič (2005, str. 43) pravi, da ta pravica obsega tudi posameznikov interes «da ima nadzor (in svobodo) nad tem, komu, in v kakšnem obsegu, na kakšen način in pod kakšnimi pogoji bo posredoval določeno sporočilo«.

2.1.3. Zasebnost kot kontrola nad osebnimi informacijami

Po revolucionarnem razmahu interneta se je začel poudarjati vidik kontrole toka informacij o posamezniku (Baruh, 2007). Po tej definiciji, je pravica do zasebnosti kršena, kadar je informacija o posamezniku pridobljena, uporabljena ali razširjena, brez posameznikove vednosti in privolitve (Wel, Royakkers, 2004). Vendar pa se je potrebno zavedati, da so ljudje pri svojih aktivnostih na spletu, kot je na primer spletno nakupovanje, v stalni interakciji z drugimi. Vsaka interakcija pa pomeni, da je njihova pravica do kontrole informacij o sebi, relativna in poleg tega tudi omejena s pravicami drugih (Pollach, 2005). Vendar pa to seveda za uporabnike ne pomeni, da lahko zbiralci z pridobljenimi informacijami počnejo, kar se jim zljubi. Nekateri ugovarjajo, da je tovrsten način gledanja na zasebnost morda preveč ozkogleden. Za primer navajajo hipotetičnega uporabnika, ki je o sebi širokemu krogu ljudi prostovoljno razkril velike količine intimnih informacij. Utrpel je izgubo zasebnosti, toda ker pa je informacije zaupal prostovoljno še vedno ostaja element kontrole. Coleman (2006) iz tega zaključuje, da je kontrola le eden izmed pomembnih aspektov zasebnosti, vendar pa ne konstituira zasebnosti kot take.

2.1.4. Zasebnost kot nevmešavanje javne sfere v zasebno

Eden izmed konceptov zasebnosti opredeljuje zasebnost kot pravico do nevmešavanja javnega sektorja v zasebno sfero življenja. Intimni prostor posameznika naj bi bila tako zavarovan pred vdiranjem javnega. Na tem mestu se seveda se postavlja vprašanje kako velik naj bi bil ta osebni prostor (Kovačič, 2006). Poleg tega pa je problem te definicije v tem, da predpostavlja, da je javni sektor na čelu z vlado edini, ki se lahko vmešava v človekovo zasebnost (Coleman, 2006). Vendar pa v zadnjem času temu ni tako. Zasebni sektor na področju vmešavanja v zasebnost počasi dobiva primat.

2.1.5. Pravica do zasebnosti kot lastninska pravica

V zasebnem sektorju, se pogosto pojavlja pogled na zasebnost, ki v njej vidi lastninsko pravico. Ta redukcionalistični pogled na pravico do zasebnosti prevladuje predvsem v ZDA v kontekstu pravice do zasebnosti na delovnem mestu. Tam se namreč, v večji meri kot je to značilno za Evropo, posegi delodajalcev v zasebnost zaposlenih opravičujejo z lastništvom komunikacijskih sredstev (Kovačič, 2006). Tako lastninsko razumevanje zasebnosti pripelje do tega, da lahko posameznik s svojo lastnino naredi karkoli. Tako lahko na primer svoje osebne podatke proda z enim samim klikom miške in na ta način izgubi vsak nadzor nad njimi, saj le ti postanejo last podjetja, ki lahko z njimi prosto razpolaga (Kovačič, 2006).

2.2. Delitev pravice do zasebnosti

Po mnenju poročila Global Internet Liberty Campaign (1999) o zasebnosti in človekovih pravicah, lahko zasebnost razdelimo na teritorialno zasebnost, informacijsko zasebnost, komunikacijsko zasebnost in zasebnost telesa. Teritorialna zasebnost ščiti posameznika v njegovih prostorih, informacijska zasebnost varuje uporabnikove osebne podatke, zasebnost komunikacije ščiti posameznikovo zasebno komunikacijo, zasebnost telesa pa ščiti posameznike pred različnimi posegi njihovo fizično telo (Kovačič, 2006).

Vendar pa kljub je, kljub množici definicij zasebnosti in njihovih dimenzij, le ta ena izmed najpomembnejših temeljnih človekovih pravic. Pravica do zasebnosti pa je celo več kot to. Zasebnost je tudi vrednota celotnega družbenega telesa, saj omogoča, da se

ljudje drug z drugim avtonomno združujejo in tako tvorno vplivajo na celotno družbo (Kovačič, 2006).

2.3.Čemu toliko različnih definicij?

Zasebnost je izredno subjektiven pojem. Dojemanje zasebnosti variira od posameznika do posameznika in temelji na njegovih osebni vrednotah in percepcijah (O'Neil, 2001).
Za zasebnost je značilna tudi kulturna pogojenost. Na zahodu je koncept zasebnosti orientiran k posamezniku, medtem ko je ima zasebnost na primer v Vzhodnih in nekaterih Afriških državah, ki so kulturno orientirane k skupnosti, včasih celo negativno konotacijo (Capuro, 2005). Nekateri menijo, da je tako negativno dojemanje pravice do zasebnosti, lahko tudi posledica razmeroma mladih demokracij. Tako se je za večino azijskih držav demokracija začela šele v dvajsetem stoletju. Ljudem primanjkuje občutka glede svoje zasebnosti ter nadzora in še vedno ohranjajo totalitaren pristop do svoje vlade (Hsu, 2006).

Poleg tega je bilo v preteklosti prehajanje med javnim in zasebnim relativno dobro definirano. Razvoj informacijsko komunikacijske tehnologije pa je s seboj prenesel prepletanje obeh segmentov in ustvaril novo kategorijo zasebne javnosti oziroma javne zasebnosti (Pinterič, Grivec, 2007). Na ta način posameznik iz zasebnosti svojega lastnega doma posega v javno dogajanje in javnost s priključitvijo v svetovni splet omogoča drugim uporabnikom dostop do svoje zasebne sfere (Pinterič in sodelavci, 2007).

Pravica do zasebnosti pa tudi ni edina človekova pravica. Pravica do zasebnosti je tako pogosto v konfliktu z drugimi pravicami in interesi, jasno hierarhijo pravic pa je nemogoče oblikovati (Kovačič, 2006).

3. Raziskave o zasebnosti

Prav tako kot ni konsenza o enotni definiciji zasebnosti, tudi raziskave na področju zasebnosti ne nudijo enotnih zaključkov o pomenu zasebnosti za uporabnike svetovnega spleta. Raziskave o zasebnosti uporabljajo različne dimenzije merjenja. Nekatere merijo uporabnikova stališča do zasebnosti, druge skrb za zasebnost, tretje vedenjske namere v zvezi z zasebnostjo, spet druge pa dejansko vedenje (Norberg, Horne, Horne, 2007). Vse to povzroča kar precej zmede.

Veliko študij uporablja demografske podatke kot neodvisno spremenljivko, kar pa pogosto vodi do konfliktnih rezultatov (Hsu, 2006). Tako na primer nekatere raziskave ugotavljajo, da so ljudje z višjo stopnjo izobrazbe bolj zaskrbljeni glede svoje zasebnosti, kot tisti z nižjo (O'Neil, 2001). Drug izsledek te iste raziskave pa je, da so ljudje z višjim socioekonomskim statusom in višjimi prihodki izrazili manjšo stopnjo zaskrbljenost (O'Neil, 2001). Ta ugotovitev je nekoliko nenavadna, saj imajo bolj izobraženi ljudje ponavadi tudi višji ekonomski status.

Nekatere raziskave kažejo, da so respondenti iz študentskih vrst v večjem odstotku pripravljeni zaščititi svojo zasebnost kot druge starostne skupine in so tudi bolj tehnično podkovani (Milne, Rohm, Bahl, 2004). Vendar pa so po podatkih drugih raziskav odrasli tisti, ki so bolj proaktivni pri zaščiti svoje zasebnosti. Najpogostejši ukrepi, ki se jih poslužujejo za zaščito svoje zasebnosti pa so neodpiranje nezaželene elektronske pošte, neregistriranje na spletne strani in zaprosila za odstranitev elektronskih naslovov z mailing list (Moscardelli , Divine, 2007).

Študije, ki temeljijo na demografskih spremenljivkah velikokrat prihajajo do različnih ugotovitev glede istih vprašanj. Ena izmed razlag za protislovne rezultate je subjektivnost dojemanja zasebnosti. Percepcija zasebnosti variira med populacijo in tudi znotraj določenih segmentov populacije (Norberg in sodelavci, 2007). Ljudje v podobnih socialnih situacijah, z podobno stopnjo izobrazbe in podobnim številom izkušenj na internetu, imajo lahko zelo različna mnenja in zavedanja svoje zasebnosti (Woo, 2006). Percepcija zasebnosti pa je tudi kulturno pogojena. Respondenti iz različnih držav imajo različne prioritete, zaskrbljenosti in prakse za zaščito zasebnosti (Hsu, 2005). Prav tako

pa nekateri tudi opozarjajo, da zasebnost ni statičen koncept. Dojemanje zasebnosti je dinamično, saj imajo ljudje drugačno zaskrbljenost glede zasebnosti v različnih situacijah (Hsu, 2006).

Poleg konfliktnosti izsledkov raziskav, je zanimivo tudi dejstvo, da zaskrbljenost glede zasebnosti ni vzporedna s praksami ki se jih ljudje poslužujejo za zaščito zasebnosti. Tako je na primer velika večina vprašanih ljudi zelo zaskrbljenih glede svoje zasebnosti, vendar pa se njihova zaskrbljenost ne odraža v njihovih vsakodnevnih praksah na internetu (Hsu, 2006). Še več, celo posamezniki z negativnimi percepcijami o razkrivanju določenih osebnih informacij, bodo pod določenimi pogoji na zahtevo pripravljeni te informacije zaupati (Norberg in sodelavci, 2007). Tako so na primer uporabniki včasih pripravljeni zaupati marsikatero osebno informacijo v zameno za materialno kompenzacijo v obliki prejemanja majhnih ugodnosti (Woo, 2006). Čeprav rezultati nekaterih raziskav ugotavljajo, da kar 78% uporabnikov interneta bolj ceni zasebnost kot pa ugodnosti (O'Neil, 2001). Vendar pa v praksi temu očitno ni tako. Posamezniki se tako »zavedajo ogroženosti zasebnosti na načelni ravni, vendar na te grožnje oziroma na nadzor pristajajo in se niti ne poskušajo zaščititi-pogosto tudi na škodo udobja in zaradi neznanja« (Kovačič, 2006, str. 90). Ženske se po nekaterih raziskavah veliko bolj zaskrbljene glede svoje zasebnosti kot moški (O'Neil, 2001). Vendar pa rezultati drugih raziskav kažejo, da je za moške bolj verjetno da bodo poskrbeli za zaščito svoje zasebnosti kot za ženske (Milne in sodelavci, 2004).

Tako se pojavlja vprašanje, kako pojasniti to odstopanje med nameravanim vedenjem in dejanskim vedenjem. Norberg in sodelavci (2007) menijo, da je ta razkorak posledica tega, da je percepcija zaupanja in tveganja drugačna, ko merimo samo namen v primerjavi z vedenjem v dejanskih okoliščinah. Druga razlaga pa je slabo poznavanje možnost za zaščito zasebnosti. Tako je poznavanje zaščitnih tehnologij med slovenskimi uporabniki slabo, saj jih od 40 do 70 odstotkov ne pozna različnih zaščitnih sistemov, uporablja pa jih le slaba desetina uporabnikov (Kovačič, 2000). Za obstoječo situacijo nekateri krivijo slabo izobraževanje uporabnikov in internetna podjetja, ki dajejo svojim strankam lažen občutek o njihov zasebnosti v spletnem okolju (Wafa, 2008).

Določene druge raziskave pa ponujajo drugačne izsledke glede korelacije zaskrbljenosti in dejanskih praks uporabnikov v spletnem okolju. Nekatere študije namreč ugotavljajo,

da so uporabnikova zaskrbljenost in njegova stališča do zasebnosti in močan pokazatelj vedenja v svetovnem spletu (Milne in sodelavci, 2004). Po podatkih raziskave izvedene med mladostniki, so tisti ki so izrazili večjo zaskrbljenost glede svoje zasebnosti, tudi pogosteje zaprosili, da se jih odstrani z raznih mailing list in pogosteje fabricirali svoje osebne podatke (Moscardelli in sodelavci, 2007). Druga študija prav tako kažejo, da so tisti kupci, ki so bolj zaskrbljeni in imajo več izkušenj z delom v spletnem okolju, tudi bolj nagnjeni k uporabi zaščitnih ukrepov (Milne in sodelavci, 2004).

4. Razumno pričakovanje zasebnosti

Za formalnopravno presojanje vprašanja, kdaj gre za poseg v posameznikovo zasebnost se je uveljavila doktrina razumnega pričakovanja zasebnosti. Razvilo jo je ameriško vrhovno sodišče v primeru Katz proti ZDA. Kasneje pa se je ta standard uveljavil tudi v sodbah evropskih sodišč.

Razumno pričakovanje zasebnosti je sestavljeno iz dveh elementov: iz pričakovanja zasebnosti in utemeljenosti tega pričakovanja (Jančič in sodelavci, 2007). Po tem konceptu varovanja komunikacijske zasebnosti, gre za »poseg v zasebnost takrat, ko posameznik pri posredovanju svojega sporočila razumno in upravičeno pričakuje, da bo njegova komunikacija nenadzorovana« (Klemenčič, 2005, str. 45).

Vendar pa nekateri postavljajo to doktrino pod vprašaj, saj je v javnosti splošno razširjeno mnenje, da internet ni varno in zasebno okolje. Tako nekateri menijo, da ta splošno razširjena vednost o pomanjkanju zasebnosti na internetu, spodkopava utemeljenost pričakovanja o zasebnosti komunikacij (Coleman, 2006). Po tej teoriji je torej nerazumno pričakovati komunikacijsko zasebnost pri pošiljanju elektronskih sporočil, saj le ta po omrežju večinoma potujejo nešifrirana in jih je tako dokaj lahko prestrezati in se seznaniti z njihovo vsebino. Vendar pa Coleman (2006) meni, da je ljudskost tega vedenja potrebno postaviti pod vprašaj in poleg tega ugotavlja, da tudi drugih medijev ne bi mogli označiti za stoodstotno varne, pa zanje vseeno vejajo pravna načela.

V ZDA pa v nekaterih drugih primerih ni moč upravičeno pričakovati zasebnosti. Tako posameznik na primer »ne more upravičeno pričakovati zasebnosti pri bančnih in drugih zapisih, ki jih vodi tretja stranka. To je z vidika informacijske zasebnosti nadvse problematično, saj so zbirke osebnih podatkov v Ameriki večinoma vse pod nadzorom oziroma v lasti tretjih oseb in podjetij« (Kovačič, 2006, str. 54).

5. Normativna ureditev pravice do zasebnosti v ZDA in v Evropi

Evropa in ZDA se za presojanje vprašanja kdaj gre za poseg v posameznikovo zasebnost poslužujeta doktrine utemeljenega pričakovanja zasebnosti. Kljub temu sta pristopa k regulaciji pravice do zasebnosti v ZDA in Evropi diametralno nasprotna. Medtem, ko Evropa poslužuje strogega zakonodajnega urejanja tega področja, v ZDA velja tržno baziran laissez-faire pristop (Nijhawan, 2003).

Pravna ureditev v ZDA ločuje med regulacijo zasebnega in privatnega sektorja. Medtem ko za državne akterje velja pravna ureditev, se zasebniki ravnajo po samoregulaciji (Kovačič, 2006). Samoregulaciji mnogi očitajo veliko pomanjkljivosti, o čemur bo več zapisano v nadaljevanju.

Evropa je pri urejanju tega vprašanja ubrala drugačno pot. Za zasebni in javni sektor velja ista zakonodajna ureditev. Pravica do zasebnosti je v večini evropskih držav zavarovana z ustavo (Kovačič, 2006). V ZDA temu ni tako, saj pravica do zasebnosti ni ustavna kategorija. Originalna ustava, državljanom ne zagotavlja pravice do zasebnosti, pač pa jo je kot človekovo pravico konstituiralo šele Vrhovno zvezno sodišče, ki pa te pravice še vedno ni razširilo na varstvo osebnih podatkov (Radcliff, 2007). Nekateri so konstituiranje pravice do zasebnosti celo smatrali za »pravno izumljanje« (Kovačič, 2006, str. 56). Za ZDA je tako značilen stihijski pristop k regulaciji zasebnosti. Urejanje pravice do zasebnosti v ZDA je namreč partikularno urejeno v različnih zakonih, ki so večinoma nastali kot odziv na kakšen javno odmeven primer zlorabe(Kovačič, 2006).

Ena izmed pomembnih razlik med obema načinoma urejanja je tudi, da Evropska ureditev zaščite zasebnosti ščiti človeško dostojanstvo, medtem ko Ameriški pravni red ščiti svobodo. Dostojanstvo je socialni koncept medtem ko je svoboda političen. Dostojanstvo kot socialni koncept pomeni zaščito določenih družbenih norm znotraj družbe in bolj trpi zaradi aktivnost znotraj družbe, kot pa zaradi vmešavanja države, čeprav tudi preveč slednjega vodi v erozijo dostojanstva (Levin, 2005). Svoboda pa je političen koncept, ki mu največjo grožnjo predstavlja delovanje državnih akterjev.

Razlike pa so vidne tudi v uveljavljanju predpisov. Federal trade comission (FTC), ameriška agencija zadolžena za zaščito pred vdiranjem v zasebnost, le redko ukrepa proti kršiteljem. Tudi v primeru da pride do ukrepanja s to zgodi ponavadi v obliki zunaj sodnih poravnav simbolično majhnih kazni, medtem ko je izdajanje kazni v Evropi dokaj pogosta praksa (Sullivan, 2006).

Za evropski način urejanje te problematike obstajajo različne razlage. Po eni izmed njih je Evropska občutljivost glede osebnih podatkov zapuščina holokavsta, V času tretjega Rajha so se nacisti posluževali uporabe javnih in cerkvenih baz podatkov ter na ta način lažje identificirali Žide in jih nato deportirali v koncentracijska taborišča (Sullivan, 2006).

Druga izmed možnih razlag različnega pristopa urejanja področja pravice do zasebnosti je globoko zasidrana sumničavost Američanov do vladajočih struktur. Američani so že od nekdaj paranoični o svoji vladi in se trudijo omejiti njeno moč kolikor je najbolj mogoče. V Evropi je situacija nekoliko drugačna, saj se Evropejci zanašajo na svojo vlado, da jih zavaruje pred korporacijami (Wafa, 2008). Strah in paranoja pred nosilci oblasti v ZDA pa se odraža v tem, da nekateri Ameriški kritiki dojemajo obsežno zakonodajno urejanje kot grožnjo. Problem tovrstnega urejanja tiči v tem, da posameznik izgubi kontrolo nad svojimi informacijami v razmerju z vlado, saj si morajo na primer podjetja priskrbeti soglasja posameznikov in jih posredovati pristojni avtoriteti, preden jih lahko dejansko uporabijo (Nijhawan, 2003). Po mnenju nekaterih kritikov Evropska ureditev ni v skladu z Ameriško tradicijo. Evropska zakonodaja daje vladi veliko večjo kontrolo nad osebnimi podatki, kar nasprotuje široko uveljavljenim ameriškim vrednotam (Nijhawan, 2003). Tako na primer trči ob prvi amandma, ki zagotavlja svoboden pretok informacij. Iz tega bi se dalo sklepati, »vprašanje zasebnosti in obdelave osebnih podatkov v ZDA ni toliko vprašanje informacijske zasebnost, temveč svobode trgovanja in svobode komercialnega govora«(Kovačič, 2006, str. 66). Eden izmed pomislekov zakonodajnem urejanju je tudi, da bi taka obsežna zakonodaja negativno vplivala na svoboden pretok informacij v ekonomiji, ki je bistvenega pomena za poslovanje ameriških podjetij (Niijhawan, 2003).

V Evropi je varovanje zasebnosti prvenstveno usmerjeno v varovanje državljanov pred zlorabami zasebnosti s strani korporacij in vlade večinoma ne predstavljajo take grožnje, medtem, ko je v ZDA situacija ravno obratna (Sullivan, 2006). Ameriško gledanje je tehtanje interesov med pravicami posameznikov, da ohranijo svojo zasebnost proti

legitimnim ekonomskim interesom podjetij, da od posameznika pridobivajo osebne informacije in jih uporabljajo v tržne namene (Nijhawan, 2003).

Tendenco nezaupanja Ameriških uporabnikov v svojo vlado potrjujejo tudi nekateri izsledki raziskav. Po podatkih raziskave o nivoju zaupanja v načine, kako vlada skrbi za zaščito zasebnosti potrošnikov, so najmanjše zaupanje v vlado izrazili prav respondenti iz ZDA, največje pa respondenti iz Nemčije (Regan, 2003). V raziskavi, ki jo je izvedel Hsu (2006), rezultati kažejo, da Američani najbolj zaupajo komercialnim internetnim stranem, medtem ko respondenti iz Nizozemske in Azije bolj zaupajo vladnim spletnim stranem in so komercialnim pripravljeni zaupati veliko manj osebnih podatkov. Podobna raziskava kaže, da kar 64% Američanov zaupa svojim podjetjem, da bodo ravnali z njihovimi osebnimi informacije na korekten način, medtem ko je takih v Angliji 59% in v Nemčiji 55% (Regan, 2003). Vendar pa to ne pomeni, da Američani niso zaskrbljeni zaradi svoje pravice do zasebnosti. Po rezultatih drugih raziskav je namreč velika večina Ameriških uporabnikov spleta zaskrbljenih glede svoje zasebnosti na internetu (Milne in sodelavci, 2004).

5.1. »Safe harbour agreement«

Svet je globalen. Globalnost in različno pravno urejanje, pa prinašata težave pri poslovanju med državami. S svojo pravno ureditvijo Evropska unija vpliva tudi na tretje države. Te se morajo, vkolikor želijo poslovati z državami članicami EU, držati določenih standardov varstva osebnih podatkov. Tako evropska direktiva iz leta 1995 dovoljuje iznos podatkov samo v tiste države, v katerih je zagotovljeno ustrezno varstvo osebnih podatkov (Kovačič, 2006).

V devetdesetih letih prejšnjega stoletja, je po sprejetju te direktive, skoraj prišlo do zaustavitve trgovanja med ZDA in Evropo (Sullivan, 2006). Evropska Unija je menila, da so Ameriški standardi varstva osebnih podatkov pomanjkljivi. Evropska pravna ureditev je prišla v konflikt za Ameriško, kar je vodilo do dve leti trajajočih debat in se zaključilo s sporazumom Safe Harbour (Radcliff, 2007). Ta sporazum predvideva overjanje Ameriških podjetij, ki bi po taki overitvi lahko prejemala osebne podatke iz držav članic Evropske Unije (Kovačič, 2006).

Vendar pa je na račun tega sporazuma slišati mnogo kritik. Eden izmed problemov je, da ta »sporazum predvideva samo-certificiranje, saj je t.i. *'status safe harbour'* podeljen že s tem ko se podjetje obveže da bo spoštovalo načela o zaščiti zasebnosti«(Kovačič, 2006, str. 79). Vendar pa se Radcliff (2007) s tem ne strinja in pravi, da posamezna podjetja in njihovo zadostnost spoštovanja sporazuma, ocenjuje Evropska Unija. Šele ko le ta ugotovi, da so standardi zadostni, so potem vse države članice zavezane da spoštujejo te ugotovitve. Zavezanost vseh držav članic, da se podrejajo ugotovitvam organov EU, pa po mnenju nekaterih predstavlja veliko prednost, saj ta sporazum rešuje potrebo, da bi se ZDA morale dogovarjati z vsako članico posebej (Regan, 2003).

Ena izmed pomanjkljivosti tega sporazuma je tudi nizek nivo participacije. Le majhno število ameriških podjetji je del Safe Harbour sporazuma (Nijhawan, 2003). Tako po je po desetih letih obstoja, pristopilo k temu sporazumu le 1300 podjetij in niti enemu izmed teh podjetij tega dovoljenja niso suspendirali (Wafa, 2008). Tako na primer multinacionalno podjetje Google ni pristopilo k Safe Harbour sporazumu. Še več Podjetje se je tudi odvezalo vsakršne odgovornosti za varnost podatkov in v splošnih pogojih uporabe uporabnike seznanja s tem, da se »strinjajo s prenosom svojih osebnih podatkov v ZDA ali katerokoli drugo državo, kjer ima Google svoje podružnice« (Kovačič, 2006, str. 53). Uporabniki Googleove storitve GMail, pa dobijo na voljo tudi ogromne količine prostora za shranjevanje svoje elektronske pošte. To pa niti ni taka prednost kot se zdi na prvi pogled, saj na ta način posameznikov poštni nabiralnik hrani celotno zgodovino elektronskih sporočil, ki jih lahko Google po mili volji vsebinsko skenira (Dobosz, Green, Sisler, 2006). Google analizira elektronsko pošto svojih uporabnikov, z namenom odstranjevanja nezaželene pošte, virusov in za prikazovanje usmerjenih oglasov. Podjetje v tem ne vidi prav nič spornega in se brani z argumentom, da tovrstne analize izvajajo računalniški programi in je ne prebirajo fizične osebe (Kovačič, 2006).

Neintuziastični odziv in nepripravljenost za pristopanje k sporazumu nekateri pripisujejo zaskrbljenosti Ameriških podjetij. Podjetja naj bi namreč skrbelo ali se sploh lahko ravnajo po zapovedanih pravilih na način, ki bo zadovoljil Evropsko Unijo (Regan, 2003). Ta sporazum naj bi bil celo tako strog, da ga ameriška podjetja verjamejo, da ga ne morejo stoodstotno izpolnjevati. Tako nekatera izmed njih iščejo strokovno pomoč in hodijo k svetovalcem po nasvete kaj bi morala storiti, da bi ga lahko na primer spoštovala samo približno 70 odstotno (Sullivan, 2006).

Ameriški kritiki prav tako menijo, da načela tega sporazuma presegajo vse zahteve glede spoštovanja pravice do zasebnosti, ki so kdajkoli veljale v ZDA. Na ta način naj bi resno postavljal pod vprašanj ameriško suverenost (Regan, 2003). Teoretično lahko FTC, EU ali katerakoli država članica EU sproži tožbo proti podjetju, ki je del Safe Harbour sporazuma (Nijhawan, 2003). Ameriška združenja potrošnikov in skupine, ki se zavzemajo za zasebnost, pa izražajo skrb zaradi diskriminiranosti Američanov v primerjavi z Evropejci. Tako menijo, da ta sporazum državljanom EU nudi veliko večjo zaščito pred kršitvami njihove pravice do zasebnosti s strani Ameriških podjetij, kot jo nudi njihovim lastnim potrošnikom (Regan, 2003).

Evropska perspektiva je nekoliko drugačna. Evropski kritiki menijo, da Safe Harbour sporazum ne ponuja zadostne zaščite evropskim državljanom, saj se zanaša na samoregulacijski sistem, ki je očitno neuspešen v ZDA (Regan, 2003). Tako nekateri menijo, da je velika težava pri implementaciji tega sporazuma, nevmešavanje Ameriške vlade. EU se ponavadi dogovarja z vladami, vendar vlada ZDA, odklanja, da bi pri urejanju tega problema imela kakšno večjo vlogo. Uveljavljanje tega sporazuma je zaupala primarno privatnemu sektorju, tako da posledično ni nobene vladne entitete ki bi nadzirala njegovo implementacijo. Namesto tega so za to zadolžene samo fragmentirane državne in lokalne agencije z včasih nejasnimi pristojnostmi (Regan, 2003).

V ZDA so informacije, ki jih podjetja zberejo od kupcev za potrebe direktnega marketinga, pogosto njihovo edino premoženje. Onemogočanje pridobivanja informacij, pa ogroža uspeh mnogih ameriških podjetij na evropskih tleh (Nijhawan, 2003). Ameriška poslovna perspektiva tako interpretira ukrepe za zaščito zasebnosti kot ovire za svobodno trgovanje in vmešavanje v prost pretok informacij (Regan, 2003). Nekatera Ameriška podjetja celo vidijo Evropsko zakonodajo, kot preventiven način, kako ščititi evropska podjetja prej vstopom tujih podjetij na Evropsko tržišče. Podjetja, ki želijo vstopiti na evropski trg morajo tako tehtati stroške, ki jih imajo s ravnanje po pravilih ali pa preprosto sploh ne poslovati. (Nijhawan, 2003). Tako nekateri predlagajo, da bi bilo ravno zaradi finančnih in časovnih resursov, ki jih zahteva implementacija teh standardov v Ameriki, za ameriška podjetja morda koristno, da te standarde čim hitreje implementirajo (Radcliff, 2007).

Poleg tega pa nekateri vidijo problem tudi v nedefiniranju standarda zadostne zaščite podatkov, ki ga nalaga Evropska Unija. Podjetja morajo poskrbeti za zadostno mero zaščite podatkov, vendar pa je s stališča ameriških podjetji težava v tem, da zadostni standardi niso zadovoljivo precizirani, kar pomeni, da se morajo ameriška podjetja podrejati subjektivnem standardu (Nijhawan, 2003).

Nekateri ameriški kritiki menijo, da evropska ureditev preveč ceni individualno zasebnost pred komercialno svobodo govora, zavarovano s prvim amandmajem (Nijhawan, 2003). Po drugi strani pa so tudi taki, ki verjamejo, da se sčasoma te skrbi počasi umirjajo, saj so se ameriška podjetja počasi privadila na stroške in ostale posledice te ureditve (Levin, 2005).

Po mnenju nekaterih, pa je Evropska ureditev, bolj fasada, kot rešitev, ki bi dejansko delovala tudi v praksi. Prav iz tega razloga, poleg nekompatibilnega evropskega pravnega okvira, ne vidijo potrebe po uvajanju podobne stroge in nedelujoče regulacije v ameriški pravni red (Nijhawan, 2003). Poleg neizvedljivosti, ji očitajo tudi pomanjkanje uniformnosti. Uniformnost tako spodkopavajo različni standardi varovanja podatkov med posameznimi državami članicami in različna interpretacija direktiv v okviru nacionalnih zakonodaj (Nijhawan, 2003). Tako na primer nemška podjetja za pridobitev soglasja zahtevajo pisno privolitev posameznika, medtem ko v drugih državah to ni potrebno in zadostujejo druge oblike izražanja soglasja (Sullivan, 2006). Ureditev pa je tudi težko implementirati, saj je Evropa soočena z široko razširjenimi praksami zbiranja osebnih podatkov. Nad njimi težko drži pregled , kar posledično tudi zmanjšuje možnost, da bi regulirala prakse neevropskih podjetij (Nijhawan, 2003).

5.2. Slabosti in prednosti državne regulacij

V začetku so zakonski posegi v internet veljali za omejevanje svobode, vendar pa je pojav nezaželene elektronske pošte in čedalje večje ogrožanje informacijske zasebnosti privedlo do tega, da uporabniki čedalje bolj zahtevajo zakonodajno regulacijo interneta, da lahko zaščitili svoje pravice (Kovačič, 2006). Po podatkih raziskave, okrog 80% respondentov iz ZDA in Nemčije meni, da so izgubili nadzor nad tem, kako se zbirajo njihove osebne informacije in kako z njimi ravnajo podjetja. Iz teh rezultatov Regan (2003) zaključuje,

da obstaja mednarodno soglasje o izgubi potrošnikove pravice do zasebnosti. Vendar pa se nekateri sprašujejo ali bo taka regulacija res pomagala rešiti problem. Entitete, ki ogrožajo zasebnost so namreč postale zelo široko razširjene in jih je težko identificirati (Woo, 2006).

Šibka točka državne regulacije je tudi v tem, da ne more slediti hitremu razvoju tehnologije in vnaprej predvideti množico različnih situacij (Jančič in sodelavci, 2007). Prav tako lahko zakonodajna regulacija ureja in vnaprej prepoveduje le aktivnosti, ki so znane in jih je moč identificirati (Woo, 2006). Tako Hsu (2006) ugotavlja, da je samoregulacija morda bolj primerna, ker je bolj fleksibilna se hitreje prilagaja tehnološkim zahtevam in lažje skrbi za standardizacijo.

Državna regulacija pa zahteva tudi oblikovanje določenih izdelanih ciljev, kar pa v zvezi z pravico do zasebnosti ni možno. Pravica do zasebnosti je namreč subjektiven koncept. Zaradi te njene subjektivnosti, obstaja množica različnih ciljev in različnih izbir, za zadovoljevanje katerih je najbolj primeren način samoregulacija (Singelton, 1999). Težava je tudi v tem, da regulacija ne more regulirati niti obstoječe situacije in da je kar naprej soočena z grožnjo, da bi regulacija lahko pomembno zavirala razvoj (Jančič Bogatj in sodelavci, 2007). Nadzor z državne strani je tudi težko uveljavljati, saj obstaja veliko število različnih spletnih strani (Lee, 2003). Poleg tega je internet je preprosto prevelik medij, da bi ga lahko centralizirano kontrolirali (Lee, 2003). Tako prihaja do kršitev zakonodaje v mnogih državah, tudi tistih z dolgo demokratično tradicijo kot je na primer Francija. Po nekaterih podatkih se kar 90 držav ukvarja z nezakonitim prisluškovanjem in nadzorovanjem svojih državljanov (Global internet liberty capaign, 1999).

Vendar pa po drugi strani neupoštevanje zakonodaje ni nov fenomen. Tako kot na vseh drugih področjih, se v praksi zakonodaj tudi na tem mnogokrat ne upošteva. Vendar je njena prednost v tem, da imajo evropski državljani, vsaj možnost pritožbe, popravka napačnih podatkov in uporabe drugih pravnih sredstev, kar pa za državljane ZDA v zasebnem sektorju pogosto ne velja (Kovačič, 2006).

Druga slabost obsežnega zakonodajnega urejanja pravice do zasebnosti in prevelike anonimnosti uporabnikov, naj bi bilo preveč zasebnosti. Ta presežek zasebnosti bi lahko po mnenju nekaterih imel velike družbene stroške. Prevelika anonimnost naj bi

spodbujala dajanje napačnih in neresničnih informacij ter zmanjševala odgovornost (Nijhawan, 2003). Poleg tega si nekateri postavljajo vprašanje ali se je smiselno znašati samo na zakonodajne ukrepe, saj so po raziskavah sodeč, potrošniki pripravljeni popolnoma prostovoljno zaupati svoje osebne informacije (Norberg in sodelavci, 2007).

Državna regulacija pa je po mnenju nekaterih bolj učinkovita. Podjetjem tako predstavlja neko zunanjo spodbudo oziroma grožnjo, podjetjem ki se ne držijo pravil, medtem ko pri samoregulaciji te zunanje spodbude ni in ostane le moralna zavezanost potrošnikom (Kovačič, 2006). Državna regulacija ima torej svoje prednosti in pomanjkljivosti. Pozitivne in negativne lastnosti pa so značilne tudi za sistem samoregulacije.

5.3. Prednosti in pomanjkljivosti samoregulacije

Samoregulacija temelji na ideji «po kateri ponudniki sami sprejmejo določene zaveze glede načina in oblike ponudbe storitev ali opredelitve dolžnih ravnanj ali sprejmejo določene omejitve ponudbe« (Bogataj Jančič in sodelavci, 2007,str. 38).

Nekateri menijo, da je samoregulacija za kontrolo interneta veliko bolj učinkovita kot državna regulacija. Samoregulacija lahko hitreje sledi razvoju in se prilagaja novim situacijam. Vendar pa drugi vidijo njen nastanek zgolj kot posledico strahu pred državno regulacijo (Lee, 2003).

Samoregulacija ima tudi svoje ekonomske prednosti. Cenejša je z vidika podjetij in z vidika državnega aparata, ker oblastem ni treba aktivirati dragega državnega aparata za sprejem obsežne regulative in vpeljati obširnih nadzornih mehanizmov (Singelton, 1999). Samoregulacija ne potrebuje dragega zunanjega nadzora tretje strani, saj je ponujanje slabih storitev sankcionirano s strani tržnih zakonitosti in konkurence (Singelton, 1999). Vendar pa nekateri opozarjajo, da samoregulacija prav tako ni zastonj. Podjetja, ki se ne ravnajo po samoregulacijskih načelih, lahko s svojo neudeležbo prihranijo denar. Tako so podjetja, ki dejansko sodelujejo v samoregulaciji ekonomsko depriviligirana (Lee, 2003). To je eden izmed razlogov, zakaj se je mnoga podjetja ne udeležujejo. Nivo sodelovanja v samoregulacijski shemi je majhen. Večja podjetja ponavadi sploh niso del samoregulacije (Lee, 2003). Takšna situacija pa pomeni problem za potrošnika. Z vidika kupca je namreč

težko dognati katera podjetja niso udeležena, kar posledično še povečuje dobičke, tistih podjetjih ki v tej shemi ne sodelujejo (Lee, 2003).

V primeru, da podjetja pristanejo na samoregulacijo se pojavi naslednja težava. Prav tako kot državno regulacijo, je tudi samoregulacijo težko uveljavljati v praksi. Nadzorovanje zahteva veliko virov, ki se jih v ZDA pridobiva tudi s pomočjo sponzorskih sredstev. Tako ureditev pa s pridom izrablja Microsoft, saj se lahko na ta način izogne kritiki o svojih standardih varovanja zasebnosti (Lee, 2003).

Mnogi samoregulaciji očitajo popolno neučinkovitost. Samoregulacijski mehanizmi so prostovoljni in tako ni zakona ki bi odškodovanemu posamezniku omogočil pravico do odškodnine (Lee, 2003). Edino jamstvo za nerazkritje osebnih podatkov iz zbirk je «samo dobra volja in etika različnih nadzornih sistemov, pravna zaščita ni več možna mogoči so le neformalni pritiski javnosti« (Kovačič, 2006, str. 67). Odsotnost zakonodajne ureditve podjetjem ne nudi dovolj spodbud, da bi se podrejala samoregulaciji. Profitna orientiranost pa jim narekuje, da lahko veliko zaslužijo z na primer prodajo baz podatkov (Lee, 2003). Igra po pravilih podjetjem seveda ne ponuja tovrstnih ekonomskih spodbud.

6. Viri ogrožanja

Internet je v svojih začetkih veljal za kraj neomejen svobode in anonimnosti. Z njegovim razvojem pa se je izkazalo, da uporabnikom ne nudi teh prednosti, saj v spletnem okolju na njih preži mnogo nevarnosti.

Čedalje več je slišati o panoptični moči internetne tehnologije. Panopticum je Benthamov koncept zapora, kjer je zapornik konstantno nadzorovan in nikoli ne more biti prepričan ali ga v danem trenutku nadzorujejo ali ne. Zavedanje, da je posameznik opazovan pa vodi v samocenzuriranje vedenja in spreminjanje vedenja, kar je nekompatibilno z idejo človekove svobode (Klang, 2004).

Tehnologija pa poleg svoje panoptičnosti, zaradi svojih lastnosti omogoča zlorabe, ki bi bile v fizičnem svetu mnogo manj mogoče in uporabniki interneta izgubljajo varovalno funkcijo fizičnega prostora (Kovačič, 2006). »Po poročilu Privacy & Human Rights 1999 ogrožajo zasebnost trije pomembni trendi: globalizacija (odstranjuje geografske omejitve pri pretoku podatkov), konvergenca med tehnologijami (le te so med seboj čedalje bolj povezane in medoperabilne) ter multidmedialnost (podatki v neki obliki se hitro lahko spremenijo v drugo obliko« (Kovačič, 2003, str. 34). Z razvojem tehnologije se veča število informacij, ki jih moč shraniti, poleg tega pa se nižajo tudi stroški tovrstnega shranjevanja (Norberg in sodelavci, 2007). Po nekaterih ocenah se »moč tistih, ki zlorabljajo računalniške sisteme, vsakih deset mesecev podvoji, in sicer zato, ker razvoj tehnologije omogoča, da si napadalci za isti denar kupijo čedalje boljšo tehnologijo, hkrati pa se veča še število nezaščitenih računalnikov« (Kovačič, 2006, str. 206).

Za današnji čas je značilna rast uporabnikov svetovnega spleta na obrobju. Ti uporabniki nimajo ustreznega računalniškega znanja in zadosti izkušenj in se tako niso zmožni zaščiti pred nevarnostmi, ki prežijo nanje v spletnem okolju (Kovačič, 2006). Uporabniki se počutijo čedalje bolj ogrožene in se vse bolj zavedajo nevarnosti, vendar pa nimajo dovolj znanj, da bi razumeli na kakšne načine spletne strani zbirajo njihove osebne podatke in se ne znajo ustrezno tehnično zaščititi (Milne in sodelavci, 2004). Tako se čedalje bolj poudarja vidik izobraževanja internetnih uporabnikov. Še posebej so tukaj na udaru

mladostniki, ki v velikem obsegu uporabljajo internet za različne namene, vendar pa se v varnem zavetju svojih sob ne zavedajo nevarnosti (Moscardelli in sodelavci, 2007).

V zadnjem času pa se pojavlja tudi nova grožnja v obliki prikritih omrežij. Prikrita omrežja so med seboj omrežja med seboj povezanih računalnikov, ki se jih lahko uporabi za shranjevanje podatkov in izvrševanje drugih aktivnosti na napadenem računalniku. Napadalci pri novačenju novih računalnikov za prikrita omrežja, ne merijo na točno določeno in konkretno žrtev, pač pa je žrtev anonimna in kot taka ni pomembna, pač pa je pomembna populacija (Kovačič, 2006). Praviloma se upravljavci takih prikritih omrežij sploh ne zanimajo za podatke na napadenem računalniku, pač pa izkoriščajo sistemske vire tega računalnika za kriminalne dejavnosti (Kovačič, 2006). Na ta način nič hudega slutečega uporabnika vpletajo v izvajanje kaznivih dejanj.

6.1. Veliki brat

Vlade imajo na voljo mnogo orodij za zbiranje informacij o populaciji. Dostop do teh informacij pa ima tudi mnogo vladnih uslužbencev. Taka situacija pripelje do tega, da bi lahko zbrane informacije na primer kaj hitro zlorabil kak podkupljiv vladni uslužbenec (Attaran, Vanlaar, 1999). Vendar pa nekateri menijo, da vlade pravzaprav niso tako zelo velik zbiralec osebnih podatkov.

Po mnenju Jamnika (2008), javni sektor sploh ne zbira večjih količin osebnih podatkov, kot jih včasih. Vendar pa je v informacijski dobi pri zbiranju podatkov pomembna kvalitativna razlika. Vsi podatki so namreč digitalizirani, kar pa za razliko od papirnate dobe, ker bi iskanje želenih podatkov trajalo mesece, omogoča hiter priklic podatkov v sekundi (Jamnik, 2008). Vendar pa to ni edini problem. Pomembna razlika tiči tudi v dejstvu, da ima država dostop tudi do bolj zasebnih osebnih podatkov, kot ga ima na primer komercialni sektor(Kovačič, 2006).

Vendar pa se je po mnenju nekaterih drugih obseg vladnega zbiranja podatkov v zadnjem času močno povečal. Eden izmed pokazateljev tendence povečevanje zbiranja podatkov, bi utegnila biti Evropska direktiva o obvezni hrambi prometnih podatkov, ki je ob sprejetju dvignila veliko prahu. Direktiva prinaša, obvezno hrambo prometnih podatkov

telefonskih in internetnih komunikacij, vključno z naslovi elektronske pošte in lokaciji mobilnih telefonov da se za obdobje od 6 do 24 mesecev (Kovačič, 2006). Ta direktiva omogoča «hrambo podatkov na zalogo«, saj se bodo vsi ti podatki hranili za vse uporabnike brez vnaprejšnje sodne presoje (Bogataj Jančič in sodelavci, 2007, str. 387). Kar seveda v praksi pomeni, da se bodo vsi uporabniki vnaprej neselektivno in preventivno obravnavali kot potencialni kriminalci (Kovačič, 2006). Tovrstna obravnava državljanov pa seveda ni v skladu s konceptom domneve nedolžnosti. Prav tako stroške za tako hrambo nosijo operaterji, kar pomeni, da se stroški zakonitega prestrezanje prenašajo na pleča zasebnega sektorja (Kovačič' 2006).

V ZDA pa uporabljajo sistem Carnivore, ki po začetnih nasprotovanjih, naletel na plodna tla po terorističnih napadih 11. septembra. Ta sistem je poseben program, ki je nameščen na strežnikih pri ponudniku dostopa in beleži uporabnikovo aktivnosti na spletu in celo prestreza njegova elektronska sporočila (Kovačič, 2003). Vendar pa drugi ugovarjajo, da teroristični napadi pravzaprav niso pristna grožnja nacionalni varnosti tako velike države kot je na primer ZDA in da je verjetnost, da bi bil tak program uspešen pri preprečevanju terorističnih napadov tako majhna, da ne opravičujejo škode, ki jo povzroča masovno vdiranje v zasebnost (Coleman, 2006). Države tako izkoriščajo potrebo ljudi po večji varnosti in jim v takih trenutkih ponudijo rešitve, ki jih v običajnih razmerah javnost verjetno ne bila pripravljena sprejeti (Makarovič, 2001). Vendar pa tukaj tiči past. Varnost je potrebna za zaščito zasebnost, in ni zasebnosti brez varnosti, medtem ko nasprotno ni nujno res, vkolikor je ogrožena naša zasebnost to za sabo potegne tudi grožnjo naši varnosti (Katos in sodelavci, 2007).

Poznamo pa tudi bolj evropsko različico sistema za prestrezanje komunikacij. Escalon je partnerski sitem NSA (National Security Agency), Velike Britanije, Kanade, Avstralije in Nove Zelandije. Sprva naj bi bil namenjen prestrezanju zasebnih in poslovnih komunikacij, ki se nanašajo na mednarodni terorizem, promet z mamili in orožje za množične uničevanje, vendar se je izkazalo, da se ga da koristno uporabljati tudi za zbiranje informacij o prijateljskih državah, njihovi ekonomski politiki, gospodarstvu (Praprotnik, 2006).

6.2. Mali brat

Nevarnost pa v zadnjem času ne preži več zgolj s strani države, saj so se neslutene možnosti nadzora odprle tudi zasebnikom. Tako ni več toliko pomembno, da nadzorujmo tradicionalne in znane entitete vmešavanja v zasebnost, kot so na primer država in mediji (Woo, 2006). Kovačič (2006, str. 139) pravi, da smo prišli do točke «ko poglavitni problem ni več država, temveč družba, in ko bi morala država posameznike zaščititi pred družbenimi akterji«.

Tako nam danes ni potrebno skrbeti več samo glede nevarnosti, ki nam preži s strani države in telemarketerjev, saj so se razmahnili tudi mali brati, ki sestojijo iz naših sosedov, šefov in trgovcev (Forcht, 1994). Za sto dolarjev je na primer možno kupiti spywere progam, ki nam pomaga, da sledimo aktivnostim svojih bližnjih na internetu. Z njegovo pomočjo je možno dostopiti do vseh elektronskih sporočil, ki so jih prebrali ali sestavili, dobiti v pogled v zapise pogovorov v spletnih klepetalnicah, zgodovino obiskanih spletnih strani in gotovo še mnogo več (Baruh, 2007).

V ZDA pa je prišlo tudi do privatizacije javnih nadzornih sistemov. Mnogim se zdi to precej problematično, saj je nad zasebnimi podjetji oziroma nedržavnimi akterji, stopnja nadzora veliko manjša kot nad državo (Kovačič, 2006).

6.3. Virusi

Velika večina uporabnikov, je pod vtisom, da so virusi največja grožnja na internetu. Proti virusom se da dokaj dobro zavarovati s protivirusno programsko opremo. Seveda so družbe, ki se ukvarjajo s prodajo protivirusnih programov, zainteresirane za njihov obstoj, saj bi drugače izgubile svoj vir dohodka (Ozimek, 2005). Ozaveščenost uporabnikov interneta, da ne nalagajo neznanih programov z interneta, bi upočasnila širjenje virusov in lahko celo nadomestila protivirusne programe (Ozimek, 2005).

Virusi tako, razen tega da vplivajo na normalno delovanje računalnika, nimajo kakšnih strašnih implikacij s stališča pravice do zasebnosti. Iz tega razloga jim v tem diplomskem delu ne bomo posvečali preveč pozornosti.

6.4. Elektronska pošta

Za razliko od navadne pošte, je elektronsko pošto veliko lažje prestrezati, saj nešifrinirana potuje po svetovnem internetnem omrežju. Njena vsebina je tako vidna upraviteljem poštnih strežnikov in posredniških strežnikov. Vendar pa k sreči v veliki večini držav, preko katerih potujejo naša elektronka sporočila, velja načelo pisemske tajnosti in morajo biti sporočila izbrisana, takoj ko so bila posredovana naprej (Kovačič, 2003). V Sloveniji je elektronska pošta, prav tako kot konvencionalna pisemska pošta, zavarovana z 34. členom Ustave in jo tehnično relativna nezahtevnost poseganja vanjo, ne dela prav nič manj zasebne (Jančič in sodelavci, 2007). Problem zasebnosti elektronske pošte je največkrat izpostavljen v kontekstu zasebnosti na delovnem metu.

6.5. Zasebnost na delovnem mestu

Nadzorovanje in vdiranje v zasebnost na področju pošiljanja elektronske pošte je posebej pereč problem na delovnem mestu. Slovenska ustava pod okriljem 34. člena zagotavlja pravico do tajnosti pisem in drugih občil. Med pisma in druga občila štejemo tudi elektronsko pošto in sms sporočila, pri čemur ni ključnega pomena, da se ta sporočila prenašajo le po javnem telekomunikacijskem omrežju. Pravica do zasebnosti je zavarovana tudi v privatnih omrežjih, čeprav je v slednjih obseg varstva manjši (Kovačič, 2003).

Vendar pa določbe glede tajnosti vsebine sporočila Zakona o Elektronskih Komunikacijah veljajo zgolj nasproti državnim organom in se nanašajo le na odprte telekomunikacijske sisteme, ki so dostopni javnosti. Tako jih ni možno uporabljati za notranja računalniška omrežja v posameznih podjetjih ali državnih ustanovah (Klemenčič, 2005). V ZDA je situacija podobna. Četrti amandma sicer ščiti zasebnost, vendar je ta zaščita mišljena samo za dejanja s strani države (Hartman, 2001). To je razlog, da imajo slovenski delojemalci, podobno kot v ZDA, razmeroma dobro zaščito pisemske tajnosti, pred posegi s strani državnih akterjev. Državni organi za poseg v pravico do komunikacijske zasebnosti potrebujejo sodno odredbo, medtem ko tovrstni posegi v zaposlitvenem odnosu ostajajo pravno nedorečeni, saj podjetja na primer ne morejo pridobiti sodne odredbe (Jančič in sodelavci, 2007).

Področje varstva zasebnost na delovnem mestu je zaznamovano s konfliktom interesov. Nasproti si stojijo predvsem trije različni interesi: delodajalca, da nadzira delovni proces; delojemalca, ki ima legitimen interes do svoje zasebnosti in tretjih oseb, ki vstopajo v stik z zaposlenim.

Delodajalec ima oblast nad opremo in upravičen interes, da nadzira ali se le ta uporablja skladno z namenom. Prav tako ima tudi interes, da odkriva, preprečuje in sankcionira disciplinske prekrške (Klemenčič, 2005). Tovrstno rekreacijsko deskanje po internetu ozirom cyberslacking namreč ni popolnoma nedolžno. Tako lahko v najboljšem primer povzroči le izpad produktivnosti, prinaša finančne izgube in upočasnjujejo delovanje računalniškega sistema v podjetju, v najhujšem primeru pa lahko rezultira v pravne posledice (Mills, Beldona, Clay, 2001).

Nadzorovanje elektronske pošte na delovnem mestu je najpogosteje opravičeno z lastništvom opreme. Vendar pa samo lastništvo nad opremo ne bi smelo opravičevati na primer pregledovanja elektronske pošte zaposlenega in drugega vdiranja v pravico do zasebnosti. Nadzor nad tem kako zaposleni uporabljajo službeno opremo bi se lahko vršil tudi na kak drug način, ki ne bi pomenil tako velikega posega v človekove pravice (Coleman, 2006).

V Sloveniji lahko delodajalec zasleduje svoje zakonite interese, vendar morajo biti njegovi ukrepi sorazmerni z legitimnim ciljem, ki ga z svojimi ukrepi zasleduje (Jančič in sodelavci, 2007). To pomeni, da morata obseg in oblika nadzora stremeti k najmanjšemu možnemu posegu, s katerim je še mogoče doseči namen nadzora, kamor bi lahko na primer uvrstili preprečitev hujše zlorabe službenih sredstev (Makarovič, Klemenčič, Klobučar, Bogataj, 2001). Tako nekateri menijo, da je najboljša ideja oblikovanje internega akta s katerim se zaposleni seznanijo z internimi predpisi o uporabi elektronske pošte in pogoji v katerih je dopustno da delodajalec vpogleda v elektronski nabiralnik zaposlenih ter na kakšen način lahko to stori (Jančič in sodelavci, 2007). Zaposleni morajo v ta nadzor privoliti. Vendar pa je pri tem pomembno, da privolitev za tak nadzorni ni v celoti nesorazmerna in izsiljena z strani delodajalca, ki je v tem primeru močnejša stranka (Makarovič in sodelavci, 2001).

V ZDA delojemalec nima takih pravic. Delodajalec ima izredno široke pravice in lahko kadarkoli vpogleda v elektronsko pošto zaposlenega in nadzoruje druge komunikacije, za vršitev katerih se uporablja lastnina podjetja in službena oprema (Sullivan, 2006). V primeru, da delodajalec zaposlenega vnaprej obvesti, da bo izvajal nadzorovanje, se šteje da je s tem uničil vsako razumno pričakovanje zasebnosti s strani zaposlenega (Hartman, 2001). To pa še ni vse. Ameriško sodišče je med drugim ugotovilo, da tudi če delodajalec zaposlenim izrecno zagotovi, da jih ne bo nadzoroval, še vedno ni razumnega pričakovanja zasebnosti, da delodajalec ne bo bral elektronskih sporočil svojih uslužbencev (Hartman, 2001).

Tako je nadzor na delovnem mestu v ZDA cvetoča dejavnost. Potreba po nadzorovanju uslužbencev je ustvarila pol bilijona dolarjev vredno industrijo za nadzor in upravljanje interneta na delovnem mestu od filtrov pa do druga programske in strojne opreme (Millis in sodelavci, 2001). Sem na primer sodijo razni programi za sledenje internetne aktivnosti, prepoved dostopa do nekaterih spletnih strani, seznanjanje z prenesenimi datotekami, programi ki beležijo koliko časa je nekdo preživel na neki spletni strani in tako naprej (Hartman, 2001). Po nekaterih podatkih, je tako kar 80% zaposlenih Američanov na delovnem mestu izpostavljeno neki vrst nadzora in zbiranja podatkov, ne glede na to koliko se poskušajo zaščititi (Hartman, 2001).

Vendar pa v tej debati ni prisoten le delodajalčev interes,da nadzira delovni proces. Tako ne smemo pozabiti na interese in pravice zaposlenega. Delojemalec ima interes do zasebnost in zagotovljeno pravico, da na delovnem mestu vzpostavlja osebne in socialne stike (Jančič in sodelavci, 2007). Ukvarjanje z zasebnimi zadevami na delovnem mestu je pravzaprav postala nuja. Zaposleni se ne more izogniti, da med službenim časom ne bi urejal zasebnih zadev, saj je večino časa, ko so ima privatne opravke, v službi (Hartman, 2001).

To razumevanje potreb zaposlenih je vidno tudi iz odločbe francoskega kasacijskega sodišča. Čeprav v Sloveniji še nimamo izrazite pravna prakse s tega področja, je primerjalno pravno gledano pomembna odločitev francoskega kasacijskega sodišča, ki ugotavlja, »da je popolna prepoved uporabe elektronske pošte na delovnem mestu v neslužbene namene v informacijski dobi povsem nerealna in krši načela sorazmernosti« (Jančič in sodelavci, 2007,str. 190). Prav tako je to taisto sodišče odločilo, da se na ta

način pridobljeni dokazi ne smejo uporabljati v civilnem ali disciplinskem postopku, ki bi imel za rezultat odpust delavca z delovnega mesta (Makarovič in sodelavci, 2001). Prav tako pa je tudi ugotovilo tendenco, da delo počasi prežema celotno posameznikov življenje. Med drugim tako ugotavlja, da »evolucija novih delovnih razmerij in njihovih oblik (trajanje delavnika, honorarno delo, delo na domu, fleksibilni delovni časi, delo na daljavo ipd.) ter nove tehnologije, prinašajo vse večje prepletanje zasebnega in delavnega okolja« in tako delo nujno tudi vdira v vse kotičke zasebnega življenja (Makarovič in sodelavci, 2001).

Pri nadzoru delojemalca pa seveda ne smemo pozabiti na človeško plat. Tovrstno nadzorovanje in vmešavanje v zasebnost zaposlenih, ima za slednje tudi psihične posledice. Tako imajo lahko take nadzorovalne prakse in totalna kontrola nad zaposlenimi, negativne posledice na čustveno stabilnost zaposlenih, saj lahko na primer vodi v občutke negotovosti in nesigurnosti (Hartman, 2001).

Vendar pa si pri poseganju elektronske komunikacije ne nasprotujejo le interesi delodajalca in zaposlenega. Pojavlja se tudi vprašanje vpletenosti tretjih oseb, katerimi zaposleni navezuje stike na delovnem mestu. Te tretje osebe, ki vstopajo v stik z delojemalcem in morda sploh ne vedo, da je naslov oziroma telefon služben, pa imajo prav tako legitimen interes, da njihova komunikacija ostane zasebna (Klemenčič, 2005).

6.6. Komercialni sektor in zbiranje osebnih podatkov

Komercialni sektor je velik, če že ne največji zbiralec in obdelovalec osebnih podatkov. V začetku so bili sicer nekateri avtorji prepričani, da bo nezaupanje kupcev močno oviralo razvoj spletne trgovine, vendar pa se je kasneje izkazalo da do tega ni prišlo. Spletno trgovanje je, kljub načelni zaskrbljenosti uporabnikov, doživelo ekspotencialen razmah (Wafa, 2008).

Kljub njegovi praktičnosti, pa spletno nakupovanje še vedno budi pomisleke. Spletna trgovina pa je za razliko od navadne trgovine veliko bolj tvegana. Poleg tega pa večino tveganja nosi kupec, saj le ta plača in izpolni svoj del obveznosti, medtem ko trgovec svojo obvezo opravi kasneje (Jančič in sodelavci, 2007). Pri spletnem nakupovanju na

potrošnika prežijo tri vrste nevernosti. Tako so lahko ogroženi podatki na njihovih računalnikih, lahko je ogrožen prenos podatkov do spletnega podjetja ali pa so lahko ogroženi podatki, ki jih o kupcu hrani podjetje (Milne in sodelavci, 2004).

Poleg tega je spletna trgovina tudi globalna. Globalnost predstavljava težavo, saj imajo različne države različno urejeno oziroma neurejeno področje spletnega trgovanja Tako se lahko zelo hitro zgodi, da kupec vstopi v poslovni odnos z podjetjem o katerem nima nobenih podatkov in je locirano v drugi državi (Jančič in sodelavci, 2007). Na ta način spletni trgovci izkoriščajo to teritorialno razdrobljenost. Slednja jim omogoča, da v okviru svojega prava z različnimi metodami prekrijejo stroške kakovost in druge lastnosti nekega izdelka ali storitve in tako zavedejo potrošnika (Jančič in sodelavci, 2007).

Spletno nakupovanje pa je tudi mnogo manj anonimno od običajnega nakupovanja, saj je za uspešno transakcijo potrebno, da kupec zaupa na primer svoje ime, naslov, številko kreditne kartice in druge osebne podatke (Pollach, 2005). Po slovenski zakonodaji lahko spletni trgovci zbirajo tovrstne podatke za opravo transakcije brez osebne privolitve, vendar to ne pomeni, da lahko potem z zbranimi podatki prosto razpolagajo in jih lahko uporabljajo za kakršne koli druge namene (Jančič in sodelavci, 2007). Tako je v primeru, da namerava upravljavec baze osebnih podatkov, te podatke posredovati naprej za namene neposrednega trženja ali jih oddati podizvajalcem, pred posredovanjem dolžan na lastne stroške obvestiti uporabnika in pridobiti njegovo pisno soglasje (Antić, 2007). Tako obvestilo mora vsebovati katere podatke se posreduje, komu se jih posreduje in za kakšen namen (Antić, 2007)

Osebni podatek je definiran v 6. členu ZVOP-1 kot »katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko v kateri je izražen« (Jančič in sodelavci, 2007, str. 202). Fizična oseba je določljiva, če jo je možno posredno ali neposredno identificirati in sicer na način, da taka identifikacija ne povzroča nesorazmerno veliko časa, finančnih sredstev in napora (Antić, 2007). Slovenska ureditev dovoljuje zbiranje naslednjih osebnih podatkov brez soglasja uporabnikov: osebno ime, naslov stalnega ali začasnega prebivališča, telefonska številka, elektronski naslov in število telefaksa (Antić, 2007).

Podatki iz velikih podatkovnih baz podjetji so lahko tudi ukradeni s strani hackerejev ali goljufivih uslužbencev na kateri koli točki procesa obdelave teh podatkov (Elovici,

Glezer, Shapira, 2005). Eden izmed večjih problemov pri varovanju podatkov je outsourcing ali oddaja del podizvajalcem. Ameriška podjetja za opravljanje manj zahtevnih programerskih del in administrativnih del, pogosto posredujejo občutljive oseben podatke v države z cenejšo delovno silo. Pri tem pa lahko kaj hitro pride do zapletov, saj ob morebitni zlorabi zasebnosti zunaj ZDA posamezniki nimajo na voljo pravnih sredstev za ukrepanje (Kovačič, 2006). Kovačič (2006) v zvezi s tem, navaja primer indijske prepisovalke medicinskih krotek, ki je ameriškemu podjetju grozila, da na internetu objavila občutljive podatke, v kolikor ji ne bodo plačali za opravljeno delo.

Zaskrbljeni posamezniki svojo identiteto pogosto branijo s tem, da fabricirajo podatke o sebi, Prekrivanje podatkov in ponarejanje identitete, je postalo orodje uporabnikov za ohranitev anonimnosti in zaščito pred morebitnim vdorom v zasebnost. Kot tako ima po mnenju nekaterih, pozitiven namen in svoje prednosti ter si zato zasluži družbeno dovoljenje (Woo, 2006). Zaščita osebnih podatkov je tako v interesu podjetij, saj v nasprotnem primeru stranke oblikujejo protiukrepe, kot so na primer uporaba lažnih imen, več elektronskih naslovov, zamenjava gesel za dostop do različnih spletnih strani (Larose, Rifon, 2006). Podjetja bi morala, namesto da zaskrbljenost kupcev glede njihove zasebnosti vidijo kot grožnjo, raje videti kot način kako izboljšati zaupanje svojih strank, zgraditi svoje ime, se izogniti stroškom, izboljšati zadovoljstvo svojih kupcev in ustvariti nove vire dohodkov (Miller, Arning, 2003). Tovrstno izmišljevanje identitete in potvarjanje podatkov ima lahko za podjetje velike finančne in druge posledice, saj le ta na podlagi napačnih podatkov napačno sklepajo na trende in napačno ciljajo svoj trg (Lwin, Williams, 2003). Podjetja imajo lahko od poštenih standardov zbiranja osebnih informacij koristi, saj zbiranje, procesiranje in hramba nepotrebnih in napačnih informacij velik vir izčrpavanja finančnih in drugih sredstev (Collier, 1995). Po drugi strani pa je tudi res da sama hramba velikega števila podatkov sploh ne predstavlja več pomembnega problema, saj se hrambene kapacitete nenehno povečujejo (Kovačič, 2006). Kvaliteta zbranih podatkov je omejena tudi iz drugih razlogov. Tako se lahko na primer zamenja uporabnikov IP naslov. Tudi ko se ugotovi da gre za isti računalnik (na primer z uporabo cookija) je še vedno možno, da ga uporablja neka druga oseba (Wel in sodelavci, 2004).

Vendar pa to niso edini problem z zbiranjem napačnih osebnih podatkov. Zbiranje napačnih osebnih podatkov ima lahko za posledico ustvarjanje napačnih sklepov o osebi, kar ima lahko za posameznika velike posledice na delovnem mestu, pri najemu kredita in

drugje (Forcht, Tomas, 1994). Uporabniki v Evropski Uniji, pa imajo vsaj možnost zahtevati popravek napačnih informacij, medtem, ko v ZDA to razen v kreditnih poročilih, ni možno, saj komercialnih baz podatkov ne ureja nobena regulativa (Sullivan, 2006). Pritožbe kupcev prav tako negativno vplivajo na posel in izgubljanje strank, ter zmanjšujejo finančne vire podjetja (Collier, 1995).

Nekateri pa v množičnem zbiranju in obdelavi osebnih podatkov, pravzaprav ne vidijo nobenega problema v smislu poseganja v zasebnost uporabnikov interneta in jo razumejo zgolj kot svobodno izmenjavo informacij in problem svobode trgovanja (Kovačič, 2006). Poleg tega je vedno večja količina mladih uporabnikov pripravljena povsem prostovoljno deliti svoje osebne podatke na straneh kot so Myspace in Facebook in v tem ne vidijo nobenega problema, čeprav so tovrstne strani lahko zlata jama za oglaševalce. Vzrok temu je morda, da se morda ne zavedajo nevarnosti, ki jih predstavlja ta nova paradigma (Wafa, 2008). Tako nekateri v tem vidijo dilemo. Zakonodajna zaščita tovrstnih uporabnikov, ki prostovoljno posredujejo svoje osebne informacije je morda nepotrebna, saj je njen namen ta da bi uporabnike ščitila pred sami sabo, ko bi morali le ti nadzorovati svoje lastno vedenje (Norberg in sodelavci, 2007). Tako bi bilo hinavsko, pokroviteljsko in neučinkovito, določati kaj je dobro za apatično javnost, ki ji ni mar kako se ravna z njihovimi osebni podatki in je to sploh ne skrbi (Woo, 2006).

Vendar pa podatki nekaterih raziskav dajejo drugačen vtis. Tako bi se iz nekaterih izmed njih dalo sklepati, da uporabniki spleta morda le niso tako zelo apatični in pripravljeni svoje podatke zaupati komurkoli in kadarkoli. Po podatkih ene izmed raziskav je kar 78 % Američanov zavrnilo dajanje osebnih informacij podjetjem, če so smatrali da podjetje teh informacij ne potrebuje ali če so bile zahtevane informacije preveč osebne, medtem, ko je bilo Angleških respondentov, ki so zavrnili dajanje takih informacij je bilo le 58% (Regan, 2003). Ta ugotovitev je nekoliko protislovna, glede na to da so v isti raziskavi Angleži izrazili veliko manjšo stopnja zaupanja v komercialni sektor. Odstopanje avtor pojasnjuje s tem, da Ameriška podjetja verjetno zahtevajo več osebnih informacij, saj imajo bolj razvit direktni marketing (Regan, 2003).

6.7. Soglasje

Za zbiranje in obdelovanje osebnih podatkov se običajno zahteva soglasje. Vendar pa to ne bi smelo biti soglasje zavoljo soglasja. Pomembna je namreč tudi kvaliteta. V praksi se ta vidik pogosto zanemarja. Mnogi trgovci z informacijami svoje spletne strani opremijo z izjavami o politiki zasebnosti, katerih glavni namen je odvračanje bralca od branja. Napisane so na tak način, da sicer ne lažejo, vendar jih je vseeno takorekoč nemogoče razmeti (Pollach, 2005). Informiran pristanek zahteva, da je človek prejel zadostno količino razumljivih informacij in nato eksplicitno izrazil svoje soglasje (Faden in Beauchamp, 1886 v Pollach, 2005). V primerih zavajanja torej ne gre za informiran pristanek. Privoljenje pa ima tudi svojo subjektivno dimenzijo. Soglasje pomeni različno za različne ljudi, od katerih nekateri ne premišljuje ravno preveč skrbno, kaj jim v prihodnosti lahko prinese razkritje osebnih podatkov (Woo, 2006).

Zbiranje podatkov brez informiranega privoljenje je neetično in ima za posledico družbene stroške vdiranja v zasebnost posameznikov. Te stroške je seveda potrebno pretehtati v razmerju do koristi, ki jih imajo podjetja od tovrstnega zahrbtnega zbiranja podatkov (Pollach, 2005). Tako velja razmisliti ali se ne bilo morda bolje posluževati bolj etičnih načinov, zmanjšati občutke ogroženosti in vzpostaviti zaupanje strank.

6.8. Profiliranje

Internet dovoljuje komercialnemu sektorju, da le ta cilja svoj trg bolj direktno, kot je to možno s klasičnim načinom oglaševanja v tisku ali na televiziji, saj sta slednja načina omejena na široke demografske skupine (Dobosz in sodelavci, 2006). Poleg tega, so v dobi ko je potrebno potrošnika poznati bolj kot pozna sam sebe, dobili podatki in informacije, ki so bili včasih popolnoma vsakdanji in nezanimivi, veliko tržno vrednost (Kovačič, 2003). Z natančnim profiliranjem naj bi tako podjetja svojim strankam omogočala tako imenovane personalizirane storitve (Graven 2001, v Kuchera, Plaisent, Bernard, Lassana, 2005). Tovrsten behavioralni marketing pa je po mnenju nekaterih bolj sporen od klasičnega marketinga, saj za učinkovito delovanje zahteva zbiranje osebnih

podatkov v povezavi z osebno brskalno zgodovino nekega posameznika (Dobosz in sodelavci, 2006).

Uporaba podatkov marketinške namene ima svoje dobre lastnosti. Tovrstna uporaba namreč omogoča, da nekatere spletne strani ostanejo brezplačne. Popolna prepoved tovrstne uporabe bi lahko resno zmanjšala funkcionalnost spleta in zavrla razvoj internetne ekonomije (Kovačič, 2003). Nekateri ugovarjajo, da ta tovrstno profiliranje in identifikacija uporabnikov dovoljuje podjetjem, da na račun povratnih kupcev ustvarijo mnogo več dobička. To pa pripomore k temu, da podjetja povečajo tržno učinkovitost in dobičke (Cigiliano, 2000, v Kuchera in sodelavci, 2005). Zagovorniki tovrstnega zbiranja podatkov in njihovo uporabo v tržne namene menijo, da je preprosto poskušajo doseči kupca bolj učinkovito in njegov nabiralnik napolniti s pošto, ki je stranka zaradi njene relevantnosti glede na svoje potrebe, ne smatra za odpadno pošto (Collier, 1995).

Vendar pa je možno temu ugovarjati. Pojavljajo se pomisleki, da bodo podjetja s tovrstnim oglaševanjem manipulirala s posameznikom. Na ta način mu bodo na primer ponujala predvsem storitve, ki jih bo glede na ocenjene preference lažje sprejel, kot pa storitve, ki bi jih potrošnik v resnici potreboval (Gandy, 1996, vBaruh, 2007). Poleg tega pa precej verjetno, da bi se kljub večji natančnosti zanimivih ponudb, število takih 'posebnih' ponudb še povečalo (Wel in sodelavci, 2004). Po podatkih raziskav večina respondentov ni zainteresirana za prejemanje oglaševalskega materiala. V Angliji je zainteresiranih na primer samo 29%, medtem, ko je zainteresiranih v ZDA kar 48% ljudi (Regan, 2003).

Pri vprašanju profiliranja gre s pravnega stališča predvsem za »sporno sekundarno uporabo osebnih podatkov, ki jih posameznik pusti med deskanjem po svetovnem spletu in uporabo elektronske trgovine« (Klemečič, 2005, str.52). V primeru, da se take baze nanašajo na določljive uporabnike, predstavljajo baze osebnih podatkov. Po slovenski zakonodaji bo moral v tem primeru upravljavec spletne strani pridobiti osebno privolitev, prijaviti zbirko in opredeliti namen zbiranja kot neposredno trženje po spletu z oblikovanjem konkretnemu uporabniku prilagojenih ponudb (Jančič in sodelavci, 2007). Tako pridobljeni osebni podatki se lahko uporabljajo le za vnaprej opredeljen namen. To pa mnenju nekaterih kritikov predstavlja problem v mednarodnem kontekstu, saj mora

biti vse na ta način zbrane informacije uničene po njihovi uporabi (Nijhawan, 2003). Vendar pa s stališča uporabnikove zasebnosti, to predstavlja prednost.

Obstaja pa tudi drug način profiliranja strank. Podjetje lahko ustvari podroben profil o posamezniku, brez da bi ga identificiralo. Lahko mu na primer dodeli samo identifikacijsko številko. Na ta način prav tako lahko oblikuje sklepe o njegovem prihodnjem obnašanju, se odloča o tem ali bi ga izključilo iz ciljne skupine in išče načine kako bi mu kar najbolje prikrojilo sporočila (Baruh, 2007). Tovrstni anonimni profili s vidika varstva osebnih podatkov v slovenski ureditvi niso sporni, saj se ne nanašajo na fizično določljive osebe. Zbiralec pa mora seveda kljub temu skrbno premisliti ali se uporabnika res ne da kako posredno ali neposredno identificirati (Jančič in sodelavci, 2007). Vendar pa nekateri opozarjajo da anonimizacija profilov morda le ni tako zelo nesporna. Taki profili anonimnih posameznikov, združeni v profile skupin, se lahko uporabljajo na isti način kot, da bi šlo za osebne podatke, kar posledično vodi v nepravične sodbe o ljudeh in deindividualizacijo (Wel in sodelavci, 2004).

6.9. Personalizacija storitev

Personalizacija storitev v obliki raznih kartic zaupanja, ki omogoča bolj kupcu prilagojeno nakupovalno izkušnjo, je bila v uporabi že dolgo prej preden se je razvil internet in spletno nakupovanje (Nijhawan, 2003). Vendar nekateri tej zgodovinski danosti oporekajo. Sicer je res, da so bile tovrstne tehnike v uporabi že prej, vendar pa internet omogoča zbiranje in obdelavo podatkov na nove načine. Tako Wel in sodelavci (2004) menijo, te da tehnologije povečujejo obseg tovrstnega profiliranja in s pomočjo tehnik podatkovnega rudarjenja, omogočajo uporabo podatkov za odkrivanje novih vzorcev brez posebnih novih raziskav. To pa ni edina težava. Podjetja kot na primer Amazon, ponujajo kupcu izdelke glede na njegovo nakupovalno zgodovino in mu s tem zapirajo pot, da bi naslednjič kupil produkte, ki ne bili v veliki meri podobni prejšnjim (Woo, 2006). Tovrstno usmerjeno nakupovanje pa bi lahko vodilo k fragmetiranju populacije v različne segmente. Te skupine bodo v manjši meri izpostavljene mnenju drugih skupin, kar bi lahko imelo za posledico polarizacijo družbe (Baruh, 2007).

Možna negativna posledica je tudi izključevanje določenih segmentov ljudi iz koristenja določenih produktov in storitev s cenovno diskriminacijo. Tako bi se podjetja usmerjala

na kupce, ki jim bodo prinašali dolgotrajen dobiček in vsem ostalim zaračunavale večje cene (Baruh, 2007). Tovrstno gibanje cen glede na ponudbo, povpraševanje in potrošniške preference je znano pod imenom dinamično določanje cen. Primer tega se je zgodil konec leta 2000 pri uporabi spletne trgovine Amazon, saj so uporabniki ugotovili, da za nekatere izdelke plačujejo več, kot drugi. Razlika v ceni pa je temeljila na njihovih potrošniških preferencah (Kovačič, 2003).

Tovrstni nadzor in vdori v zasebnost potrošnikov, so navidez do uporabnika zelo prijazni. Kupcem je všeč, da jih prepoznajo in jih obravnavajo, kot da so posebni. Vendar pa to lahko velja za trgovca v trgovini, ki ima omejeno kapaciteto stvari, ki si jih je zmožen zapomniti o svoji stranki. Pri podatkovnih bazah te omejitve ni, saj jih je vedno možno nadgraditi (Wel in sodelavci, 2004). Po raziskavi med slovenskimi uporabniki interneta, ti ogrožanje zasebnosti dojemajo v smislu vdora v računalniški sistem in se ne zavedajo nevarnosti podatkovnega nadzora v smislu izdelovanja uporabniških profilov, ki bolj prefinjeno in posredno ogrožajo zasebnost (Kovačič, Vehovar, 2000).

6.10. Izjave o zasebnosti

Podjetja poskušajo zaupanje strank pridobiti z izjavami o zasebnosti. Vendar pa slednje na žalost ne prinašajo zagotovila, da bodo uporabnikovi osebni podatki v varnih rokah. Izjave o zasebnosti so ponavadi tudi precej dvoumne, kot je na primer zagotovilo spletnih strani, da informacij ne bodo delili s tretjimi strankami. V velikih podjetjih je tako možnost diseminacije veliko večja kot si na primer uporabniki predstavljajo (Wel in sodelavci, 2004).

Vsebina izjav o zasebnosti je večkrat videti kot poskus preprečevanja obiskovalcev spletne strani, da o sebi prostovoljno razkrijejo več informacij. Take izjave ponavadi poudarjajo zgolj dobre strani takega razkritja kot na primer dostop do informacij ter udobnost in poskušajo minimizirati morebitna tveganja pri takem razkritju (Larose in sodelavci, 2006). Poleg tega za uporabnika ni lahka naloga, da išče in temeljito prebira izjave o zasebnosti na vsaki spletni strani, ki jo obišče in preverja ali se je spremenila odkar je zadnjič obiskal spletno stran (Wel in sodelavci, 2004).

Po podatkih nekaterih raziskav, kar 50% respondentov v ZDA in UK išče izjave o zasebnosti na internetu in 63% uporabnikov interneta zavrača razkrivanje informacij tistim spletnim stranem, ki imajo nejasno izjavo o zasebnosti Vendar pa nekatere raziskave kažejo, da je takih ki jih dejansko tudi pozorno preberejo bore malo (Milne in sodelavci, 2004). Po podatkih drugih raziskav, pa je takih ki tovrstnim izjavam o zasebnosti tudi verjamejo in jim zaupa le 34% (Lwin in sodelavci, 2003). To razširjeno nezaupanje, bi lahko v prihodnosti povzročilo upor med uporabniki interneta proti spletnim stranem, ki slovijo po svojih slabih informacijskih praksah in jih pripravilo do tega da bi začeli uporabljati druge zasebnosti bolj prijazne spletne strani (Wafa, 2008).

Vendar pa nekateri menijo, da so izjave o zasebnosti kljub temu koristne. V članku Sullivana (2006) je omenjena študija, ki ugotavlja, da so ameriška podjetja celo dosegla višji rezultat na petih od osmih pogostih informacijskih praksah, med drugim imajo tako predanega uslužbenca zadolženega za varovanje zasebnosti in tudi bolje skrbijo za varnost podatkov. V svoji raziskavi Peslak (2006), da se velika mednarodna podjetja in podjetja, ki ne prihajajo iz ZDA ter nimajo izjav o zasebnosti in še najpogosteje ne držijo poštenih informacijskih praks, medtem ko tista tuja podjetja, ki imajo take izjave, ne odstopajo pomembno od ZDA v poštenih informacijskih praksah.

V zadnjem času pa se pojavlja tudi tendenca jamčenja za politiko zasebnosti določne spletne strani s strani zunanjih entitet. Tako imenovani privacy seal programi omogočajo zainteresiranim spletnim stanem, ki dosegajo določene kriterije, da pokažejo zank določene tretje organizacije, ki jih je overila z pečatom (Lwin in sodelavci, 2003). Izsledki pa raziskav kažejo, da nezapečatene spletne strani ponujajo skoraj enaka zagotovila zasebnosti, kot zaščitene strani. Poleg tega pa imajo nezaščitene spletne strani še dodatno prednost, saj zbirajo manj osebnih podatkov, čeprav zaščitene strani nudijo boljši dostop do informacij in več zagotovil o varnosti podatkov (Larose in sodelavci, 2006)

6.11. Zbiranje javno dostopnih in prostovoljno posredovanih podatkov

Veliko uporabnikov sodeluje na spletnih forumih, pišejo bloge, imajo svojo spletno stran, sodelujejo v novičarskih raznih skupinah , izpolnjujejo vprašalnike, oddajo male oglase in išče zasebne stike. Vsa ta dejavnost je lahko vir osebnih podatkov (Kovačič, 2006). Prav tako je možno pridobiti razne podatke s spletnih strani raznih društev ali vladnih strani, ki jih lahko le te pomotoma objavijo na svojih spletnih straneh. Te nepazljivosti seveda s pridom izkoriščajo kriminalci ki so na primer specializirani za iskanje informacij na spletnih straneh (Milne in sodelavci, 2004). Zbiranje prostovoljno posredovanih osebnih podatkov po javno dostopnih podatkih in imenikih elektronske pošte je razmeroma enostavno in poceni, saj se da za ta namen uporabiti tudi razne iskalnike kot so na primer roboti, pajki črvi in podobna golazen (Kovačič, 2006). Pri tem pa se je potrebno zavedati da so tudi nekatere take objave pravno urejene. Objava osebnih podatkov na spletni strani (na primer osebnih podatkov o članih nekega društva) se po stališču evropskega sodišča smatra za obdelavo osebnih podatkov, in zahteva osebno privolitev posameznika (Jančič in sodelavci, 2007).

6.12. Data mining in Povezovanje podatkov iz različnih baz podatkov

Nekateri menijo, da je podatkovno rudarjenje lahko uporabno kot orodje za preprečevanje in zatiranje kriminala. Tako se ga da uporabiti za prijemanje kriminalcev, preprečevanje vstopa v letala nekaterim varnostno tveganim osebam, zaznavanje izogibanja davkom, preprečevanje pranja denarja in goljufij (Slobogin, 2008). Medtem ko nadzor zavira določeno vrsto vedenja, kot na primer branje subverzivne literature in preprečuje delikventno vedenje, pa pomeni veliko grožnjo posameznikovi avtonomiji. Največja grožnja posameznikovi avtonomiji tiči v tem, da posameznik ne more predvidevati katera njegova vedenja bodo ocenjena kot ogrožajoča in vzeta pod drobnogled (Baruh, 2007). V razvoju sodobnih nadzorovalnih sistemov postajajo čedalje pomembnejši kategoriziranje, predvidevanje in preventiva. »Posledica tega je, da krivda ali nedolžnost posameznika nista pomembni, pomembno je tveganje (ali priložnost), ki ga skupina ljudi predstavlja za organizacijo« (Kovačič, 2006, str. 209).

Danes lahko močni internetni iskalniki in data mining tehnologije pomagajo, da je relativno lahko zbirati osebne informacije, jih navzkrižno primerjati in jih za prihodnjo uporabo shraniti v sofisticirane baze podatkov (Attaran in sodelavci, 1999). Pomemben etičen problem je, da se posameznik ne zaveda, da se zbirajo njegovi osebni podatki in ne ve kako bodo uporabljeni ter tako nima priložnosti, da bi privolil v tako zbiranje (Wel in sodelavci, 2004). Poleg tega se pojavljajo tudi drug težave. Tako so informacije lahko zmotne, kar vodi v kriminalizacijo in izobčenje napačnih ljudi. V ZDA se zasebnem sektorju soočajo z velikim problemom napačnih kreditnih poročil, ki na podlagi zmotnih informacij onemogoča upravičenim posameznikom pridobiti kredite (Slobogin, 2208). Prav tako je pri uporabi teh tehnik, težko vnaprej vedeti kakšni vzorci bodo odkriti, zato je nemogoče vnaprej specificirati namen zbiranja, kar je nasprotju z evropsko direktivo (Wel in sodelavci, 2004).

6.13. Cookies

Piškotki oziroma cookies so majhne tekstovne datoteke, ki se namestijo na disk pri deskanju po spletnih straneh in uporabnikom omogočajo hitrejšo navigacijo po internetu (Ozimek, 2005). Tako omogočajo kontinuiteto med obiski spletne strani in dovoljujejo lastniku strani, da šteje svoje obiskovalce in ugotavlja kdo so novi obiskovalci (Dobosz in sodelavci, 2006). Prav tako pa so koristni tudi za oglaševalce. Oglaševalcem lahko pomagajo, da boljše targetirajo trg in prilagodijo spletno stran uporabniku. Poleg tega tudi pospešujejo spletne transakcije, sredstva od oglaševanja, pa omogočajo da ostaja internet brezplačen za uporabnika (Dobosz in sodelavci, 2006).

V Sloveniji so piškotki zakonsko so urejeni v Zakonu o Elektronskih Komunikacijah, ki temelji na Evropski direktivi. Piškotki pomenijo shranjevanje podatkov v uporabnikovem računalniku oziroma drugi terminalski opremi, to pa je dovoljeno samo »pod pogojem, da je bil naročnik ali uporabnik predhodno jasno in razumljivo obveščen o upravljavcu in namenu obdelave teh podatkov« in da ima uporabnik «pravico, da zavrne takšno obdelavo ali izrazi soglasje« (Jančič in sodelavci, 2007, str. 205). V takih primerih pri namestitvi piškotkov ne gre za kaznivo dejanje neupravičenega vnašanja virusov in drugih zlonamernih podatkov v uporabnikov računalnik.

Piškotki bodo po zakonu dovoljeni brez obvestila ali soglasja v primeru, da je shranjevanje piškotov namenjeno le za prenos sporočila po omrežju, gre za tehnično shranjevanje ali pa je njihova uporaba nujno potrebna za zagotovitev storitve in jo uporabnik izrecno zahteva in mu tako na primer ob vsakem obisku ni potrebno ponovno vpisovati gesla (Jančič in sodelavci, 2007). Privolitev pa ne more biti implicitna. Tako na primer za privolitev ne bo dovolj, da uporabnik v svojem brskalniku nima vklopljene funkcije za onemogočanje piškotkov.

Onemogočanje piškotkov, pa ni vselej brez škode. Za posledico ima lahko nezmožnost dostopa do storitve, na spletnih straneh na katerih upravljavec storitve zahteva namestitev cookija, kot pogoj za uporabo storitve (Trček, 2006). Ta tertium non datur logika, pa postaja čedalje bolj razširjena. Ponudnik storitev, da uporabniku ponavadi na voljo samo dve možnosti. V primeru da hoče stranka uporabljati določeno storitev mora priskrbeti svoje podatke ali pa je popolnoma izključena in te storitve ne more uporabljati (Woo, 2006). Po mnenju Kovačiča (2006) gre pri tem gre za »vsiljeno izbiro«. Neuporabljati internet se ne zdi nepravična možnost in je lahko visoka cena, ki jo mora plačati posameznik za zaščito svoje zasebnosti (Wel in sodelavci, 2004).). Kritiki tako ureditev smatrajo za vsiljivo in menijo, da gre za uporabo njihoihv osebnih podatkov v druge namene za katere so bili zbrani (Collier, 1995).

6.14. Prikriti programi Adware and spyware

Prikriti programi so velik vir ogrožanja, saj je po nekaterih podatkih okuženih okrog 90% vseh računalnikov povezanih na internet (Močnik, 2005) Preživetveni čas nezaščitenega računalnika povezanega v svetovni splet se je zelo zmanjšal.

Problem tovrstnih programov je v tem, da se uporabniki niti ne zavedajo, da je njihov računalnik okužen, dokler ni prepozno (Močnik, 2005). Na ta način »prikrit način zbiranja in obdelave podatkov na internetu posamezniku jemlje možnost uporabe učinkovitega pravnega sredstva za zaščito svojih pravic (do katerega ima pravico po ustavi) saj: 1. praviloma ne ve, da je do posega v njegovo zasebnost sploh prišlo; 2. težko ugotovi, kdo od udeležencev v zapleteni verigi njegove dejavnosti v svetovnem spletu je v zasebnost posegel; 3. je zbiralec podatkov pogosto v drugi državi, kar za večino

predstavlja dodatno nepremagljivo oviro za pravno zavarovanje pravic; 4. obstoječe pravo, prirejeno klasičnemu varstvu zasebnosti, nudi malo ali nič pravnih sredstev, s katerimi bi zavaroval svoje pravice« (Jančič in sodelavci, 2007, str. 397).

Uporaba tovrstnih programov je inkriminirana v Kazenskem Zakonikom z kaznivim dejanjem neupravičenega vstopa v informacijski sistem (225.člen KZ) ali kaznivim dejanjem vdora v informacijski sistem (242. člen KZ) (Jančič in sodelavci, 2007). Prav tako je spywere kriminaliziran s strani evropske unije, saj le ta zahteva, da uporabnik soglaša z tovrstnim zbiranjem osebnih podatkov. Vendar pa je zakonodajo v praksi nemogoče nadzirati in uveljaviti (Klang, 2004).

Poleg tega pa ti programi velikokrat ne delujejo povsem prekrito, saj pogosto uporabnika v »drobnem tisku obvestijo o tem kaj nameravajo početi« (Kovačič, 2006, str. 165). Uporabniki se s pogoji ponavadi strinjajo, brez da bi jih sploh prebrali. Tako na primer v primeru programa za izmenjavo datotek KaZaA, s strinjanjem dajemo vohunskim programom pravico do dostopa in uporabe prostega pomnilnika, računalniške moči, dostopa do interneta in porazdeljeno uporabo računalnikov, brez pravice do kakršnega koli denarnega povračila in to še celo po prekinitvi pogodbe (Kovačič, 2006).

Prikriti programi se običajno namestijo na uporabnikov računalnik skupaj z namestitvijo začasnih (shareware) in neplačljivih (freeware) programov (Močnik, 2005). V raziskavi o razširjenosti spywera, ki so jo izvedli Kuchera in sodelavci (2005), so pregledali pet izmed osumljenih programov in ugotovili, da so bili trije izmed njih res opremljeni z vohunsko programsko opremo. Po podatkih neke druge raziskave, pa je imelo kar 90% uporabnikov, ki so sodelovali, računalnik okužen s spywareom (Milne in sdelavci, 2004). Veliko uporabnikov se ne zaveda vpliva spywera na njihovo zasebnost. Poleg tega ne vedo kako ga odstraniti, katere programe uporabiti za odstranjevanje in lahko pri nalaganju teh programov v najslabšem primeru na svoj računalnik naložijo celo še več spywera (Klang, 2004)

Spywere dovoljuje zbiranje velikega števila različnega tipa podatkov hkrati. Tovrstni programi tako lahko zbirajo informacije o osebnih podatkih uporabnika, fizičnem naslovu, elektronskem naslovu, številki kreditne kartice in o vedenju na internetu (Ozimek, 2005) Prikrita programska oprema zbrane podatke posreduje na različne

lokacije, kar poraja vprašanje kdo točno zbira te osebne podatke (Kuchera in sodelavci, 2005).

Poleg grožnje naši zasebnosti, pa vohunska programska oprema povzroča tudi druge težave. Tovrstni programi predstavljajo veliko breme za delovanje računalnika, saj upočasnjujejo in ovirajo njegovo delovanje (Ozimek, 2005). Prav tako jih je zelo težko odstraniti. Tudi po odstranitvi shareware in freeware aplikacij, nekatere komponente ostanejo in nadaljujejo z delom, zato se je pogosto potrebno poslužiti orodja za njihovo odstranitev ali v skrajnem primeru celo ponovno naložiti celoten operacijski sistem (Kuchera in sodelavci, 2005).

6.15. DRM ali upravljanje dostopa do digitalnih vsebin

Trusted computing ali zaupanja vredno računalništvo je ime za naslednjo generacijo računalniških okolij, v katere naj bi bilo vgrajeno upravljanje dostopa do digitalnih vsebin (DRM). Na ta način naj bi vpeljali večji nadzor nad digitaliziranimi vsebinami in naredili konec piratstvu (Kovačič, 2006). Vendar pa Sullivan v enem izmed svojih esejev meni, da bi bil bolj primeren izraz za poimenovanje teh tehnologij »Treacherous computing« ali zahrbtno oziroma izdajalsko računalništvo (Guy, 2006, str. 117).

»DRM ali upravljanje dostopa do digitalnih vsebin je skupek tehnologij, ki naj bi omejile dostop in uporabo računalniških datotek oziroma digitaliziranih vsebin. Omejitev dostopa naj bi dosegli tako, da bi »onemogočili anonimen dostop do digitalnih vsebin, poleg tega bi se vsak dostop do vsebine tudi zapisal« (Kovačič, 2006, str. 168). Cilj upravljanja dostopa do digitalnih vsebin, je priskrbeti lastniku avtorskih pravic pravico do kontrole nad svojim izdelkom. To je na primer možno z enkripcijo, zasidranjem določenega izdelka na določen računalnik, v zadnjem času pa tudi z sistemi, ki dovoljujejo lastniku avtorske pravice, da sledi kaj se z njegovim izdelkom dogaja (Baruh, 2007). Vendar je Evropska delovna skupina za zaščito podatkov mnenja, da imajo uporabniki pravico do anonimnega dostopa do interneta in jim ni treba razkriti svoje identitete, v vseh primerih, kjer osebni podatki niso nujno potrebni za zagotovitev neke storitve (Broersma, 2005).

Avtorska pravica je zgodovinsko gledano nastala zavoljo uporabnikov. Njen namen je bil spodbujanje avtorjev, da bi napisali in objavili več del in tako obogatili javni fond znanja, kar je seveda v javnem interesu (Gay, 2002). Toda danes temu ni več tako. Situacija je ravno nasprotna. Avtorske pravice so postale monopol založniških hiš, avtorji pa imajo od tega bore malo. Nekateri menijo, da je taka ureditev celo kontraproduktivna, saj strogo avtorsko pravo ovira nastajanje novih uporabnih del (Gay, 2002). Sulivan tako navaja primer legendarnega Shakespeara, ki si je kar nekaj izmed svojih zgodb sposodil iz objavljenih del drugih avtorjev in iz njih ustvaril mojstrovine (Gay, 2002). To v današnjih časih vsemogočne vladavine založniških hiš po mnenju Sullivana, ne bi bilo več mogoče (Gay, 2002). Poleg tega smo tudi priča razširjeni retoriki o naravnost katastrofalnem razmahu piratstva, ki se ji dandanes le malokdo drzne oporekati. Vendar pa tovrsten diskurz ne upošteva dejstva, da je funkcija avtorskih pravzaprav služenje interesom javnosti, pač pa domneva, da je kopiranje nelegitimno nepošteno in samo po sebi narobe (Gay, 2002)

V Sloveniji je predvidena zaporna kazen do treh let za tistega, ki »uporabi (poseduje) eno ali več avtorskih del ali njihovih primerkov, katerih skupna tržna cena pomeni večjo premoženjsko korist«, kar v praksi pomeni nekaj več kot 4.000 evrov (Jančič in sodelavci, 2007). V času, ko nakup trdega diska, ki se meri v terabajtih, ne predstavlja velikega stroška, je tako za skoraj povprečnega uporabnika dokaj lahko doseči teh 4.000 evrov. V primeru, da uporabnik poseduje in uporablja avtorska dela, katerih vrednost je opredeljena kot velika premoženjska korist oziroma petdeset povprečnih plač, je predvidena zaporna kazen temu primerno večja in znaša do osem let (Jančič in sodelavci, 2007). V Sloveniji so pravno zavarovani tudi tehnološki ukrepi za varovanje avtorskih del. Tako ni dovoljeno niti izogibanje tehnološkim ukrepom za namene njihovega preučevanja, česar evropske direktive ne prepovedujejo (Jančič in sodelavci, 2007).

V Evropi je izmenjavi datotek najbolj nenaklonjena Francija. Francija se je tako pred časom, po ameriškem vzoru vojne proti kriminalu, močno trudila uveljaviti pravilo three strikes and you are out. Uveljavitev takega pravila bi v praksi pomenila, da bi moral po treh dejanjih piratstva, ponudnik dostopa do interneta takega vztrajnega kršilca preprosto odklopiti (Timmer, 2008). Nad tako drakonskimi ukrepi pa ostale Evropske države k sreči niso preveč navdušene.

Nekatere druge države članice EU pa namesto zasebnosti, raje izpostavljajo problem nekompatibilnosti in pomanjkanje medsebojne združljivost in transparentnosti različnih DRM shem. Slednje za uporabnike prav tako predstavljajo varnostno tveganje in jim preprečujejo, da bi predvajali vsebine na napravah po svoji izbiri (Timmer, 2007). Tako zgleda, da se Evropa najbolj osredotoča ravno na problem nekompatibilnost in predlaga vpeljavo nekega kupcem prijaznega DRM sistema, čeprav bi bilo po mnenju nekaterih boljše, da bi se tej sicer pozitivni pobudi, popolnoma odpovedala (Riley, 2008).

Upor proti upravljanju dostopa do digitalnih vsebin, pa se pojavlja tudi v deželi rojstva in razvoja DRM sistemov. Tako se v ZDA na primer že pojavljajo DRM free glasba. Izkušnje celo kažejo da so kupci zavoljo pripravnosti zanjo pripravljeni plačati več, saj odpravlja frustracije ki jih imajo na primer z prenosom glasbe iz ene naprave na drugo (Sullivan, 2008). Taka težave se na primer pojavljajo z nekompatibilnostjo Microsofta in Applea, kar vodi v diskriminacijo kupcev, ki želijo svoje popolnoma legalno kupljene produkte uporabljati na več različnih napravah (Riley, 2008).

Po drugi strani imajo lastniki založniških pravic do neke mere legitimen interes, da zaščitijo svoje izdelke pred prekršitvami avtorskih pravic, vendar imajo lahko na žalost, ti legitimni interesi po razvoju tehnologije za zaščito založniških pravic, pogubne posledice za zasebnost uporabnikov (Broersma, 2005). Tako so tehnike za upravljanje dostopa do digitalnih pravic v konfliktu z zasebnostjo, ker lahko oskrbujejo industrijo avtorskih pravic z natančnimi in v preteklosti nedosegljivimi informacijami o bralnih, poslušalnih in gledalnih navadah posameznikov (Cameron, 2004). Microsoft je tako naprimer za ameriške uporabnike Windows XP, uvedel obvezno aktivacijo. Ta aktivacija pa v praksi pomeni da se ob »namestitvi operacijskega sistema v del registracijskega ključa vgradi tudi informacija o strojni opremi(serijska številka procesorja, omrežne kartice, diska itd.)« (Kovačič, 2006). Problem se seveda pojavi, če uporabnik zamenja velik del strojne opreme, kupi nov računalnik ali pa na primer želi svoj operacijski sistem prekopirati v drug računalnik, saj operacijski sistem ne bo več hotel delovati in ga je potrebno ponovno aktivirati (Kovačič, 2006).

V zvezi z upravljanjem dostopa do digitalnih vsebin, pa se pojavljajo tudi drugi pomisleki. Kovačič (2006) opozarja, da bo otežen bo prehod na konkurenčno programsko opremo. V njen nekateri vidijo tudi grožnjo prosti programski opremi. Tako naj bi bila

ena izmed zadev na dnevnem redu prepoved uporabe opreme, ki se lahko uskladi z HDTV. Taka oprema naj bi bila dovoljena le v primeru, da je zasnovana na tak način, da je javnost ne more po svoje spreminjati in modificirati, kar praktično seveda pomeni konec odprtokodne programske opreme (Gay, 2002). Po mnenju Kovačiča (2006) bi bilo sistem mogoče zlorabiti tudi za cenzuro, saj bi se z njegovim sprejemom povečala možnost nadzora nad dokumenti in elektronsko pošto. Ena izmed kritik tega koncepta je, da bo odvzel uporabniku pravico do nadzorovanja lastnega računalnika, saj bo v bistvu prejemal ukaze od velikih medijskih korporacij in računalniških podjetij (Gay, 2002).

6.16. Spam

Spam oziroma smetje je eden izmed velikih problemov interneta in ogroža uporabnost elektronske pošte, saj se količina nezaželenih elektronskih sporočil povečuje in je v letu 2003 obsegala kar okoli 50% vseh sporočil (Kovačič, 2003). Glavne značilnost nezaželene elektronske pošte so «neprijetna vsebina, zavajanje, varljive ponudbe, kršenje zasebnosti in nelegalnost« (Mramor, 2007, str. 11). Nezaželena elektronska sporočila polnijo nabiralnike in ogrožajo prejemanje za uporabnika vredne legalne pošte. V primeru da je nezaželene pošte več kot legitimne, se stopnja uporabnosti elektronske pošte namreč močno zmanjša (Novak, 2004),

Na področju pošiljanja nezaželene elektronske pošte imajo pošiljavci odprte široke možnosti. Internetno omrežje omogoča pošiljanje velike količine sporočil na številne naslove, ki jih je dokaj lahko pridobiti ter povezati s potrošniškim profilom kar za razliko od navadne pošte ne predstavlja skoraj nobenega stroška (Jančič in sodelavci, 2007).

Nenaročeno komercialno sporočilo je možno pogledati z več različnih pravnih vidikov. Z vidika varstva osebnih podatkov (na primer sporne prodaje elektronskih naslovov s strani upravljavcev), z vidika človekovih pravic pomeni vdor v zasebnost, z vidika konkurenčnega prava gre za delanje nelojalne konkurence in tudi z vidika varstva potrošnikov (Klemenčič, 2005).

S stališča varstva osebnih podatkov se posameznikov elektronski poštni naslov smatra za osebni podatek in sicer ne glede na to ali vsebuje posameznikova pravo ime ali pa zgolj

psevdonim, saj lahko tudi slednji vodi do pravega imena (Makarovič in sodelavci, 2001). Zbiranje elektronskih poštnih naslovov je relativno preprost postopek. Elektronske naslove je mogoče pridobiti od samega uporabnika, jih kupiti, najeti od upravljavcev spletnih strani in ponudnikov dostopa, iz javnih imenikov elektronske pošte ali pa poiskati z javno dostopnimi programi za zbiranje elektronskih naslovov (Jančič in sodelavci, 2007). Smetje pa po mnenju nekaterih »ne pomeni neposrednega vdora v zasebnost v smislu nadzorovanja, ga pa lahko štejemo za poseg v pravico biti puščen pri miru, skratka v tisti del zasebnosti, ki posamezniku omogoča da se umakne iz družbe« (Kovačič, 2006, str. 159).

V Sloveniji področja nezaželene elektronske pošte urejajo trije specialni zakoni (Zakon o elektronskih komunikacijah, Zakon o varstvu potrošnikov, zakon o elektronskem poslovanju na trgu) in sistemski Zakon o varstvu osebnih podatkov (Mramor, 2007). Pošiljanje tovrstne nezaželene elektronske pošte, pa ni kaznivo dejanje in se po Zakonu o varstvu potrošnikov in Zakonu o Elektronskih Komunikacijah smatra zgolj za prekršek (Jančič in sodelavci, 2007). Za kaznivo dejanje gre le v primeru, da je zasipanje z nezaželeno elektronsko pošto storjeno z namenom preplaviti nek informacijski sitem in onemogočiti ali upočasniti njegovo dejanje: V tem primeru gre za kaznivo dejanje iz 225. člena KZ, ki inkriminira oviranje prenosa podatkov ali delovanje informacijskega sistema (Jančič in sodelavci, 2007).

Na evropski ravni pa na področje pravnega urejanja nezaželene elektronske pošte posega pet direktiv (direktiva o zaščiti podatkov, direktiva o elektronski zasebnosti, direktiva o zasebni telekomunikaciji, direktiva o pogodbah na daljavo in direktiva o elektronskem poslovanju), ki pa so vezane samo na sporočila poslana v Evropi (Mramor, 2007)

Zakonodajno se problem smetja ureja s pomočjo opt in ali opt out načela. Opt in načelo dovoljuje pošiljanje elektronskih poročil samo tistim osebam, ki so vnaprej privolile v to, medtem ko opt out koncept predvideva pošiljanje sporočil tistim osebam, ki prejemanja tovrstnih sporočil niso izrecno zavrnile (Skrt, 2003). Slabost opt out načela je, da dovoljuje vsaj prvo pošiljanje nezaželenega sporočila, kar povečuje pošiljanje smetja (Jančič in sodelavci, 2007). Pravo Evropske Unije dopušča posameznim državam članicam možnost izbire katerega načela se bodo posluževale pri urejanju tega področja (Jančič in sodelavci, 2007). V Slovenji na področju pošiljanja elektronski sporočil velja

opt in načelo, kar pomeni, da mora dati uporabnik izrecno soglasje. To pa je izjema, saj splošno gledano za druga področja velja optout načelo (Skrt, 2003). Vendar pa mora imeti prejemnik komercialnih sporočil, ki poda osebno soglasje vedno tudi možnost, da to svoje soglasje kadarkoli umakne (Jančič in sodelavci, 2007). Upravljavec pa uporabnika ne sme zavajati. Tako mu na primer ni dovoljeno, da bi uporabniku ob podpisu soglasja podtaknil tudi kake klavzule v drobnem tisku na primer o iznosu osebnih podatkov tretjim osebam(Jančič in sodelavci, 2007).

Zakonodaja pa velja le na področju komercialnih elektronskih sporočil. Ta predstavljajo velik del spama, vendar pa ne smemo pozabiti, da se v nezaželena elektronska sporočila prav tako uvrščajo razne ankete, verižna sporočila, prošnje za dobrodelne namene, propaganda in podobna navlaka, ki pa je zakonodaja ne ureja in lahko tako nemoteno pristaja v nabiralnikih (Novak, 2004). Za taka verižna sporočila bi lahko rekli, da so neke vrste virus, saj se po medmrežju širijo zelo hitro in povzročajo velik zastoj v internetnem prometu (Mramor, 2007). Poleg tega pa je zelo zanimivo dejstvo, da je spam zakonsko prepovedan, medtem ko naše nabiralnike prav tako polni nezaželena reklamna pošta. Po mnenju Klemenčiča (2005) gre pri nezaželeni elektronski pošti zaradi njene nematerializiranosti, za manjši vdor v zasebnost, kot pri sporočilih v poštnih nabiralnih ali nezaželenih komercialnih telefonskih klicih. Pojavljajo pa se tudi nove oblike zasipanja z komercialnimi sporočili, ki so zakonsko še nedorečene. Taka je na primer storitev, ko lahko uporabnik prijatelju pošlje sporočilo na koncu katerega pa ponudnik storitev priključi še svoje komercialno sporočilo in tako pridobiva potencialne stranke in njihove telefonske številke (Jančič in sodelavci, 2007).

Prav tako nekateri izražajo pomisleke nad učinkovitostjo zakonodaje, saj menijo, da zakonodajno urejanje ne bo imelo prevelikega efekta, ker večina nezaželene elektronske pošte tako ali tako prihaja iz tujine, prvenstveno iz ZDA (Skrt, 2003). Razlog zakaj je temu tako, je pravna neurejenost tega področja znotraj samih ZDA, ki omejuje zgolj pošiljavce nezaželene elektronske pošte, ki delujejo pri svojih ponudnikih na ozemlju ZDA (Mramor, 2007). Za učinkovito reševanje tega problema bi torej potrebovali urejen mednarodnopravni okvir.

Marsikdo bi se vprašal v čem je sploh profit spama glede na to da ga uporabniki kar naprej filtrirajo in brišejo? V tem aspektu je problem precej podoben televizijskim

reklamam, ki se kar naprej ponavljajo. Na ta način ustvarjajo prepoznavnost izdelka, ki ga prodajajo ter ciljajo na to, da bodo dosegle vsaj enega kupca, ki ga v nekem trenutku nakup takega izdelka zanima dovolj, da je pripravljen obiskati spletno stran (Grunch, 2009).

Uporabniki imajo posredne stroške z nezaželenimi elektronskimi sporočili, saj jim le ta odžirajo del pasovne širine, povzročajo finančne stroške in jim poleg tega še kradejo čas, ki ga imajo s pregledovanjem in brisanjem nezaželene elektronske pošte (Kovačič, 2003). To niti ni zamerljiv čas, če upoštevam da je po podatkih raziskav v Sloveniji, kar 48% elektronske pošte nezaželene (Mencigar, 2004). Po raziskavah med uporabniki in mnenju uporabnikov, pa cenovno spam niti ne predstavlja takega finančnega stroška, saj je večina uporabnikov priklopljena za fiksen strošek ves dan (Mramor, 2007). Vendar pa uporabniki interneta niso edini, ki imajo stroške z nezaželeno elektronsko pošto. Slednja namreč predstavlja tudi velike izdatke za podjetja saj predstavlja motnjo v delovnem procesu. Tako podjetja trpijo zaradi izgube produktivnosti, izgubljenih delavnih ur, zakasnjenih poslovnih komunikacij in uporabe strežniških virov, kar po nekaterih podatkih zmanjšuje produktivnost za kar 1.3% (Mencigar, 2004).

7. Prihodnost

Soodvisnost, ki jo generirata globalni trg in globalna zaskrbljenost glede varstva pravice do zasebnosti, bo lahko v prihodnosti v spodbudo razvoju bolj poenotenih standardov varovanja zasebnosti in varovanja informacij (Regan, 2003). Eden izmed prvih poskusov harmonizacije mednarodne skupnosti so smernice, ki jih je oblikovala OECD. Te smernice vsebujejo naslednja načela: omejitev zbiranja podatkov, kvaliteto podatkov, natančno določitev namena zbiranja podatkov, omejitev uporabe podatkov, zagotovitev varnosti podatkov, odprtost, individualno participacijo in odgovornost (Praprotnik, 2006).

Poleg tega je za podjetja upoštevanje kompleksnosti teretiorializirane zakonodaje o varovanju v zasebnosti lahko prava logistična nočna mora. Podjetja se morajo tako soočiti z vprašanji ali naj imajo eno spletno stran ali več spletnih strani prikrojenih posamezni pravni ureditvi, ali naj najamejo goro pravnikov, ki bodo oblikovali izjave o zasebnosti ali naj jih preprosto kopirajo. To pomeni, da morajo temu vprašanju nameniti velike količine finančnih in drugih virov, poleg tega pa to vpliva tudi na funkcionalnost njihovih rešitev (Wafa, 2008)

Obstajajo pa tudi mnenja, da je nemogoče ustvariti res globalen okvir za varovanje zasebnosti, ker se v igro vmešavajo močni lobiji. Vendar drugi menijo, da to mogoče drži za zdaj. Vendar pa je pravica do zasebnosti tako pomembna človekova pravica, da se je uporabniki interneta ne bodo pripravljeni odpovedati (Wafa, 2008). Po terorističnih napadih legendarnega 11. septembra, je sicer prišlo do pozivov k harmonizaciji prava, ki ureja to področje, vendar nekateri opozarjajo, da tako sodelovanje kaj hitro lahko zaide k krepitvi represivnih organov in zmanjševanje civilnih svoboščin (Regan, 2003).

Pojavlja pa se tudi vprašanje kako harmonizirati mednarodno pravo. Nekateri so leta nazaj verjeli, da internetna tehnologija ne bo nikoli uspela, zaradi pomanjkanja standardizacije in konfliktnih pogledov različnih držav glede tega vprašanja, vendar se je kmalu izkazalo, da temu ni tako (Wafa, 2008). Sodelovanje je te oviro premagalo in omogočilo, da je internetna tehnologija doživela nesluten razmah. Morda se bo to zgodilo tudi na področju harmonizacije pravnih standardov, ki bodo varovali uporabnikove

človekove pravice v spletnem okolju, med katerimi na pomembnem mestu najdemo pravico do zasebnosti.

8. Predstavite rezultatov in interpretacija ankete

V empiričnem delu svoje diplomske naloge smo izvedli anketo med uporabniki interneta. Respondenti so bili starejši od 15 let in mlajši od 36. Anketa smo razdelili prijateljem in znancem, ki so nanjo odgovarjali v pisni obliki. Med reševanjem ankete smo bili svojim respondentom na voljo za morebitna dodatna pojasnila. Anketiranje je bilo izvedeno v obdobju med 1. in 30. majem 2009. V tem času smo pridobili 30 izpolnjenih vprašalnikov.

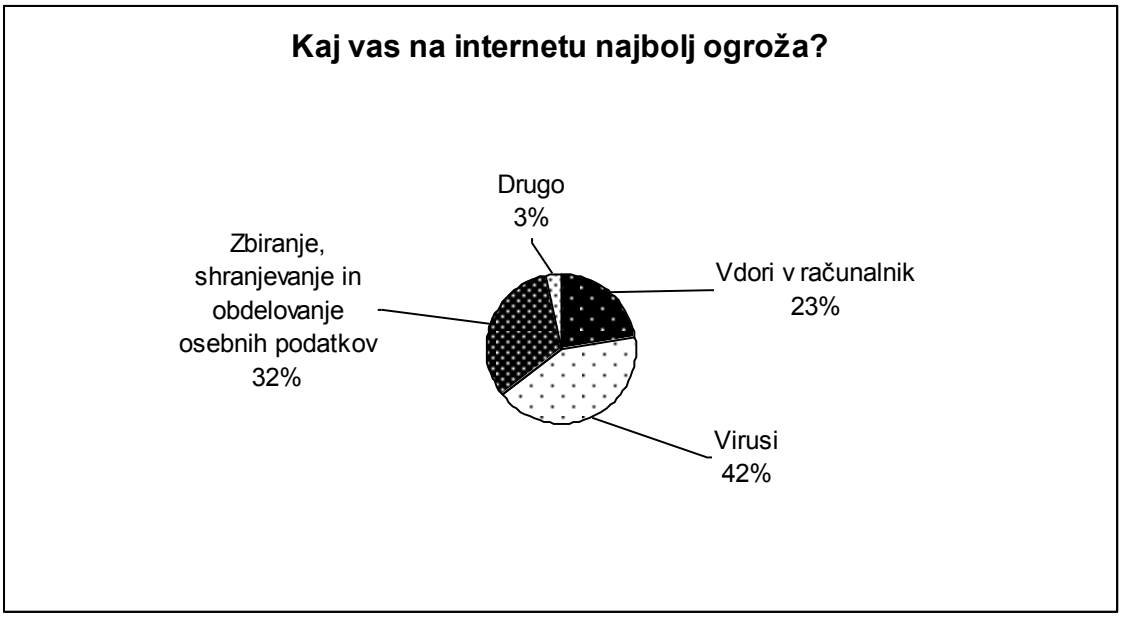
Anketni vprašalnik (priloga 1) je obsegal 11 vprašanj in je sestavljen iz dveh delov. V prvem delu nas je zanimalo v kolikšni meri se anketirancem zdi pomembna pravica do zasebnosti, kaj jih po njihovem mnenju najbolj ogroža pri njihovih aktivnostih na internetu in ali se jih zdi njihova pravica do zasebnosti ogrožena. Prav tako smo želeli tudi izvedeti kdo je po njihovem mnenju najbolj odgovoren za varovanje njihove zasebnosti. V drugem delu pa smo poskušali ugotoviti s katerimi aktivnosti se ukvarjajo na spletu, katere stvari jih po njihovem mnenju najbolj ogrožajo in kakšne so njihove dejanske prakse pri varovanju zasebnosti. Anketni vprašalnik smo pred izvedbo anketiranja tudi testirali na manjši skupini respondentov, ki niso imeli vsebinskih pripomb. Dobljene podatke smo analizirali in interpretirali ter nekatere rezultate bolj pregledno predstavili z grafi.

Na vprašanje kako pomembna je pravica do zasebnosti, je večina vprašanih odgovorila, da se jim zdi zelo pomembna. Nihče izmed anketiranih ni na to vprašanje odgovoril, da se mu zasebnost ne zdi pomembna ali da mu je vseeno. Kar 72% vprašanih je odgovorilo, da se jim zdi pravica do zasebnosti zelo pomembna. Ostalih 28% pa meni, da je pomembna. Iz teh rezultatov lahko sklepamo, da uporabniki svetovnega spleta svoji zasebnosti pripisujejo velik pomen.

V internetnem okolju na uporabnika preži mnogo nevarnosti. Zanimalo nas je katera je po mnenju anketirancev tista stvar, ki jih v spletu najbolj ogroža. Večina vprašanih (42%) meni, da jih najbolj ogrožajo virusi. Velik odstotek anketiranih (32%) pa je kot veliko grožnjo izpostavilo zbiranje, shranjevanje in obdelovanje osebnih podatkov. Preostalih 23% uporabnikov pa najbolj skrbijo vdori v računalnik. Dobljeni rezultati kažejo, da se

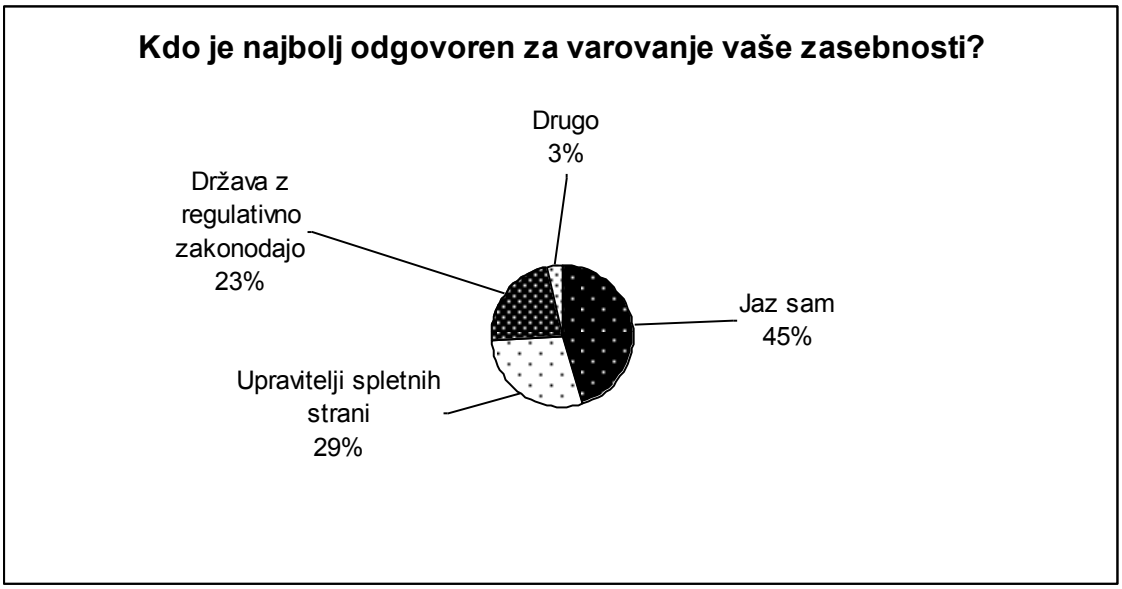
dobri tretjini vprašanih zdi zbiranje, shranjevanje in obdelovanje velika grožnja, kar kaže na to, da se zavedajo pomena svoje zasebnosti.

Graf 1: Kaj vas na internetu najbolj ogroža?



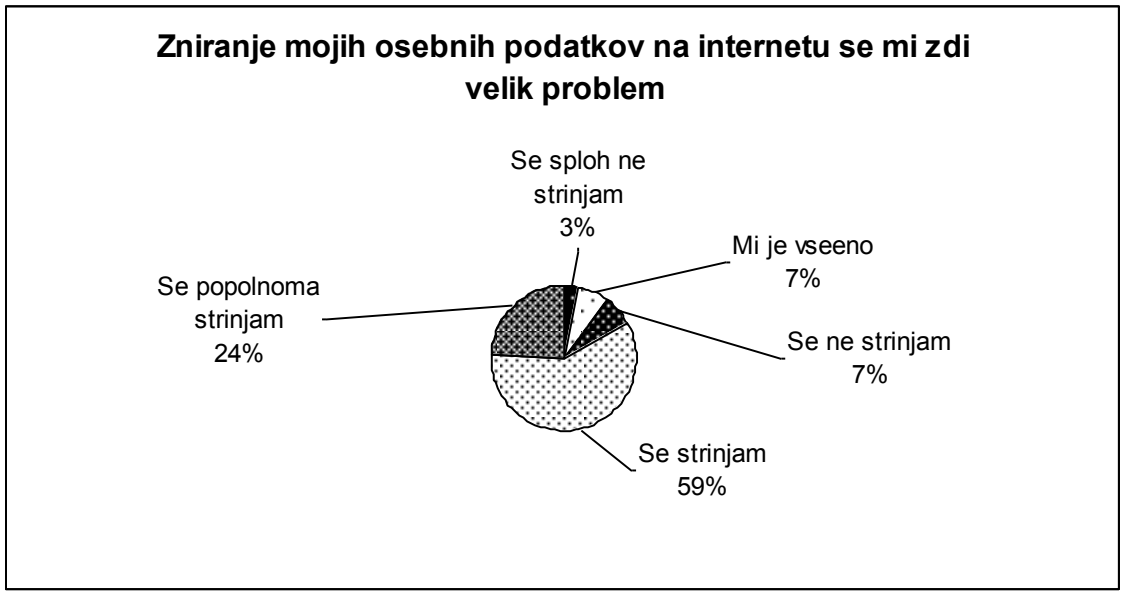
Večina uporabnikov (45%) največjo odgovornost za varovanje svoje zasebnosti pripisuje sebi. Takih, ki menijo, da so za to pristojni upravitelji spletnih strani je 29%. Preostanek vprašanih (23%) pa meni, da je odgovornost za varovanje svoje zasebnosti na plečih države in regulativne zakonodaje.

Graf 2: Kdo je najbolj odgovoren za varovanje vaše zasebnosti?



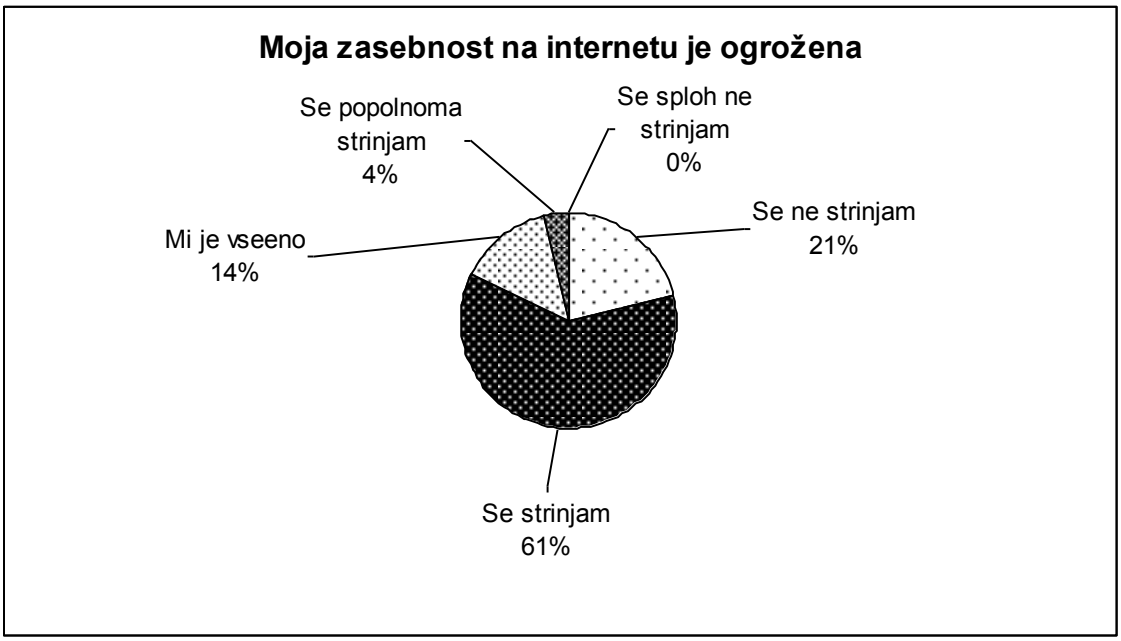
Iz grafa je razvidno, da se veliki večini uporabnikov zdi zbiranje osebnih podatkov na internetu velik problem. Takih, ki se s tem strinjajo je 59%. Kar 24% vprašanih pa s tem popolnoma strinja. Nekaj anketirancev je na vprašanje odgovorilo, da jim je vseeno (7%), se s tem ne strinjajo (7%) ali pa se sploh ne strinjajo (3%).

Graf 3: Zbiranje mojih osebnih podatkov na internetu se mi zdi velik problem.



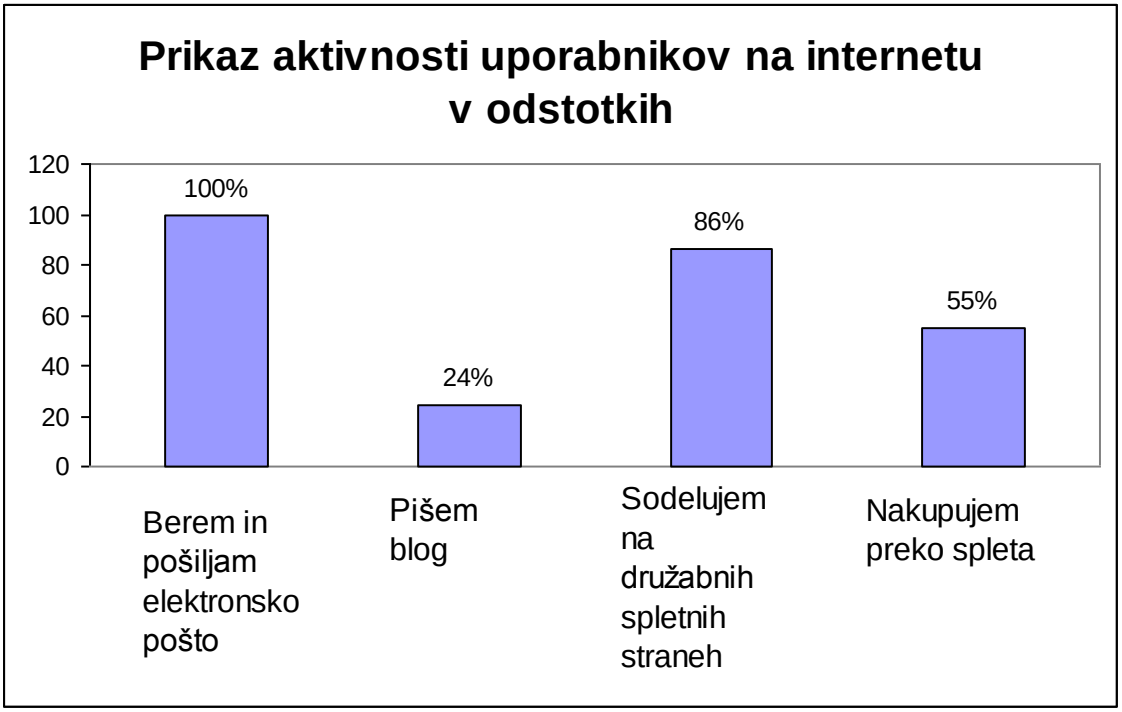
Na vprašanje ali se uporabnikom zdi njihova zasebnost na internetu ogrožena je 61% anketirancev odgovorilo, da se s tem strinjajo. Takih, ki se s tem popolnoma strinjajo pa je bilo 4%. Kljub temu, da se uporabniki zavedajo pomena zasebnosti v spletnem okolju, pa kar velik delež uporabnikov meni, da njihova zasebnost ni ogrožena (21%) ali pa se jim zdi vseeno (14%).

Graf 4: moja zasebnost na internetu je ogrožena.



Uporabniki interneta se na spletnih straneh ukvarjajo z različnimi aktivnostmi, ki lahko predstavljajo grožnjo njihovi zasebnosti. Iz grafa je razvidno, da vsi anketirani (100%) uporabljajo elektronsko pošto. Večina (86%) jih tudi sodeluje na različnih družabnih spletnih straneh kot na primer facebook myspace in podobno Zelo velik odstotek vprašanih (56%) tudi nakupuje preko spleta. Takih, ki uporabljajo blog, pa je nekoliko manj (24%).

Graf 5: Prikaz aktivnosti uporabnikov na internetu v odstotkih.



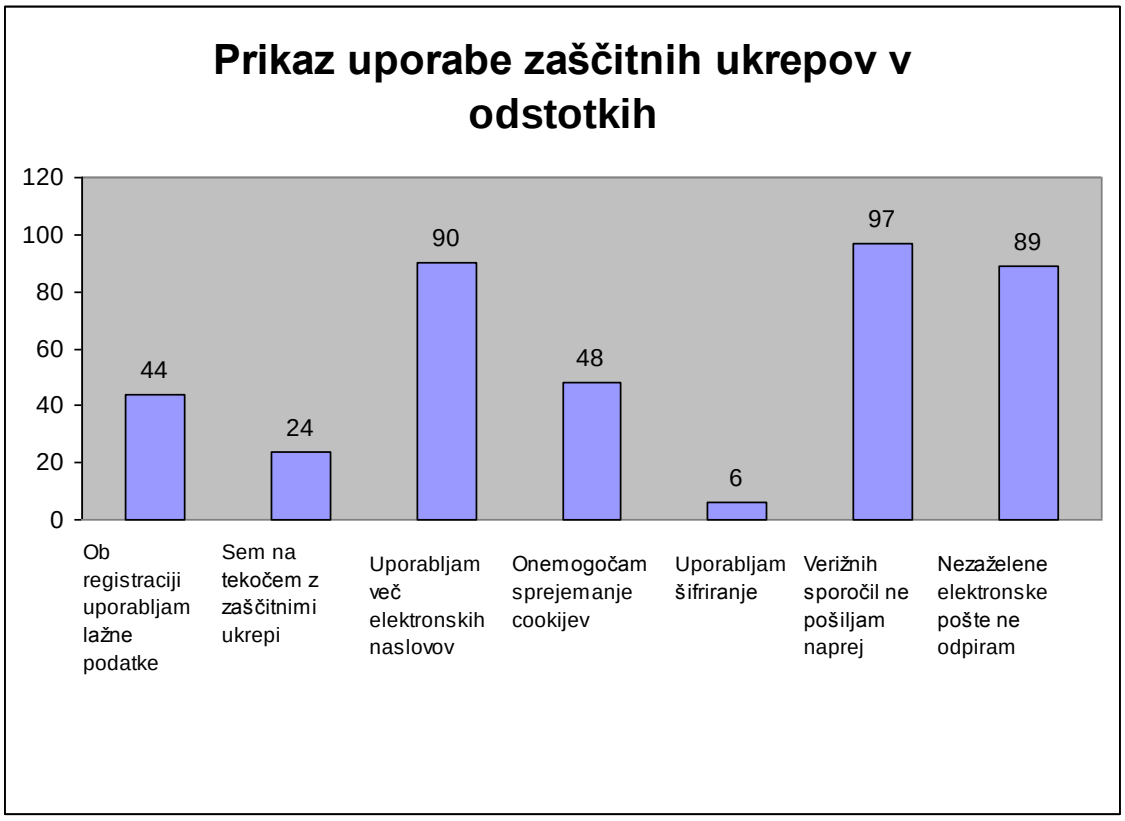
Pri uporabi različnih storitev na internetu, so uporabniki izpostavljeni različnim nevarnostim. Največji odstotek vprašanih (86%) dopušča možnost, da utegne biti njihov računalnik okužen s prikrito programsko opremo. Podoben odstotek anketiranih (79%) se zaveda, da spletne strani lahko profilirajo svoje uporabnike z namenom pošiljanja prilagojenih ponudb. Zelo velik delež anketiranih meni, da elektronska pošta potuje po omrežju nešifrirana in jo je zato enostavno prestrezati in se seznaniti z njeno vsebino. Najmanj uporabnikov pa verjame, da me deskanjem po internetu puščajo elektronske sledi na podlagi katerih je možno identificirati (65%) in da je njihov računalnik lahko del prikritega omrežja (62%).

Graf 6: Prikaz virov ogrožanja v odstotkih.

Spletne strani v zameno za dostop do svojih vsebin in prejemanje drugih ugodnosti, od uporabnika velikokrat zahtevajo njegove osebne podatke. Večina anketiranih (66%) spletnim stanem ni pripravljenih zaupati svojih osebnih podatkov. Takih, ki so za prejemanje raznih ugodnosti pripravljeni posredovati svoje osebne informacije pa je kljub temu kar velik odstotek (34%).

Za varstvo svoje zasebnosti lahko posamezniki veliko storimo s poznavanjem zaščitnih tehnologij. V zadnjem delu ankete nas je zanimalo, kateri so tisti zaščitni ukrepi, ki se jih uporabniki poslužujejo za zaščito svoje zasebnosti. Iz grafa je razvidno, da velika večina anketirancev verižnih sporočil ne pošilja naprej (97%), ne odpira nezaželene elektronske pošte (89%) in uporablja več različnih elektronskih naslovov (90%). Manj kot polovica vprašanih (48%) ima internetni brskalnik nastavljen tako, da onemogoča sprejemanje cookijev. Podoben odstotek anketirancev (44%) ob registraciji na različne spletne strani uporablja lažne osebne podatke. Približno četrtina uporabnikov (24%) zase meni, da so na tekočem z zaščitnimi ukrepi za zaščito svoje pravice do zasebnosti. Najmanj vprašanih (6%) za pošiljanje elektronske pošte uporablja šifriranje.

Graf 7: Prikaz uporabe zaščitnih ukrepov v odstotkih



Ugotovitve te raziskave kažejo, da je slovenskim uporabnikom pravica do zasebnosti zelo pomembna. Kot veliko grožnjo so izpostavili zbiranje, shranjevanje in obdelovanje osebnih podatkov in se jim zdi zbiranje osebnih informacij velik problem. Večina anketirancev meni, da je njihova zasebnost ogrožena. Približno tretjina uporabnikov pa kljub temu meni, da njihovi pravici do zasebnosti ne grozi nobena nevarnost oziroma jim

je vseeno. Zelo velik odstotek vprašanih spletnim stranem ne zaupa svojih osebnih podatkov v zameno za prejemanje raznih ugodnosti. To bi storila le dobra tretjina anketiranih. Veliko uporabnikov se tudi poslužuje različnih zaščitnih ukrepov za varovanje svoje zasebnosti. Takih, ki so na tekočem z zaščitnimi ukrepi in uporabljajo bolj tehnične ukrepe za zaščito svoje zasebnosti, pa je zelo malo. Rezultate te ankete težko posploševati na širšo populacijo, saj je bil vzorec vprašanih relativno majhen. Respondenti pa so bili večinoma študenti.

9. Zaključek

Z razvojem internetne tehnologije se čedalje več naših aktivnost seli na svetovni splet. Splet nam prinaša mnogo prednosti, skriva pa v sebi tudi mnogo pasti. Ena izmed njih je grožnja naši zasebnosti. Na prvi pogled popolnoma neškodljiv internet, pa seveda ni edina tehnologija, ki ogroža naše človekove pravice. Je le ena izmed njih. Uporabniki se teh groženj do neke mere zavedamo, vendar se jim zaradi pomanjkljivega znanja, premajhne osveščenosti in pomanjkanja angažiranja težko zoperstavljamo.

Internetna tehnologija bo v prihodnosti še bolj zaznamovala naša življenja in vplivala na našo pravico do zasebnosti. Čas bo pokazal kako se bo razvijalo naše zasebno življenje v okolju novih tehnologij. Nekateri trendi, ki smo jih identificirali v tej diplomski nalogi, kažejo dokaj zaskrbljujočo sliko. To področje bi bilo v prihodnosti nadvse koristno uvrstiti višje na seznam družbenega zanimanja in na politično agendo.

Pomembno je, da se začnemo o tem pogovarjati na širšem družbenem nivoju, ne pa le v ozkih strokovnih krogih in kot pripadniki informacijske družbe oblikujemo stališča. Kolikor tega ne bomo storili, bodo namesto nas govorili tisti, ki imajo pri vsej stvari največji interes (beri korporacije, državni aparat, delodajalci, založniške hiš in drugi zainteresirani akterji). Čas je da soočimo različna mnenja, ne pa da na primer kar naprej vneto premlevamo problematiko partizanov, domobrancev, tajkunov in drugih tako imenovanih perečih tem, katerih največji cilj je po vsej verjetnosti preusmerjanje pozornosti javnosti od zares pomembnih stvari. Evropska unija je sprejela novo direktivo o obvezni hrambi vseh prometnih podatkov. Število komentarjev o novici na spletni strani: 0. V Ljubljani želijo neko minorno ulico preimenovati v Titovo ulico. Število komentarjev na spletni strani: 300 in raste. Pa kaj me briga, če kdo zbira moje osebne podatke na internetu. Kaj mi mar, če država na zalogo hrani podatke o mojih elektronskih komunikacijah. Zakaj bi me skrbelo, da lahko delodajalec prebira mojo elektronsko pošto in ima pri vdiranju v mojo zasebnost večja pooblastila kot policija. Pa kaj če nimam nobenega prostega časa, še dobro da imam službo. Namesto takega odnosa do zasebnosti, bi bil mogoče bolj na mestu kakšen drug. Kaj pa kogarkoli briga kako mi je ime, kdaj sem rojena in katera je moja najljubša barva. Kaj državo zanima koga in ob kateri uri sem klicala po telefonu. Kaj briga mojega delodajalca katere spletne strani sem obiskala na

delovnem mestu, komu sem poslala elektronsko sporočilo in kakšna je njegova vsebina. Moja stvar.

Svet je čedalje bolj podoben majhni vasi, zato vprašanje naše zasebnosti ne bo zgolj domena posamezne države, pač pa vprašanje celega sveta, saj je internet po svoji naravi globalen medij. Na posameznikih, ki sestavljamo družbeno telo, pa leži odgovornost, da aktivno zaščitimo sfero našega zasebnega življenja, ne pa zgolj da apatično posedamo po nakupovalnih centrih in čakamo, kaj se bo zgodilo. Čakamo na razprodaje. Razprodajajo pa se naše človekove pravice. Zasebnost je na voljo po neverjetno nizki ceni. Zraven priložimo še IQ test. Vse kar morate storiti je le, da nam zaupate še vaše ime in priimek, vašo letnico rojstva in telefonsko številko. Poslali vam bomo sporočilo z rezultati. Ne obremenjujte se z drobnim tekstom. (Vsak teden vam pošljemo še dve nadvse neuporabni komercialni sms sporočili po neverjetni ceni 2.99 evra za sporočilo).

10. Viri

Antić, F. (2007). *Pravni vidiki spletnega portala*. Pridobljeno 20. 1. 2009, iz http://mladipodjetnik.si/internetno-podjetnistvo/razvoj-spletnih-strani/pravni-vidiki-spletnega-portala

Attaran, M. & Vanlaar, I. (1999). Privacy and security on the internet: How to secure your personal information and compnay data. *Information Managment & Computer Security*, 7 (5), 241-246. Članek je dobljen 8.6.2008 iz Emerald Group Publishing Limited.

Baruh, L. (2007). Read at your own risk: Shrinkage of privacy and interactive media. *New Media & Society*, 9 (2), 187-211. Članek je dobljen 5.12.2008 iz SAGE Publications.

Broersma, M. (2005). *Eu warns of DRM privacy threat*. Pridobljeno 20. 1. 2009, iz http://www.eweek.com/c/a/Security/EU-Warns-of-DRM-Privacy-Threat/

Cameron, A. (2004). Digital rights managment: Where copyright and privacy collide. Članek je dobljen 17.12.2008 na www.idtrail.org.

Capuro, M. (2004). Privacy. An intercultural perspective. *Ethics and Information Technology*, 7, 37-47. Članek je dobljen 17.12.2008 iz ProQuest database.

Coleman, S. (2006). E-mail, terrorism, and the right to privacy. *Ethics and Information Technology*, 8, 17-27. Članek je dobljen 17.12.2008 iz ProQuest database.

Collier, G. (1995). Information privacy: Just how private are the private details of individuals in company's database? *Information Managment & Computer Security*, 3 (1), 41-45. Članek je dobljen 8.6.2008 iz Emerald Group Publishing Limited.

Dobosz, B., Green, K., Sisler, G. (2006). Behavioral marketing: security and privacy issues. *Journal of Information Privacy & Security*, 2 (4), 45-58. Članek je dobljen 8.6.2008 iz Emerald Group Publishing Limited.

Elovici, Y., Glezer, C., Shapira, B. (2005). Enhancing customer privacy while searching for products and services on the world wide web. *Internet Research*, 15 (4), 378-399. Članek je dobljen 8.6.2008 iz Emerald Group Publishing Limited.

Forcht, A. K. & Tomas, D. S. (1994). Information Compilation and disbursement: Moral, legal and ethical considerations. *Information managment & Computer Security*, 2 (2), 23-28. Članek je dobljen 8.6.2008 iz Emerald Group Publishing Limited.

Gay, J. (ur.). (2002). *Free software, free society: Selected essays of Richard M. Stallman.* Pridobljeno 20. 1. 2009, iz http://www.gnu.org/philosophy/fsfs/rms-essays.pdf

Global Inetnet Liberty Campaign (1999). *Privacy and human rights: An internation*

survey of privacy laws and practice. Pridobljeno 15. 2. 2009, iz http://gilc.org/privacy/survey

Grunch, M. (2009). *Benefits of spam.* Pridobljeno 20. 1. 2009, iz http://www.articles-about-spam.com/benefits-of-spam.shtml

Hsu, J. C. (2006). Privacy concerns, privacy practices and web sites categories: Toward a situational paradigm. *Online Information Review*, 30 (5), 569-586. Članek je dobljen 8.6.2008 iz Emerald Group Publishing Limited.

Hartman, P. L. (2001). Technology and ethics: Privacy in the workplace. *Business and Society Review*, 106 (1), 1-27. Članek je dobljen 8.6.2008 iz Blackwell database.

Jamink, M. (2008). *Zakaj na osebno izkaznico ne tudi vozniškega in prometnega dovoljenja?* Pridobljeno 11. 2. 2009, iz http://ius-info.ius-software.si/Novice/prikaz_clanek.asp?id=34666&Skatla=17

Jančič Bogataj, M., Klemenčič, G., Makarovič, B., Tičar, K., Toplišek, J. (2007). *Pravni vodnik po internetu*. Ljubljana, GV Založba.

Katos, V., Patel, A. (2007). A partial equlibrium view on security and privacy. *Information Managment & Computer Security*, 16 (1), 74-83. Članek je dobljen 8.12.2008 iz Emerald Group Publishing Limited.

Klang, M. (2004). Spyware-the ethics of covert software. *Ethics and Information Technology*, 6, 193-202. Članek je dobljen 17.12.2008 iz ProQuest database.

Klemenčič, G. (2005). Nekateri pravni vidiki zaščite zasebnosti uporabnikov informacijskih sistemov. *Varstvoslovje*, 7 (1), 42-54.

Kovačič, M. (2006). *Nadzor in zasebnost v informacijski družbi: Filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu*. Ljubljana, Fakulteta za Družbene Vede.

Kovačič, M. (2003). *Zasebnost na internetu*. Ljubljana, Mirovni Inštitut.

Kovačič, M., Vehovar, V. (2000). *Slovenski uporabniki interneta in zasebnost.* Pridobljeno 11. 2. 2009, iz http://www.ljudmila.org/matej/privacy/vsebina/odnos.html

Kucera, K., Plaisent, M., Bernard, P. & Lassana, M. (2005). An empirical investigation of the prevalnece of spyware in internet shareware and freeware distributions. *Journal of Enterprise Information Managment*, 18 (6), 697-708. Članek je dobljen 8.6.2008 iz Emerald Group Publishing Limited.

Larose, R. & Rifon, N. (2006). Your Privacy is assured-of being disturbed: Websites with and without privacy seals. *New Media & Society*, 8 (6), 1009-1029. Članek je dobljen 5.12.2008 iz SAGE Publications.

Lee, Y. (2003). Will self-regulation work in protecting online privacy? *Online*

Information Review, 27 (4), 276-283. Članek je dobljen 8.6.2008 iz Emerald Group Publishing Limited.

Levin, A. (2005). *Privacy law in the United States, the Eu and Canada: The allure of the middle ground.* Pridobljeno 20. 1. 2009, iz http://www.uoltj.ca/articles/vol2.2/2005.2.2.uoltj.Levin.357-395.pdf

Lwin, M. O., Williams, J. D. (2003). A model integrating the multidimensional theory of privacy and theory of planned behaviour to examine fabrication of information online. *Marketing Letters*, 14 (4), 257-272. Članek je dobljen 17.12.2008 iz ProQuest database.

Makarovič, B., Klemenčič, G., Klobučar, T., Bogataj, M. (2001). *Internet in pravo: Izbrane teme s komentarjem Zakona o elektronskem poslovanju in elektronskem podpisu*. Ljubljana, Založba Pasadena.

Mencigar, B. (2004). *Nezaželena elektronska pošta (»spam) in Evropska Unija*. Seminarska naloga. Koper: Visoka šola za management v Kopru. Pridobljeno 20. 1. 2009, iz http://www.fmc.si/bin?bin.svc=obj&bin.id=A711BCB3-BBAC-841F-A781-982F8C22DDE0

Miller, J., Arning, R. (2003). How companies can benefit by adressing privacy isues. *The CPA Journal,* 73 (5), 73. Članek je dobljen 17.12.2008 iz ProQuest database.

Mills, E.J., Hu, B., Beldona, S., Clay, J. (2001). Cyberslacking!:A liability issue for wired workplaces. *Cornell Hospitality Quarterly*, 42, 34-46. Članek je dobljen 8.6.2008 iz SAGE Publications.

Milne, R. G., Rohm, J.R., Bahl, S., (2004). Consumers' protection of online privacy and identity. *The Journal of Consumer Affairs*, 38 (2), 217-232. Članek je dobljen 17.12.2008 iz ProQuest database.

Močnik, P. (2005). Škodljivi Računalniški programi. *Varstvoslovje,* 7 (1), 55-68.

Moscardelli, D. M., Divine, R. (2007). Adolescents' concern for privacy when using internet: An empirical analysis of predictors and relationship with privacy-protecting behaviors. *Family and Consumer Sciences Research Journal,* 35 (3), 232-252. Članek je dobljen 5.12.2008 iz SAGE Publications.

Mramor, D. (2007). Etika in nezaželena elektronska pošta. Raziskovalna naloga. Ljubljana: Zavod Razvojno Izobraževalni Center. Pridobljeno 20. 1. 2009, iz http://www.merkur.eu/fileadmin/datoteke/ostalo/dokumenti/2007_DN_Etika_in_neza__elena_elektronska_po__ta_Mramor.pdf

Nijhawan, D. R.(2003), The emperor has no clothes: A critique of applying the European Union privacy regulation in the United States. *Vanderbilt Law Review*, 56 (3), 939-976. Članek je dobljen 17.12.2008 iz ProQuest database.

Norberg, A. P., Horne, D. R. Horne, A. D. (2007). The privacy paradox: Personal

information disclosure intentions versus behaviors. *The Journal of Consumer Affairs*, 41 (1), 100-126. Članek je dobljen 8.6.2008 iz Blackwell database.

Novak, M. (2004). *Problematika in regulacija spam sporočil*. Diplomsko delo. Ljubljana: Univerza v Ljubljani, Fakulteta za Družbene Vede.

O'Neil, D. (2001). Analysis of Internet users' level of online privacy concerns. *Social Science Computer Review*, 19 (1), 17-31. Članek je dobljen 8.6.2008 iz SAGE Publications.

Ozimek, M. (2005). Orodja za zaščito računalniških sisitemov. *Varstvoslovje*, 7 (1), 76-81.

Peslak, R. A. (2006) Internet privacy polices of the largest international companies. *Journal of Electronic Commerce and Organizations,* 4 (3), 46-62. Članek je dobljen 17.12.2008 iz ProQuest database.

Pinterič, U., Grivec, M. (2007). *Informacijsko komunikacijske tehnologije v sodobni družbi: Multidisciplinarni pogledi*. Nova Gorica, Fakulteta za uporabne družbene vede.

Pollach, I. (2005). A typology of cummunicative strategies in online privacy policies: Ethics, power and informed consent. *Journal of Business Ethics*, 62, 221-232.

Praprotnik, D. (2006). *Varovanje podatkov in zasebnosti na internetu.* Magistrsko delo. Ljubljana: Univerza v Ljubljani, Ekonomska Fakulteta

Radcliff, S. (2007). Commentary: Legal effect of revealing private information in the US and abroad. *Information Systems Management,* 24 (4), 343-344. Članek je dobljen 17.12.2008 iz ProQuest database.

Regan, M. P. (2003). Safe harbours or free frontiers? Privacy and transborder data flows. *Journal of Social Issues*, 59 (2), 263-289. Članek je dobljen 8.6.2008 iz Blackwell database.

Riley, D. (2008). *Europe wants to force DRM interoperability*. Pridobljeno 21. 1. 2009, iz http://www.techcrunch.com/2008/01/04/europe-wants-to-force-drm-interoperability/

Singelton, S. (1999). *Self-regulation: Regulatory fad or market forces?* Pridobljeno 21. 1. 2009, iz http://www.cato.org/pubs/wtpapers/990507report.html

Skrt, R. (2003). *Nezaželena e pošta in slovenska zakonodaja*. Pridobljeno 21. 1. 2009, iz http://www.nasvet.com/nezazelena-posta/

Slobogin, C. (2008). *Governement web data mining and the fourth amendment.* Članek je dobljen 17.12.2008 iz ProQuest database.

Sullivan, B. (2006). *'La difference' is stark in EU, U.S. privacy laws: Eu citizens well*

protected against corporate intrusion, but red tape is tick. Pridobljeno 20. 1. 2009, iz http://www.msnbc.msn.com/id/15221111/

Sullivan, D. (2008). EU's DRM proposal: Does it solve the right problem? Pridobljeno 21. 1. 2009, iz http://www.realtime-websecurity.com/articles_and_analysis/2008/01/eus_drm_proposal_does_it_solve.html

Timmer, J. (2007). *EU bashes DRM, won't support »three strikes« rules*. Pridobljeno 20. 1. 2009, iz http://arstechnica.com/tech-policy/news/2008/11/eu-bashes-drm-wont-support-three-strikes-rules.ars

Trček, D. (2006). *Managing information systems security and privacy*. Berlin, Springer.

Wafa, T.(2008). *Today's inefficient and impotent global internet privacyy rights regime & Tomorrow's inferior alternative.* Pridobljeno 20. 1. 2009, iz http://works.bepress.com/cgi/viewcontent.cgi?article=1000&context=tim_wafa

Wel, L. & Royakkers, L. (2004). Ethical issues in web data mining. *Ethics and Information Technology*, 6, 129-140. Članek je dobljen 17.12.2008 iz ProQuest database.

Woo, J. (2006). The Right not to be identified: Privacy and anonimity in the interactive media enviroment. *New Media Society*, 8 (6), 949-967. Članek je dobljen 8.6.2008 iz SAGE Publications

Priloga 1: Anketa

Sem Maja Žbogar, absolventka Fakultete za Varnostne Vede in pripravljam diplomsko nalogo z naslovom *Zasebnost in internet*. V ta namen izvajam raziskavo o stališčih do zasebnosti med uporabniki. Prosim, da si vzamete nekaj trenutkov in izpolnite spodnjo anketo. Za vaše odgovore se vam iskreno zahvaljujem.

Spol (obkrožite ustrezno): M Ž Starost_____let.

Koliko ur na dan povprečno uporabljate internet (obkrožite ustrezno)?

1. ga ne uporabljam
2. manj kot 1 uro
3. 1-2 ure
4. 3-4 ure
5. 4-5 ur
6. več kot 6 ur

Kako pomembna se vam zdi pravica do zasebnosti posameznika (obkrožite ustrezno)?

1. kaj je to?
2. ni pomembna
3. manj pomembna
4. je pomembna
5. je zelo pomembna

Katera pravica se vam zdi pomembnejša (obkrožite ustrezno)?

1. pravica do zasebnosti
2. pravica do varnosti
3. nimam mnenja

Kaj menite, da vas na internetu najbolj ogroža (obkrožite ustrezno)

1. Vdori v računalnik
2. Virusi in druga škodljiva programska oprema
3. Zbiranje, shranjevanje in obdelovanje osebnih podatkov
4. drugo_____

Kdo je po vašem mnenju najbolj odgovoren za varovanje vaše zasebnosti (obkrožite ustrezno)?

1. jaz sam
2. upravitelji spletnih strani
3. država z regultativno zakonodajo
4. drugo_____

Zbiranje mojih osebnih podatkov na internetu se mi zdi velik problem (obkrožite ustrezno):

1. se sploh ne strinjam
2. se ne strinjam
3. mi je vseeno
4. se strinjam
5. se popolnoma strinjam

Moja zasebnost na internetu je ogrožena (obkrožite ustrezno):

1. se sploh ne strinjam
2. se ne strinjam
3. mi je vseeno
4. se strinjam
5. se popolnoma strinjam

Ali se na internetu ukvarjate z naslednjimi aktivnostmi (obkrožite ustrezno):

- Berem in pošiljam elektronsko pošto DA NE
- Pišem blog DA NE
- Sodelujem na družabnih spletnih straneh kot so MySpace, Facebook DA NE
- Nakupujem preko spleta DA NE
- drugo_____

Ali se strinjate z naslednjimi trditvami (obkrožite ustrezno):

- Med deskanjem po internetu puščam elektronske sledi, na podlagi katerih me je možno identificirati DA NE
- Spletne strani lahko profilirajo uporabnike in jim na podlagi izdelanega potrošniškega profila pošiljajo prikrojene ponudbe DA NE
- Elektronska pošta po omrežju potuje nešifrirana, zato jo je enostavno prestrezati in se seznaniti z njeno vsebino DA NE
- Moj računalnik je lahko okužen s prikrito programsko opremo DA NE
- Moj računalnik je lahko del prikritega omrežja DA NE

Ali se strinjate z naslednjimi trditvami (obkrožite ustrezno):

- V zameno za prejemanje raznih ugodnosti (naprimer dostop do določene vsebine, prejemanje obvestil, sodelovanje v nagradnih igrah ipd), sem pripravljen spletnim stranem zaupati svoje osebne podatke DA NE
- Ob registraciji na spletne strani uporabljam lažne osebne podatke. DA NE
- Vedno sem na tekočem z zaščitnimi ukrepi za zaščito svoje pravice do zasebnosti DA NE
- Uporabljam dva ali več različnih elektronskih naslovov DA NE
- Internetni brskalnik imam nastavljen, da onemogoča sprejemanje piškotkov (cookies) DA NE
- Pri pošiljanju elektronske pošte uporabljam šifriranje DA NE
- Ko prejmem verižno sporočilo, ga pošljem ponavadi pošljem naprej DA NE
- Nezaželene elektronske pošte nikoli ne odpiram DA NE

Približno koliko nezaželenih elektronskih sporočil(spam) prejmete na dan?

1. ne prejemam nezaželenih elektronskih sporočil
2. do 5
3. 5-10
4. več kot 10

Hvala lepa za vaše odgovore in lep dan!

Delovni življenjepis kandidata-Curriculum Vitae

Kakšna je moja izobrazba?

Sem Zoisova štipendistka.
Leta 2004 sem maturirala na Gimnaziji Poljane.
Letos sem končala 4. letnik Fakultete za Varnostne Vede. Sedaj sem v absolventskem stažu. Diplomirala bom predvidoma konec šolskega leta 08/09.

Kaj sem že dosegla do sedaj in kje sem nabirala delavne izkušnje?

V šolskem letu 07/08 sem se udeležila izmenjave v okviru programa EU-AU Exchange. V okviru te izmenjave sem preživela semester na Griffith University v Brisbanu. Tekom tega študija sem napisala kar nekaj esejev v angleškem jeziku na različne teme. Po opravljeni izmenjavi sem se udeležila konference z naslovom Post Conflict Policing v Piranu in pripravila samostojen prispevek.

V šolskem letu 06/07 sem se udeležila Erasmus izmenjave v Turčiji. Študirala sem na Policijski Akademiji v Ankari. Poleg študija, sem se naučila sporazumevati v turškem jeziku. Opravljala pa sem tudi pripravništvo na UNCHR v Ankari, kjer sem se dodobra seznanila z begunsko problematiko, sodelovala pri predstavitvi slovenskega vidika urejanja tega področja in pomagala pri organiziranju njihove knjižnice.

Dalj časa sem delala tudi v podjetju Aragon, kjer sem poleg telefonskega anketiranja, opravljala tudi terenske ankete in večkrat sodelovala pri organizaciji fokusih skupin. Terenske ankete sem izvajala tudi za druge delodajalce. Opravljala pa sem tudi administrativna dela v Centralni Knjižnici Medicinske Fakultete, kjer sem sodeloval pri inventuri. Poleg tega pa sem delala tudi v mednarodni pisarni Fakultete za Varnostne Vede. Veliko sem se ukvarjala tudi z promocijami. Tako sem med drugim promovirala Mladinsko Knjigo, Simobil in Collegium. Na Zavodu Moja Soseska sem bila zadolžena za promocijo varovanja okolja in v okviru tega skupinam šolarjev izvajala predstavitve ekoloških vsebin. Poleg tega pa sem delala tudi za Amnesty International, kjer sem pridobivala nove podpornike.
Nekaj izkušenj imam tudi z delom v gostinstvu.

V katerih jezik lahko komuniciram?

Obvladam angleški jezik in ga tudi redno uporabljam. Sporazumevam se lahko tudi v turškem in nemškem jeziku, ki ju občasno uporabljam. Pasivno pa do neke mere razumem španski in latinski jezik. Trenutno pa se učim japonščino.

Poleg tega pa še….

Microsoft Office, osnove java programiranja, vozniški izpit kategorije B

Za konec pa še moja zanimanja.

V šolskem letu 08/09 se udeležujem tečaja japonskega in ruskega jezika, saj me že od nekdaj zanimata. V prostem času rada hodim na daljše in krajše izlete. Rada hodim v hribe, na morje in se ukvarjam s športom. Včasih pa preprosto ne počnem ničesar.

Kdo sem jaz in kako me lahko kontaktirate

Maja Žbogar
Luče 19, 1290 Grosuplje
Telefon: 040 244 477
Email: myopicself@gmail.com

Izjava o avtorstvu

Spodaj podpisana Maja Žbogar izjavljam, da je zaključno delo z naslovom **»Zasebnost in internet«** rezultat lastnega dela in da so rezultati korektno navedeni.

Ljubljana, 17.7.2009 Maja Žbogar