**UNIVERZA V LJUBLJANI**
*EKONOMSKA FAKULTETA*

**DIPLOMSKO DELO**

# *SISTEMI IN METODE ZA ZAGOTOVITEV ZASEBNOSTI NA INTERNETU*

**Ljubljana, december 2003** **VOJKO KERCAN**

## *Izjava*

Študent Vojko Kercan izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisal pod mentorstvom dr. Borke Jerman-Blažič in dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne _____ Podpis: _____

# *Kazalo*

## *Kazalo slik*



## *Kazalo primerov*

# 1. Uvod

***"We must reserve a little back-shop, all our own, entirely free, wherein to establish our true liberty."***

**(Moramo imeti pravico do naše zasebne sobe, popolnoma naše, kjer lahko vzpostavimo našo resnično svobodo.)**

**Michael Eyugem de Montaigne, francoski renesančni mislec, 1533-1592**

Sodoben koncept zasebnosti sloni na osnovni razdelitvi med okoljem in posameznikom, kjer na eni strani meje leži »zasebno« na drugi strani »javno«.[1] Osnovni namen pri varovanju zasebnosti je v postavitvi meje med zasebnim in javnim ter v dilemi, v kolikšni meri in pod kakšnimi pogoji je dostop do zasebnih podatkov možen. Iz te definicije lahko sklepamo, da vdor v zasebnost pomeni vdor »javnega« na področje »zasebnega« brez posameznikove privolitve. Kontrola meje med »zasebnim« in »javnim« in pravica do odločanja, katere informacije in pod kakšnimi pogoji je le-te posameznik pripravljen odkriti, sta osnovna elementa zaščite in varovanja zasebnosti.

V zadnjih 35 letih je bila tema varovanja zasebnosti stalno prisotna tako v akademskih krogih kot v širši javnosti. Dolga leta so bila prizadevanja za zaščito zasebnosti usmerjena v izdelavo primerne zakonodaje. Leta 1973 je *US Department of Health Education and Welfare* izdal Primerna informacijska načela (*Fair Information Principles*) z namenom nadzorovanja vpliva informatizacije na zasebnost zdravstvenih kartonov in zapisov (A Review of the Fair Information Principles, 1997, str. 1). V skladu s tem je leta 1981 Organizacija za ekonomsko sodelovanje in razvoj *(Organization for Economic Cooperation and Development - OECD)* izdelala Navodila za varovanje pri čezmejnemu prenosu podatkov *(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)*, ki so postala podlaga kasnejši evropski zakonodaji za zaščito zasebnosti DDP (*Directive on Data Protection*) v letu 1995 in Kanadski zakonodaji za zaščito zasebnosti (*Canadian privacy legislation Bill C-6*) v letu 1999.

Kljub takšnim napredkom v zakonodaji je zbiranje in shranjevanje osebnih podatkov postala osrednja značilnost moderne družbe in zato potreba po zaščiti zasebnosti dramatično raste. Meja med »zasebnim« in »javnim« se vse bolj krči in odločitve o odkrivanju osebnih podatkov skorajda niso več v rokah posameznika.

[1] *Sodobno definicijo zasebnosti je postavil Gary T. Marx profesor na M.I.T. univerzi v Združenih državah Amerike. Njegova dela so bila natisnjena v več kot 250-ih knjigah in publikacijah po vsem svetu in prevedena v številne jezike (Marx, 1999).*

Zaradi ne dovolj dodelane zakonodaje in zaradi razvoja novih tehnologij se je rodil nov pristop za zaščito zasebnosti, ki obljublja zaščito zasebnosti v elektronskem svetu: tehnologije za boljšo zaščito zasebnosti (*Privacy Enhancing Technologies - PETs*). Njihov cilj je opremiti posameznika z določenimi orodji, s pomočjo katerih lahko nadzira mejo med »zasebnim« in »javnim« in omogoči kontrolo nad vsemi zasebnimi informacijami, ki jih posameznik poseduje.

Tehnologije za boljšo zaščito zasebnosti in možni načini zaščite v e-poslovanju so osrednja tema diplomskega dela. Celotna raziskava in analiza temelji na trenutno obstoječih tehnologijah, njihovem vplivu na uporabnost spleta in možno implementacijo na posameznikovi ravni. Projekta, ki raziskujeta in razvijata načrte in platforme za zaščito zasebnosti, kot sta PISA *(Privacy Incorporated Software Agent)*[2] in RAPID *(Roadmap for Advanced Research in Privacy and Identity Management)*[3] ter opisi slovenskih in evropskih *(EU GUIDES Project)*[4] zakonodaj na področju zaščite zasebnosti so v študiji izvzeti, ker je raziskava zastavljena izključno na analizi in možni uporabi tehnologij zaščite na uporabnikovi oz. osebni ravni. Nadzor in ohranjanje zasebnosti posameznika na internetu s pomočjo spletnih tehnologij sta ključni vprašanji in smernici celotne diplomske naloge.

Problemi zaščite zasebnosti na svetovnem spletu predstavljajo vprašanja, ki močno vplivajo na ekonomski model spletnih storitev. Ker je celotna e-poslovna struktura odvisna od odnosa do uporabnikov in njihovega zaupanja, je zaznavanje problema zaščite ključnega pomena za njen uspeh. Kako se zbirajo podatki na spletu, kaj podjetja in posamezniki zgubijo ali pridobijo s takšno prakso in kako zagotoviti ustrezno varovanje, so vprašanja, na katera bom skušal odgovoriti. Nadalje želim s tem diplomskim delom vsem ponudnikom spletnih storitev predstaviti vprašanje zaščite tudi kot družbeni problem, ki se dotika vsakega posameznika, saj bodo lahko podjetja le s takim razumevanjem svojega nastopa gradila ravnopraven odnos do svojih kupcev, kar bo končno privedlo do večjega zaupanja uporabnikov spletnih storitev in uspešnega e-poslovanja.

## 1.1. Zgodovinski pregled zasebnosti

V moderni zahodni zgodovini je razlika med »javnim« in »zasebnim« nekaj popolnoma naravnega. Prvi, ki je poudaril razliko med »javnim« in »zasebnim«, je bil pisatelj Michael de Montaigne (1533-1592)[5] (Stalder, 2002, str. 3). Zanj je človeško življenje skupek dveh svetov - notranji jaz in zunanji svet. Da bi lažje ilustriral povezavo med obema svetovoma, je uporabil metaforo hiše. Človek ima v hiši dnevno sobo oz. sobo, kjer se

---

[2] *PISA projekt (http://www.pet-pisa.nl) promovira tehnologije zaščite zasebnosti, kot varno in stabilno tehnologijo za zaščito zasebnosti uporabnikov na področju e-poslovanja in m-poslovanja (Privacy Incorporated Software Agent, 2002).*

[3] *RAPID projekt (http://www.ra-pid.org/default/) je strateški načrt EU razvoja na področju zasebnosti in upravljanja identitete (privacy and identity management - PIM) (Huizenga, 2003, str. 3).*

[4] *Namen EU GUIDES projekta je v izdelavi zakonodaje na evropski ravni za ocenjevanje skladnosti spletnih tehnologij za procesiranje in zbiranje podatkov z zakonodajo EU Data Protection Directive (95/46/EC) (GUIDES Final Report - Deliverable D5.2, 2002, str. 3).*

[5] *Michael Eyugem de Montaigne; veliki francoski renesančni mislec, ki je v svojih Esejih vzel sebe kot objekt opazovanja in študiranja (de Montaigne, 2003).*

odvija življenje z drugimi, sobo ki je izrednega socialnega pomena. Vendar ima hiša tudi spalnico, v katero nima vstopa kdorkoli. Paralela med dnevno sobo in spalnico je enaka kot med zasebnim in javnim življenjem. V paraleli med zasebnimi in javnimi podatki dnevna soba predstavlja javne, spalnica pa zasebne podatke.

Na komunikacijski ravni se vrzel med dvema poloma vidi v razlikovanju med tistim, ki poseduje znanje, in tistim, ki je znan. Pri izdaji knjige recimo lahko pisec poda svoje znanje, ne da bi v procesu razkril svojo identiteto. Četudi je ime avtorja natisnjeno na platnicah knjige, bo za večino bralcev on ali ona ostal nepoznan in nedosegljiv. Tudi branje knjige mrtvega avtorja ni nič drugačno od branja knjige živečega avtorja. Enako velja za bralca. Če se ne razkrije sam, nihče ne ve, da je knjige bral. Knjige in ostali natisnjeni materiali tako posamezniku omogočajo učenje in razkrivanje, ne da bi bil sam v procesu razkrit. Popolnoma drugače je na spletu. Vsak obisk bralca oz. uporabnika spletne strani je zapisan in obstaja veliko načinov, kako slediti bralcu in odkriti njegovo identiteto.

V zadnjih 50-ih letih je ravno pojav tiskane kulture in množičnega tiska povečal našo individualnost in zaščito zasebnosti. V oralni kulturi sta se komunikacija in znanje vedno prenašala v stvarnem času iz oči v oči med vsaj dvema sogovornikoma. Mnenja in misli so bila vedno deljena z drugimi in o pravi zasebnosti nismo mogli govoriti. Stvari so se spremenile s pojavom cenenega tiskanega materiala.

Lahko bi tudi trdili, da je pojav zasebnosti nenamerna posledica novega modela komuniciranja - tiska. Zasebnost se lahko razume kot del kulture, v kateri dominirajo tiskani materiali, ker tisk predstavlja enosmerno komunikacijo. Avtor govori skozi knjigo, bralec bere knjigo sam. Avtor podaja svoje znanje brez razkritja osebnosti, bralec sprejema znanje brez razkritja svoje identitete. Tiskani materiali so lahko tako brez večjih problemov in zanesljivo obdržali vrzel med javnim in zasebnim.

Vendar se je s širitvijo elektronske komunikacije vrzel med javnim in zasebnim nepričakovano zmanjšala in tako sta oba pola pričela sovpadati. Lahko tudi trdimo, da se je problem zaščite zasebnosti pojavil ob socialno-tehnološkem premiku v našem družbenem načinu komuniciranja. Od dvosmerne (oralne) k enosmerni (tiskani) komunikaciji se je sledeč tej logiki, ob novem premiku družbenega komuniciranja v elektronsko komunikacijo, ki je tudi dvosmerna, vrzel zmanjšala, kar postavlja koncept zaščite zasebnosti pod vprašaj. V takšni družbi se je sila težko učiti in razkrivati, ne da bi bili razkriti. Zaradi takšnega premika se zasebnost, ki smo jo poznali v tiskani kulturi, počasi zmanjšuje in naš koncept zasebnosti postaja čedalje bolj problematičen v tako imenovani mrežni ali informacijski družbi (*Network Society, Information Society*).

Trendi kažejo, da se nadzor še povečuje, saj se procesi klasifikacije, zbiranja in zapisovanja podatkov in informacij neprenehoma množijo, življenja posameznikov pa postajajo čedalje bolj transparentna. Ambicija države je videti in nadzorovati vse, enako

ambicijo pa imajo tudi zasebna podjetja. V moderni državi je nadzor maksimalen, zato bi bilo morebiti namesto pojma mrežna oz. informacijska družba bolje uporabljati pojem družba nadzora.

## 1.2. Nadzor in informacijska tehnologija

Nadzor bi obstajal tudi brez informacijske tehnologije, vendar je le-ta nadzorovanje poglobila in okrepila. Značilen primer prednosti uporabe tehnologije je popis prebivalstva.

Popisi prebivalstva so bili za države vedno izjemno pomembni, vendar tudi izjemno zapleteni. Največji problem ni bilo zbiranje podatkov, pač pa njihova analiza. Razvrščanje, katalogizacija in preštevanje podatkov je bila pred izumom računalnika izjemno dolgotrajna naloga, saj so morali vse analize opravljati ročno. Konec 19. stoletja pa je Herman Hollerith izumil posebno napravo za obdelavo podatkov. Poimenovali so jo Hollerithov stroj, ki je bil prvič uporabljen pri ameriškem popisu prebivalstva leta 1890 in pri tem so prihranili približno pet milijonov takratnih dolarjev (Kovačič, 2003, str. 26). Uporaba Hollerithovih strojev je torej analizo podatkov pocenila in pospešila. To so kmalu spoznale ne samo vlade drugih držav, pač pa tudi različna podjetja, ki so začela za analizo svojih podatkov (o strankah in potrošnikih) uporabljati tovrstne naprave.

Hitrejša in cenejša analiza ni prinesla samo veliko prednosti, ampak tudi nove nevarnosti, ki se jih pred pojavom tehnologij ni nihče dobro zavedal. Po navedbah pisatelja knjige »*IBM and the Holocaust: The Strategic Alliance Between Nazi Germany and America's Most Powerful Corporation*« Edwin-a Black-a so namreč leta 1933 v Tretjem rajhu začeli popisovati prebivalstvo in eden od namenov popisa je bil tudi identifikacija judovskega prebivalstva. Pri tej identifikaciji so si nacisti pomagali s Hollerithovimi stroji, identifikaciji pa so kasneje sledile zaplembe premoženja in deportacije. Avtor nadalje še razkriva, da je IBM v času Tretjega rajha za nacistično Nemčijo izdeloval Hollerithove stroje, ki so bili uporabljeni v koncentracijskih taboriščih in vojni industriji, mesečno pa je IBM tudi servisiral stroje in učil naciste njihove uporabe (Black, 2002, str. 20).

Večina današnjega nadzora na začetku 21. stoletja je nevidna, ker se pojavlja na območju digitalnih signalov. Pojavlja se v vsakodnevnem življenju pri opravljanju vsakdanjih opravil. Imenujemo jo elektronska sled, ki jo posamezniki puščajo za seboj. Vsakič, ko posameznik dvigne slušalko, uporabi bankomat ali plačilno kartico, gre na banko, obišče zdravnika, uporabi mobilni telefon ali se priključi na internet, ... avtomatski sistemi ali institucije dogodek zaznajo in zabeležijo. Elektronska sled je torej informacija, ki se shranjuje rutinsko in kaže dejavnost nekega posameznika (Kovačič, 2000a, str. 1023).

Povečana moč nadzorovanja s konstantnim spremljanjem elektronske sledi posameznika je v povezovanju tako zbranih podatkov. Čebulj[6] v publikaciji »Varstvo informacijske zasebnosti v Evropi in Sloveniji« navaja, da s povezavo in njihovo obdelavo lahko pridemo do novih pomembnih podatkov in informacij, kar je za posameznika lahko škodljivo ali celo nevarno zaradi ogrožanja njegovih pravic (Čebulj, 1992, str. 9). Čebulj nadalje še navaja, da je problem informacijske zasebnosti še večji zato, ker vodenje in vzdrževanje avtomatskih baz podatkov ni vezano le na državne organe, temveč tudi na organizacije izven državne oz. javne uprave (Čebulj, 1992, str. 8). Prav povezavo in kombiniranje različnih podatkov pa omogočajo sodobne informacijsko-komunikacijske tehnologije. Matej Kovačič[7] v knjigi »Zasebnost na internetu« navaja ugotovitev, da spremljata razvoj nadzorovalnih sistemov dva nevarna trenda, zaradi katerih se posamezniki ne zavedajo obsega nadzorovanja v tolikšni meri, kot bi se ga lahko sicer. Po eni strani posamezniki s svojimi dejanji samodejno sprožajo te sisteme (npr. z nakupom s kreditno kartico), hkrati pa ti sistemi podatke in informacije tudi iščejo in preverjajo sami, predvsem iz sekundarnih virov (Kovačič, 2003, str. 28). Takšna dejanja predstavljajo nove nevarnosti, ki se pojavljajo v postopku analize in vrednotenja. Po mnenju Čebulja je posledica takega postopka nova vsebina podatka, ki lahko ne ustreza več dejanskim lastnostim posameznika. Z napačnim vrednotenjem ogromne količine podatkov, ki se zbirajo o posamezniku, lahko pridemo do novih informacij, ki so za posameznika škodljive ali celo nevarne (Čebulj, 1992, str. 8).

Poleg tega računalniki skupaj z naprednimi statističnimi tehnikami in tehnikami rudarjenja podatkov (*data mining*)[8] vzpostavljajo nove razsežnosti nadzora *(web mining)*[9]. Uporaba računalniške tehnologije ta proces lahko nadgradi tudi s sistemi umetne inteligence, kar pomeni preskok na novo raven, na raven preventive in predvidevanja. S tem je ogroženo eno temeljnih pravnih demokratičnih načel, namreč domnevne nedolžnosti. Kljub vsemu ni dvoma, da postaja preventiva čedalje bolj pomembna usmeritev v razvoju sodobnih nadzorovalnih sistemov. Celotna ameriška varnostna politika, še posebej od 11. septembra naprej, temelji na predvidevanju in preventivi. 1. januarja 2004 naj bi se pričel projekt *US Visit*, kar pomeni, da bi vsak potnik, ki pripotuje v ZDA z vizo, pustil svoje prstne odtise in podatke in bi bil nato primerjan s podatkovno bazo znanih teroristov in kriminalcev (India Express Bureau, 2003). Tudi celotna zgodba ameriškega napada na Irak je temeljila na preventivi in predvidevanjih o orožjih za množično uničevanje. Dokaz, da je sistem nadzora na podlagi

---

[6] *Janez Čebulj; redni profesor na Fakulteti za upravo in avtor številnih publikacij, med njimi tudi na področju varstva zasebnosti: Varstvo osebnih podatkov z zakonom in pojasnili in Varstvo informacijske zasebnosti v Evropi in Sloveniji.*

[7] *Matej Kovačič; diplomirani sociolog in mladi raziskovalec ter asistent na Fakulteti za družbene vede na Univerzi v Ljubljani. Avtor znanstvenega članka »Zasebnost v informacijski družbi« in vrste drugih publikacij na področju zasebnosti (Kovačič, 2003).*

[8] *Data mining; rudarjenje podatkov je tehnika za odkrivanje zakonitosti v podatkih, ki odpirajo nove možnosti podjetjem pri iskanju novih potencialnih kupcev za njihove izdelke in obravnavanju stalnih kupcev glede na njihove zahteve.*

[9] *Web mining; rudarjenje podatkov zbranih na spletni strani, ki omogočajo ugotavljanje uporabnikovih interesov in nato dinamično določanje storitev za vsakega posameznika posebej.*

predvidevanja ušel iz rok tudi Američanom, je v vzpostavitvi standardiziranega terminskega trga *(features market)*, na katerem bi se trgovalo s terorističnimi napadi, atentati in drugimi dogodki na Bližnjem Vzhodu. Investitorji bi lahko stavili na možnost atentata na palestinskega vodjo Yasser-ja Arafata-a ali na možnost strmoglavljenja jordanskega kralja Abdullah-a II ali na manj nasilne dogodke, kot je ameriško priznanje palestinske države. Projekt PAM *(Policy Analisys Market)*, ki je bil predstavljen v juliju 2003, bi Pentangonu in ostalim varnostnim službam služil za pridobivanje informacij, investitorji, ki so kupili standardizirano terminsko pogodbo dogodka, ki bi se kasneje tudi uresničil, pa bi zaslužili. Projekt, ki je povzročil ogorčenje tudi samih Američanov (predvsem demokratov) in ostalih svetovnih političnih vodij, je bil že po nekaj dneh ustavljen. (Policy Analysis Market, 2003; Guggenheim, 2003; Milchen, 2003).

Množični podatkovni nadzor se ponavlja rutinsko in je namenjen odkrivanju podatkov oseb, ki bi utegnile koristiti kakšni organizaciji ali vladni instituciji. Gre za to, da posameznika uvrstijo v neko kategorijo, kjer je na podlagi svojih karakteristik, ne pa dejanj, označen za sumljivega oz. vrednega pozornosti. Postopek, ki se imenuje profiliranje (o katerem bo tudi več govora v nadaljevanju), so začeli na veliko uporabljati v ZDA še posebej po 11. septembru. Proces profiliranja sproža mnoga vprašanja, recimo že omenjeni problem domneve nedolžnosti, saj je neki posameznik tako označen za krivega, dokler ne dokaže svoje nedolžnosti (namesto, da bi bilo nasprotno). Uporaba računalnikov je tako moč nadzorovalnih sistemov izjemno povečala, zato nas od družbe popolnega nadzora loči samo omejena zmogljivost nadzorovalnih sistemov, za katere so pomembne naslednje štiri sestavine (Kovačič, 2003, str. 29):

1. velikost datotek, ki jih sistem lahko shrani,
2. stopnja, do katere so lahko ti sistemi centralizirani,
3. hitrost pretoka podatkov in informacij med točkami v sistemu,
4. število stičnih točk med sistemom in subjektom.

# 2. Definicija zasebnosti in modeli zaščite zasebnosti

***"The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow though it; the storms may enter; the rain may enter - but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement."***

**(Tudi najrevnejši človek se v svoji koči lahko upira vsej moči Kroni. Lahko je slaboten, lahko se maje streha njegove koče, skoznjo lahko piha veter, vanjo lahko pride nevihta ali dež, toda kralj Anglije ne sme vstopiti; vsa njegova moč si ne sme drzniti prestopiti praga razdejanega doma.)**

**William Pitt, britanski državnik, 1708-1778**

## 2.1. Definicija zasebnosti

Zasebnost je temelj človeškega dostojanstva, kot je to svoboda druženja in svoboda govora, nekateri avtorji celo trdijo, da so vse človekove pravice neke vrste posamični vidiki pravice do zasebnosti. Pravica do zasebnosti je sicer temeljna, vendar ni absolutna, v sodobni družbi pa je postala ena najpomembnejših človekovih pravic. Podobno kot Gary T. Marx je Banisar[10] pravico do zasebnosti določil kot »mejo, do katere družba lahko vdre v posameznikove zadeve«. Zasebnost ni enodimenzionalen pojem; različni avtorji vidijo več dimenzij zasebnosti (Čebulj, 1992, str. 7):

1. zasebnost v prostoru (želja posameznika, da ima možnost biti sam, torej ločen od fizične prisotnosti drugih ljudi),
2. zasebnost osebnosti (svoboda misli, opredelitve, izražanja) in
3. informacijska zasebnost (možnost posameznika, da obdrži podatke in informacije o sebi, ker ne želi, da bi bili z njimi seznanjeni drugi).

Poročilo Privacy & Human Rights[11] 2003 loči naslednje vrste zasebnosti (Laurant, 2003):

1. informacijska zasebnost, ki določa načine zbiranja in uporabe zasebnih podatkov, kot so informacije plačilnih kartic, zdravstvene, vladne informacije in druge,
2. zasebnost telesa, ki obsega zaščito fizičnega telesa človeka pred nasilnimi postopki, kot so genetični testi, testi na poživila in preiskave človeških votlin,
3. zasebnost komunikacij, ki zajema zaščito in zasebnost pošte, telefonskih pogovorov, e-pošte in drugih načinov komuniciranja in

---

[10] *David Banisar, namestnik direktorja Privacy International in eden od ustanoviteljev Electronic Privacy Information Center (EPIC). Avtor številnih študij in knjig (The Electronic Privacy Papers, Privacy and Human Rights: An International Study of Privacy Laws and Practices).*

[11] *Vsako leto Privacy International in Electronic Privacy Information Center izda poročilo Pravicy and Human Rights, pregled o zasebnosti in varstvu pravic v več kot 50-tih državah na svetu; med njimi tudi v Sloveniji (Privacy International, 2003).*

4. prostorska zasebnost, ki vzpostavlja mejo vdora v domače, poslovno ali javno okolje, kot so video nadzori.

Poročilo nadalje ugotavlja, da sta v sodobni družbi najbolj ogroženi informacijska zasebnost in zasebnost komunikacij.

Leta 1890 je takratna vrhovna sodnica Združenih držav *(Supreme Court Justice)* Louis Brandeis zagovarjala koncept zasebnosti kot »pravico biti puščen pri miru« (Laurant, 2003). Danes lahko trdimo, da je ta koncept v ZDA močno narušen, saj se morajo Američani prijaviti na »*Do not call*« listo, v kolikor ne želijo biti moteni s telefonskimi reklamami v svojem domačem okolju. Od 16. septembra 2003 do 25. septembra 2003 se je prijavilo več kot 50 milijonov Američanov (Davidson, 2003; National Do Not Call Registry, 2003). Robert Ellis Smith, založnik *Privacy Journal*[12], pa je definiral zasebnost kot »željo vsakega izmed nas imeti fizičen prostor, kjer smo nemoteni, brez nadlegovanja in zadreg ter posedujemo kontrolo nad časom in načinom, kako bodo naši osebni podatki razkriti« (Laurant, 2003).

Po poročilu Privacy and Human Rights 1999 ogrožajo zasebnost trije pomembni trendi (Banisar, 1999):

1. globalizacija (odstranjuje geografske omejitve pri pretoku podatkov),
2. skladnost med tehnologijami (le-te so med seboj čedalje bolj povezljive) in
3. multi-medialnost (podatki v neki obliki se hitro lahko spremenijo v drugo obliko).

Lahko trdimo, da je bila zasebnost posameznika sicer ogrožena že pred pojavom informacijsko-komunikacijskih tehnologij in računalniških zbirk podatkov, da pa nova tehnologija ogroženost zasebnosti samo stopnjuje in je privedla do tega, da so se ljudje začeli zavedati nevarnosti bolj kot v času ročno vodenih evidenc.

## 2.2. Modeli zaščite zasebnosti

Poročilo Privacy and Human Rights 2003 navaja štiri osnovne modele zaščite zasebnosti. Odvisno od njihove uporabe so lahko ti modeli med seboj kontradiktorni ali komplementarni. V državah, kjer je zaščita zasebnosti največja, se uporabljajo vsi štirje modeli.

Nadzorni zakoni (*Comprehensive Laws*)

V večini držav na svetu obstaja krovni zakon o zbiranju in uporabni osebnih podatkov za javni in komercialni sektor, kjer državni nadzorni odbor nadzira njegovo uporabo. To je priporočljiv model za vse države, ki sprejemajo zakone o zaščiti zasebnosti, in je bil sprejet tudi v Evropski Uniji. Pri tem pristopu industrija sama določi pravila zaščite zasebnosti in jih sama tudi uveljavlja, nadzoruje pa jih agencija za zaščito zasebnosti.

[12] *Privacy Journal - najbolj ugledna in najstarejša (ustanovljena 1974) publikacija na svetu, na področju varstva pravic in zasebnosti (Privacy Journal, 2003).*

Sektorski zakoni *(Sectoral Laws)*

Nekatere države, kot recimo ZDA, niso vpeljale enotnega nadzornega zakona, pač pa zakone za posamezne sektorje (zakoni na področju finančnega sektorja, IT sektorja, ...). Slaba plat takšnega modela je, da je za vsako novo tehnologijo potrebno predstaviti in sprejeti nov zakon, zato dejanska zaščita zasebnosti (vsaj ob uveljavitvi nove tehnologije) velikokrat zaostaja v primerjavi z zakonodajo. V številnih državah se sektorski zakoni uporabljajo kot dopolnilo glavnemu nadzornemu zakonu in tako natančneje delujejo v sektorjih (zakoni v telekomunikacijskem sektorju, zakoni o uporabi podatkov v kartotekah policije, zakoni o uporabi podatkov imetnikov kreditnih kartic, ...).

Samo-regulacija (*Self-Regulation*)

Zaščita zasebnosti oz. zaščita podatkov je lahko dosežena, vsaj teoretično, z vrsto samo-regulativ, kjer komercialni in javni sektorji vzpostavijo pravila in načela o zbiranju podatkov in tako sama sebe nadzorujejo. Vendar se je v večini držav, še posebej v ZDA, ta model izkazal za zelo slabega, saj ni bilo nikakršnih potrdil, da so podjetja sledila pravilom in načelom o zbiranju podatkov. Ustrezna pravila in nadzor sta glavna problema v uporabi takšnega modela.

Tehnologije zaščite zasebnosti *(Technologies of Privacy)*

Ker so tehnologije zaščite zasebnosti postale dostopne širši javnosti, se je zaščita zasebnosti pomaknila tudi v doseg posameznika. Uporabniki interneta imajo na voljo vrsto sistemov in aplikacij za zaščito zasebnosti. Mednje sodijo šifriranje, anonimni strežniki za elektronsko pošto, proxy[13] strežniki in drugi, vendar so te tehnologije za večino uporabnikov neznane in pretežavne za uporabo. Še večkrat pa se posamezniki sploh ne zavedajo problema zaščite zasebnosti.

Simone Fischer-Hübner[14], avtorica knjige *»IT-Security and Privacy: Design and Use of Pravicy Enhancing Security Mechanisms«*, navaja podobne štiri osnovne načine, kako doseči zaščito zasebnosti na svetovnem spletu (Fischer-Hübner, 2001, str. 3):

1. vladni ukrepi na področju zaščite zasebnosti in zakoni o varstvu podatkov,
2. zbirka predpisov o zbiranju podatkov, ki jih uveljavljajo podjetja pri poslovanju,
3. vpeljava tehnologij zaščite zasebnosti (na posameznikovi ravni),
4. izobrazba uporabnikov in IT profesionalcev o zaščiti zasebnosti.

[13] *Proxy; vmesni strežnik, ki deluje kot strežnik pri odjemalcu in kot odjemalec k strežniku (Jerman-Blažič, 2001).*

[14] *Dr. Simone Fischer-Hübner; profesorica računalniških znanosti na Karlstadski univerzi in avtorica številnih člankov, publikacij in knjig na področju varnosti računalniških sistemov in zasebnosti posameznika na spletu (Fischer-Hübner, 2003).*

# 3. Tehnologije nadzora

***"Every man should know that his conversations, his correspondance and his personal life are private."***

**(Vsak človek bi moral vedeti, da so njegovi pogovori, dopisovanja in osebno življenje zasebni.)**

**Lyndon B. Johnson, 36. predsednik Združenih držav (1963-69), 1908-1973**

Razvoj tehnologije je omogočil povečanje in pocenitev zbiranja ter obdelave podatkov in informacij, zato je nadzor nad posameznikom lahko postal večji. Hkrati je, predvsem zaradi nadzorovanja potrošnikov, prišlo do tega, da imajo podatki in informacije veliko tržno vrednost. Z vidika varnostnih analitikov in same industrije je pri zbiranju potrošniških informacij ključna razlika med ekonomskim zbiranjem podatkov in željo po kontroli nad informacijami o posamezniku. Industrija trdi, da je zbiranje podatkov o potrošnikih namenjeno le poznavanju želja svojih kupcev in ne nadzoru. Zagovorniki zbiranja osebnih podatkov v ekonomskem smislu kategorizirajo prednosti v naslednje tri kategorije:

1. Uporabniška pripravnost *(User convenience);* zbiranje informacij o posameznem uporabniku nudi možnost personalizacije in ponudbe po meri posameznika, kar končno privede uporabniško izkušnjo in uporabnost na višjo raven.
2. Marketing in poslovni razvoj *(Enhanced marketing and business development);* ker je svetovno internetno okolje izredno tekmovalno, je za pridobivanje tržnega deleža ključnega pomena zagotovitev zaupanja kupcev in povečanje transakcij na uporabnika oz. povečanje (ponovne) prodaje. Ker je zadržanje kupcev veliko ceneje kot pridobivanje novih, je relacija z obstoječimi kupci odločilen faktor v uspešnem e-poslovnem modelu. Personalizirana ponudba, hiter odziv na uporabnikove zahteve in spoštovanje uporabnikovih želja so pomembni dejavniki v izgradnji odnosa z uporabniki. Zato morajo podjetja dobro poznati svoje kupce in trg, kar lahko dosežejo z zbiranjem informacij o obstoječih kupcih.
3. Zaščita potrošnikov *(Consumer protection);* ker imajo podjetja shranjene osebne podatke uporabnikov, so lahko ti uporabljeni pri potrditvi nakupa. Povratni kontakt je opravljen direktno s kupcem in so tako možnosti napak manjše.

Poročilo OECD *»Inventory of Privacy Enhancing Technologies«* navaja dva osnovna načina zbiranja podatkov.

Pasivno zbiranje podatkov

Zbiranje ne-osebnih podatkov oz. podatkov, ki ne razkrivajo fizične identitete uporabnikov in so predvsem uporabni za upravitelje in administratorje spletnega mesta. Število obiskov, najbolj obiskane strani znotraj spletnega mesta, hitrost dostopa do interneta, operacijski sistem, vrsta spletnega brskalnika, resolucija monitorja so izredno pomembni podatki, s pomočjo katerih je spletno mesto mogoče prirediti njihovim uporabnikom in tako povečati njegovo

uporabnost in primernost vsebine (v nadaljevanju je ta postopek zbiranja podatkov opisan kot *HTTP Chattering*).

Nekaj osebnih podatkov pa je le mogoče prestreči s pasivnim zbiranjem podatkov. To predvsem velja za uporabnike, ki imajo v svojih spletnih brskalnikih shranjene osebne podatke, kot sta ime in spletni naslov. Večina uporabnikov se ne zaveda, da se njihovi osebni podatki shranjujejo, čeprav se je temu sila lahko izogniti. Uporabnik v nastavitvah spletnega brskalnika enostavno ne vključi svojih osebnih podatkov, saj ti niso nujni za pravilno delovanje brskalnikov.

Aktivno zbiranje podatkov
Številne spletne strani aktivno zbirajo podatke uporabnikov s pomočjo različnih tehnologij (v nadaljevanju so postopki opisani kot piškotki, spletni hrošči, e-profiliranje, vstavljena programska oprema *(embeded software)*, elektronske sledi pri ponudniku dostopa do interneta, povezovanje, zbiranje in prestrezanje podatkov), ali pa s poslovnimi procesi, ki v zameno za informacije, ugodnosti ali uporabo zahtevajo osebne podatke (spletni obrazec, osebni računi v spletnih trgovinah, spletne e-pošte, ...).

## 3.1. Elektronske sledi pri ponudniku internetnih storitev in vsebin *(HTTP chattering[15], browser's chattering)*

Najbolj pogosto uporabljena storitev v svetovnem komunikacijskem omrežju interneta je brskanje po svetovnem spletu, ki je omogočeno s HTTP[16] protokolom. HTTP protokol deluje na podlagi izmenjave informacije med odjemalcem *(remote user)* in spletnim strežnikom *(web server)*. Da bi se vzpostavil zahtevek za ogled spletne strani, je iz odjemalčevega računalnika poslan niz podatkov spletnemu strežniku, na katerem se nahaja spletna stran. Že v začetku, ob vzpostavitvi zahtevka, se shranijo določene informacije o odjemalčevem računalniku, kot so IP[17] naslov, vrsta in verzija operacijskega sistema in brskalnika, ter URL[18] lokacija pred obiskom trenutne spletne strani *(referer)*. Takšne informacije se prenašajo brez privolitve in vednosti uporabnika spletnega brskalnika. S pomočjo IP naslovov in tehnologije za izsledbo izvora TCP/IP[19] paketov je mogoče določiti približno lokacijo uporabnika. Z vzpostavitvijo IP v6[20], ki vsebuje veliko bolj natančno informacijo o geografski lokaciji v ovojnici (*header*) HTTP protokola, se bo vdor v zasebnost le še povečal. Podoben problem se pojavlja tudi pri ostalih internetnih

---

[15] *to chatter = čenčati, klepetati*
[16] *HTTP = Hyper Text Transfer Protocol; opredeljuje potek in vsebino komunikacije med spletnim odjemalcem in strežnikom.*
[17] *IP = Internet Protocol*
[18] *URL = Uniform Resource Locatior; enotni identifikator za internetne vire, ki določa metode dostopa in lokacijo.*
[19] *TCP/IP = Transport Control Protocol / Internet Protocol; osnovni standardni protokol za internet, ki omogoča različnim računalnikom, ki so priključeni na internet, komunikacijo drug z drugim (Jerman-Blažič, 1999, str. 40).*
[20] *IP v6 = nova generacija internetnega protokola, ki ga je ustvarila IETF (The Internet Engineering Task Force - http://www.ietf.org) z namenom zamenjave trenutnega internet protokola IP v4.*

protokolih (SMTP[21] in FTP[22]) (GUIDES E-Business Guidlines on Data Protection Directive 95/94/EC, 2002, str. 5 - 6; Seničar, Jerman-Blažič, Klobučar, 2003, str. 2 - 3).

Takšni mehanizmi in tehnologije omogočajo administratorjem spletnih strani identifikacijo uporabnikov po imenu ali IP naslovu, ne glede na to, ali je ta sploh opravil kakršno koli dejanje ali izpolnil obrazec. Če temu dodamo še spletno tehnologijo imenovano *cookie* oz. piškotek, dobimo mehanizem za zasledovanje, profiliranje in opazovanje aktivnosti uporabnika.

V poročilu z naslovom *»Privacy on the Internet - An Integrated EU Approach to On-line Data protection«* je bilo s primerjalno analizo različnih spletnih brskalnikov ugotovljeno, da Microsoft Internet Explorer razkrije celo, ali ima uporabnik na svojem računalniku nameščene programske pakete Word, Excel ali PowerPoint (Data Protection Working Party, 2000, str. 15). S pomočjo Jave[23] in JavaScripta[24] pa je mogoče med obiskom spletne strani o uporabniku dobiti tudi informacije o resoluciji zaslona, o nastavljenem časovnem pasu, ali ima uporabnik vključeno podporo za Javo, katere priključne module ima naložene *(plug-ins)*, oceno hitrosti dostopa do interneta, itd. Lahko pa je ugotoviti tudi, ali ima uporabnik na svojem računalniku shranjeno kakšno avtorsko izvirno vsebino (film, glasba, knjige, ...), za katero ni plačal avtorske pravice.

***Primer 1:*** *enostaven prikaz zbranih informacij pri ponudniku internetnih storitev*

| IP naslov računalnika | Čas obiska | Prihaja od strani | OS in spletni brskalnik |
|---|---|---|---|
| 213.250.11.174 | 30.10.2003 19:58:00 | http://www.agencija imelda.si/1.html | Mozilla/5.0(Macintosh; U; PPC Mac OS X; en-us) AppleWebKit/85.7 (KHTML, like Gecko) Safari/85.5 |
| 212.13.227.107 | 21.10.2003 8:49:16 | http://www.matkurja.com/slo/search?keys=intelektualni | Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) |

*Vir: Interni podatki Dhimahi d.o.o., 2003.*

## 3.2. Piškotki *(cookies)* in spletni hrošči *(web bugs)*

HTTP piškotki so podatkovni mehanizem, ki omogoča interakcijo med uporabnikom in spletno stranjo in priskrbijo strežniku, na katerem se nahaja spletna stran, informacije o uporabnikovi identiteti (osebni podatki, informacije o aktivnostih na spletni strani, podrobnosti o kreditnih karticah, uporabniško ime in geslo spletne strani). Po času

[21] *SMTP = Simple Mail Transfer Protocol; protokol za elektronsko pošto, ki omogoča dostavo in usmerjanje paketov, ki nosijo vsebino elektronske pošte.*
[22] *FTP = File Transfer Protocol; protokol, ki omogoča prenos datotek med računalniki v internetu.*
[23] *Java; objektno orientiran programski jezik, ki je neodvisen od platforme.*
[24] *JavaScript; skriptni jezik za programiranje spletnih strani, ki je vključen v HTML stran.*

trajanja ločimo t.i. sejne piškotke (*session cookies* - potečejo, ko uporabnik zapre spletni brskalnik) in vztrajne piškotke (*presistent cookies* - daljši čas trajanja). Razen tega ločimo piškotke obiskane spletne strani *(first party cookies)* in piškotke, ki jih pošiljajo druge spletne strani, ki so vključene v obiskano spletno stran *(third-party cookies)* (Data Protection Working Party, 2000, str. 42, 52).

Digitalni piškotki omogočajo tudi avtomatizacijo v poslovnih spletnih aplikacijah, kar je uporabno predvsem v elektronski trgovini, ker povečujejo interaktivnost same spletne strani. Ne glede na to, da so digitalni piškotki zelo močno orodje, obstajajo številne napake v uporabi in možnost zlorabe, kar je dodatna grožnja zaščiti zasebnosti:

1. Varnostni neuspeh *(Security failures)*; občutljive informacije so shranjene v digitalnih piškotkih, ki se prosto prenašajo po svetovnem spletu. Vsebina piškotkov je teoretično dostopna vsakomur, ki je zmožen prestreči datoteko, ali pa tistemu, ki zlonamerno pridobi dostop do mrežnega računalnika. Zato morajo biti podatki v piškotkih šifrirani. Načeloma imajo uporabniki zelo malo nadzora nad varnostnimi ukrepi, ki zajemajo shranjevanje in prenos piškotkov.

2. Opazovanje *(Monitoring);* veliko ljudi meni, da je identifikacija uporabnika s pomočjo piškotkov vdor v njihovo zasebnost. Ljudje imajo v resničnem svetu možnost vstopiti v trgovino in opraviti nakup, ne da bi razkrili svojo identiteto. Takšna možnost bi morala obstajati tudi v elektronskih trgovinah, kar pa je z uporabo tehnologije piškotkov nemogoče.

3. Razkritje podatkov *(Data disclosure);* stran, ki ima shranjene osebne podatke s pomočjo piškotkov, lahko zamenja te podatke z drugimi spletnimi stranmi. To pomeni, da se podatki, ki so bili zavestno podani na eni spletni strani, lahko uporabijo za identifikacijo in opazovanje uporabnika na popolnoma drugi spletni strani, kjer uporabnik nikoli ni namenoma pustil svojih informacij.

   Obstaja tudi nevarnost, da se zbrani podatki ne uporabijo za tisto, za kar so bili zbrani. Kot navaja Kovačič v »Zasebnost na internetu«, pri bankrotu nekega podjetja obstaja nevarnost, da bodo za poplačilo dolgov uporabili denar od prodaje osebnih podatkov, pa čeprav so bili podatki zbrani z zagotovilom, da ne bodo nikoli posredovani tretjim osebam brez izrecne privolitve posameznikov (Kovačič, 2003, str. 41). Znan je primer podjetja Toysmart.com, ki je šlo v stečaj, za poplačilo dolgov pa so v stečajno maso vključili ravno tako zbrane osebne podatke, čeprav je bilo zapisano v politiki zasebnosti, da se informacije zbrane na spletni strani ne bodo prodale ali zamenjale tretjim strankam. Kasneje je WaltDisney Co., ki je bil večinski lastnik podjetja Toysmart.com, obljubil, da bo odkupil zbrane osebne podatke in tako ohranil zasebnost 250.000 kupcev (Greenberg, 2000). Walt Disney je na koncu plačal podjetju Toysmart.com 50.000 USD, da so pritisnili tipko *delete* in tako uničili vse zbrane podatke svojih kupcev (Hoppe, 2001).

4. Omejen nadzor *(Limited control);* končni uporabniki imajo zelo malo nadzora nad vsebino in uporabo piškotkov, za večino uporabnikov pa so popolnoma nevidna tehnologija. Večina spletnih brskalnikov omogoča uporabniku izklop piškotkov (oz. možnost, da jih ne sprejmejo), vendar takšna odločitev nekatere spletne strani naredi popolnoma neuporabne.

5. Zbiranje podatkov *(Collecting data);* enega od prikritih načinov zbiranja podatkov ali posebno identifikacijo uporabnikov omogoča mehanizem tako imenovanega spletnega hrošča *(web bugs)*. Spletni hrošč je nevidni grafičen element na spletni strani ali v elektronskem sporočilu v velikosti 1x1 px, definiran kot HTML IMG tag. Njihova naloga je opazovanje uporabnika spletne strani ali bralca e-sporočila. (GUIDES E-Business Guidlines on Data Protection Directive 95/94/EC, 2002, str. 7; Seničar, Jerman-Blažič, Klobučar, 2003, str. 3).

   Ta postopek omogoča ugotoviti, po katerih spletnih straneh v oglaševalskem omrežju se giblje posamezni uporabnik. Če je spletno oglaševalsko omrežje dovolj veliko[25], lahko na podlagi zbranih podatkov ugotovimo brskalne navade posameznega uporabnika, te podatke pa lahko povežemo z elektronskim naslovom posameznika in celo s t.i. *off-line* ali izven mrežno fizično identiteto[26]. Fizično identiteto uporabnika je mogoče ugotoviti tako, da uporabnik svoje podatke posreduje kateri koli spletni strani v omrežju, ti podatki pa se povežejo z identifikacijsko številko piškotka.

[25] *Največja spletna oglaševalska mreža na svetu je mreža podjetja DoubleClick (http://www.doubleclick.com). V Sloveniji DoubleClick-ovo tehnologijo DoubleClick AdServer uporablja podjetje HTTPOOL (http://www.httpool.si).*

[26] *V začetku leta 2000 je časnik USA Today razkril, da je DoubleClick zbiral imena uporabnikov in skušal piškotke povezati tudi z identiteto uporabnikov v resničnem življenju. DoubleClick se je povezal s podjetjem Abacus Alliance (http://www.abacus-direct.com), ki je v ZDA vodilno podjetje za zbiranje podatkov o potrošnikih, in podjetji sta začeli združevati podatke o potrošnikih iz obeh svojih baz (Kovačič, 2003, str. 48).*

***Primer 2**: piškotek podjetja DoubleClick*

```
SITESERVER
ID=587596117a7350bcbf2e4c04d114247d
doubleclick.com/
1536
642859008
31887777
1967594368
29592742
*
```

*Vir: <vojkokercan@doubleclick.com.txt>, podatki zbrani iz Internet Explorer brskalnika.*

***Primer 3**: spletni hrošč na strani Quicken.com, ki pošilja podatke o zadetkih na DoubleClick*

```
<img src="http://ad.doubleclick.net/ad/pixel.quicken/NEW" width=1
height=1 border=0>
```

*Vir: Privacy Foundation, 2003.*

***Primer 4**: spletni hrošč v e-sporočilu*

```
<img src=http://www.m0.net/m/logopen 02.asp?vid=3&catid=
370153037&email=SMITHS%40tiac.net width=1 height=1>
```

*Vir: Privacy Foundation, 2003.*

## 3.3. E-profiliranje

E-profiliranje je proces izgradnje podatkovne baze, ki vsebuje aktivnosti in lastnosti e-uporabnikov. V teh podatkovnih bazah se nahaja na milijone spletnih uporabnikov. Uporabnikovi interesi, vzorci brskanja po spletu in nakupna izbira so samo nekateri podatki od mnogih, ki so shranjeni v podatkovnih bazah brez uporabnikove vednosti ali privolitve in se uporabljajo pri postavitvi spletnih pasic in oblikovanju ponudbe in storitev ob obisku spletnih strani. Zbrane informacije so predvsem neosebne, vendar, ko uporabnik spletne strani pusti svoje podatke (ime, naslov, ...), se le-te lahko povežejo z e-naslovom, IP naslovom in demografijo, kar ustvari veliko natančnejši in bolj oseben profil uporabnika (GUIDES E-Business Guidlines on Data Protection Directive 95/94/EC, 2002, str. 6 - 7; Seničar, Jerman-Blažič, Klobučar, 2003, str. 3 - 4).

Organizacije vpletene v e-profiliranje trdijo, da je takšna dejavnost le v dobro kupca oz. potrošnikom, ker s tem vsakemu posamezniku lahko ponujajo storitve in proizvode glede

na njegov profil. Mnogi pa vidijo e-profiliranje kot vdor v zasebnost, ker se uporabnikove informacije zbirajo in širijo brez uporabnikovega vedenja ali zavestne privolitve.

Takšen nadzor nad potrošniki pogosto vključuje tudi izgradnjo t.i. skupnosti potrošnikov s pomočjo raznih kartic zaupanja in klubov zvestobe. S programi zvestobe, kot so igre, ankete, vprašalniki in spletni bilteni, pridobivajo lastniki spletnih mest osebne podatke o svojih obiskovalcih. Kovačič navaja, da je profiliranje do posameznika na videz prijazno, saj potrošnika potiska, kamor si sam želi, oz. ga zalaga z vsebinami po njegovem okusu (Kovačič, 2003, str. 32 - 33). Vendar pa ima tudi ta vrsta nadzora negativne posledice, predvsem na področju diskriminacije potrošnikov. Takšna diskriminacija se lahko dogaja v raznih programih zvestobe, predvsem pri uporabi marketinškega koncepta dinamičnega določanja cen *(dynamic pricing)*[27]. Določanje cen že obstaja v fizičnem svetu, zato ne preseneča napoved, da bo personalizirano določanje cen zagotovo del naravnega razvoja spleta. Znan je primer spletne trgovine Amazon.com iz leta 2000, ko so nekateri uporabniki ugotovili, da za enake DVD izdelke plačujejo več kot drugi, in pojavil se je sum, da je cena odvisna od njihovih potrošniških preferenc. Spletni magazin Computerworld je opravil raziskavo in ugotovil, da so cene odvisne od izbire ponudnika dostopa do interneta, glede na to, ali se uporabnik vrača na isto mesto nakupa *(repeat user)* ali je na mestu nakupa prvikrat *(first-time user)*, in tudi od vrste spletnega brskalnika. Cene so se razlikovale, če je uporabnik uporabljal MS Internet Explorer ali Netscape. Amazon se je izgovoril, da testirajo različne dele spletne strani, navigacijski meni, celotno obliko spletne strani in storitve na prvi strani, kasneje pa je le priznal, da so testirali vpliv cene na nakupne navade potrošnikov. Amazon.com se je na koncu potrošnikom tudi opravičil in jim dal možnost povrnitve preplačane vrednosti, če so uporabniki sumili, da so izdelek preplačali (Rosencrance, 2000; Rosencrance, 2000a; Weiss, 2000; Coursey, 2000). V Sloveniji se je izkazalo, da so nekatere knjige, ki jih prodaja Amazon.com v spletni trgovini dražje od istih knjig v slovenskih knjigarnah.

Drug problem e-profiliranja izhaja iz samih potrošnikov, saj nekateri ne želijo izstopa iz sistema, ki jim na videz prinaša dodatne ugodnosti in popuste. Na nekaterih straneh je izstop potrebno celo plačati[28], v večini primerov pa izstop sploh ni mogoč *(opt-out)*. Kot pravi Kovačič: »Potrošniki in državljani tako živimo v svetu, v katerem se moramo nujno odpovedati delu svoje zasebnosti na račun večje funkcionalnosti in obvladovanja kompleksnosti življenja v sodobni družbi.« (Kovačič, 2003, str. 34).

## 3.4. Vstavljena programska oprema *(Embeded Software, Internet Enabled Software)*

Le v nekaj letih je bilo ustvarjeno nekaj izredno zmogljivih programskih jezikov uporabnih za spletne aplikacije, ki so močno povečali zmogljivost spleta. Mednje štejemo

[27] *Dinamično določanje cen je definirano kot »kupovanje in prodaja blaga in storitev na prostih trgih, kjer so cene odvisne od ponudbe, povpraševanja in spreminjajočih se potrošniških preferenc«.*
[28] *Problem poštnega marketinga. Če ne želimo prejemati reklamne pošte, moramo plačati Pošti Slovenije.*

Javo, JavoScript, XML[29] in Active X[30]. Spletnim strežnikom omogočajo zagon aplikacij na uporabnikovem računalniku in so lahko orodje komercialnemu sektorju, ki z njihovo pomočjo pridobi kontrolo nad uporabnikovim računalnikom in shranjeno vsebino. Večina uporabnikov se ne zaveda nevarnosti, ki jih na področju zasebnosti predstavljajo tako imenovani omrežno zasnovani *(Internet enabled)* programi. Te nevarnosti so vse večje, ker splet postaja čedalje bolj razširjeno multimedijsko komunikacijsko orodje za zabavno industrijo (avdio, video, igre na srečo, igrice, ...) (GUIDES E-Business Guidlines on Data Protection Directive 95/94/EC, 2002, str. 8; Seničar, Jerman-Blažič, Klobučar, 2003, str. 4). Med takšne programe sodijo različice programov RealPlayer in Windows Media Player. Podjetji RealNetworks in Microsoft sta zbirali podatke o tem, kakšne glasbene in video vsebine si ogledujejo potrošniki, nekateri pa so sumili, da se ti podatki povezujejo z elektronskimi naslovi. Seveda sta obe podjetji zanikali vpletenost v takšne aktivnosti. Avtor knjige »Zasebnost na internetu« pa navaja, da je Microsoft v svoj Office paket vgradil t.i. GUID, globalni univerzalni identifikator *(Global Unique Identifier)*, ki se zapiše v vsak MS Office dokument. Če ima uporabnik na svojem računalniku vgrajeno mrežno kartico, serijska številka te kartice postane del GUID, na podlagi česar je mogoče natančno ugotoviti, na katerem računalniku je dokument nastal (Kovačič, 2003, str. 58). Na ta način je FBI leta 1999 izsledil avtorja makrovirusa Melissa, ker je avtor za pisanje virusa uporabil skriptni jezik, ki je del MS Office okolja.

## 3.5. Elektronske sledi pri ponudniku dostopa do interneta

Med gibanjem in brskanjem po spletu puščajo uporabniki veliko elektronskih sledi, največ prav pri svojem ponudniku dostopa do interneta. Ta namreč lahko zapisuje vse dejavnosti uporabnika; kdaj in katere storitve interneta je uporabljal, uporabniško ime (kar je kasneje enostavno povezati z uporabnikovo fizično identiteto, saj imajo ponudniki dostopa do interneta vse fizične podatke o svojih naročnikih), IP številko, telefonsko številko oz. vstopno točko, preko katere se je povezal na internet. Vsi ti podatki se zbirajo v t.i. datotekah aktivnosti ali datotekah dogodkov *(log files)*.

[29] *XML = Exstensible Markup Language; standard za strukturirane dokumente na spletu, razvit znotraj W3C.*

[30] *Active X; Microsoft Active platforma je razvojna platforma, ki omogoča razvijalcem izdelavo zmogljivih aplikacij za internet in intranete. ActiveX je podmnožica Active platforme. Za razvoj tehnologije ne skrbi Microsoft, ampak The Open Group (http://www.opengroup.org/), katere člani so razvijalci programske opreme, ki lahko sodelujejo pri razvoju in razširitvi tehnologije v prihodnosti.*

***Primer 5:*** *datoteka dogodkov na strežniku*

```
webo.vtcif.telstra.com.au - - [03/Jul/2000:16:42:42 +1000]
"GET /ssd/sarb/enrlrecs/index.htm HTTP/1.0" 200 4577
"http://www.monash.edu.au/info/currstudents/admincourse.htm"
"Mozilla/4.0 (compatible; MSIE 4.01; Windows NT; CLS4)"
```

**webo.vtcif.telstra.com.au** – naslov strežnika, ki dostopa do datoteke
**[03/Jul/2000:16:42:42 +1000]** – datum in čas dostopa
**"GET /ssd/sarb/enrlrecs/index.htm HTTP/1.0"** – naslov datoteke
**200** – status zahteve dostopa (200 pomeni OK)
**4577** – velikost datoteke (v zlogih)
**"http://www.monash.edu.au/info/currstudents/admincourse.htm"** – stran pred zahtevkom datoteke
**"Mozilla/4.0 (compatible; MSIE 4.01; Windows NT; CLS4)"** – spletni brskalnik in operacijski sistem

*Vir: Sample Server Log Entry, 2000; A web server log file sample explained, 2000.*

Ponudnik dostopa do interneta lahko beleži, katere spletne strani obiskuje nek uporabnik, in na podlagi tega izdela profiliranje uporabnikov. Ponudniki dostopa do interneta imajo lahko v lasti tudi portale, preko katerih zapisujejo, do katerih vsebin dostopa posamezni uporabnik. Ti lahko ugotovijo, koliko reklam posamezni uporabnik vidi, kako pogosto obišče določene dele spletne strani (predvsem je to pomembno za elektronsko trgovino), katere izdelke je kupil in koliko je zanje plačal. Možno je tudi ugotoviti finančno zmogljivost posameznika glede na opravljene elektronske nakupe.

## 3.6. Povezovanje, zbiranje in prestrezanje podatkov

### 3.6.1. Povezovanje in zbiranje podatkov

Na internetu je dostopno velikansko število podatkov in informacij, in večina jih je nepovezanih, kar pa ne pomeni, da se jih ne da povezovati. Informacije so shranjene v podatkovne baze, ki jih je mogoče povezovati s pomočjo tehnik računalniškega ujemanja in povezovanja zapisov, lahko pa so že v osnovi zasnovane kot relacijske, kar omogoča zelo enostavno povezovanje. Zbiranje in klasifikacija na spletnih straneh objavljenih osebnih podatkov že dolgo nista večja tehnična problema, sta pa izjemno učinkovita in poceni. Tehnologija za zbiranje podatkov objavljenih na spletnih straneh je javno dostopna. Programi se imenujejo roboti, pajki ali črvi *(robot, spider, worm)*. Najpogosteje so namenjeni zbiranju elektronskih naslovov, ki se kasneje uporabljajo pri pošiljanju nezaželene elektronske pošte *(spam)*. Programi iščejo po spletnih straneh, spletnih forumih, novičarskih skupinah in arhivih poštnih seznamov. Roboti so lahko napisani tako, da iščejo samo naslove določene domene z namenom ciljanja posebnih skupin. Takšni primeri so znani predvsem pri vladnih oz. državnih organizacijah, saj se njihovi

elektronski naslovi končajo z vladno domeno (v Sloveniji @gov.si) in jih je tako zelo lahko zbrati v podatkovno bazo in uporabiti v proti-vladne ali druge namene.

Podatke o uporabnikih je možno zbirati na še enostavnejši in učinkovitejši način. Mnoge spletne strani ali storitve na internetu namreč od uporabnikov v zameno za ponujene informacije, nekatere ugodnosti ali uporabo, zahtevajo osebne podatke. Pogosto uporabljajo tudi trik z nagradno igro ali žrebanjem. Na takšnih straneh velikokrat ni razvidno, v kakšne namene se bodo uporabljali takšni podatki. Včasih se podatki kljub zagotovilom uporabijo v drugačne namene, kot naj bi se. Zbiranje podatkov lahko poteka preko registracije različnih programov (Working Party on Information Security and Privacy, 2002, str. 9 - 10; Kovačič, 2003, str. 52).

### 3.6.2. Prestrezanje podatkov in elektronske pošte

Prestrezanje podatkov v računalniških omrežjih je mogoče izpeljati s pomočjo tehnike prestrezanja paketov. S pomočjo te tehnike prisluškovalec prestreza in analizira promet tujih računalnikov oz. TCP/IP paketke, ki se uporabljajo na internetu pri izmenjavi podatkov. Prisluškovalec namreč samo prestreza oz. spremlja promet, zato ga je težko odkriti, hekerji pa pogosto to tehniko uporabljajo za prestrezanje in krajo gesel *(password sniffing)* (Kovačič, 2003, str. 52 - 53).

Prav tako je mogoče prestrezati elektronsko pošto, saj se ta po internetu načeloma prenaša nešifrirano, torej kot navadno besedilo *(plain text)*. Do elektronske pošte uporabnikov imajo načeloma povsem prost dostop upravitelji poštnih strežnikov in upravitelji posredniških poštnih strežnikov *(relay server)*, preko katerih se v internetu sporočilo posreduje od enega poštnega strežnika do drugega. Pri prenosu elektronske pošte velja, da mora biti sporočilo s končnega in posredniškega poštnega strežnika izbrisano takoj, ko je bilo posredovano naprej.

Pomembno je tudi ločevanje med prometnimi podatki, ki so nujni za prenos sporočila in zaračunavanje stroškov, ter osebnimi podatki in vsebino sporočila. Poštni strežnik namreč o sporočilu samodejno zabeleži nekaj tehničnih podatkov, in sicer velikost sporočila, elektronski naslov pošiljatelja in prejemnika, datum in čas pošiljanja sporočila, ter še nekaj tehničnih podatkov o poteku prenosa sporočila *(E-Mail Headers: MIME-Version, User-Agent, Originating-IP, Mailer, ...)*. S posebno programsko opremo oz. posebnimi nastavitvami je mogoče beležiti še veliko drugih podatkov, kot so število in velikost datotečnih prilog *(attached files*), uporabljeni nabor znakov *(Content-Type)*, temo ter vsebino sporočila. Nekateri upravitelji poštnih strežnikov nekatere od teh podatkov napačno obravnavajo kot prometne podatke in jih zato shranjujejo, kar pa ogroža zasebnost uporabnikov elektronske pošte (Kovačič, 2003, str. 54).

***Primer 6:*** *ovojnice e-sporočila*

```
Subject: email headers
From: peter.kralj@dhimahi.com
Date: 9.10.2003 2:45
To: vojko.kercan@dhimahi.com
Cc: vojkokercan@yahoo.com
Return-Path: <peter.kralj@dhimahi.com>
Received: from kurircek.acmolotov.org
(postfix@tm.213.143.79.69.dc.telemach.net [213.143.79.69]) by
phobos.webteh.com (8.12.9/8.12.9) with ESMTP id h990j4SN016115 for
<vojko.kercan@dhimahi.com>; Thu, 9 Oct 2003 02:45:04 +0200
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.4)
Gecko/20030714 Debian/1.4-2
X-Accept-Language: en
MIME-Version: 1.0
Content-Type: text/plain; charset=ISO-8859-2; format=flowed
Content-Transfer-Encoding: 8bit
X-MIME-Autoconverted: from quoted-printable to 8bit by
phobos.webteh.com id h990j4SN016115
```

*Vir: Podatki zbrani iz Netscape Mail odjemalca za elektronsko pošto, 2003.*

# 4. *Tehnologije za boljšo zaščito zasebnosti (Privacy Enhancing Technologies - PETs)*

***"There are virtually no online activities or services that guarantee absolute privacy."***
**(Pravzaprav ne obstaja nobena on line aktivnost, ki bi omogočila popolno zasebnost.)**

**Privacy Rights Clearinghouse, neprofitna, izobraževalna in raziskovalna organizacija, na področju varstva osebnih pravic**

V zadnjih desetletjih je nastalo veliko zakonov in predpisov z namenom zaščite zasebnosti posameznika v elektronskih komunikacijah, vendar se je ta kljub temu zmanjšala. Lahko trdimo, da je s pojavom novih tehnologij in zaradi dogodkov, kot je 11. september, zasebnost posameznika ogrožena bolj kot kadar koli prej. Ker je smoter zakonodaj in predpisov z omejevanjem določenih praks zmanjšanje priložnosti za kršenje zasebnosti, je njihova idealna situacija orisana tako, da je posameznikova zaščita zasebnosti nekaj samoumevnega in da se vsako kršenje zasebnosti lahko razreši znotraj zakonodaje. Ravno takšna (ne)idealna situacija in njena nerealnost, še posebej v okolju elektronskih komunikacij, je podlaga za nastanek in razvoj nove zaščite zasebnosti. Bolj kot to, da je zaščita zasebnosti nekaj samoumevnega, je samoumeven nadzor, poskusi vdora v zasebnost pa so redni in rutinski. V času, ko so uporabniki čedalje bolj zaskrbljeni nad dejstvom, da se rutinsko shranjuje ogromna količina zasebnih podatkov v podatkovne baze, nad katerimi nimajo nikakršne kontrole, nove tehnologije omogočajo organizacijam in korporacijam vse lažje shranjevanje podatkov. Z minimalizacijo shranjenih podatkov bi se zaščita lahko drastično povečala, vendar bi se še vedno shranjevala neka določena količina informacij.

Kot odgovor na neuspelo zakonodajo in razvoj tehnologij se je v zadnjih letih pojavil nov pristop k zaščiti zasebnosti. Nova vrsta tehnologij, tako imenovane tehnologije za boljšo zaščito zasebnosti (*Privacy Enhancing Technologies - PETs*), je bila ustvarjena z namenom povečevanja posameznikovega nadzora nad podatki, ki jih želi razkriti v elektronskih transakcijah. Njihov namen je izenačiti moč med posameznikom in celotno elektronsko skupnostjo, ki želi zbrati čim več osebnih podatkov. Njihov končni cilj je ustvariti informacijsko samo-odločanje. Tehnologije za boljšo zaščito zasebnosti predstavljajo velik korak k zaščiti zasebnosti posameznika.

Fischer-Hübner navaja štiri osnovne principe delovanja tehnologij za boljšo zaščito zasebnosti (Fischer-Hübner, 2001, str. 21-24):

1. Anonimnost *(Anonymity);* možnost uporabe spletnih storitev in virov, pošiljanje in sprejemanje elektronskih sporočil brez razkritja svoje identitete.

2. Psevdonimnost *(Pseudonymity);* možnost, da uporabnik pod psevdonimom uporablja spletne storitve in vire, pošilja in sprejema elektronska sporočila brez razkritja svoje identitete.
3. Nepovezljivost *(Unlinkability);* možnost uporabe spletnih storitev in virov, ne da bi tretje stranke imele možnost povezovanja uporabnikovih dejanj, ter možnost, da pošiljatelj in prejemnik elektronskih sporočil ne moreta biti identificirana kot neposredna komunikatorja.
4. Neopazovanost *(Unobservability);* možnost uporabe spletnih storitev in virov brez nadzora tretje stranke.

Avtor poročila *»The Voiding of Privacy«*[31] tehnologije za boljšo zaščito zasebnosti klasificira v tri kategorije (Stalder, 2003, str. 8-9):
1. zaščita s proxy strežnikom *(privacy trough proxy),*
2. zaščita z zavestno privolitvijo *(privacy trough informed consent),*
3. zaščita z neizsledljivostjo *(privacy trough untracebility)*.

Poročilo OECD *»Inventory of Privacy Enhancing Technologies«* navaja naslednjo klasifikacijo tehnologij za boljšo zaščito zasebnosti (Working Party on Information Security and Privacy, 2002, str. 17-24):
1. tehnologije zaščite zasebnosti na osebni ravni *(Personal Privacy Enhancing Technologies),*
2. spletne tehnologije zaščite zasebnosti *(Web Based Technologies),*
3. informacijski posredniki *(Information Bokers),*
4. mrežne tehnologije zaščite zasebnosti *(Network Based Technologies).*

Vse tehnologije in vsi principi zaščite zasebnosti se med seboj prepletajo in izredno težko je določiti in kategorizirati določeno skupino tehnologij. Zato v tem delu predlagam oseben pogled na problem in s tem v zvezi novo razdelitev, ki je le nekoliko drugačna kot zgoraj naštete:

1. Tehnologije zaščite na osebni ravni; zaščita uporabnika je odvisna predvsem od njegove angažiranosti. Katere rešitve bo uporabljal in kako pogosto so ključni pojmi uporabnikove zasebnosti. Povedano z drugimi besedami, če se bo uporabnik odločil za zaščito, bo moral zanjo tudi poskrbeti. V to kategorijo zaščite sodijo tehnologije šifriranja in upravniki piškotkov.

2. Tehnologije zaščite identitete; čeprav sistem zaščite identitete prav tako zahteva uporabnikovo angažiranost, pa zaščita njegove zasebnosti ni odvisna samo od lastne vpletenosti v sistem. Zaščita je odvisna od celotnega sistema in od vseh vpletenih v sistem zaščite zasebnosti, kot so ponudniki internetnih storitev, ponudniki dostopa do interneta, strežniški administratorji, izdelovalci spletnih mest in sistemov, ponudniki sistemov zaščite zasebnosti itn. Če smo zgornje tehnologije poimenovali glede na njihovo delovanje na

[31] *Dr. Felix Stalder, avtor poročila »The Voiding of Privacy«, ki je izšlo v »Sociological Research Online« avgusta 2002.*

osebni ravni, bi lahko tehnologije zaščite identitete razvrstili tudi kot tehnologije na sistemski ravni, med katere sodijo zaupni centri, anonimni proxy in psevdonimni strežniki, ponovni pošiljatelji in slepi digitalni podpisi.

3. Tehnologije zaščite z neizsledljivostjo; ključni pojem pri takšnem principu zaščite je skrivanje akcij enega v akcijah mnogih. Akcije uporabnika so nepovezljive z njegovo identiteto in je torej neizsledljiv. Med takšne tehnologije sodijo Freenet, GNUnet in sistem Crowds.

4. Tehnologije zaščite s privolitvijo; tehnologija, ki spada v to kategorijo, je trenutno le P3P *(Platform for Privacy Preferences)*. Njena specifika je v tem, da je dejansko odvisna od samih izdelovalcev spletnih mest in sistemov. Če ti vključijo standard za pisanje politik zasebnosti *(privacy policy),* so uporabniki pred vsakim obiskom spletnega mesta obveščeni o politiki zbiranja osebnih podatkov in tako lahko sami odločajo, ali želijo spletno mesto obiskati ali ne. Dejansko bi to tehnologijo lahko imenovali tudi tehnologija obveščanja, saj uporabniku ponuja le informacije (v kolikor uporablja brskalnike, ki podpirajo P3P *(P3P enabled browser)* ali dodatne programe za branje P3P XML dokumenta) in ne anonimne in psevdonimne storitve.

Kriterij, po katerem sem to razdelitev opravil, je predvsem odvisna od uporabnika do celotnega sistema. Trditev, da je vsak dogodek na spletu dejansko odvisen od celotnega sistema, je vsekakor resnična, a vendar obstajajo sistemi, ki so bolj ali manj odvisni od celotne arhitekture spleta. Na primer, tehnologije zaščite na osebni ravni so odvisne le od proizvajalcev programske opreme. Na kakšen način in kako pogosto bodo te uporabljene, pa je prepuščeno slehernemu posamezniku. V nasprotnem primeru, ko uporabnik uporablja tehnologije zaščite identitete, so njegovi zaupni podatki prepuščeni tretjim strankam (primer zaupnih centrov), kar pa zopet predstavlja popolnoma drugo plat v vprašanju zaščite zasebnosti, saj so lahko centri, ki shranjujejo ogromno količino zasebnih podatkov, tarča različnih napadov. In kot navaja avtor članka »Why worry about Web bugs? Here is the real privacy threat.« David Coursey, resnična nevarnost zasebnosti ne izhaja iz tehnologij nadzorovanja, temveč iz ponudnikov zaščite zasebnosti. Microsoft Passport na primer shranjuje ogromne količine informacij kreditnih kartic in nakupnih navad posameznikov in tako dejansko predstavlja vir tisočih informacij (MS Passport ima 200 mio uporabnikov) o uporabnikih spletnih storitev (Coursey, 2001). Je Microsoft res tako varen, da bi mu prepustili svoje PIN številke bančnih kartic? Mislim, da je bil odgovor prikazan maja 2003, ko je bila ugotovljena sistemska napaka na MS Passport storitvi, saj je lahko napadalec zamenjal geslo uporabnika določene spletne strani in tako pridobil dostop do njegovih informacij kreditnih kartic in drugih osebnih podatkov (Stevenson, 2003).

## 4.1. Tehnologije zaščite na osebni ravni

### 4.1.1. Šifriranje in stenografija

Eden od najstarejših mehanizmov za zagotavljanje varstva podatkov je šifriranje. Šifriranje je transformacija podatkov v nečitljivo obliko. Njen namen je zagotavljanje zasebnosti podatkov s tem, da jih skrije pred vsemi tistimi, ki jim podatki niso namenjeni. Obratni proces šifriranja je dešifriranje, kar pomeni pretvorba podatkov v čitljivo oz. uporabno obliko. Sistem deluje tako, da poslano sporočilo zakrijemo z šifrirno metodo in šifrirnim ključem in tako dobimo kriptogram, ki ga lahko pošljemo naslovniku. Naslovnik nato s pomočjo dekripcijske metode in dekripcijskega ključa predela sporočilo v izvorno obliko. Z vidika šifrirnega in dešifrirnega ključa poznamo dve vrsti kriptografije: simetrično ali konvencionalno, ki za kodiranje in dekodiranje sporočila uporablja isti ključ (isto geslo - glavni problem: kako prenesti ključ do prejemnika, ne da bi ga tretja stranka prestregla), ter nesimetrično ali šifriranje z javnim ključem, kjer je ključ za kodiranje različen od ključa za dekodiranje (An Introduction to Cryptography, 2003, str. 11-13).

Leta 1978 so na Massachusetts Institute of Technology razvili kodirani algoritem RSA[32], ki omogoča praktično nezlomljivo kriptografijo. Metoda RSA deluje tako, da imata tako tisti, ki sporočilo pošilja, kot tisti, ki sporočilo sprejema, vsak svoj par ključev. Zasebnega, ki je tajen, in javnega, ki je javno dostopen. Ključa sta med seboj povezana v posebnem matematičnem razmerju, ki omogoča, da oseba, ki sporočilo pošilja, le-to zakodira s svojim tajnim in naslovnikovim javnim ključem[33]. Tako zakodirano sporočilo pa lahko odkodira samo naslovnik, in sicer s svojim zasebnim in pošiljateljevim javnim ključem (Kovačič, 2003, str. 65). Za pošiljanje kodiranega sporočila torej potrebujemo samo naslovnikov javni ključ (svoj zasebni ključ že imamo), naslovnik pa potrebuje samo pošiljateljev javni ključ (svojega zasebnega že ima). Tak sistem kodiranja omogoča tudi verifikacijo pošiljatelja oz. tako imenovani elektronski podpis.

Leta 1991 je Phil Zimmerman[34] napisal program PGP *(Pretty Good Privacy)*, ki vsebuje RSA algoritem za kodiranje sporočil na osebnih računalnikih, in tako uporabnikom programa omogočil nenadzorovano elektronsko komuniciranje. Zimmerman je svoj program javno objavil in dovolil brezplačno kopiranje (freeware program - zadnja

---

*[32] RSA algoritem je dobil ime po ustvarjalcih: Ron Rivest, Adi Shamir in Leonard Adleman (An Introduction to Cryptography, 2003, str. 13).*

*[33] Javni ključi se nahajajo na strežniku, in ko želimo poslati šifrirano sporočilo, lahko na spletni strani najdemo naslovnikov javni ključ. Javni PGP ključi so na naslovu http://www.keyserver.net/en/ (OpenPGP Public Key Server) ali http://pgp.mit.edu/ (MIT PGP Public Key Server).*

*[34] Phill R. Zimmerman; leta 1991 se je program PGP razširil po celem svetu kot freeware, kar pa so ZDA smatrale za ogrožanje nacionalne varnosti. Leta 1996 je bila triletna preiskava zoper Zimmermana ukinjena, in sicer brez obtožb, saj proti osumljencu niso našli dokazov za kaznivo dejanje (Zimmerman, 2003).*

različica za Windows in Mac okolje 8.0.2). Dve leti kasneje so na njegova vrata potrkali agenti FBI zaradi suma, da je omogočil nezakoniti izvoz vojaške tehnologije (An Introduction to Cryptography, 2003, str. 34-36; Testimony of Philip R. Zimmermann to the Subcommittee on Science, Technology, and Space of the US Senate Committee on Commerce, Science, and Transportation, 1996).

Ponavadi pa samo šifriranje ni dovolj, saj uporabnik želi skriti tudi samo dejstvo, da so podatki šifrirani. To lahko stori s pomočjo stenografije; umetnosti skrivanja znakov znotraj samih znakov, kar pomeni, da so občutljive informacije shranjene znotraj popolnoma nedolžne datoteke. Tehnologija stenografije omogoča, da so občutljive informacije popolnoma nevidne znotraj datoteke, medtem ko prejemnik lahko odkrije skrite informacije. S tem načinom uporabniki ne skrijejo samo svojih podatkov, ampak tudi dejstvo, da so bili kakršni koli občutljivi podatki sploh poslani (Seničar, Jerman-Blažič, Klobučar, 2003, str. 5). Stenografija vključuje vrsto različnih tehnik in mehanizmov za skrivanje podatkov na različnih medijih, kot je skrivanje podatkov znotraj teksta in skrivanje podatkov v slikah in avdio zapisih (Michaud, 2003, str. 2-6).

#### 4.1.1.1. Crypto-Heaven

Crypto-Heaven je uporabniku prijazen sistem, kjer tretje stranke, kot so strežniški administratorji, vladne agencije in ostali, nimajo dostopa do poslanih informacij. Informacija je šifrirana in shranjena na Crypto-Heaven strežniku in ključ do informacije imata samo pošiljatelj in prejemnik. Vse rešitve, ki jih ponuja sistem Crypto-Heaven (varno shranjevane dokumentov, varno razpošiljanje dokumentov, varni forumi in varna e-pošta), so šifrirane z najnovejšo tehnologijo nesimetrične kriptografije (Crypto-Heaven Security, 2003).

Ko je ustvarjen nov uporabniški račun, uporabnik ustvari svoj javni in zasebni ključ. Javni ključ je nato poslan na strežnik, kjer je dosegljiv vsem vključenim v omrežje, zasebni ključ pa je šifriran z geslom in shranjen na uporabnikovem osebnem računalniku ali pa celo na strežniku. Če je uporabnikov zasebni ključ shranjen na strežniku, lahko s pomočjo interneta dostopa do svojega računa kjer koli na svetu in uporablja varne storitve sistema. Varna komunikacija se prične tako, da strežnik pošlje uporabniku naključno zgeneriran (*one-time-short-term)* sejni *(session)* ključ, šifriran z uporabnikovim javnim ključem. Uporabnik nato uporabi svoj zasebni ključ, da dekriptira sejni *(session)* ključ s svojim geslom. Od tega trenutka dalje je vse, kar poteka po komunikacijskem kanalu med odjemalcem in strežnikom, šifrirano s tem ključem (SSL[35] komunikacija s šifriranjem). Takšen komunikacijski protokol zagotavlja zaupnost informacij, varuje pred izpuščanjem

[35] *SSL = Secure Sockets Layer; sloj varnega žepka je protokol, ki omogoča šifrirano povezavo med strežnikom in odjemalcem. Netscape ga je predstavil leta 1994.*

paketov (*packet dropping)*[36], preureditvijo vrstnega reda paketov *(reordering)*[37] ali kakršno koli drugo manipulacijo (Crypto-Heaven Security, 2003).

Druga plast varnostnega sistema Crypto-Heaven je tako imenovana tehnologija transparentnega šifriranja *(Transperent Encryption Technology - TTE)*, ki predstavlja podatkovno šifrirno plast *(Data encryption layer)*. Aplikacija, ki uporablja tehnologijo TTE, izvede šifriranje samodejno in tako zagotavlja varno komunikacijo med uporabnikom in prejemnikom, saj so podatki šifrirani že na uporabnikovi strani. Če uporabnik pošilja elektronsko pošto, dokumente ali uporablja spletne klepetalnice *(on-line chat)*, dodatni koraki za varno pošiljanje informacij niso potrebni. Tudi če pride do prestrezanja podatkov med komunikacijo, so informacije že šifrirane s prejemnikovim javnim ključem (Crypto-Heaven Security, 2003).

Naslednja pomembna prednost sistema je v šifrirnem centru Crypto-Heaven *(Crypto-Heaven Data Center)*. Sistem omogoča shranjevanje informacij na Crypto-Heaven strežnikih, ki hrani le šifrirane podatke, kar pomeni, da jih lahko dekriptira le prejemnik s svojim zasebnim ključem. Crypto-Heaven strežnik ni končni prejemnik šifriranih podatkov, ampak samo center shranjenih podatkov oz. kurir, ki nato podatke razpošlje končnim prejemnikom. Varnost podatkov je tako bistveno povečana, saj jih tudi Crypto-Heaven ne more dekriptirati (Crypto-Heaven Security, 2003).

Podjetje Crypto-Heaven je tako prepričano v svojo tehnologijo, da je na svojih spletnih straneh 19. novembra 2001 objavilo izziv *(CryptoChallenge #1)*, kar bolj natančno pomeni nagrado v vrednosti 10.000 USD tistemu, ki lahko razbije šifrirano informacijo (Crypto-Heaven Challenge, 2002). Crypto-Heaven je tedensko beležil povprečno 1000 kopiranj izvorne kode šifrirane datoteke, a vendar je bilo 31. maja 2002, ko se je izziv končal, 10.000 USD še zmeraj v podjetju.

#### 4.1.1.2. PGP *(Pretty Good Privacy)*

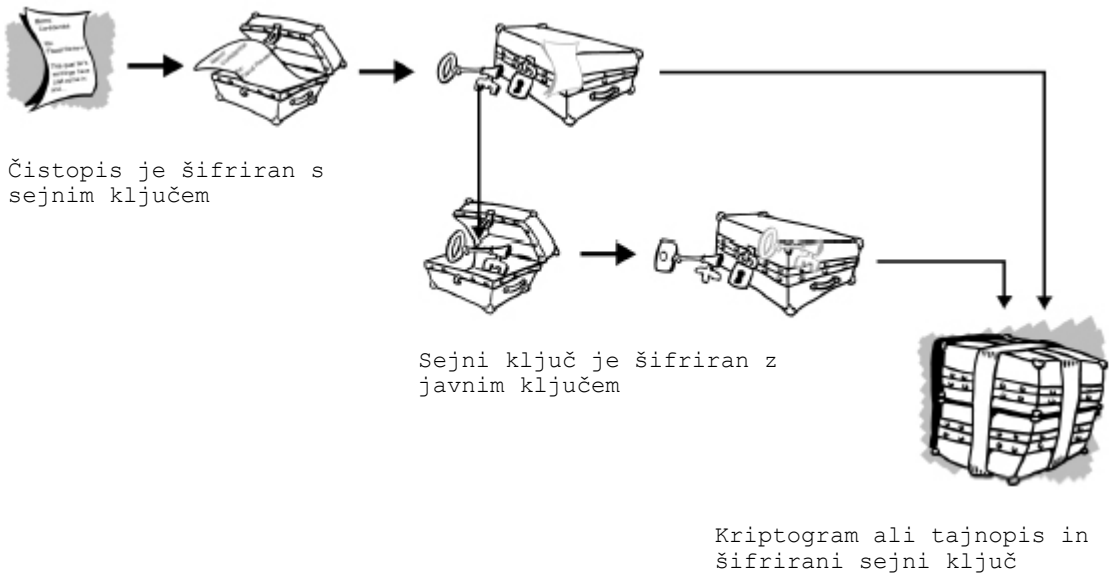
PGP je hibriden kriptosistem, ki združuje tako simetrično kriptografijo kot kriptografijo javnih ključev. Ko uporabnik šifrira navaden tekst oz. čistopis *(plain text)* s PGP sistemom, ta najprej kompresira navaden tekst. Kompresija podatkov prihrani čas pri prenosu in prostor na disku in najpomembnejše, poveča moč kriptografije. PGP nato ustvari enkraten *(one-time only)* sejni *(session)* ključ, ki je naključna številka zgenerirana s premiki miške na zaslonu in črkami vtipkanimi na tipkovnici. Sejni *(session)* ključ je nato uporabljen z varnim in hitrim konvencionalnim šifrirnim algoritmom ob šifriranju navadnega teksta, in nastane kriptogram ali tajnopis *(ciphertext)*. Ko so enkrat podatki

[36] *Packet dropping; ko napadalec enostavno zbriše vse ali samo del poslanih paketov. Največji problem packet dropping napadov je v tem, da niti pošiljatelj niti prejemnik ne vesta, zakaj in kje so bili paketki spuščeni. Napadi vplivajo na daljši časovni prenos, daljši odzivni čas, kvaliteto in pasovno širino.*

[37] *Reordering; ko TCP paketi, ki so bili poslani po določenem zaporedju in času, prispejo do končnega odjemalca v drugem vrstnem redu ali pa sploh ne prispejo.*

šifrirani, se sejni *(session)* ključ šifrira k prejemnikovemu javnemu ključu. Ta javni ključ, šifriran s sejnim *(session)* ključem, je nato s kriptogramom poslan prejemniku (An Introduction to Cryptography, 2003, str. 13-15).

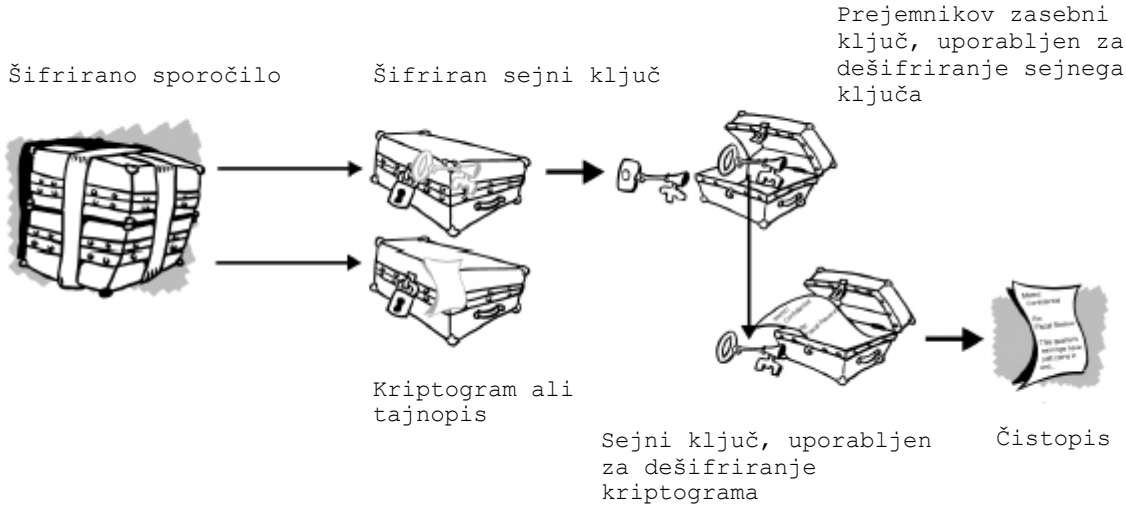
***Slika 1:*** *Grafičen prikaz šifriranja s programom PGP*




*Vir: An Introduction to Cryptography, 2003, str. 14.*

Dešifriranje deluje v nasprotno smer. Prejemnikova različica programa PGP uporabi zasebni ključ prejemnika, da pridobi sejni *(session)* ključ, ki ga nato PGP uporabi za dešifriranje originalnega sporočila.

***Slika 2:*** *Grafičen prikaz dešifriranja s programom PGP*




*Vir: An Introduction to Cryptography, 2003, str. 14.*

Kombinacija teh dveh šifrirnih metod združuje pripravnost šifriranja z javnim ključem s hitrostjo simetrične kriptografije. Simetrična kriptografija je 10.000-krat hitrejša od šifriranja z javnim ključem, ta pa rešuje problem razpošiljanja ključev. V skupni uporabi sta učinkovitost in razpošiljanje ključev izboljšana brez žrtvovanja varnosti (An Introduction to Cryptography, 2003, str. 15).

### 4.1.2. Upravitelj elektronskih piškotkov *(Cookie management, Cookie Viewer)*

Elektronski piškotki so majhni paketi podatkov, ki jih spletni strežnik pošlje spletnemu brskalniku, le-ta pa jih shrani na uporabnikov računalnik in vrne strežniku ob prihodnjem zahtevku. Elektronski piškotek navadno vsebuje interno identifikacijsko številko, s pomočjo katere lahko spletni strežnik ob naslednjem obisku uporabnika ugotovi, ali je uporabnik spletno stran že obiskal in kakšne so bile njegove aktivnosti. Čeprav so bili elektronski piškotki prvotno namenjeni sledenju uporabnika samo znotraj ene spletne strani, se danes piškotki uporabljajo tudi za sledenje uporabnikov po celotnem omrežju spletnih strani, z njihovo uporabo pa je možno pridobiti celo resnično identiteto uporabnika in povezljivost z njegovimi brskalnimi navadami.

Podjetji, kot sta DoubleClick ali Httpool, preprodajata oglasni prostor spletnih strani, ki so v oglaševalskem omrežju. Ko uporabnik obišče npr. neko erotično spletno stran, oglas, ki se prikaže na spletni strani, prihaja iz DoubleClick-ovega strežnika, DoubleClick hkrati z oglasom pošlje tudi elektronski piškotek, ki se shrani na uporabnikov računalnik. Na ta način si strežnik DoubleClick zapomni, da je uporabnik z interno identifikacijsko številko, ki je zapisana v elektronskem piškotku, obiskal določeno erotično spletno stran. Ko ta uporabnik čez nekaj časa obišče npr. spletno prodajalno knjig, DoubleClick preko oglasa na tej spletni strani ugotovi, da je uporabnik pred tem obiskal erotično spletno stran, in pošlje oglas z erotično vsebino (Kovačič, 2000, str. 31). Ker je DoubleClick prisoten na mnogih spletnih mestih, lahko sledi uporabnikovemu gibanju po svetovnem spletu in shranjuje njegove brskalne navade. Na podlagi pridobljenih informacij kasneje postavlja primerne oglasne pasice in prireja vsebino in ponudbo spletnih storitev. Če pa uporabnik na kateri izmed spletnih strani, kjer je tudi prisoten DoubleClick, pusti svoj elektronski naslov ali druge podatke, lahko DoubleClick poveže uporabnikove podatke z njegovimi brskalnimi navadami ali pa celo z dejansko identiteto.

Eden od možnih načinov preprečevanja sledenja s piškotki, ki jih prakticira DoubleClick in mnoga druga spletna mesta, je z upraviteljem elektronskih piškotkov *(Cookie Management)*, ki onemogoči HTTP elektronske piškotke. Elektronski piškotki so ena od najbolj zaskrbljujočih tehnologij, kar se tiče zaščite zasebnosti na spletu, in ravno zato je vrsta organizacij (komercialnih in javnih) izdelala orodja za upravljanje elektronskih piškotkov, ki omogočajo (Seničar, Jerman-Blažič, Klobučar, 2003; str. 7, Working Party on Information Security and Privacy, 2002, str. 17):

1. rutinsko brisanje piškotkov iz trdega diska,

2. onemogočanje elektronskih piškotkov - preprečevanje shranjevanja elektronskih piškotkov na uporabnikov računalnik,
3. selektivno sprejemanje elektronskih piškotkov - omogoča uporabniku izbiro sprejemanja ali zavračanja piškotkov,
4. pregled datotek elektronskih piškotkov - omogoča uporabniku pregled nad shranjenimi piškotki ter shranjeno vsebino,
5. pregled spletnih strani, ki so postavile piškotke in
6. pregled časa trajanja posameznih piškotkov.

Upravniki elektronskih piškotkov tako omogočajo večjo kontrolo posameznika nad elektronskimi piškotki. Pomembno je tudi, da vsi komercialni spletni brskalniki omogočajo kontrolo nad piškotki, ki jih lahko uporabnik pregleda, saj so piškotki le preproste tekstovne datoteke, shranjene na trdem disku (Working Party on Information Security and Privacy, 2002, str. 17 - 18).

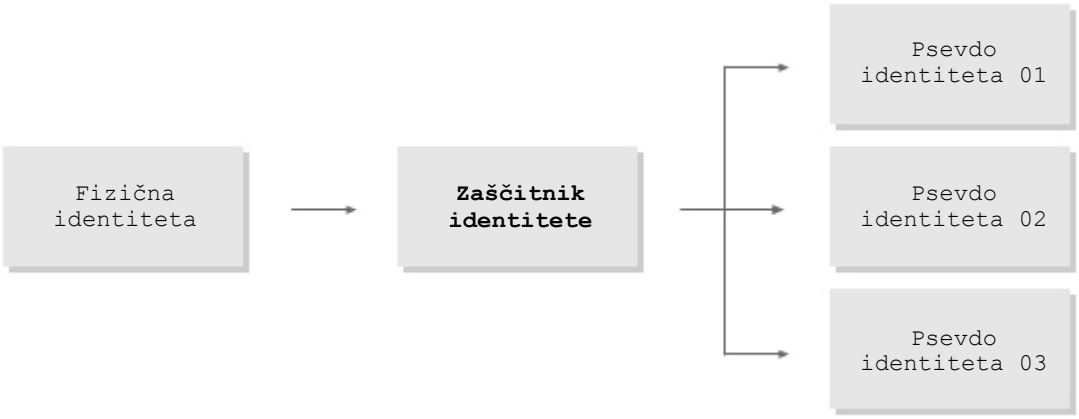
## 4.2. Tehnologije zaščite identitete *(The Identity Protector)*

Zaščitnik identitete je del sistema, ki kontrolira razkrivanje posameznikove identitete znotraj informacijskega okolja. Njegov namen je zaščititi identiteto uporabnika pred sistemom, ki ne potrebuje resničnih podatkov. Najpomembnejša funkcija zaščitnika identitete je sprememba uporabnikove resnične identitete v psevdo-identiteto (digitalna identiteta, ki se pripiše uporabniku v času, ko ta uporablja sistem zaščite identitete), ki izvaja naslednje funkcije (Fischer-Hübner, 2001, str. 33):

1. generira psevdo identitete,
2. pretvarja psevdo identitete v dejanske identitete in obratno,
3. spreminja psevdo identitete v druge psevdo identitete,
4. poroča in kontrolira primere, ko je identiteta razkrita,
5. bojuje se proti prevari in zlorabi sistema.

Ko je zaščitnik identitete vključen v informacijski sistem, sta ustvarjeni dve področji: področje dejanske identitete in področje psevdo identitete. Zaščitnik identitete je uporabljen kjer koli v sistemu, kjer se zbirajo osebni podatki, in pri tem loči dejansko in psevdo identiteto. Ker je zaščitnik identitete pod kontrolo uporabnika, lahko ta določi vrsto funkcij, kot je razkrivanje uporabnikove dejanske identitete nekaterim storitvenim ponudnikom in drugim ne. Na ta način lahko uporabnik uporablja storitve ali izvaja transakcije anonimno, storitveni ponudniki pa ne shranjujejo osebnih podatkov in spletnih navad (profil brskanja po spletu, nabor kupljenih stvari, ...) uporabnikov pod njihovimi dejanskimi identitetami, temveč pod psevdo identitetami. Ker je zaščitnik identitete nekakšen vmesni člen oz. posrednik med uporabnikom in ponudnikom storitev, mu morata zaupati obe stranki, saj mora imeti storitveni ponudnik kontrolo nad avtoriziranimi dejanji uporabnika. Zaščitnik identitete tako omogoča ponudnikom storitev preverjanje uporabnikove identitete in pravice brez razkritja njegove dejanske identitete (Seničar, Jerman-Blažič, Klobučar, 2003, str. 6 - 7).

***Slika 3:*** *Zaščitnik identitete*




*Vir: Fischer-Hübner, 2001, str. 33.*

Zaščitnik identitete je lahko integriran v informacijski sistem kot zaupni center, anonimni proxy strežnik, anonimni / psevdonimni strežniki, ponovni pošiljatelj ali slepi digitalni podpis.

### 4.2.1. Zaupni centri *(Trust Centres, Trusted Third Party)* ali anonimni proxy strežniki *(Anonymus Proxies)*

Zaupni center je samostojna tretja stranka, ki ji zaupajo tako uporabniki kot ponudniki storitev. Glavna naloga zaupnega centra je izdaja digitalnega ključa in pripis psevdonima posameznemu uporabniku. Uporabnik lahko nato opravlja spletne transakcije pod psevdonimom in med tem ne razkrije svoje identitete. Ker zaupnemu centru zaupata tako uporabnik kot ponudnik spletnih storitev, je njun odnos nemoten in lahko transakcije tečejo popolnoma enako, kot če bi uporabnik uporabljal svojo fizično identiteto. Način, na katerega zaupni centri delujejo, je lahko primerljiv z notarjevim, saj je ta nevtralen oz. je nevpletena stranka (Macaulay, 2002, str. 6 - 7; Seničar, Jerman-Blažič, Klobučar, 2003, str. 5 - 6). Trenutno obstajata dva osnovna modela zaupnega centra, in sicer komercialni ali javni zaupni center *(Trusted Third Parties; TTPs)* in privatni center, imenovan *Personal Trust Center (PTC)*, ki je pod kontrolo uporabnikov (Seničar, Jerman-Blažič, Klobučar, 2003, str. 5-6). Ne glede na to, kakšen model zaupnega centra je v uporabi, mora ta zadovoljiti pričakovanja in želje vseh vpletenih strank, tako uporabnikov kot poslovnih partnerjev, operaterjev informacijsko komunikacijskega sistema in ponudnikov spletnih storitev. Nevtralnost in samostojnost zaupnega centra ne smeta biti v nikakršni meri ogroženi zaradi nasprotja interesov.

Princip delovanja zaupnega centra oz. anonimnega proxy strežnika je zelo enostaven. Računi so odprti pri centru, ki mu zaupajo tako ponudniki kot uporabniki. Uporabnik lahko pri odprtju računa zlahka pusti vse svoje osebne podatke, saj ima zagotovilo, da ponudnik anonimnega proxy strežnika ne bo posredoval njegovih podatkov drugim komercialnim podjetjem ali jih kakor koli zlorabil za marketinške namene. Ustvarjeni so

lahko številni psevdonimi ali aliasi, ki jih uporabnik uporablja pri brskanju po spletu in pri izvajanju določenih transakcij. Za uporabnika je najbolj pomembno dejstvo, da bo njegova identiteta ostala zaščitena v času izvedbe transakcije pod psevdonimom. Če bo njegova identiteta zakonito razkrita, uporabnik zaupa zaupnemu centru, da ga bo nemudoma obvestil, komu je bila razkrita in v kakšne namene. Operater informacijsko-komunikacijskega sistema in ponudnik spletnih storitev zaupata zaupnemu centru, da jima bo, če bi bilo to potrebno, razkril identiteto uporabnika, da bi lahko zaščitila svoje pravice in interese. Pogoji, pod katerimi bo razkrita uporabnikova identiteta, morajo biti znani uporabniku in ponudniku pred podpisom dogovora z zaupnim centrom.

### 4.2.2. Anonimni / psevdonimni strežniki

Anonimni / psevdonimni strežniki omogočajo uporabnikom vzpostavitev anonimnih elektronskih poštnih predalov, ki jim je dodeljena edinstvena ID številka tako, da lahko prejemnik anonimnega sporočila odgovori na prejeto sporočilo. Poleg anonimnih elektronskih poštnih predalov anonimni / psevdonimni strežniki omogočajo vzpostavitev novičarskih skupin *(newsgroups)* ter račune za aktivnosti vezane na brskanje po spletu (Macaulay, 2002, str. 9).

Primer zaščite z anonimnim / psevdonimnim strežnikom je programska rešitev Freedom podjetja Zeroknowledge iz Montreala. Freedom je tehnologija, ki omogoča uporabniku interneta ustvariti do pet različnih psevdonimov, ki jih lahko uporablja pri brskanju po spletu ali pošiljanju e-sporočil. Pravi napredek pred ostalimi konkurenti je podjetje Zeroknowledge naredilo v tem, da še sami niso mogli povezati psevdonima s stvarno identiteto uporabnika in tako ustvarili najbolj prefinjen izdelek na tržišču. Freedom je prišel na tržišče leta 1999 in skupnost za zaščito zasebnosti je bila navdušena nad tehnologijo izdelka. Podjetje Zeroknowledge so poimenovali »Mercedes-Benz med podjetji anonimnih tehnologij«. V času internetnega buma je bilo podjetje Zeroknowledge v poletu in je celo tiskalo majice z napisom *»Internet Freedom Fighter«* in *»Privacy is Sacred«*. Kljub velikim uspehom pa podjetje ni preživelo padca dot.com industrije in je oktobra 2001 ukinilo svojo storitev. Čeprav številke niso bile objavljene, je bilo očitno, da je novo poslovno okolje in majhno število naročnikov onemogočilo komercialno delovanje storitve anonimnega strežnika (Seničar, Jerman-Blažič, Klobučar, 2003, str. 8; Stalder, 2002, str. 10 - 11).

Leta 2000 je na tržišče s podobnim proizvodom vstopilo podjetje Safeweb.com. Safeweb je ustvarilo spletni proxy strežnik, skozi katerega so lahko uporabniki dostopali do spletnih storitev, ne da bi v procesu razkrili svojo identiteto. V nasprotju s proizvodom podjetja Zeroknowledge sistem ni bil tako dodelan in je omogočal povezavo med psevdonimom in dejansko identiteto uporabnika. A vendar se je Safeweb osredotočil na enostavno uporabo in ustvaril enostaven grafičen vmesnik, ki ga je lahko uporabljal in konfiguriral povprečen uporabnik brez tehničnega znanja (Stalder, 2002, str. 11).

Z ekonomskega vidika je največja slabost takšnega modela zaščite usmerjanje uporabnikov skozi centralno središče (proxy strežnik), kar predstavlja problem ozkega grla, saj centralni proxy strežnik potrebuje veliko računalniške moči in pasovne širine *(bandwidth)*, pri čemer sta oba zelo draga. Bolj ko je storitev popularna oz. čim več ljudi uporablja storitev, težje in dražje je za lastnike vzdrževanje. Ravno ta problem povzroča, da so ponudniki takšnih storitev odvisni od predplačniškega sistema, kar pa ni preveč dobičkonosno, saj je malo uporabnikov, ki bi plačali za zaščito zasebnosti na spletu. Safeweb je spoznal ta problem že konec leta 2001 in tako ustavil svojo javno storitev in svoj razvoj usmeril v izdelavo sistemov za korporacije. 15. oktobra 2003 je podjetje Symantec kupilo Safeweb Inc. z namenom integracije varnih spletnih rešitev v ponudbo podjetja Symantec (Safeweb Inc., 2003). Podobno odločitev je sprejelo podjetje Zeroknowledge v upanju, da bodo korporacije lažje plačale za svojo varnost kot predplačniški naročniki za storitve anonimnega proxy strežnika. Kljub temu podjetje Zeroknowledge poleg rešitev za podjetja še vedno ponuja požarne zidove in upravitelje piškotkov za posamezne uporabnike (Stalder, 2002, str. 11; Zero-Knowledge Systems, 2003; Freedom, 2003).

Anonymizer.com, eno najstarejših in uveljavljenih podjetij, kljub zgoraj opisanim problemom, še vedno ostaja na trgu kot podjetje, ki ponuja svoje storitve anonimnega strežnika v predplačniškem sistemu (zadnja različica programa je Anonymizer PrivateSurfing 2.1). Kljub dobri znamki in uveljavljenosti na trgu pa podjetje ni uspelo zbrati več kot 17.000 uporabnikov, kar jih uvršča v sicer uveljavljene, vendar majhne igralce na tržišču (Stalder, 2002, str. 12; Anonymizer, 2003).

### 4.2.3. Ponovni pošiljatelj *(Re-mailer)*

To so programi, ki sprejemajo e-sporočila, zbrišejo informacije, ki kažejo na izvor e-sporočila (ovojnice) in posredujejo sporočilo na zastavljeno destinacijo. Najbolj enostavna različica takšnih programov so t.i. »Type I« ali »Cypherpunk« ponovni pošiljatelji. (Stalder, 2002, str. 9). V polju od: *(from:)* v e-sporočilu se pojavi naslov ponovnega pošiljatelja, velikokrat z opombo, da ta ni začetni pošiljatelj, in v kolikor se več takšnih ponovnih pošiljateljev poveže skupaj v verigo, je praktično nemogoče odkriti izvornega pošiljatelja. Vendar pa, kdor kontrolira *re-mailer*, ima dostop do podatkov pošiljateljev in prejemnikov. Takšen problem je mogoče rešiti s šifriranjem javnega ključa, kar je lahko uporabljeno za overjanje sporočila. Verižni ponovni pošiljatelji so prav tako brez pomena brez šifriranja. Vsebina, naslov pošiljatelja in prejemnika so informacije, ki so vidne vsem, ki lahko prestrežejo sporočilo ali imajo dostop do sporočila (upravniki *re-mailer* strežnikov). Kadar se uporablja šifriranje, to ni več mogoče. Vsak ponovni pošiljatelj bo vedel samo od kod je sporočilo prišlo in kam gre, ne pa kdo je še v verigi ponovnih pošiljateljev in kakšno je samo sporočilo (Seničar, Jerman-Blažič, Klobučar, 2003, str. 8).

Bolj prefinjena različica ponovnega pošiljatelja je t.i. *»pseudonimus re-mailer«*. Takšni ponovni pošiljatelji zamenjajo pošiljateljeve podatke s psevdonimom. Ponovni pošiljatelj

seveda obdrži originalni naslov pošiljatelja preden ga pošlje naslovniku, saj je tako omogočen odgovor izvornemu pošiljatelju, ne da bi se razkrila njegova identiteta, saj se odgovor pošlje na psevdonimen naslov (kar je v resnici ponovni pošiljatelj, ki nato pošlje odgovor na dejanski e-naslov uporabnika). Takšne ponovne pošiljatelje lahko primerjamo z anonimnimi poštnimi predali, vendar je njihova negativna lastnost, da so lahko tarče napada. To je bilo prvič dramatično prikazano leta 1995, ko je finska policija napadla anon.penet.fi, enega najbolj popularnih ponovnih pošiljateljev tega časa z več kot 200.000 naročniki. Scientološka cerkev *(Churce of Scientology)* je namreč trdila, da je ponovni pošiljatelj uporabljen za pošiljanje avtorsko zaščitenih informacij in kreator ponovnega pošiljatelja Johan Helsingius je bil primoran sčasoma predati identiteto vsaj ene osebe. Naslednje leto je Helsingius zaprl svojo *re-mailer* storitev (Stalder, 2002, str. 10).

Najnovejša in najsodobnejša različica *re-mailer* tehnologije je t.i. Mixmaster, ki omogoča zaščito pred prisluškovalnimi napadi *(eavesdropping attacks)*[38], kjer vsak uporabnik v mreži vedno uporablja šifrirano povezavo z vsakim členom verige. Mixmaster prav tako omogoča zaščitni mehanizem pred napadi pri odgovoru na pošto *(replay attacks)*[39] in izboljšan sistem za prestrezanje sporočila *(message reordering)*[40] (Macaulay, 2002, str. 7; Fischer-Hübner, 2001, str. 56). Tehnologija Mixmaster temelji na »varnosti v številkah« *(safety in numbers)*, kar pomeni, da se ciljno sporočilo ne razlikuje od ostalih sporočil v mreži ponovnih pošiljateljev, saj je arhitektura zgrajena tako, da konstantno generira naključno število sporočil oz. prometa *(random cover traffic)*, z namenom skrivanja originalnega sporočila (Macaulay, 2002, str. 7).

Obstaja še ena tehnologija ponovnega pošiljatelja, in sicer *newnym* strežniki. Takšen strežnik je v resnici skupek vseh tehnologij že poznanih ponovnih pošiljateljev, kot je anon.penet.fi, z vsemi anonimnimi, verižnimi in šifrirnimi funkcijami. Uporabnik prejme psevdonim (janez@nym.alias.net) z *nym* strežnika in na psevdonim poslano sporočilo mu bo dostavljeno. Za razliko od anon.penet.fi ponovnega pošiljatelja, kjer je operater strežnika obdržal listo psevdonimov povezljivih z originalnimi naslovi, *newnym re-mailer* strežnik obdrži le listo psevdonimov povezljivo z odgovornim blokom. Operater *newnym* strežnika nima liste originalnih e-naslovov uporabnikov, temveč naslov nekega drugega ponovnega pošiljatelja in šifriran sklop podatkov, ki jih pošlje drugemu ponovnemu pošiljatelju. Ko je informacija dešifrirana, je viden naslov naslednjega ponovnega pošiljatelja in še en šifriran sklop podatkov. Končno, ko eden izmed ponovnih pošiljateljev v verigi dešifrira sporočilo, dobi originalni naslov uporabnika in mu pošlje sporočilo. Prednost takšnega sistema je v tem, da bi morali biti vsi ponovni pošiljatelji v

[38] *Eavesdropping attacks; neavtorizirano dostopanje oz. prestrezanje sporočila.*

[39] *Replay napadi; ponovno pošiljanje e-sporočila. Hacker prestreže sporočilo, ki je podpisano s certificiranim ključem, ki sproži določeno transakcijo (nakup DVD predvajalnika). Ker hacker prestreže sporočilo s ključem, ga lahko pošlje in zopet sproži transakcijo pri spletni trgovini. Uporabnik nato namesto enega DVD predvajalnika dobi npr. 20 DVD predvajalnikov. Transakcija je veljavna, saj je uporabljen uporabnikov ključ, ki potrdi istovetnost transakcije, na računu kreditne kartice pa se bremeni 20 DVD predvajalnikov.*

[40] *Message reordering system; paketki sporočila ne prihajajo na cilj v istem zaporedju, kot so bili poslani.*

verigi odgovornega bloka razkriti, če bi nekdo želel odkriti originalen e-naslov ustvarjen z *newnym* strežnikom (Macaulay, 2002, str. 7; Fischer-Hübner, 200, str. 57-63).

### 4.2.4. Slepi digitalni podpis *(Blind Digital Signature)*

Digitalni podpis je digitalni ekvivalent ročnemu podpisu. Tako kot ročni podpis na dokumentu dokazuje njegovo istovetnost, enako, če ne še bolj, stori digitalni podpis. Omogoča zagotovilo, da je digitalni podpis opravila le oseba, ki ima za to dovoljena sredstva (zasebni ključ in overjen javni ključ z elektronskim protokolom). Dokument, ki je podpisan z digitalnim podpisom, zagotavlja njegovo istovetnost (Macaulay, 2002, str. 5).

Slepi digitalni podpis, katerega ustvarjalec je David Chauman (Macaulay, 2002, str. 6), je samo ena od različic digitalnega podpisa, ki zagotavlja uporabnikovo anonimnost. Temeljna razlika med digitalnim podpisom in slepim digitalnim podpisom je v tem, da slednji ne razkrije uporabnikove identitete. Niti uporabnik niti njegova identiteta se ne pojavita na podpisu. Izvirnost podpisa garantira tretja stranka, ki je izdala e-potrdilo. Prejemnik ima ob tem zagotovilo, da je transakcija avtentična in verodostojna, ne bo pa vedel, kdo je opravil transakcijo. Enako, kot je denar anonimen, je tudi elektronski ali digitalni denar anonimen v tem smislu, da ga ni mogoče povezati z določeno individualno osebo. Zagovorniki elektronskega denarja trdijo, da je ta brezpogojno neizsledljiv (Macaulay, 2002, str. 6; Seničar, Jerman-Blažič, Klobučar, 2003, str. 5).

## 4.3. Tehnologije zaščite z neizsledljivostjo

### 4.3.1. Freenet

Freenet je nastal kot raziskovalni projekt leta 1997 Ian-a Clark-a iz Edinbruške Univerze. Leta 1999 je bila programska koda kot začetek projekta odprte kode *(open source project)* postavljena na splet (Stalder, 2002, str. 17). Danes je na voljo programska verzija 0.5.2.1, kar pomeni, da je projekt še zmeraj v razvojni fazi in še ni pripravljen za širšo uporabo. A vendarle je namen Freenet-a postal popolnoma jasen. Glavni cilj Freeneta je vzpostavitev infrastrukture, ki združuje naslednje značilnosti (Stalder, 2002, str. 17):

1. anonimnost tako za uporabnike kot za podajalce informacije,
2. nepovezljivost med informacijami in tistimi, ki hranijo informacije,
3. onemogočanje tretjim strankam preprečevanje dostopa do informacij,
4. učinkovito in dinamično shranjevanje ter usmerjanje informacij,
5. decentralizacija vseh mrežnih funkcij.

Trenutni model svetovnega spleta ne deluje po zgoraj opisanih značilnostih, saj je vsak vir mogoče identificirati z URL, zato je zelo enostavno določiti lokacijo in lastnika strežnika, kjer se nahaja informacija oz. od koder prihaja zahtevek. Danes ima večina držav na svetu uveljavljen zakon, ki določa odgovornost ponudnikov gostovanja spletnih

storitev, če vede gostijo prepovedano vsebino (npr. nacistično ali proti-vladno vsebino). In ker ponudniki gostovanja spletnih strani v večini primerov niso direktno vpleteni v samo prepovedano vsebino na njihovih strežnikih, lahko hitro in tudi brez sodnega naloga onemogočijo nadaljnje gostovanje nezaželene vsebine na njihovih strežnikih. Poleg tega spletni strežniki vse zahtevke beležijo v svojo datoteko dogodkov *(log file)* in tako lahko s pomočjo zabeleženih informacij (IP naslov, dan in čas zahtevka po informaciji) določijo uporabnika, ki je podal zahtevek po informaciji. Ker je večina informacij shranjenih samo na nekaj strežnikih, je teoretično (v praksi pa težje) zelo lahko odstraniti določene informacije. Ker je vsebina shranjena na enem mestu (in mogoče na še nekaj preslikalnih *(mirror)*[41] strežnikih), je distribucija prav tako neučinkovita, saj nenadno ali nepričakovano povpraševanje po vsebini lahko zruši manjši strežnik (takšne poplave v kratkem času se na spletu pojavljajo že tako pogosto, da ima internet skupnost poseben žargon za takšen pojav: *slash-dot effect*). In kot zadnje, na spletu je kar nekaj centraliziranih nadzorov, med katerimi je najpomembnejši sistem imenskih strežnikov *(DNS)*, ki prevede računalniško berljive naslovne številke v prijazna in lahko uporabna imena. To povzroči očitno kontrolo, ki jo trenutno upravlja ICANN[42] (Stalder, 2002, str. 17 - 18).

Da bi zaobšli zgoraj navedene pomanjkljivosti svetovnega spleta, Freenetovi oblikovalci uporabljajo popolnoma drugačno arhitekturo. V nasprotju z odjemalec - strežnik *(client-server)* relacijo, ki jo uporablja trenutni model svetovnega spleta, Freenet uporablja prilagodljivo *peer-to-peer* (P2P)[43] mrežno relacijo.

Ena od rešitev, ki jih ponuja sistem Freenet, se imenuje porazdeljeni priročni spomin *(distributed caching)*. Priročni spomin *(cashe)* so trenutno shranjeni podatki, ki jih ima vsak spletni brskalnik. V Freenet modelu vsak vključen računalniški odjemalec *(node)*[44] shranjuje minljive podatke. Sistem deluje tako, da če eden od uporabnikov v verigi Freenet odjemalcev poda zahtevek po določenem dokumentu, se ta prenese od tistega, ki ima shranjen zahtevan dokument, prek vseh vmesnih členov do začetnega odjemalca, ki je podal zahtevek *(original requester)*. Vsak odjemalec v tej verigi obdrži kopijo originalnega dokumenta. Da pa bi se izognili neskončnemu številu podvojenih dokumentov, ima vsak odjemalec v sistemu določen zapadlostni mehanizem, ki enostavno izbriše dokument ali kakšno drugo vrsto informacij, če ne dobi zahtevka po tej informaciji v določenem časovnem obdobju. Vsebina, ki je velikokrat zahtevana, se razpošilja po celotni mreži, vsebina, ki ima malo oz. nima zahtevkov, pa počasi izginja. Takšna arhitektura ima kar nekaj prednosti (Clarke et al., 2002, str. 2 - 8; Stalder, 2002, str. 18 - 21; Freenet Project, 2003):

---

[41] *Mirror sites; duplikat podatkov na drugem strežniku.*
[42] *ICANN; The Internet Corporation for Assigned Names and Numbers (http://www.icann.org/).*
[43] *Peer - to - peer (P2P); Internet mreža, ki omogoča skupini uporabnikov z istim računalniškim programom povezavo in direkten dostop do datotek na računalnikih uporabnikov, ki so vključeni v omrežje. Komunikacija ni podrejena, tako kot je komunikacija strežnik - odjemalec. Obe enoti sta pri komunikaciji enakopravni in omogočata skupno izvedbo določenih nalog.*
[44] *Node; vsak računalnik, ki je vključen v računalniško mrežo (vozlišče).*

1. Zagotavlja anonimnost med originalnim dokumentom oz. njegovo kopijo in izvorom. Ker so »popularni dokumenti« oz. dokumenti z veliko zahtevki pomnoženi, jih je sila težko odstraniti iz mreže in tudi določiti pravega izvornika.
2. Omogoča majhnim spletnim mestom razpošiljanje znanih oz. popularnih dokumentov in se tako izogniti *slash-dot* efektu. Razpoložljivost informacij raste sorazmerno s povpraševanjem. Če veliko ljudi opravi zahtevek po tej informaciji, se bo informacija tudi velikokrat shranila na odjemalcih vključenih v Freenet omrežje. Ker je shranjevanje veliko cenejše kot pasovna širina, je to izredno učinkovit sistem razpošiljanja podatkov.
3. Takšna replikacija informacij omogoča še eno prednost, saj informacije približa tistim, ki jih želijo. Kot v vseh peer-to-peer sistemih bližina ni povezana z geografsko bližino, temveč s številom preskokov *(hops)* med osebo, ki opravi zahtevek po informaciji, in tistim, ki ima shranjeno informacijo. Prvi zahtevek med A in E bo mogoče potoval tudi med B, C in D, vendar že poznejši zahtevek lahko poteka direktno med A in E. To poveča uporabnost mreže in nudi zakonsko pomoč lastnikom računalnikov vključenih v mrežo z verjetnostnim zanikanjem *(plausible deniability)*. Tudi oseba, ki je opravila zahtevek po informaciji, lahko trdi, da je bila le del celotne verige zahtevkov sistema Freenet.

Naslednji pomemben vidik arhitekture sistema Freenet je v tem, da je vsa vsebina šifrirana. Gostitelj Freenet strežnika ne more vedeti, kaj se nahaja na strežniku, ker imajo dokumenti časovno omejeno trajanje in so neberljivi brez dekripcije. Lastnik strežnika tako ne more biti odgovoren za razpošiljanje nezaželenih dokumentov. Vsebina je definirana s ključem in ne z lokacijo. Vsak odjemalec ima svojo tabelo ključev, ki definirajo lokalno shranjeno vsebino. Ker je vsebina neberljiva, dokler ni dekriptirana, je iskanje možno samo po ključu in ne po celotnih tekstih. Uporabnik, ki želi najti informacijo, mora poznati točen ključ, ki je identificiran z vsebino (Stalder, 2002, str. 21).

Najbolj sporen del Freenet sistema je v obravnavanju zaščitenih pravic in intelektualne lastnine. Sistem je bil zgrajen na sistemu svobode govora, vendar ne ponuja rešitve v prekinitvi prostega razpošiljanja avtorsko zaščitenih dokumentov ali proti-vladnih informacij, avtorskih pesmi ali nelegalnih pornografskih slik. Za oblikovalce Freenet sistema to ni problem, vendar logična posledica celotne filozofije, na kateri je sistem zgrajen. In kot pravi ustvarjalec Freenet-a Ian Clark: »Ne moreš garantirati svobode govora in istočasno uveljavljati zakon o intelektualni lastnini. Prav to je razlog, da mora Freenet, sistem oblikovan za zaščito svobode govora, onemogočiti uveljavljanje zakona o zaščiti intelektualne lastnine.« *(You cannot guarantee freedom of speech and enforce copyright law. It is for this reason that Freenet, a system designed to protect Freedom of Speech, must prevent enforcement of copyright.)* (Freenet Project Philosophy, 2003).

Freenet še ni pripravljen za razširjeno uporabo, saj je potrebno rešiti še vrsto tehničnih težav. Trenutno je program napisan v Javi, kar omogoča kompatibilnost s številnimi sistemi, vendar ga je tudi uporabnikom z velikim tehničnim znanjem težko nastaviti in

uporabljati. Tudi dejstvo, da je potrebno poznati točen ključ, če želimo najti določeno informacijo, močno zmanjša zmožnost mreže za iskanje novih dokumentov.

### 4.3.2. GNUnet

Podoben sistem, kot je Freenet, je projekt GNUnet[45]. Cilj GNUnet projekta je v vzpostavitvi *peer-to-peer* sistema, kjer je informacijska izmenjava popolnoma prosta in nekontrolirana (GNUnet, 2003). Oblikovalci sistema cenijo svobodo govora in prosto izmenjavo informacij daleč od državne skrivnosti ali zakonov o intelektualni lastnini. Primarni cilj je v zaščiti uporabnikove zasebnosti in zaščiti pred možnimi napadi in zlorabami. V GNUnet sistemu ni mehanizma, ki bi kontroliral, nadzoroval ali cenzuriral dejanja uporabnikov. Ravno nasprotno, GNUnet protokoli so oblikovani na tak način, da je praktično nemogoče ugotoviti, kaj se dogaja na mreži, ali onemogočiti njeno delovanje (Kügler, 2003, 1 - 2). Oblikovalci omrežja konceptirajo GNUnet v naslednjih točkah (GNUnet Philosophy, 2003):

1. Anonimnost *(Anonymity)*; glavni cilj celotnega sistema je v anonimnosti uporabnikov in njihovih dejanj. GNUnet temelji na ideji, da so uporabnikove akcije anonimne, če so le te skrite v akcijah drugih, kar z drugimi besedami pomeni, da se akcije uporabnika ne smejo razlikovati od akcij ostalih uporabnikov.
2. Zanikanje *(Deniability)*; čeprav sta uporabnik, ki poda zahtevek, in strežnik, ki hrani podatke, anonimna, so lahko vmesni členi peer-to-peer mreže tarča napadov. Če vmesni členi lahko vidijo, katere podatke prenašajo, jih lahko tretja stranka prisili v cenzuriranje določene vsebine. V GNUnet sistemu to ni mogoče, saj so zahtevki in vsebine šifrirani tako, da tudi vmesni členi ne vedo, po čem je opravljen zahtevek in kakšna je vsebina prenosa.
3. Istovetnost *(Authentication)*; istovetnost vseh komunikacijskih procesov je dosežena z izmenjavo RSA skrivnih sejnih *(secret session)* ključev. Ta sejni *(session)* ključ je nato uporabljen za šifriranje komunikacij med dvema uporabnikoma, kar omogoča overjanje poslanih paketkov. Poleg tega šifriran promet oteži kakršno koli analizo prometa.
4. Kriptografija *(Cryptography);* GNUnet uporablja RSA ključ za izmenjavo sejnega *(session)* ključa in simetričen ključ za šifriranje podatkov in P2P komunikacijo.
5. Poročanje *(Accounting);* V GNUnet sistemu vsak odjemalec spremlja obnašanje drugih odjemalcev, s katerimi je bil v kontaktu, kar omogoči reševanje sistema pred *freeload*[46] napadi.
6. Zaupnost *(Confidentiality);* nasprotniki izven GNUnet omrežja ne smejo vedeti, kakšne akcije opravlja posamezen odjemalec, prav tako udeleženci GNUnet mreže ne vedo, kdo in po čem je opravil zahtevek in kakšna je vsebina prenosa.

[45] *GNU; Projekt izgradnje Unix kompatibilnih programov, ki temeljijo izključno na odprti kodi. Projekt vodi Free Software Foundation (Free Software Foundation, 2003; GNU, 2003).*
[46] *Freeload (flooding the network with traffic); preplavljanje mreže s prometom.*

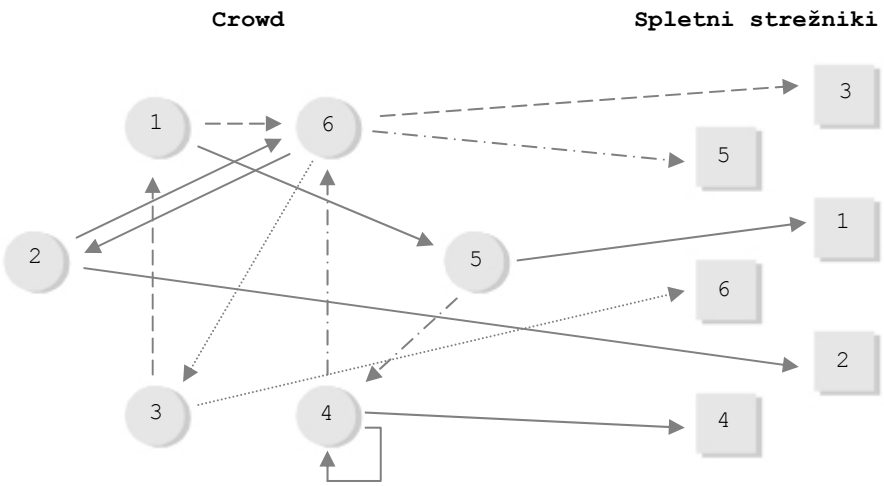
Prve verzije GNUnet sistema so omogočale samo anonimno izmenjavo podatkov. Prihodnje verzije bodo omogočale varno e-pošto in novičarske mailing liste, kar bo zagotovo povečalo uporabo sistema, saj je z velikim številom udeležencev anonimnost vedno dosežena.

### 4.3.3. Crowds

Crowds je sistem, ki zaščiti zasebnost med brskanjem po spletu, saj preprečuje spletnim strežnikom pridobivanje informacij o uporabniku. Sistem Crowds grupira uporabnike v velike, geografsko diverzificirane skupine in v njihovem imenu izdaja zahtevke po informacijah. Sistem deluje na način »pomešaj se v gnečo«, kar pomeni skrivanje akcij enega uporabnika v akcijah mnogih in tako onemogoči spletnemu strežniku definirati izvor zahteve. Da bi bila spletna transakcija izvršena, se uporabnik najprej pridruži skupini drugih uporabnikov, uporabnikova prvotna zahteva spletnemu strežniku pa se prenese naključnemu uporabniku sistema Crowds. Naključni uporabnik se nato lahko odloči, da bo izvedel zahtevek ali pa ga bo posredoval naključnemu članu sistema. Prav tako lahko naslednji naključno izbrani član zopet prenese zahtevek naslednjemu naključnemu uporabniku ali pa izvrši zahtevek na končnem strežniku. Ko je zahtevek končno izvršen, je izvršen s strani naključnega udeleženca sistema in tako končni strežnik ne more dobiti informacije o izvoru zahtevka. Enako tudi člani sistema Crowds ne morejo izvedeti, kdo je izvornik zahtevka (Reiter, Rubin, 2001, str. 3 - 5; Seničar, Jerman-Blažič, Klobučar, 2003, str. 8). Sistem Crowds tako omogoča pridobivanje želenih informacij, ne da bi bila v procesu razkrita identiteta. Ne glede na njegovo uporabnost ima sistem vrsto nevarnosti pri uporabi (Crowds, 2003):

1. proxy strežnik izvaja določene zahteve, ki niso prišle od uporabnika tega računalnika, ker proxy strežnik nekatere zahteve udeležencev sistema poda naprej, druge pa izvede na končnem strežniku,
2. na spletnih straneh, ki zahtevajo geslo in uporabniško ime, je sistem Crowds popolnoma neuporaben, saj obstaja velika nevarnost razkritja podatkov, ko zahtevek potuje po sistemu.

***Slika 4:*** *Prikaz delovanja sistema Crowds*




opomba: izvornik zahtevka je označen enako kot končni strežnik

*Vir: Reiter, Rubin, 2001, str. 8.*

## 4.4. Tehnologije zaščite s privolitvijo

### 4.4.1. P3P *(Platform for Privacy Preferences)*

P3P je standard obveščanja uporabnika o zbiranju osebnih informacij ob obisku spletne strani, ki ga je izdelala organizacija W3C *(World Wide Web Consortium)*[47]. Lahko bi ga tudi definirali kot standarden niz vprašanj, ki celovito pokriva politiko zasebnosti *(privacy policy)* (P3P, 2003). P3P uporabnikom dejansko omogoča vpogled nad tem, katere osebne informacije zbirajo spletne strani. Če bi spletna stran poskušala pridobiti informacije o uporabniku, ki jih on ne bi želel razkriti, je o tem nemudoma obveščen. P3P ni namenjen postavljanju minimalnih standardov zaščite zasebnosti niti ne more nadzorovati pravilne implementacije politike zasebnosti, vendar zelo dobro omogoča vpogled nad zbiranjem osebnih podatkov na spletu (Macaulay, 2002, str. 10).

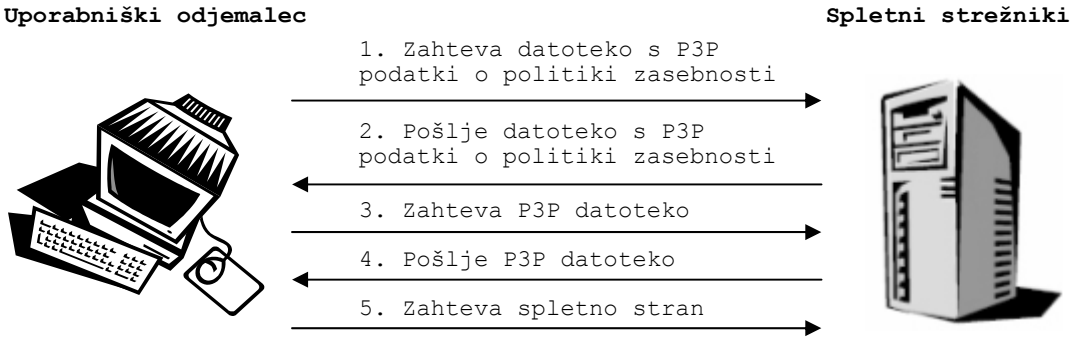
P3P standard je XML dokument (vedno se nahaja na root/W3C/p3p.xml), ki omogoča brskalnikom, ki podpirajo P3P *(P3P enabled browsers)*, strežnikom ali P3P aplikacijam analizo politike zasebnosti spletne strani. Ker P3P temelji na XML platformi, omogoča spletnim brskalnikom in strežnikom komunikacijo, še preden se zahtevek po informaciji izvrši. Ko uporabnik poda zahtevek preko spletnega brskalnika za dostop do določene spletne strani, bo brskalnik spletno stran vrnil le v primeru, če so uporabnikove P3P nastavitve v brskalniku enake kot nastavitve spletne strani. Takšen sistem komunikacije omogoča uporabnikom brskanje po spletu in samodejno dobivanje informacij o politikah zasebnosti, ne da bi bilo potrebno na vsaki spletni strani poiskati in analizirati politiko zasebnosti, še posebej ker politike zasebnosti pišejo odvetniki, ki jim je glavni cilj zaščita lastnikov spletne strani, ne pa obveščanje uporabnikov o zbiranju in uporabi osebnih podatkov (Working Party on Information Security and Privacy, 2002, 19 - 21). Zagovorniki P3P tehnologije predvidevajo masovno uporabo P3P tehnologije, saj je Ameriški Internet Education Foundation sporočil, da je več kot 40 od 100 najpopularnejših ameriških strani že implementiralo P3P ali pa bodo to storile v kratkem (Železnikar, 2002).

Druga prednost P3P tehnologije je, da omogoča uporabnikom nastavitve, katere informacije, kdaj in pod kakšnimi pogoji bodo, če sploh, razkrite. Takšna tehnologija daje uporabniku moč nad postavitvijo meje med zasebnim in javnim vidikom. P3P tudi ne zahteva stalne uporabnikove angažiranosti. Ko so nastavitve nastavljene, poteka brskanje po spletnih straneh in analiziranje politik zasebnosti skorajda neopazno. Uporabnik lahko tudi zanemari svoje nastavitve in obišče spletno stran, ki nima implementirane P3P tehnologije, ali pa zbira informacije, ki jih ne želi razkriti, vendar je uporabnik o tem obveščen pred dejansko uporabo.

[47] *World Wide Web Consortium (W3C); neprofitna organizacija, ki skrbi za razvoj spleta in postavitev standardov.*

Najnovejša verzija P3P je trenutno 1.0. Obstaja kar nekaj orodij za brskanje po spletu z implementacijo P3P standarda, npr. brskalnika Netscape in Microsoft Explorer, ter samostojni program AT&T Privacy Bird (Seničar, Jerman-Blažič, Klobučar, 2003, str. 9).

***Slika 5:*** *prikaz delovanja P3P tehnologije*




**Uporabniški odjemalec:**

1. zahteva datoteko s P3P podatki o politiki zasebnosti,
2. zahteva P3P datoteko politike zasebnosti,
3. primerja politiko zasebnosti spletne strani z uporabnikovimi nastavitvami,
4. sprejme / zavrne / obvesti / opozori.

**Oznanitev datoteke P3P s politiko zasebnosti skozi:**

1. vedno znano lokacijo (root/w3c/p3p.xml),
2. HTML link tag,
3. HTTP ovojnice.

*Vir: Fischer-Hübner, 2001, str. 8.*

# 5. *Zaščita zasebnosti v e-poslovanju*

***"Trough 2006 information privacy will be the greatest inhibitor for consumer-based e-business."***

**(Do leta 2006 bo informacijska zaščita največja ovira potrošniškemu e-poslovanju.)**

**Gartner Group, raziskovalno in svetovalno podjetje**

## 5.1. Tehnologije zaščite zasebnosti v e-poslovanju

Po navedbah Forrester Research bo zaradi novih elektronskih kupcev in novih proizvodov e-poslovanje v ZDA v naslednjih petih letih raslo s stopnjo 19 odstotkov na leto in doseglo 230 milijard USD prometa, ter tako do leta 2008 znašalo 10 odstotkov celotne prodaje (Johnson, Delhagen, Yuen, 2003). V EU znaša spletna B2B prodaja 12 odstotkov in B2C 10 odstotkov celotne prodaje. Finska, Danska in Velika Britanija imajo najvišji odstotek prodaje preko spleta in trend spletnega nakupa se bo le še zviševal (SIBIS Pocket Book 2002/03, 2003, str. 51). V povprečju 20 odstotkov EU populacije kupuje storitve ali proizvode preko spleta, v ZDA pa je ta številka več kot podvojena in znaša 45 odstotkov (Vehovar, Lobe, Kovačič, 2003, str. 8). E-poslovanje postaja vse pomembnejše tako za kupce kot podjetja, vzporedno pa za kupce raste pomembnost vprašanja varstva osebnih podatkov. Po RIS-ovih raziskavah junija 2002 večina anketirancev ne kupuje preko spleta, ker se boji, da bodo njihove informacije s plačilnih kartic ali njihovi osebni podatki zlorabljeni (Vehovar, Lobe, Kovačič, 2003, str. 23). Na podlagi teh ugotovitev lahko trdimo, da je rešitev problema zaščite uporabnikove zasebnosti in pravilna izbira tehnologije ključnega pomena za vsak uspešen model e-poslovanja. Enako lahko tudi trdimo, da zloraba zasebnih podatkov predstavlja poslovno tveganje, v mnogih primerih pa še velik strošek. Ko je ameriški FTC *(Federal Trade Commission)* objavil, da je Geocitis zlorabil osebne podatke svojih uporabnikov, se je vrednost delnic Geocitis vsako minuto zmanjšala za 1 mio USD (Camp, Osorio, 2002, str. 9).

Za uspešen model e-poslovanja poročilo *»Privacy Enhancing Technologies for Internet Commerce«* navaja različne modele zaščite, ki izhajajo iz treh različnih konceptov zasebnosti (Camp, Osorio, 2002, str. 7, 9):

1. Pravica do samostojnosti *(a right to autonomy)*, kjer je vprašanje nadzora temelj zasebnosti.
2. Pravica do umika oz. samote *(a right to seclusion)* ali pravica biti puščen pri miru. Nadzor v takem primeru ni kritičen, dokler namen nadzora ni v prihodnjem (potencialno nadležnem) kontaktu (nezaželena e-pošta).

3. Pravica do lastnine *(a right to property)*, kjer je nadzor dopusten le v primerih, ko uporabnik z nadzorom pridobi. Če je nadzor sam sebi namen, je nesprejemljiv, nadzor zaradi pridobivanja različnih personaliziranih ali boljših storitev pa je dopuščen.

Na podlagi opisanih konceptov zasebnosti lahko tudi kupce razdelimo v tri različne skupine:

1. Kupci, ki razumejo zasebnost kot osnovno človeško pravico in zaščite svoje zasebnosti ne bodo prepustili trgovcem. Takšni uporabniki bodo brskali po spletu, vendar je verjetnost njihovega spletnega nakupa zelo majhna.
2. Kupci, ki menijo, da je zasebnost pravica do miru (oz. do nenadlegovanja), se ne razlikujejo veliko od prve skupine. Njihova idealna poslovna relacija je enkratna transakcija, ki ni nadzorovana in ki ne omogoča nadaljnjega kontakta. Takšni kupci ne bodo kupovali pri trgovcih, ki si želijo trajen stik s svojimi kupci, ali prodajalcih, ki za nakup zahtevajo ustvarjanje spletnih računov.
3. Tretja skupina so tisti kupci, ki verjamejo, da se njihove podatke lahko vrednostno oceni. Za takšne kupce morajo vse transakcije predstavljati ravnotežje med nagrado in tveganjem. Veliko število takšnih kupcev bo z veseljem razkrilo svoje osebne podatke v zameno za popust, vendar je zelo malo takšnih, ki bodo razkrili svoje podatke prodajalcu, ki jim ne nudi ničesar.

Na podlagi treh različnih konceptov zasebnosti in kupcev lahko razdelimo tehnologije zaščite zasebnosti v e-poslovanju v tri skupine:

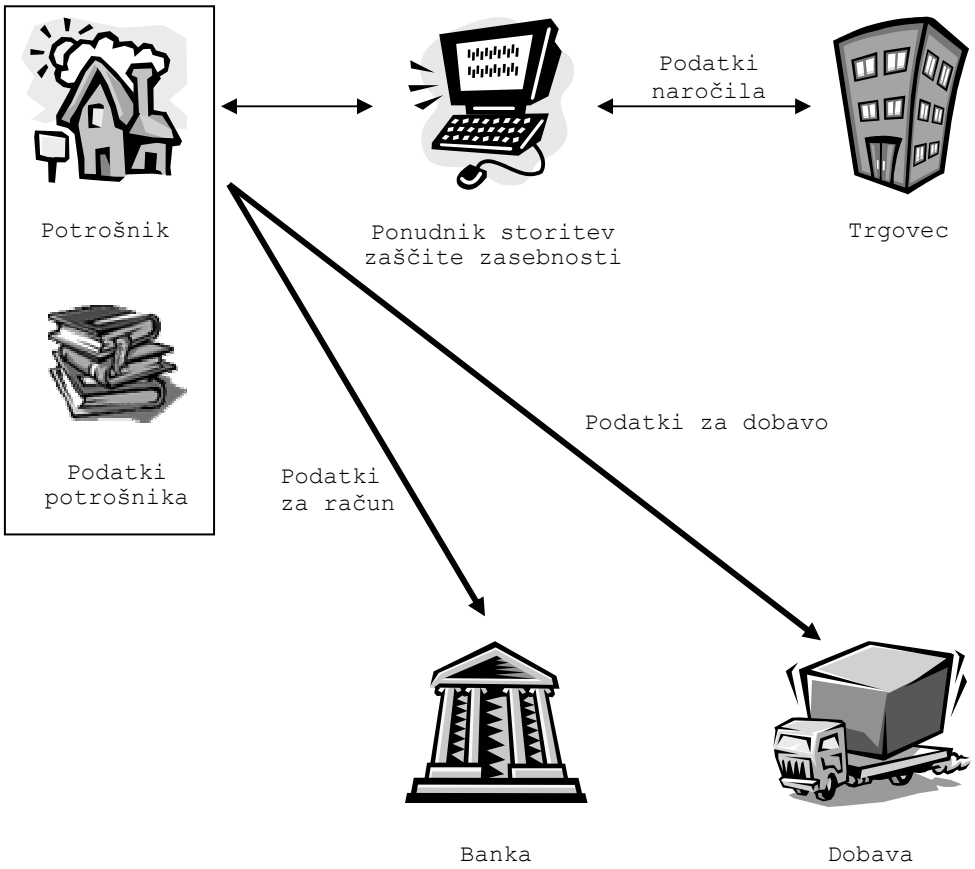
1. tehnologije povečanja zasebnosti *(Autonomy-Enhancing Technologies)*,
2. tehnologije, ki omogočajo biti nenadlegovan *(Seclusion-Enhancing Technologies)* in
3. rešitve za nadzor lastnine *(Property-Managing Solutions)*.

### 5.1.1. Tehnologije povečanja zasebnosti *(Autonomy-Enhancing Technologies)*

Tehnologije povečanja zasebnosti omogočajo uporabniku dostop do informacij, ne da bi v procesu razkril svoje podatke. Prav tako onemogočijo delovanje mnogih tehnologij uporabljenih pri spletnih trgovinah, kot so JavaScript, piškotki in Active X. V takšnem sistemu uporabnik obdrži celotno kontrolo nad podatki in transakcijami (na sliki 7 so osebni podatki prikazani kot knjiga). Tehnologije povečanja zasebnosti ne omogočajo izvensodnega reševanja sporov *(dispute resolution)*[48], saj je zanj potrebno pustiti osebne podatke pri trgovcu ali ponudniku storitev zaščite zasebnosti.

[48] *Izvensodno reševanje sporov (dispute resolution); proces uporabljen za odgovarjanje na poizvedovanje kupca, reševanje morebitnih problemov in neskladij med kupcem in prodajalcem. Za uveljavljanje dogovora mora prodajalec seveda imeti osebne podatke kupca.*

***Slika 6:*** *Prikaz delovanja tehnologij povečanja zasebnosti*



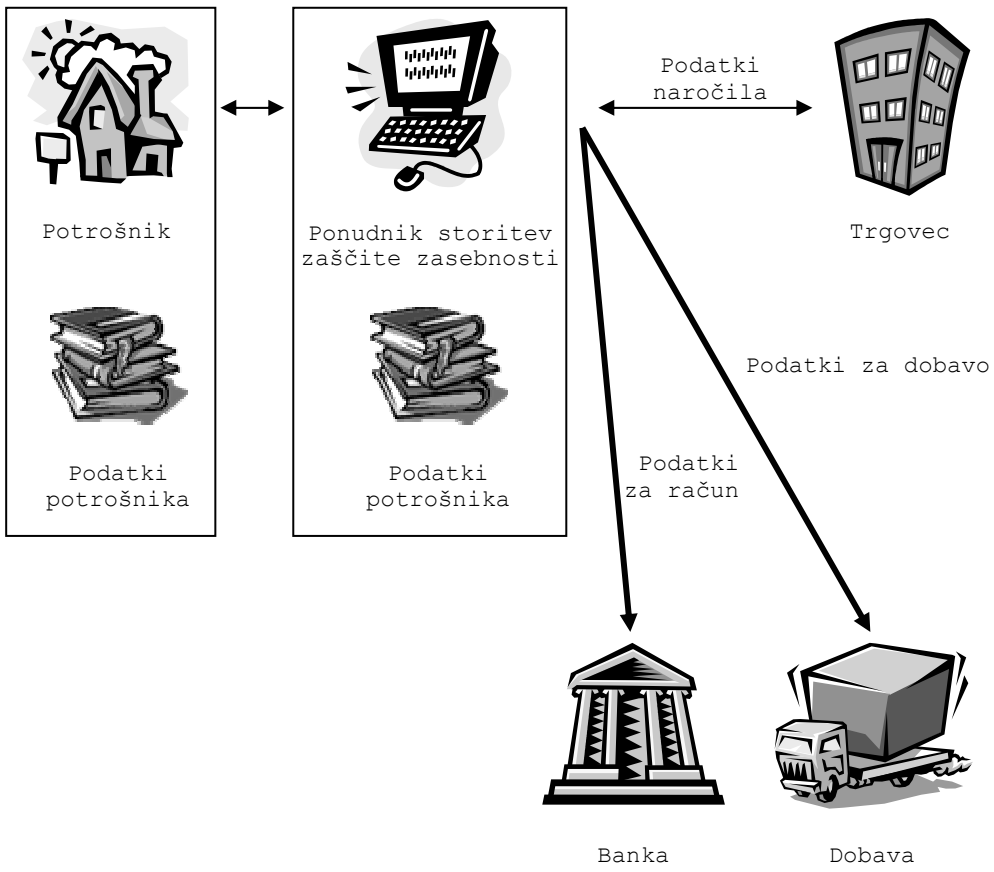

*Vir: Camp, Osorio, 2002, str. 11.*

Primer takšnega sistema je rešitev podjetja Anonymizer, ki ponuja anonimne rešitve za brskanje po spletu.

### 5.1.2. Tehnologije, ki omogočajo biti nenadlegovan *(Seclusion-Enhancing Technologies)*

Tehnologije, ki omogočajo biti nenadlegovan, ponujajo uporabniku zaupanja vredno tretjo stranko, ki obljublja, da ne bo nadlegovala uporabnika in daje uporabniku možnost prekinitve kontakta s katerim koli trgovcem. Potrošnik še naprej odloča sam. Tehnologije, ki omogočajo biti nenadlegovan, se razlikujejo od tehnologij povečanja zasebnosti v tem, da obstaja tretja vmesna stranka, ki hrani nekaj podatkov o uporabniku. V takšnem sistemu uporabnik ne obdrži celotne kontrole nad podatki in transakcijami (na sliki 8 so osebni podatki zopet prikazani kot knjiga).

***Slika 7:*** *Prikaz delovanja tehnologij, ki omogočajo biti nenadlegovan*




*Vir: Camp, Osorio, 2002, str. 13.*

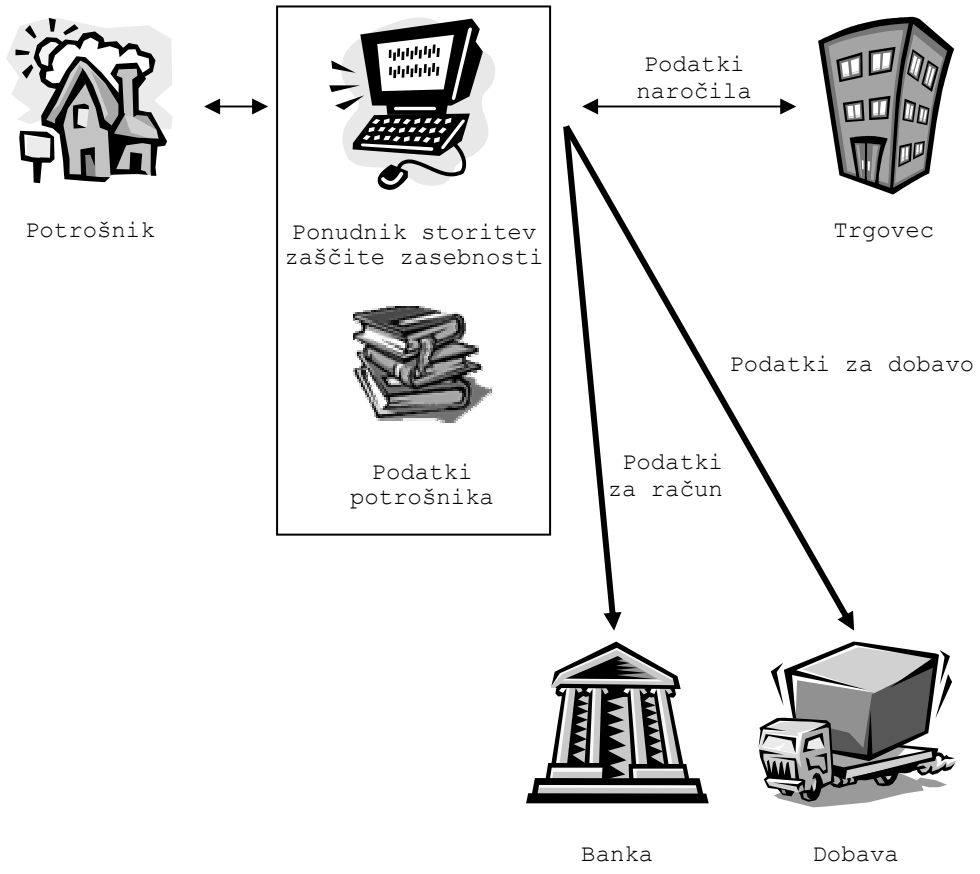
Primer takšne zaščite predstavlja iPrivacy, ki ponuja proxy strežnik za brskanje in nakupovanje po spletu. iPrivacy deluje kot vmesni člen med kupcem in podjetjem (iPrivacy, 2003). iPrivacy šifrira podatke prodajalcem in dostavnim službam tako, da oba vesta le minimalno število potrebnih podatkov, da je lahko transakcija opravljena. Takšen sistem ne ponuja popolne anonimnosti, temveč zmanjšuje možnost prodajalcu, da shranjuje in zbira kakršne koli podatke svojih kupcev. Podjetja kreditnih kartic imajo v takšnem sistemu vse informacije o opravljenih transakcijah in nakupih. Glavna prednost sistema iPrivacy je, da prodajalci ne shranjujejo osebnih podatkov kupcev in kasneje po opravljenem nakupu ne morejo več stopiti v stik s kupci. Prav tako iPrivacy omogoča izvensodno reševanje sporov, saj hrani osebne podatke uporabnika.

### 5.1.3. Rešitve za nadzor lastnine *(Property-Managing Solutions)*

Rešitve za nadzor lastnine se od drugih tehnologij ločijo predvsem v dveh značilnostih: po lokaciji podatkov in kontroli nad podatki.

Ponudniki tehnologij, ki omogočajo biti nenadlegovan, shranjujejo samo potrebne podatke za izvensodno reševanje sporov. Ponudniki rešitve za nadzor lastnine pa shranjujejo detajlne podatke. Druga razlika je v kontroli podatkov. Ponudniki tehnologij, ki omogočajo biti nenadlegovan, omogočajo odločitev uporabnika o nadaljnjem stiku s trgovcem. Pri ponudnikih rešitve za nadzor lastnine pa so uporabnikovi podatki dani v zamenjavo za storitve, ki jih nudi ponudnik rešitve za nadzor lastnine. Uporabniki tehnologij, ki omogočajo biti nenadlegovan, se lahko odločijo, da ne bodo posredovali podatkov trgovcu, pri rešitvah za nadzor lastnine pa so podatki v lasti ponudnika rešitev za nadzor lastnine in ta lahko podaja podatke tretjim strankam v zameno za ugodnosti, popuste, ... V takšnem sistemu uporabnik nima kontrole nad podatki in transakcijami (na sliki 9 so osebni podatki prav tako prikazani kot knjiga).

***Slika 8:*** *Prikaz delovanja rešitev za nadzor lastnine*




*Vir: Camp, Osorio, 2002, str. 16.*

Primer takšnega sistema je Microsoft Passport, ki omogoča shranjevanje vseh uporabniških imen in gesel v eno shrambo *(singl log-in)*[49] v zameno za uporabnikove podatke. Microsoft tako shranjuje vse komunikacijske in transakcijske podatke vsakega

[49] *Single log-in; storitev, ki omogoča shranjevanje vseh uporabniških imen in gesel v eno shrambo, kar omogoča uporabnikom logiranje le enkrat za vse spletne strani ali storitve, ki potrebujejo log in (spletne trgovine, spletne e-mail aplikacije, ...).*

posameznika. Passport nedvoumno jemlje zasebnost kot storitev, saj takšen sistem vrednoti zasebnost in uporabnikove podatke izključno kot dobrino.

## 5.2. Standardi zaščite zasebnosti v e-poslovanju *(privacy seals)*

V e-poslovanju trenutno ne obstaja organizacija, ki bi določala standarde zaščite zasebnosti, a vendar na tržišču obstajajo štirje ponudniki, ki zagotavljajo zaščito zasebnosti *(privacy assurance providers)* s tako imenovanim sistemom zaščitnih znakov oz. pečatov *(privacy seals)*. TRUSTe (http://www.truste.org), neprofitna organizacija, ustvarjena leta 1996 z namenom zaščite zasebnosti na spletu, je kot prva vstopila na tržišče in ima trenutno največje število strank (1.830). Better Business Bureau, ki ponuja storitev BBB Online (http://www.bbbonline.org), je z 851-imi strankami druga organizacija, ki ji sledita še PriceWaterhouseCoopers BetterWeb (http://www.betterweb.co.za) s 100-timi klienti in WebTrust (http://www.cpawebtrust.org) z 28-imi klienti (Jamal, Maier, Sunder, 2003, str. 289).

Sistem zaščitnih znakov deluje tako, da trgovec plača letno članarino pri enem od ponudnikov, ta pa v zameno opravi pregled in po potrebi preoblikovanje politike zasebnosti. Lahko jih imenujemo tudi tretja stranka, ki ji zaupata tako ponudnik spletnih storitev kot uporabnik. Uporabniki dopustijo zbiranje svojih podatkov spletnim mestom vedoč, da za njimi stoji zaupanja vredna stranka, ki garantira, da njihovi podatki ne bodo zlorabljeni in uporabljeni v druge namene, kot je zapisano v politiki zasebnosti. Celoten sistem tako ponuja rešitev za trgovce in kupce, saj trgovcem omogoča pridobitev zaupanja kupcev, kupci pa lažje opravijo transakcijo na spletnem mestu z zaščitnim znakom, saj imajo tako garancijo o zasebnosti svojih podatkov.

Članarina pri TRUSTe in BBB Online se izračunava na podlagi prihodka stranke. Največja članarina pri TRUSTe je 12.999 USD (pri prodaji večji od 2 milijardi USD) (TRUSTe, 2003), pri BBB Online pa največja članarina znaša 7.000 USD (pri prodaji večji od 2 milijardi USD) (BBB Online, 2003). Takšne članarine ne vključujejo natančnejšega pregleda dejanskih izpolnjevanj zaščite zasebnosti klientov, ampak le pregled napisanih politik zasebnosti. WebTrust ponuja celoten pregled v vrednosti letne članarine 100.000 USD (Jamal, Maier, Sunder, 2003, str. 289). PWC ponuja storitev BetterWeb v vrednosti 15.000 USD.

Primerjavo med vsemi štirimi ponudniki standardov zaščite zasebnosti lahko strnemo v naslednje tri točke:

1. Vsi štirje standardi zahtevajo, da je v politiki zasebnosti napisano, kako se zbirajo zasebni podatki posameznika na spletni strani. TRUSTe in PWC BetterWeb sta bolj zahtevna kot BBB Online in WebTrust, saj zahtevata tudi določitev načina, kako so podatki zbrani.
2. Vsi štirje standardi zahtevajo od spletnih strani razkritje informacij o tem, kako bodo zbrani podatki uporabljeni in dostopni tretjim strankam. Zopet sta TRUSTe in PWC

standarda bolj zahtevna, saj zahtevata tudi razkritje načinov komuniciranja, ki jih lahko uporabnik pričakuje od spletne strani (pošta, e-pošta, telefon).

3. TRUSTe standard zahteva od spletne strani razkritje načina uporabe piškotkov, kako se zbrane informacije s piškotki povezujejo z identiteto uporabnika, kateri podatki se zbirajo s piškotki, razlago možnosti in posledic, če uporabnik ne želi prejeti piškotka, razkritje, ali so zbrani podatki povezljivi z dobljenimi podatki tretjih strank, in razkritje tretje stranke, ki zbira podatke na spletni strani. To je najzahtevnejši standard pri uporabi piškotkov. Naslednji standard je BBB Online, ki zahteva razkritje uporabe piškotkov, povezljivost s piškotki zbranih podatkov in podatkov dobljenih od tretjih strank ter razkritje morebitnih tretjih strank, ki zbirajo podatke na spletni strani. WebTrust standard je manj specifičen in zahteva le razkritje uporabe piškotkov, ne omenja pa razkritja podatkov morebitnih tretjih strank, ki zbirajo podatke na spletni strani. PWC BetterWeb pa ne zahteva razkritja uporabe piškotkov, vendar se le-ta lahko razkrije na podlagi zbiranja podatkov, kar je opisano pod prvo točko.

Na podlagi te primerjave lahko sklepamo, da ima TRUSTe najstrožje zahteve po razkritju zbiranja in uporabe podatkov, sledi mu BBB Online. Ostala dva standarda, WebTrust in PWC BetterWeb, sta manj zahtevna. Bolj zahtevni standardi imajo nižje cene, manj zahtevni standardi pa višje. Najbolj zahteven standard TRUSTe je tudi najbolj razširjen standard z največjim tržnim deležem v industriji.

# 6. *Sklep*

***"If privacy is outlawed; only outlaws will have privacy."***
**(Če je zasebnost izven zakona, bodo zasebnost imeli samo tisti, ki so izven zakona.)**

**Philip R. Zimmerman, ustvarjalec programa PGP**

Trditev, da spletne tehnologije za boljšo zaščito zasebnosti lahko dosežejo svoj cilj le, če je ta postavljen zelo ozko, predstavlja upravičeno skrb. Ponovni pošiljatelji onemogočijo razkritje pošiljatelja e-sporočila in spletni-proxy strežniki otežijo zasledovanje in zbiranje uporabnikovih brskalnih navad. P3P, če je implementiran, omogoča uporabnikom boljšo informiranost o politiki zasebnosti. Freenet in GNUnet onemogočata določanje lokacij shranjene vsebine in tako zagotavljata anonimnost in prost pretok informacij. Vendar, če razširimo cilje tako, da povečajo zaščito na internetu za večino uporabnikov, lahko trdimo, da tehnologije za boljšo zaščito zasebnosti ne dosežejo zastavljenega namena.

V zadnjih petih letih je postalo zelo jasno, da predplačniški sistemi zaščite zasebnosti, kot sta jih uveljavljali podjetji Zeroknowledge in Safeweb, niso komercialno uspešni, vsaj kar zadeva rešitve za posamezne uporabnike. Po drugi strani so korporacije pričele z implementacijo tehnologij zaščite, da bi dosegle usklajenosti z regulativami zaščite zasebnosti. Tudi trditev, da ponudniki spletnih storitev vidijo uporabo tehnologij zaščite bolj v zmanjšanju korporativne odgovornosti kot v povečanju uporabniške zaščite zasebnosti, je še kako resnična. Problem, ki ga predstavlja vzpostavitev tako imenovanega trga storitev za zaščito zasebnosti *(PET market)*, je v zelo znanem paradoksu. Velika večina uporabnikov namreč trdi, da je njihova največja skrb pri uporabi spleta varstvo osebnih podatkov, a vendar v resnici zelo malo naredijo za zaščito svoje identitete. Večina zagovornikov problema zaščite zasebnosti trdi, da je razlog v premajhni informiranosti posameznikov. Ljudje se preprosto ne zavedajo, koliko informacij je zbranih v komercialnih ali vladnih agencijah, še manj pa potencialno škodljivih posledic tega zbiranja. Ko je po Evropi divjala bolezen norih krav, se je večina državljanov seznanila z dejstvi o sami bolezni in njenih posledicah, ter potrebnih ukrepih zaščite. Osebna informiranost je tako za vsakega posameznika ključnega pomena, če se dogodki ali dejanja tičejo njegovega vsakdanjega življenja. Zakaj ni tako z zaščito zasebnosti? Res je, da mediji, ki so dejansko vključeni v celoten sistem zbiranja podatkov, ne posvečajo toliko pozornosti zaščiti zasebnosti kot nekaterim drugim temam. Prav tako z odvračanjem javne pozornosti in zakrivanjem dejstev ne obravnavajo problema zaščite zasebnosti, kot bi ga morali sicer, vendar, kot trdi Stalder, to ni glavni razlog, zaradi katerega se povprečen posameznik ne poglobi v svojo osebno zaščito. Razlogi izhajajo predvsem iz treh pomembnih ugotovitev.

Prvič, povezava med spletno akcijo in njeno negativno posledico ni takojšnja, pogosto pa je velikokrat direktna povezava med akcijo in pozitivnim efektom. Ponavadi, ko uporabnik pusti

svoje podatke v zameno za storitev (recimo za dostop do člankov na spletu časnika Wall Street Journal - WSJ.com), je pozitiven efekt takojšen. Uporabnik izpolni spletni obrazec, se prijavi, dobi želene informacije in to vse le v nekaj sekundah. Po drugi strani zasledovanje in analiziranje uporabniških navad lahko poteka mesece, ne da bi se uporabnik tega sploh zavedal. Takšen problem ni značilen samo za zasebnost na internetu. Pojavlja se tudi pri naravovarstvenih vprašanjih. Problem kislega dežja, recimo, je bil znan veliko prej, preden so ljudje začeli dejansko spreminjati svoje okolje. Odpeljati se do trgovine ima za posameznika direkten učinek (dostop do blaga in trgovin), nakup katalizatorja pa lastnikom avtomobila predstavlja takojšen strošek. Če bi katalizator ostal le draga storitev rezervirana samo za ljudi, ki res želijo skrbeti za svoje okolje, ne bi bil nikoli široko sprejet. Isti princip obstaja pri tehnologijah zaščite zasebnosti. Za uporabnika predstavlja plačevanje za zaščito takojšen strošek v primerjavi z nedoločeno koristjo v prihodnosti, ki se je trenutno ne zaveda. Iz te ugotovitve izhaja še en problem. Dejansko je posameznik primoran plačevati za nekaj, kar naj bi bilo samoumevno. Večina uporabnikov spleta in vseh ostalih elektronskih orodij se ne zaveda, da je zasebnost, ki je temeljna pravica vsakega posameznika, v današnji družbi razkošje, za katerega je potrebno plačati.

Drugič, ustvarjanje osebnih relacij med posameznikom in vladno ali javno agencijo mogoče le ni tako slaba izbira. Uporabnik si npr. želi, da ima banka njegove podatke, saj lahko na ta način koristi vse ugodnosti, ki jih ta nudi. Prav tako si uporabnik želi, da imajo ponudniki kreditnih kartic zabeležene vse transakcije uporabnika, saj ima tako pregled nad opravljenimi stroški. Seznam situacij, v katerih si želimo, da so naše informacije znane tretjim strankam, ni samo dolg, ampak se tudi sama sestava razlikuje od uporabnika do uporabnika. Nekateri uporabniki vidijo v policijskem nadzoru vdor v zasebnost, drugi pa večjo varnosti.

Tretjič, če želimo recimo brati WSJ na spletu, obstaja samo eno spletno mesto, ki nam to ponuja. V takšnih primerih velikokrat do odločitev o posredovanju osebnih podatkov posameznika pride na način »sprejmi ali pusti«. Takšno neravnotežje moči daje veliko boljšo pozicijo ponudniku storitev kot uporabniku, ki želi le priti do določene vsebine. V takšni situaciji je zbiranje podatkov za ponudnike storitev nekaj popolnoma običajnega in z današnjimi tehnologijami izredno lahko. Dalje, zbiranje podatkov je direktno povezano s celotnim namenom elektronskih medijev: dati, kadar želiš in kar želiš. Elektronsko procesiranje podatkov, zbiranje, katalogizacija in profiliranje so le sistemi in orodja za izpolnjevanje te obljube.

Dosedanji princip zaščite zasebnosti je postal neučinkovit v svetu elektronskih komunikacij. To lahko tudi sklepamo na podlagi izjave direktorja Sun Microsistems Scott-a McNealy-ja: “You have no privacy. Get over it.” Veliko avtorjev trdi, da je naša družba postala organizirana kot mreža digitalnih informacij in komunikacijskih tehnologij. V sistemu, kjer je vsak povezan v mrežo, je opcija izolacije redka. Potrebno je postaviti popolnoma nov koncept zaščite zasebnosti. Potreben je premik od individualnega k strukturnemu in od zaščite k nadzorovanju. Nadzor je vsekakor tehnika moči. Daje moč tistim, ki zbirajo in procesirajo osebne podatke, in oblikuje usodo tistih, katerih informacije imajo. Nov način zaščite je v iskanju orodij za

vzpostavitev odgovornosti. Če sledimo principu reševanja problema kislega dežja z vzpostavitvijo katalizatorja kot standarda v vseh vozilih, lahko upamo, da bo problem zaščite zasebnosti rešen na podoben način. Z generalnim orodjem, ki bo pokrival celotno populacijo in ne samo posameznikov, ter reševal zasebnost kot celoto in ne samo kot ozek cilj.

Na podlagi tega novega razmišljanja morajo podjetja in ponudniki spletnih storitev prevzeti odgovornost za zbrane podatke in tako celoten družbeni sistem postaviti na novo pot, pot k povečani zaščiti zasebnosti.

# 7. Literatura


1. A Review of the Fair Information Principles: The Foundation of Privacy Public Policy. San Diego: Privacy Rights Clearinghouse, 1997. 9 str.
2. An Introduction to Cryptography. Palo Alto: PGP Corporation, 2003. 74 str.
3. Black Edwin: IBM and the Holocaust: The Strategic Alliance Between Nazi Germany and America's Most Powerful Corporation. New York: Crown Publishing Group, 2001. 528 str.
4. Camp L. Jean, Osorio Carlos A.: Privacy-Enhancing Technologies for Internet commerce. Cambridge: Kennedy School of Government, Harvard University, 2002. 15 str.
5. Clarke Ian, Miller Scott G., Hong Theodore W., Sandberg Oskar, Wiley Brandon: Protecting Free Expression Online with Freenet. New York: Institute of Electrical and Electronics Engineers, 2002. 10 str.
6. Čebulj Janez: Varstvo informacijske zasebnosti v Evropi in Sloveniji. Ljubljana: Inštitut za javno upravo pri Pravni fakulteti v Ljubljani, 1992. 74 str.
7. Data Protection Working Party: Privacy on the Internet - An Integrated EU Approach to On-line Data protection. Bruselj: The European Commision, 2000. 99 str.
8. Huizenga Jan: Roadmap for Advanced Research in Privacy and Identity Management, Deliverable RD 3.0, Overall Roadmap 'Privacy and Identity Management' Final Report, 2003. 61 str.
9. Jamal Karim, Maier Michael, Sunder Shyam: Privacy in E-Commerce: Development of Reporting Standards, Disclosure and Assurance Services in an Unregulated Market. Chicago: Journal of Accounting Research Vol. 41, 2003. str. 285 - 309.
10. Jerman-Blažič Borka: Izbrana poglavja računalniških komunikacij in elektronsko poslovanje, zapiski iz predavanj, poletni - semester 1999/2000, Ljubljana, 1999. 77 str.
11. Kovačič Matej: Zasebnost na internetu. Ljubljana: Mirovni inštitut, 2003. 111 str.
12. Kovačič Matej: Zasebnost v informacijski družbi. Diplomsko delo. Ljubljana: Fakulteta za družbene vede, Univerza v Ljubljani, 2000. 64 str.
13. Kovačič Matej: Zasebnost v informacijski družbi. Ljubljana: Teorija in praksa družboslovna revija 37, (2000a), 6. str. 1019-1034.
14. Kügler Dennis: An Analysis of GNUnet and the Implications for Anonymus, Censorship-Resistant Networks. Bonn: Federal Office for Information Security, 2003. 17 str.
15. Macaulay Linda: Privacy Enhancing Technologies State of the Art Review Version 1. Manchester: Institute of Science and Technology, University of Manchester, 2002. 22 str.
16. Michaud Erin: Current Steganography Tools and Methods. Bethesda: SANS Institute, 2003. 9 str.
17. Reiter Michael K., Rubin Aviel D.: Crowds: Anonymity for Web Transactions. New Jersey: AT&T Labs Research, 2001. 23 str.
18. Seničar Vanja, Jerman-Blažič Borka, Klobučar Tomaž: Privacy Enhancing Technologies - approaches and development. Ljubljana: Laboratory for Open Systems and Networks, Inštitut Jožef Štefan, 2003. 11 str.
19. Stalder Felix: The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy. B.k.: Sociological Research Online, 7, (2002), 2. 33 str.

20. Vehovar Vasja, Lobe Bojana, Kovačič Matej: Confidentiality Concern and On-line Shopping. Ljubljana: Faculty of Social Sciences, University of Ljubljana, 2003. 30 str.
21. Working Party on Information Security and Privacy: Inventory of Privacy Enhancing Technologies (PETs). Paris: Organisation for Economic Co-operation and Development, 2002. 29 str.

# 8. Viri


1. A web server log file sample explained. [http://www.jafsoft.com/searchengines/log_sample.html], 26.4.2000.
2. Anonymizer. [URL: http://www.anonymizer.com/], 12.10.2003.
3. Banisar David: Privacy & Human Rights 1999. Washington: Electronic Privacy Information Center; London: Privacy International. [URL: http://www.privacyinternational.org/survey/index99.html ], 1.9.1999.
4. BBB Online [URL: https://www.bbbonline.org/privacy/price.asp], 15.10.2003.
5. Coursey David: Behind Amazon's preferential pricing. [URL: http://zdnet.com.com/2100-11-523742.html], 10.9.2000.
6. Coursey David: Why worry about Web bugs? Here's the real privacy threat. [http://reviews-zdnet.com.com/4520-6033_16-4206310.html], 16.8.2001.
7. Crowds. [URL: http://www.research.att.com/projects/crowds/], 1.10.2003.
8. Crypto-Heaven Challenge. [URL: http://www.cryptoheaven.com/Security/CryptoChallenge.htm], 31.5.2002.
9. Crypto-Heaven Security. [URL: http://www.cryptoheaven.com/Security/Security.htm], 15.9.2003.
10. Davidson Paul: Call list impact 'unclear'. [URL: http://www.usatoday.com/money/industries/telecom/2003-10-01-donotcall_x.htm], 1.10.2003.
11. de Montaigne Michael Eyugem. [URL: http://oregonstate.edu/instruct/phl302/philosophers/montaigne.html], 4.9.2003.
12. Fischer-Hübner Simone. [URL: http://www.cs.kau.se/~simone/], 15.10.2003.
13. Fischer-Hübner Simone: Privacy Enhancing Technologies winter 2001 course overhead projector slides. Karlstad: Department of Computer Science, Karlstad University, 2001. 151 str.
14. Free Software Foundation (FSF). [URL: http://www.fsf.org/], 7.11.2003.
15. Freedom. [URL: http://www.freedom.net], 12.10.2003.
16. Freenet Project Philosophy.[URL: http://www.freenetproject.org/index.php?page=philosophy], 28.9.2003.
17. Freenet Project. [URL: http://www.freenetproject.org/], 9.9.2003.
18. GNU. [URL: http://www.gnu.org], 7.11.2003.
19. GNUnet Philosophy. [URL: http://www.ovmj.org/GNUnet/philosophy.php3?xlang=English], 17.10.2003
20. GNUnet. [URL: http://www.ovmj.org/GNUnet], 17.10.2003.
21. Greenberg Paul A.: Toysmart Flap Triggers Privacy Bill. [URL: http://www.ecommercetimes.com/perl/story/3766.html], 13. julij 2000.
22. Guggenheim Ken: Pentagon's Futures Market Plan Condemned. [URL: http://informationclearinghouse.info/article4267.htm], 29.7.2003.
23. GUIDES E-business Guidlines on Data Protection Directive 95/46/EC, 2002. 45 str.
24. GUIDES Final Report - Deliverable D5.2, 2002. 10 str.

25. Hoppe D. Ian: Toysmart Database to Be Destroyed: Dot-com Tried to Sell Customer Information After Business Failed. [URL: http://abcnews.go.com/sections/scitech/DailyNews/toysmart010110.html], 10. januar 2001.
26. India Express Bureau: Are you 'legitimate' for a US visa? [URL: http://www.indiaexpress.com/news/world/20030721-2.html], 21.6.2003.
27. Interni podatki Dhimahi d.o.o., 1.9.2003.
28. iPrivacy. [URL: http://www.iprivacy.com/], 3.11.2003.
29. Jerman-Blažič Borka, Tehnologije elektronskega poslovanja prosojnice predavanj 2001/2002. Ljubljana: Ekonomska fakulteta, Univerza v Ljubljani, 2001.
30. Johnson Carrie A., Delhagen Kate, Yuen Esther H.: US eCommerce Overview: 2003 To 2008. Cambridge: Forrester Research, Inc., 2003.
31. Kovačič Matej. [URL: http://www.ljudmila.org/matej], 6.9.2003.
32. Laurant Cedric: Privacy & Human Rights 2003. Washington: Electronic Privacy Information Center; London: Privacy International. [URL: http://www.privacyinternational.org/survey/phr2003/], 1.9.2003.
33. Marx Gary T. [URL: http://web.mit.edu/gtmarx/www/garyhome.htm], 1.11.1999.
34. Milchen Jeff: The Lunatic Fringe of Capitalism: Trading in Terrorism. [URL: http://reclaimdemocracy.org/pam.html], 29.7.2003.
35. National Do Not Call Registry. [URL: http://www.donotcall.gov/], 1.10.2003.
36. P3P. [URL: http://www.w3.org/P3P/], 5.11.2003.
37. Policy Analysis Market. [URL: http://www.policyanalysismarket.com/], 17.11.2003.
38. Privacy Foundation. [URL: http://www.privacyfoundation.org/resources/webbug.asp#1], 25.9.2003.
39. Privacy Incorporated Software Agent (PISA) project. [URL: http://www.pet-pisa.nl], 20.6.2002.
40. Privacy International. [URL: http://www.privacyinternational.org/survey], 9.9.2003.
41. Privacy Journal. [URL: http://www.privacyjournal.net/], 5.10.2003.
42. Rosencrance Linda: Amazon charging different prices on some DVDs. [URL: http://www.computerworld.com/industrytopics/retail/story/0,10801,49569,00.html], 5.9.2000.
43. Rosencrance Linda: Customer outrage prompts Amazon to change price-testing policy. [URL: http://www.computerworld.com/industrytopics/retail/story/0,10801,50153,00.html], 13.9.2000a.
44. Safeweb Inc. [URL: http://www.safewebinc.com], 16.9.2003.
45. Sample Server Log Entry. [http://www.its.monash.edu.au/web/slideshows/webstats/slide3-0.html], 3.7.2000.
46. SIBIS Pocket Book 2002/03: Measuring the Information Society in the EU, the EU Accession Countries, Switzerland and the US. Bonn: SIBIS project and European Communities, 2003. 218 str.
47. Stevenson Reed: Microsoft says Passport flaw exposed user data. [http://in.tech.yahoo.com/030509/137/246x3.html], 9.5.2003.

48. Testimony of Philip R. Zimmermann to the Subcommittee on Science, Technology, and Space of the US Senate Committee on Commerce, Science, and Transportation. [URL: http://www.philzimmermann.com/testimony.shtml], 26.6.1996.
49. TRUSTe. [URL: http://www.truste.org/programs/pub_how_join.html], 15.10.2003.
50. Weiss Todd R.: Amazon apologizes for price-testing program that angered customers. [URL: http://www.computerworld.com/industrytopics/retail/story/0,10801,51392,00.html], 28.9.2000.
51. Zero-Knowledge Systems. [URL: http://www.zeroknowledge.com/], 12.10.2003.
52. Zimmerman Phil. [URL: http://www.philzimmermann.com], 14.9.2003.
53. Železnikar Jaka: Zasebnost na internetu. [URL: http://www.mladina.si/dnevnik/18868/], 18.4.2002.

# 9. Slovar tujih izrazov

**A**

| | | |
|---|---|---|
| *Active X* | | podmnožica Microsoft Active platforme |
| *attached files* | | datotečne priloge |

**B**

| | | |
|---|---|---|
| *bandwidth* | | pasovna širina |
| *BBB* | Better Business Bureau | |
| *blind digital signature* | | slepi digitalni podpis |

**C**

| | | |
|---|---|---|
| *chatter* | | čenčati, klepetati |
| *ciphertext* | | šifriran navaden tekst |
| *client - server* | | odjemalec - strežnik |
| *cookie managemen tool* | | upravitelj elektronskih piškotkov |
| *cookie viewer* | | pregledovalnik piškotkov |

**D**

| | | |
|---|---|---|
| *data encryption layer* | | podatkovno šifrirna plast |
| *data mining* | | tehnika izkopavanja podatkov za odkrivanje zakonitosti v podatkih |
| *DDP* | Directive on Data Protection | |
| *delete* | | izbriši |
| *DNS* | Domain Name System | |
| *dynamic pricing* | | dinamično določanja cen |

**E**

| | | |
|---|---|---|
| *eavesdropping attacks* | | neavtorizirano dostopanje oz. prestrezanje sporočil |
| *EPIC* | Electronic Privacy Information Center | |

**F**

| | | |
|---|---|---|
| *features market* | | standardizirani terminski trg |
| *first party cookies* | | piškotki obiskane spletne strani |

| | | |
|---|---|---|
| *first-time user* | | uporabnik, ki prvič dostopa do spletne strani |
| *freeload* | | preplavljanje mreže s prometom |
| *FSF* | Free Software Foundation | |
| *FTC* | Federal Trade Commission | |
| *FTP* | File Transfer Protocol | protokol, ki omogoča prenos datotek med računalniki v internetu |

**G**

| | | |
|---|---|---|
| *GNU* | | projekt izgradnje Unix kompatibilnih programov |
| *GUID* | Global Unique Identifier | globalni univerzalni identifikator |

**H**

| | | |
|---|---|---|
| *hops* | | število preskokov v P2P omrežju med osebo, ki opravi zahtevek po informaciji, in tistim, ki ima shranjeno informacijo |
| *HTTP* | Hyper Text Transfer Protocol | opredeljuje komunikacije med odjemalcem in spletnim strežnikom |

**I**

| | | |
|---|---|---|
| *ICANN* | The Internet Corporation for Assigned Names and Numbers | |
| *IETF* | The Internet Engineering Task Force | |
| *information society* | | informacijska družba |
| *IP* | Internet Protocol | internetni protokol |
| *IP v6* | Internet Protocol version 6 | nova generacija internetnega protokola |

**J**

| | | |
|---|---|---|
| *Java* | | objektno orientiran programski jezik |
| *JavaScript* | | skriptni jezik za programiranje spletnih strani |

**L**

| | | |
|---|---|---|
| *log files* | | datoteke aktivnosti ali datoteke dogodkov |

**M**

| | | |
|---|---|---|
| *M.I.T.* | Massachusetts Institute of Technology | |
| *message reordering system* | | ko paketki sporočila ne prihajajo na cilj v istem zaporedju, kot so bili poslani |
| *mirror site* | | preslikalni strežnik; duplikat podatkov na drugem strežniku |
| *MS* | Microsoft | |

**N**

| | | |
|---|---|---|
| *network society* | | mrežna družba |
| *newsgroups* | | novičarske skupine |
| *node* | | vsak računalnik, ki je vključen v računalniško mrežo |

**O**

| | | |
|---|---|---|
| *OECD* | Organization for Economic Cooperation and Development | Organizacija za ekonomsko sodelovanje in razvoj |
| *opt-out* | | možnost izstopa iz mailing liste |
| *original requester* | | odjemalca, ki je podal prvotni zahtevek |

**P**

| | | |
|---|---|---|
| *P2P* | peer - to - peer | internet mreža, ki omogoča skupini uporabnikov z istim računalniškim programom povezavo in direkten dostop do datotek na računalnikih uporabnikov, ki so vključeni v omrežje |
| *P3P* | Platform for Privacy Preferences | |
| *packet dropping* | | ko napadalec enostavno zbriše vse ali samo del poslanih paketov |
| *PAM* | Policy Analisys Market | |
| *password sniffing* | | prestrezanje in kraja gesel |

| | | |
|---|---|---|
| *PET* | Privacy Enhancing Technologies | |
| *PISA* | The Privacy Incorporated Software Agent | |
| *plain text* | | navadno besedilo |
| *plausible deniability* | | verjetnostno zanikanje |
| *presistent cookies* | | vztrajni piškotki |
| *privacy enhancing technologies* | | tehnologije za boljšo zaščito zasebnosti |
| *privacy policy* | | politika zasebnosti |
| *proxy* | | vmesni strežnik, ki deluje kot strežnik pri odjemalcu in kot odjemalec k strežniku |
| *PTC* | Personal Trust Center | |
| *PWC* | PriceWaterhouseCoopers | |

**R**

| | | |
|---|---|---|
| *RAPID* | Roadmap for Advanced Research in Privacy and Identity Management | |
| *relay server* | | posredniški poštni strežnik |
| *re-mailer* | | ponovni pošiljatelj |
| *reordering* | | ko TCP paketi, ki so bili poslani po določenem zaporedju in času prispejo do končnega odjemalca v drugem vrstnem redu, ali pa sploh ne prispejo *(glej tudi message reordering system)* |
| *repeat user* | | ponovni uporabnik |
| *robot* | | robot |
| *RSA algoritem* | | algoritem, ki je dobil ime po ustvarjalcih Ron Rivest, Adi Shamir in Leonard Adleman |

**S**

| | | |
|---|---|---|
| *session* | | seja |
| *session cookies* | | sejni piškotki |
| *slash-dot effect* | | nepričakovano povpraševanje po vsebini na spletnem strežniku |
| *SMTP* | Simple Mail Transfer Protocol | protokol za elektronsko pošto |
| *spam* | | nezaželena elektronska pošta |
| *spider* | | pajek |

| | | |
|---|---|---|
| *SSL* | Secure Sockets Layer | protokol, ki omogoča šifrirano povezavo med strežnikom in odjemalcem |

**T**

| | | |
|---|---|---|
| *TCP/IP* | Transport Control Protocol / Internet Protocol; | osnovni standardni protokol za internet, ki omogoča različnim računalnikom, ki so priključeni na internet, komunikacijo drug z drugim |
| *TET* | Transperent Encryption Technology | |
| *third-party cookies* | | piškotki, ki jih pošiljajo druge spletne strani |
| *TTP* | Trusted Third Parties | |

**U**

| | | |
|---|---|---|
| *URL* | Uniform Resource Locatior | enotni identifikator za internetne vire, ki določa metode dostopa in lokacijo |

**W**

| | | |
|---|---|---|
| *W3C* | World Wide Web Consortium | |
| *web bugs* | | spletni hrošč |
| *web mining* | | izkopavanje podatkov zbranih na spletni strani |
| *worm* | | črvi |

**X**

| | | |
|---|---|---|
| *XML* | Exstensible Markup Language | standard za strukturirane dokumente na spletu |