UNIVERZA V MARIBORU
FAKULTETA ZA ORGANIZACIJSKE VEDE

Diplomsko delo visokošolskega strokovnega študija
Smer: Informatika v organizaciji in managementu

VAROVANJE ZASEBNOSTI PRI RABI INTERNETA

Mentor: doc. dr. Igor Bernik

Kandidat: Saša Marolt

Kranj, maj 2009

ZAHVALA

Hvala mentorju, doc. dr. Igorju Berniku, za strokovne nasvete, usmerjanje in vso pomoč pri izdelavi diplomske naloge.
Posebna zahvala gre tudi družini, prijateljem ter fantu Jerneju za vso podporo med študijem.

POVZETEK

V diplomskem delu želim osvetliti problem varovanja zasebnosti ter osebnih podatkov na internetu. Definirala sem zasebnost na internetu in prikazala načine, kako se obvarovati ter se pravilno zaščititi pred morebitnimi vdori in grožnjami, ki jih dandanes predstavlja uporaba interneta. Velik poudarek pripisujem tehnologijam za boljše varovanje zasebnosti, katere podpirajo nadzor uporabnikov nad lastnimi osebnimi podatki. Predvidevam, da se uporabniki interneta premalo zavedamo oziroma premalo poznamo grožnje zasebnosti na internetu. Velikokrat brez potrebe razkrivamo svoje osebne podatke in premalo poznamo orodja za zaščito zasebnosti na internetu. Kljub temu pa čutimo določen strah pred razkritjem osebnih podatkov ter nadzorom, ki ga nove tehnologije omogočajo. Nadzor in ohranjanje zasebnosti posameznika na internetu s pomočjo spletnih tehnologij sta ključni vprašanji in smernici celotnega diplomskega dela.

KLJUČNE BESEDE

- zasebnost
- internet
- varnost
- nadzor
- zaščita

ABSTRACT

In Thesis I want to highlight the problem of privacy and personal data protection on the Internet. I have defined privacy on the Internet and I have showed some ways how to preserve it and also how to properly protect against possible intrusions and threats, which nowadays represents the use of the Internet. The task I want to highlight are technologies, performed for better protection of privacy, which enable users to protect their own personal data. I assume that internet users are insufficiently aware of the threats they are exposed to on the Internet. Internet security tools are not as known as they should be, therefore frequently comes to unnecessary personal data revelation. However, we feel a certain fear of disclosure of personal data, and also control which the new technologies allow. Monitoring and maintaining the privacy of individuals on the Internet through online technologies are the key issues in the overall guideline of this Thesis.

KEYWORDS

- privacy
- internet
- security
- control
- protection

KAZALO

1 UVOD

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

Država ter njene institucije potrebujejo informacije za učinkovito uravnavanje življenja posameznikov ter dobro delovanje družbe, zato jim posameznik ne more oziroma ne sme preprečiti zbiranja podatkov, pri tem pa je nujno potrebna transparentnost uporabe osebnih podatkov (Kovačič, 2000).

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-ta posameznik pripravljen odkriti, sta osnovna elementa zaščite in varovanja zasebnosti.

Kljub 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.

Za varovanje zasebnosti se vse bolj uveljavljajo tako imenovane tehnologije za boljšo zaščito zasebnosti (Privacy Enhancing Technologies – PETs), ki obljubljajo zaščito zasebnosti v elektronskem svetu. 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 posreduje. Namen tehnologij za zaščito zasebnosti je predvsem ustvariti infrastrukturo za zaščito zasebnosti, zmanjšati (omejiti) nadzor ter omejiti zbiranje podatkov. Na kratko lahko rečemo, da so to tehnologije, ki podpirajo nadzor uporabnikov nad lastnimi osebnimi podatki. S pomočjo uporabe tehnologij za varovanje zasebnosti lahko tudi »tradicionalna« varnostna orodja postanejo »prijazna« z vidika zasebnosti.

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

1.1 PREDSTAVITEV PROBLEMA

V današnjem času skoraj ni človeka, ki se ne bi srečal z internetom. Malo pa je takih, ki se zavedajo tudi vseh pasti, katerim so izpostavljeni. Ozaveščenost ljudi o problemih zasebnosti na internetu je še vedno na nizkem nivoju. Ponavadi se zavejo potrebe po varovanju šele takrat, ko je že prepozno in ko je bil vdor v njihovo zasebnost že storjen. Uporabniki namreč ne marajo omejitev in niso pripravljeni razumeti, zakaj na osebni računalnik oz. v brskalnik ni priporočljivo nameščati programske opreme, ki s seboj prinaša morebitne grožnje za varnost njihovih podatkov.

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 izgubijo ali pridobijo s takšno prakso in kako zagotoviti ustrezno varovanje, so vprašanja, na katera bom skušala odgovoriti. Nadalje želim s tem diplomskim delom vsem uporabnikom spletnih storitev predstaviti vprašanje zaščite tudi kot družbeni problem, ki se dotika vsakega posameznika.

1.2 METODE DELA

Metoda dela, ki sem jo uporabila pri izdelavi diplomskega dela, temelji predvsem na podlagi obstoječe literature tujih in domačih avtorjev ter virih, prispevkih, člankih z novejšimi teoretičnimi spoznanji s področja interneta, zasebnosti, varnosti in zaupanja. Prevladujoča metoda dela temelji na teoretični podlagi obravnavane tematike. Praktični del temelji na prikazu delovanja nekaterih tehnologij, ki so navedene v teoretičnem delu.

V diplomskem delu sem predstavila spoznanja o zasebnosti, varnosti in uporabi interneta, ki predstavljajo prakso v tujini, ter skušala opozoriti na nevarnosti in priložnosti, ki čakajo morebiti tudi nas. Poleg veliko zbrane literature sem vključila tudi lastno znanje, pridobljeno v praksi na področju naprednih tehnologij in tekom študija.

1.3 CILJ DIPLOMSKEGA DELA

Cilj diplomskega dela je poiskati načine, kako povišati stopnjo zasebnosti pri uporabi interneta, hkrati ugotoviti, v kolikšni meri so uporabniki seznanjeni o možnostih posega v njihovo zasebnost ob uporabi interneta in tudi preveriti, ali se zavedajo posledic, ki lahko nastanejo zaradi nepremišljenega ravnanja, nevednosti oz. neustrezne zaščite. Eden izmed ciljev je tudi opredeliti tehnologije za izboljšanje varovanja zasebnosti. Seveda pa tehnologija sama ni v nikakršno pomoč, če ljudje sami niso dovolj osveščeni, da bi poskrbeli za svojo zasebnost.

Opisala sem najrazličnejše zaščite za varnost osebnih podatkov in elektronskega poslovanja. Za varnost je potrebno poskrbeti z izbiro ustreznih tehnologij, metod in

rešitev ter jih povezati v celoto, tako da bo varnost osebnih podatkov prek interneta največja. Razvoj tehnologije poleg nevarnosti za posameznikovo zasebnost prinaša tudi nove in učinkovitejše rešitve za zavarovanje različnih interesov glede zasebnosti in anonimnosti pri uporabni internetnih storitev. Paleta rešitev je široka, obsega tako strojne kot programske rešitve. Uporabniki interneta lahko varujejo svojo zasebnost s pomočjo pristopov in tehnologij za varovanje zasebnosti. Namen prvih je predvsem odpraviti določene že znane slabosti v zasnovi internetnih aplikacij, kot sta spletni brskalnik in poštni odjemalec ter tako zmanjšati tveganja zasebnosti. Namen drugih pa je predvsem kompleksno varovanje uporabnikove zasebnosti pri navigiranju po internetu in interakciji z drugimi udeleženci v sodobni družbi, uporabljajoč elektronske komunikacije. Z vsakim dnem naša zasebnost na internetu tako vse bolj izginja, zato je treba ukrepati takoj.

1.4 STRUKTURA DIPLOMSKEGA DELA

Struktura diplomskega dela je zasnovana tako, da sem iz splošnih teoretičnih tem prišla na ožji, bolj praktični del. Uvodnemu delu, ki povzema diplomsko delo, sledi drugo poglavje, v katerem sem predstavila pomen zasebnosti in osebnih podatkov. V tretjem poglavju podrobnejše predstavim najrazličnejše grožnje zasebnosti, katerim smo izpostavljeni pri uporabi interneta in elektronske pošte. Četrto poglavje opisuje tehnologije za boljše varovanje zasebnosti ter opredeljuje različne možnosti, ki so trenutno na voljo za zaščito zasebnosti uporabnikov. V tem poglavju je prikazan tudi praktični vidik uporabe teh tehnologij. V zaključnem delu naloge poskušam povezati svoje ugotovitve z uvodnimi hipotezami.

2 DEFINICIJA ZASEBNOSTI IN OSEBNIH PODATKOV

2.1 Definicija zasebnosti

»Nikogar se ne sme nadlegovati s samovoljnim vmešavanjem v njegovo zasebno življenje, v njegovo družino, v njegovo stanovanje ali njegovo dopisovanje in tudi ne z napadi na njegovo čast in ugled. Vsakdo ima pravico do zakonskega varstva pred takšnim vmešavanjem ali takšnimi napadi.«[1]

Logično bi bilo, da bi bila ena sama definicija zasebnosti. Pa je ni! V človekovi zgodovini so bili različni pogledi na zasebnost posameznika in tudi danes imamo na voljo več definicij. Vsak gleda na svojo zasebnost drugače, pri čemer je treba upoštevati zakonske, politične in sociološke vidike. Religija ima svoj vpliv, prav tako navade. Zasebnost oziroma pravico do zasebnosti ima različno vsebino v različnih političnih ureditvah, na njeno opredelitev pa vpliva tudi časovni horizont. Ena prvih definicij se je izoblikovala že konec prejšnjega stoletja v Združenih državah Amerike. Po njej je to pravica posameznika, da se ga pusti pri miru. Takšna definicija za potrebe sodobnih sistemov, katerih najpomembnejšo značilnost in podlogo za delovanje predstavljajo informacije, prav gotovo ni ustrezna. Zato se danes pravica do zasebnosti opredeljuje kot pravica posameznika, da zahteva, da se podatki in informacije o njegovih zasebnih razmerjih ne sporočajo komurkoli. Gre torej za kontrolo pretoka in posredovanja podatkov, ki se nanašajo nanj oziroma opisujejo njegove lastnosti (Čebulj, 1992).

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[2] pravico do zasebnosti določil kot »mejo, do katere družba lahko vdre v posameznikove zadeve«. Vendar pa zasebnost ni enodimenzionalen pojem; različni avtorji vidijo več dimenzij zasebnosti.

Čebulj navaja tri sestavine zasebnosti:

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).

(Čebulj, 1992)

[1] *Citirani tekst je vsebovan v Splošni deklaraciji človekovih pravic, ki jo je sprejela in razglasila Generalna skupščina združenih narodov 10.decembra 1948. leta.*

[2] *David Banisar, namestnik direktorja Privacy International in eden od ustanoviteljev Electronic Privacy Information Center (EPIC). Avtor številnih študij in knjig.*

Poročilo Privacy & Human Rights 1999 pa loči naslednje vrste zasebnosti: informacijsko zasebnost, zasebnost telesa, zasebnost komunikacij in prostorsko zasebnost. V sodobni družbi sta najbolj ogroženi informacijska zasebnost in zasebnost komunikacij.

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).

Vsi ti procesi so privedli do potrebe po učinkoviti zakonodaji za zaščito zasebnosti. Danes skoraj vsaka država na svetu priznava v ustavi pravico do zasebnosti, se pa po posameznih državah razlikuje obseg priznavanja te pravice. Minimum, ki ga zakonodaja priznava, je nedotakljivost stanovanja in tajnost komunikacij, čedalje več držav pa razširja pravico do zasebnosti tudi na dostop in obravnavo osebnih podatkov o posameznikih.

V Sloveniji je pravica do zasebnosti temeljna človekova pravica, zaščitena s Splošno deklaracijo Združenih narodov o človekovih pravicah in zapisana v 35. členu naše ustave: »Zagotovljena je nedotakljivost človekove telesne in duševne celovitosti, njegove zasebnosti ter osebnostnih pravic.« Prav tako ustava v 38. členu opredeljuje uporabo osebnih podatkov v skladu z namenom zbiranja, pravico da se posameznik seznani z osebnimi podatki, ki se nanašajo nanj in pravico do sodnega varstva ob njihovi zlorabi. Posebno vlogo ima še en člen ustave, in sicer 39.: »Zagotovljena je svoboda izražanja misli, govora in javnega nastopanja, tiska in drugih oblik javnega obveščanja in izražanja. Vsakdo lahko svobodno zbira, sprejema in širi vesti in mnenja.«

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 (Kovačič, 2003)

2.1.1 Zgodovinski pregled zasebnosti

Že v praskupnosti je človek čutil potrebo po zasebnosti, potrebo po »biti sam, biti nemoten«. Skozi različna obdobja zgodovine je imela zasebnost različen pomen. Sprva, v manj razvitih državah, je imela zgolj pomen fizičnega umika na lokacijo, varno pred ostalimi, pred skupnostjo. Kasneje je zasebnost pridobila tudi na družbenem pomenu, v zadnjem stoletju celo kot temeljna človekova pravica.

Prve zametke zasebnosti na višji ravni najdemo v starih zapisih Korana, v Bibliji, v zapuščini zgodnje hebrejske kulture, v zakonih in kulturi klasične Grčije in Kitajske. Kot navaja Graham, je bil v družbah kot sta bili stara Grčija ali Kitajska sicer dobro razvit koncept »javno – zasebno«, vendar pa zasebnost nikoli ni bila opisana z

vidika družbene politike, pojmovala se je le kot izraz lastninske pravice (Graham, 1999).

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

Za obdobje 18. stoletja je značilna krepitev merkantilizma in buržoazije ter prevzem nadzora nad ekonomijo, ki je bil prej v rokah klera in fevdalcev. Z nadzorom nad ekonomijo si je buržoazija pridobila tudi politično moč. Za ohranitev novega položaja so potrebovali takšno zakonsko zaščito, ki bi varovala njihovo lastnino. To je privedlo do prve zakonske zaščite zasebnosti. Vendar ne v vseh državah hkrati in tudi ne v vseh državah enako. Te razlike se še danes odražajo v zakonodajah različnih držav (Graham, 1999).

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

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)[3] (Stalder, 2002). 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 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.

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.

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

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.

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.

Zgodovina po 11. 9. 2001 WTC

Po napadu na Ameriko 11. septembra 2001 se je povsod po svetu spremenil odnos do zasebnosti. Vse bolj je izražena dilema med zasebnostjo posameznikov in državno varnostjo. Tako direktiva 2002/58/ES dovoljuje državam članicam retencijo lokacijskih in prometnih podatkov preko različnih komunikacijskih sredstev: telefonije, mobilne telefonije, interneta, internetne telefonije, medtem ko direktiva 95/46/ES v 6. členu zahteva, da se podatki zbrišejo oziroma predelajo v anonimne takoj po končanem namenu, za katerega so bili zbrani. Zaradi boja proti terorizmu je vse bolj glasna zahteva članic Evropske unije po večjem nadzoru nad državljani, s tem tudi po vse daljši dobi retencije prometnih in lokacijskih podatkov. (Direktiva 2002/58/ES, 2002)

V imenu javne varnosti se je povečal in se še povečuje nadzor države nad državljani, zato je za dosego skupinske varnosti lahko ogrožena tudi zasebnost posameznika.

Pred 11. septembrom 2001 je v Združenih državah veljala stroga zakonodaja, ki je ščitila širjenje informacij med različnimi agencijami. Prevladovalo je mnenje, da takšno širjenje informacij krši človekove pravice in državne agencije so se tega morale držati. Po 11. septembru 2001 pa je Amerika sprejela paket protiterorističnih zakonov in aktov. Predvsem »US patriot Act« (2001) in »Homeland Security act« (2002) povečujeta moč elektronskemu nadzoru in prestrezanju podatkov. Z zakonoma je ogrožena »on-line« zasebnost nedolžnih, ki hkrati dopušča sledenje in zapisovanje IP naslovov ter vpogled preiskovalcev v finančne in druge transakcije vseh državljanov. Takšen nadzor zmanjšuje zasebnost posameznikov na račun državne varnosti.

2.2 Osebni podatki

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

Evropska direktiva o zaščiti podatkov navaja, da pomeni osebni podatek vsak delček informacije, ki se nanaša na točno določenega posameznika ali na posameznika, ki ga je mogoče preko te informacije identificirati (posredno ali neposredno). Neposredna identifikacija pomeni: ime in priimek, naslov, osebna številka (pri nas EMŠO), datum rojstva, nacionalnost, izobrazba, zaposlenost, zakonski stan, širše poznan psevdonim, biometrične karakteristike (prstni odtis…). Posredna identifikacija pa pomeni ostale enolično določene parametre lastnosti ali kombinacijo, z namenom da se pridobi zadostna identifikacijska informacija, na podlagi katere se lahko enolično identificira posameznik. (Direktiva 95/46/ES, 1995)

Slovenski zakon o varovanju osebnih podatkov definira osebni podatek kot »katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen.« Kot osebni podatek se šteje vsak podatek, ki se nanaša na določeno ali določljivo (npr. preko enotne matične številke občana) fizično osebo (posameznika) tako, da kaže na njegove lastnosti, stanja in razmerja, ne glede na obliko, v kateri je izražen.

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

Tehnologija je namreč pospešila zbiranje in tudi obdelavo podatkov, zmožnosti nove tehnologije so zato zahtevale posebna pravila za obravnavo osebnih podatkov. Prvi zakon o varstvu osebnih podatkov je leta 1970 sprejela Zvezna republika Nemčija, pozneje pa še Švedska (1973), ZDA (1977) in Francija (1978). Močan pritisk na države, da bi le-te ustrezno uredile to področje z nacionalno zakonodajo izvajajo danes direktive Evropske unije.

Pravno so največja nevarnost pri zbiranju podatkov zlasti nenatančnost, napačnost, nepopolnost ali neažurnost zbranih podatkov (Čebulj, 1992), poleg tega pa se lahko podatki zbirajo preventivno, »za vsak primer«, kar lahko prejudicira pravni proces (npr. policijske baze ali baze varnostnih služb). Problematičen je tudi obstoj baz osebnih podatkov, za katere posamezniki niti ne vedo, da obstajajo, ali pa vanje nimajo vpogleda.

Zato je leta 1974 generalni sekretar OZN v poročilu Človekove pravice in znanstveni in tehnološki razvoj – *Uporaba elektronike, ki lahko vpliva na pravice oseb, in omejitve, ki bi morale biti podane v demokratični družbi pri takih uporabah*,[4] priporočil predvsem tri načela, ki naj bi jih vsebovala zakonodaja s področja varovanja informacijske zasebnosti:

[4] *Omejeno poročilo je generalni sekretar OZN leta 1974 pripravil za ekonomsko socialni svet.*

1. načelo relevantnosti, ki zahteva, da se o posamezniku zbirajo samo tisti podatki, ki so nujno potrebni za dosego namena, zaradi katerega se zbirajo,
2. načelo notifikacije, ki zahteva, da je posameznik predhodno seznanjen o tem, kateri podatki se o njem zbirajo, shranjujejo in obdelujejo, ter
3. načelo privolitve, ki pravi, da naj se zbirajo samo tisti podatki, za katere je posameznik privolil, da se zbirajo.

Glavna sestavina zaščite informacijske zasebnosti je torej nadzor pretoka in posredovanja podatkov, ki se nanašajo na nekega posameznika. Zato se sodobna zakonodaja z zaščito zasebnosti ukvarja predvsem s transparentnostjo uporabe osebnih podatkov. Zbiranje podatkov se torej ne omejuje, vendar mora imeti zakonsko podlago, namen zbiranja in uporaba podatkov pa morata biti vnaprej znana in transparentna.

Zaradi tega se pravica do informacijske zasebnosti, ki je ena izmed najbolj ogroženih, danes opredeljuje kot »pravica posameznika, da zahteva, da se podatki in informacije o njegovih zasebnih razmerjih ne sporočajo komurkoli« (Čebulj, 1992) – to pomeni: tistim, ki za uporabo določenih podatkov in informacij niso pooblaščeni. Načelo transparentnosti uporabe osebnih podatkov se čedalje bolj uporablja tudi na internetu, predvsem v obliki izjave o zasebnosti (ang. privacy statement), v kateri lastnik spletne strani pove, kakšni osebni podatki se zbirajo, kakšen je namen zbiranja in za kaj bodo uporabljeni zbrani osebni podatki. (Kovačič, 2003)

2.3 Varnost in zasebnost

V današnji dobi informacije in nasploh digitalizacije našega življenja se veliko govori o varnosti podatkov, o varnosti omrežij, o varnosti elektronskega poslovanja. Prepričani smo, da z zagotovitvijo varnosti poslovanja dosegamo tudi zasebnost. Žal temu ni tako. Varnost in zasebnost sta dva pojma, ki ju mnogokrat zamenjujemo, vendar ju nikakor ne moremo in ne smemo enačiti. Tako tesna povezava med konceptoma zasebnost in varnost je pogosto razlog za zmedenost pri številih ljudeh. Trenutno še ni povsem jasno, kaj točno sestavlja zasebnost, kot tudi ni splošnega dogovora glede definicije varnosti. Na zasebnost se preprosto gleda kot na politično, na varnost pa kot na tehnološko vprašanje. Prav tako še ni dogovora o tem, kako naj bodo ti koncepti varovani (z etiko, zakoni, trgom ali drugimi mehanizmi), ali kdo naj bi bil zanje odgovoren (država, posameznik, organizacije itd.).

Kadar se v tehnološki družbi govori o varnosti, se na splošno misli na varovanje podatkov pred naključnim odkritjem, napačno uporabo ali zlorabo, uničenjem podatkov, in sicer osebno identifikacijskih ali katerih koli drugih. Varnost lahko vključuje shranjevanje, prenašanje, varnostne kopije in druge transakcije, ki vključujejo podatke. Varnostne rešitve, produkti in storitve poskušajo preprečiti aktiviranje virusov, odpraviti ranljivost omrežij, omejiti dostop neavtoriziranim uporabnikom ter preveriti podatke, sporočila ali uporabnike. To so kritična orodja za varovanje shranjenih ali prenesenih osebnih informacij. Brez varnostnih tehnologij bi bilo zelo težko ali celo nemogoče varovati podatke in ponuditi orodja zasebnosti ponudnikom, korporacijam in drugim organizacijam. Zmožnost nudenja izbire potrošnikom glede zbiranja in varovanja zbranih ali shranjenih podatkov temelji na široko dostopnih in močnih varnostnih tehnologijah. Poleg potrebe, da so osebni

podatki varovani z ustreznimi mehanizmi varnosti, vključuje varovanje zasebnosti omejitev pravno dovoljene narave zbiranja, ravnanja ali prenosa osebno identifikacijskih in agregatnih informacij, ki so bile brane od posameznih uporabnikov. Ali se osebna informacija zbira, kako je uporabljena ali deljena, kakšne možnosti ima uporabnik, ali lahko uporabnik dostopa do informacij in kdo je dostopal do zbranih informacij, pa so vsa vprašanja zasebnosti.

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

Pred 11. septembrom 2001 sta bili varnost in zasebnost podobno usmerjeni. Po terorističnem napadu na WTC pa se je ravnotežje porušilo. V svetu je prevladala zahteva po javni varnosti in v imenu javne varnosti se je povečal nadzor države nad državljani. Zasebnost državljanov je postala na ta način ogrožena, kljub temu, da državne agencije ravnajo z informacijami zaupno.

Težko je najti pravo ravnovesje med pravico do zasebnosti ter dolžnostjo države, da zaščiti svoje državljane pred zunanjimi grožnjami kot so terorizem, kriminal, nesocialno obnašanje in vse druge grožnje stabilnosti v družbi. Zbiranje osebnih podatkov za identifikacijo teroristov ali potencialnih teroristov je orodje za boj in zaščito pred terorizmom. To pa je tudi klasičen primer nasprotja med pravico posameznika do zasebnosti in pravico države da zaščiti javni interes. Grožnje varnosti so konfliktni primeri teh dveh pravic: pravice do varnosti in pravice do zasebnosti.

3 GROŽNJE ZASEBNOSTI

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*;* 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*;* 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*;* 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 (Working Party on Information Security and Privacy, 2002):

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.

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, 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 Hekerji

Tako kot v fizičnem svetu tudi na internetu poteka disciplinski in regulacijski nadzor, pogosto v obliki nadzora državljana in nadzora potrošnika. Zaradi narave kiberprostora pa je zelo razširjen tudi t.i. nezakoniti nadzor, in sicer na polje računalniške kriminalitete, izvajajo pa ga ljudje, ki jih popularno označujemo z izrazom hekerji.

Izraz »heker« (ang. hacker) je izumil Joseph Weizenbaum leta 1976, popularno pa danes z njim opisujejo posameznika, ki ima veliko računalniško-tehničnega znanja, to znanje pa izkorišča za napad na računalniške sisteme: to hekerje uvršča na polje računalniške kriminalitete. Izraz heker se večinoma uporablja za »zapleteno mešanico zakonitih in nezakonitih dejavnosti, od legitimnega ustvarjalnega programiranja, do prepovedanega vdiranja in manipulacije svetovnih telefonskih ali računalniških sistemov«; najpogosteje pa se ga dojema kot prefinjeno ilegalno dejavnost (Kovačič, 2006).

Hekerji so bili eni prvih razvijalcev prosto dostopnih šifriranih programov, prostega programja, odprte kode in nasprotniki kakršnekoli oblike cenzure in državne regulacije interneta.

Danes izraz heker poljudno označuje kateregakoli kiberkriminalca, vendar Thomas in Loader kiberkriminalce delita v dve kategoriji:

1. na hekerje in phreakerje (ang. Phreaker; gre za »telefonske hekerje«, ki se ukvarjajo z zlorabo telefonskih sistemov; phreakerji so bili predhodniki hekerjev, razvijati pa so se začeli v ZDA konec 70. let; dandanes jih skorajda ni več), ki vdirajo v sisteme večinoma iz radovednosti in ne povzročajo škode,
2. na trgovce z informacijami, katerih poglavitni motiv je profit; ter na teroriste, ekonomiste in deviantneže, ki informacijske sisteme uporabljajo za nezakonite politične ali družbene dejavnosti (npr. razširjenje sovražnega govora, otroške pornografije, napade na strežnike sovražnih držav itd.) (Kovačič, 2006).

Poznamo pa še drugo delitev: razdeli se na štiri generacije hekerjev, s katerimi se je pojem hekerja spreminjal skozi čas. Prva generacija, naj bi v 50. in 60. letih prejšnjega stoletja razvila prve programske tehnike. Drugo generacijo predstavljajo tisti posamezniki, ki so razvili prve osebne računalnike in s tem omogočili dostop računalniške tehnologije širšim množicam. Tretjo generacijo označujejo vodilni razvijalci računalniških iger. Četrto pa tisti, ki na nedovoljene načine vstopajo v tuje

računalnike. Po samodefiniciji pa se hekerji v hekerskem slovarju (Jargonfile) opisujejo kot »ljudje, ki uživajo v raziskovanju računalniških sistemov in iskanju novih načinov njihove rabe; ljudje, ki navdušeno (celo obsedeno) programirajo… ljudje, ki uživajo v intelektualnih izzivih v aktivnem premagovanju in zaobhajanju omejitev«. (Kovačič, 2006)

Sodobni avtorji vnašajo nove pojme in izpeljanke hekerjev. Izraz heker tako opisuje osebo, ki ima o računalnikih veliko znanja, vendar tega znanja ne izkorišča za slabe namene, medtem ko se za osebe, ki to znanje zlorabljajo za napade na sisteme z namenom lastne koristi ter povzročanjem škode, uporablja izraz kreker (ang. cracker). Izraz kreker se uporablja tudi za posameznike, ki se ukvarjajo z obratnim inženirstvom programske opreme, predvsem z namenom razbijanja zaščite programov pred kopiranjem. Za hekerje s slabimi nameni se včasih uporablja izraz »črni hekerji« (ang. black hat). Za razliko od njih t.i. »beli hekerji« (ang. white hat) poudarjajo, da spoštujejo določena etična načela, predvsem se izogibajo namernemu povzročanju škode. Poleg njih pa se vdorov v sisteme poslužujejo še t.i. skriptarji (ang. Script kiddie), to je tistih, ki nimajo pretiranega računalniškega znanja, pač pa za vdore izkoriščajo znane varnostne luknje, ki so jih odkrili drugi, ali uporabljajo javno dostopna vdiralska orodja. Nasprotno od krekerjev, ki so visoko motivirani in vdrejo v točno določene sisteme, pa skriptarji navadno ne iščejo točno določenih žrtev, pač pa po internetu povsem naključno iščejo slabo zaščitene strežnike, v katere potem poizkušajo vdreti. Vdiralci v sisteme sicer lahko vdirajo tudi s kriminalnimi ali terorističnimi nameni, zaradi industrijskega vohunjenja ali iz maščevanja, vendar gre pri večini teh oseb za samodokazovanje, zabavo ali vandalizem (Kovačič; 2003).

Izraz »spackers« je nastal konec leta 2003 v Wired magazinu, gre pa za skovanko angleških besed »spammer« in »cracker«. Speckerji naj bi bili tako posamezniki, ki vdirajo v računalniške sisteme z namenom pošiljanja nezaželjene elektronske pošte. Izraz pa se uporablja tudi za tiste, ki postavljajo lažne spletne strani, po katerih prodajajo različne dvomljive ali celo nezakonite izdelke ali storitve, te spletne strani pa pogosto oglašujejo z nezaželeno elektronsko pošto (Kovačič, 2006).

3.2 Iskalniki

Določene informacije o posameznikih, ki jih je bilo včasih težko odkriti, še težje pa povezovati, so danes preko internetnih iskalnikov lažje dostopne.

Vsa sporočila, ki jih pošiljamo na razna javna dostopna mesta (forumi, novičarske skupine…), so dostopna vsakomur in še leta dolgo lahko ostanejo shranjena. Z iskalniki, kot so na primer google, najdi.si, yahoo… bodo še naši zanamci lahko prebrali naša elektronska sporočila. Google na primer ima preko 8 bilijonov zapisanih informacij o internetnih straneh za kasnejšo uporabo, ki jih ne briše.

Tak primer je »Google Toolbar«, ki je programski dodatek k spletnim brskalniku, ki ga je razvilo podjetje Google, ki trenutno upravlja največji spletni iskalnik na svetu. Uporabniku omogoči uporabo Googlovih storitev neposredno iz brskalnika, ne da bi mu bilo treba iti na Googlovo spletno stran. Vendar pa Google Toolbar omogoča tudi spremljanje uporabniških spletnih dejavnosti, ki se posredujejo v nadaljnjo analizo

Googlu. Iskalniki lahko na podlagi teh podatkov in podatkov o uporabljenih iskanih pojmih izvajajo profiliranje uporabnikov in s tem izboljšujejo svoje storitve, zato so seveda zelo zainteresirani za njihovo zbiranje. Ob namestitvi Googlove orodne vrstice je uporabnik sicer jasno seznanjen s tem, kateri podatki se zbirajo in za kakšen namen, in da so anonimmizirani. Prenašanje teh podatkov lahko tudi izključi, vendar je privzeta nastavitev taka, da je zbiranje in prenašanje teh podatkov vključeno (Kovačič, 2006).

3.3 Piškotki

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). Piškotki so majhni paketi podatkov, ki jih spletni strežnik pošlje spletnemu brskalniku, ta pa jih shrani v uporabnikov računalnik in jih vrne strežniku, ko ta to od njega zahteva. Strežnik lahko nastavi čas veljavnosti piškotka in določi, kateri del spletnega strežnika ima lahko dostop do njega. Po času trajanja ločimo t. i. sejne piškotke (ang. session cookies) in trajne piškotke (ang. persistent cookies). Prvi potečejo ob koncu brskalne seje, torej ko uporabnik zapre spletni brskalnik, drugi pa imajo čas trajanja daljši, lahko tudi več let. Piškotek je strežniku dostopen ves čas trajanja, če ga seveda uporabnik prej ne izbriše. Poleg tega ločimo piškotke obiskane spletne strani (ang. first-party cookies) in piškotke, ki jih pošiljajo tretje spletne strani, ki so vključene v obiskano spletno stran (ang. third-party cookies). Razlikovati so jih začeli šele pred nekaj leti, pomembno pa je, da piškotke tretjih spletnih strani večinoma uporabljajo oglaševalska omrežja, namenjeni pa so sledenju uporabnikov.

Piškotek ima navadno interno identifikacijsko številko uporabnika in ko se uporabnik giblje po spletnem mestu, lahko spletni strežnik te identifikacijske številke zapisuje. Seveda pa se da to identifikacijsko številko povezati tudi s kakšnimi drugimi podatki, na primer z identifikacijskimi podatki posameznika. Tako lahko spletni strežnik pri naslednjem obisku uporabnika ugotovi, če je uporabnik na spletni strani že bil in kaj je na njej počel. Piškotki so bili prvotno razviti z namenom, da bi omogočili spletne nakupne košarice, danes pa jih množično uporabljajo na vseh vrstah spletnih strani. Na piškotke zato lahko gledamo kot na razpršeno zbirko podatkov, saj so podatki o obiskovalcih razpršeni po računalnikih obiskovalcev spletne strani.

Digitalni piškotki omogočajo tudi avtomatizacijo v poslovnih spletnih aplikacijah, kar je uporabno predvsem v elektronski trgovini, ker povečajo interaktivnost same spletne strani. Ne glede na to, da so digitalni piškotki zelo močno in koristno orodje na področju interaktivnih poslovnih spletnih aplikacij (bančništvo, oglaševanje…) lahko predstavljajo tudi veliko grožnjo zasebnosti uporabnika ter storitev:

1. Pomanjkanje varnosti: V piškotkih so pogosto shranjeni tudi občutljivi osebni podatki, ki se nezavarovani prenašajo preko spleta. Vsebina je teoretično zelo lahko dosegljiva vsakomur, ki piškotek prestreže. Prav bi bilo, da bi bila vsebina piškotka zakodirana, vendar ponavadi uporabnik na to nima vpliva. Načeloma imajo uporabniki zelo malo nadzora nad varnostnimi ukrepi, ki zajemajo shranjevanje in prenos piškotkov.

2. Opazovanje: Piškotki predstavljajo mehanizem, ki dovoljuje spletni strani zapisovanje naših internetnih aktivnosti, ponavadi brez naše vednosti ali dovoljenja. Preko identifikacijske številke lahko spletni strežnik ugotovi, kaj je uporabnik počel na spletni strani, lahko pa sledi uporabniku tudi na ostale spletne strežnike. Za mnoge ljudi predstavlja takšno beleženje aktivnosti napad na 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: Komercialne spletne strani, ki si pridobivajo osebne podatke preko piškotkov, lahko te podatke izmenjujejo z drugimi spletnimi stranmi. To pomeni, da uporabnik, ki spletni strani zaupa, pusti svoje osebne podatke, le-ta pa jih lahko posreduje tretji spletni strani, na kateri mogoče uporabnik sploh ni bil, niti jim ne bi zaupal svojih osebnih podatkov.
4. Omejen nadzor: Končni uporabnik ima žal zelo malo možnosti nadzora nad vsebino in uporabo piškotkov; za povprečnega uporabnika je to predvsem nevidna tehnologija. Večina spletnih brskalnikov omogoča uporabniku funkcijo izklopa piškotkov (oz. možnost, da jih ne sprejmejo), vendar postanejo tako nekatere spletne strani neuporabne. Če pa se uporabnik odloči, da piškotek sprejme, se zgodi, da nima nadzora nad njegovo vsebino in uporabo.
5. Zbiranje podatkov: Eden izmed načinov uporabe piškotkov je tudi zbiranje podatkov s pomočjo spletnega hrošča (ang. web bug). Spletni hrošč je nevidni grafični element (velikosti enega pixla, definiran kot HTML IMG tag), ki omogoča ugotovitev po katerih straneh se uporabnik giblje. Na ta način je možno ugotoviti brskalne navade posameznika. Ti podatki se lahko tudi povežejo z elektronskim naslovom posameznika, pa tudi z njegovo fizično identiteto. Fizično identiteto uporabnika je mogoče ugotoviti tako, da uporabnik zaupa svoje osebne podatke neki spletni strani v omrežje, podatki pa se potem povežejo z identifikacijsko številko piškotka (Seničar, et al., 2003; Kovačič, 2003).

Ta postopek omogoča ugotovitev, po katerih spletnih straneh v oglaševalskem omrežju se giblje posamezni uporabnik. Če je spletno oglaševalsko omrežje dovolj veliko, lahko na podlagi zbranih podatkov ugotovijo brskalne navade posameznega uporabnika, te podatke pa lahko povežejo z elektronskim naslovom posameznika in celo s t. i. off-line ali izven mrežno fizično identiteto. 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.

Obstaja tudi nevarnost, da se zbrani podatki ne uporabijo za tisto, za kar so bili zbrani. Kot navaja Kovačič v »Zasebnost na internetu«, pri bankomatu 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).

Tehnologijo piškotkov zakonodaja sicer dopušča, saj se lahko uporablja v povsem legitimne namene (analiziranje učinkovitosti spletnega oglaševanja, ugotavljanje istovetnosti uporabnikov storitev, olajša lahko zagotovitev nekaterih storitev informacijske družbe), vendar pod pogojem, da je uporabnik seznanjen z namenom

zbiranja teh podatkov. Uporabnik mora imeti možnost izbire ali bo sodeloval ali ne (opt in oziroma opt out možnost) (Možina, 2002).

3.4 Elektronske sledi

Najbolj pogosto uporabljena storitev v svetovnem komunikacijskem omrežju interneta je brskanje po svetovnem spletu, ki je omogočeno s HTTP protokolom. HTTP protokol deluje na podlagi izmenjave informacije med odjemalcem in spletnim strežnikom. 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 naslov, vrsta in verzija operacijskega sistema in brskalnika, ter URL lokacija pred obiskom trenutne spletne strani. Takšne informacije se prenašajo brez privolitve in vednosti uporabnika spletnega brskalnika. S pomočjo IP naslovov in tehnologije za izvedbo izvora TCP/IP paketov je mogoče določiti približno lokacijo uporabnika. Z vzpostavitvijo IP v6, ki vsebuje veliko bolj natančno informacijo o geografski lokaciji v ovojnici HTTP protokola, se bo vdor v zasebnost le še povečal. Podoben problem se pojavlja tudi pri ostalih internetnih protokolih (SMTP in FTP) (Seničar et al., 2003).

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. S pomočjo Jave in JavaScripta 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 priključke module ima naložene, oceno hitrosti dostopa do interneta, itd. Možno pa je ugotoviti tudi, ali ima uporabnik na svojem računalniku shranjeno kakšno avtorsko izvirno vsebino (film, glasba, knjige,…), za katero ni plačal avtorske pravice (Data Proteciton Working Party, 2000).

On-line aktivnosti, ki bi zagotavljala absolutno zasebnost ni in tega bi se morali uporabniki internetnih storitev zavedati. Če »surfamo« z domačega naslanjača, se nam zdi, da smo sami, nevidni, da smo anonimni. Na žalost temu ni tako. Obstaja možnost sledenja vseh on-line aktivnosti. Ugotoviti je mogoče, katere spletne strani smo obiskali, katere datoteke smo pobrali z interneta, do katerih novičarskih grup smo dostopali. Te informacije lahko zbirajo tako ponudniki internetnih storitev, preko katerih dostopamo do interneta, kot tudi lastniki spletnih strani. Če dostopamo do interneta na delovnem mestu, se moramo zavedati, da tudi delodajalci pogosto izvajajo nadzor nad tem, katere strani obiskujemo.

Večina spletnih strani zabeleži vsak obisk: zapiše se IP naslov in naslov spletne strani, ki jo ima uporabnik nastavljeno kot trenutno, prav tako se zabeleži datum obiska. IP naslov računalnika omogoča povezovanje z drugimi sledmi, ki vsebujejo isti IP naslov. Na ta način spletni ponudniki ugotavljajo obnašanje oziroma spletne navade uporabnikov, v mnogih primerih pa lahko preko IP naslova celo enolično identificirajo aktualnega uporabnika.

3.5 Rudarjenje

Rudarjenje podatkov (ang. data minig) 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. Pomeni tudi pridobivanje podatkov preko podatkovnih zbirk podjetij z namenom odkriti vzorce potrošniškega obnašanja. V novejšem času govorimo predvsem o spletnem rudarjenju, ki se pojavlja v dveh oblikah: rudarjenje glede na uporabnike spleta ter rudarjenje glede na spletno vsebino.

Rudarjenje pomeni niz avtomatiziranih postopkov (tehnik), ki se uporablja za izluščitev še nepoznanih delčkov informacij iz velikih podatkovnih baz. Iz teh podatkov se odkrivajo novi vzorci in odnosi, ki se uporabljajo pri poslovnem odločanju. Rudarjenje je tako usmerjeno na avtomatizirano odkrivanje novih dejstev in relacij med podatki. Pri tem se uporablja umetna inteligenca ter inteligentne tehnike, kot so živčna omrežja, matematični algoritmi, odločitvena drevesa, sklepanje…

Rudarjenje poteka v treh korakih:

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

Rudarjenje bo verjetno postalo eno največjih orodij za kapitalizacijo že obstoječih virov v poslovnem svetu, kajti informacija postaja širše dostopna, cena programske opreme pa se znižuje.

Z vse večjo uporabnostjo, predstavlja rudarjenje z vidika zasebnosti tudi vse večjo nevarnost, predvsem zaradi dejavnikov kot so:

1. Kvaliteta podatkov: Z rastjo interneta se je tudi za rudarjenju povečala količina podatkov iz različnih virov. Več podatkovnih baz je vključenih, večje je tveganje, da so podatki zastareli ali nenatančni, težje je njihovo čiščenje; kljub temu, da se podatki prečistijo, so le ti lahko netočni, nepopolni ali zastareli. Nenatančni, zastareli ali napačni podatki lahko povzročijo tudi nenatančno ali napačno interpretacijo.
2. Možnost dostopa: Potrošnik nima možnosti dostopa do teh podatkov, ne more jih pregledati, popraviti ali izbrisati.
3. Namen uporabe: Rudarjenje predstavlja drugo (ne za namen za katerega so bili podatki zbrani); nemogoče je na začetku procesa identificirati namen uporabe ter omejiti rezultate na enkratno rabo.

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

Enaka načela, kot veljajo za aktivnosti zbiranja podatkov na internetu, morajo veljati tudi za zbiranje podatkov s pomočjo tehnik rudarjenja. Dolžnost podjetij je, da informirajo uporabnike o rudarjenju, in ne uporabnikov, da sami ugotavljajo katera »on-line« podjetja uporabljajo prakso rudarjenja. Uporabnikom je potrebno jasno povedati, da so informacije o njih uporabljene tudi za rudarjenje, morali bi imeti vpogled v to, kako se te informacije sestavljajo in za kaj se uporabljajo. To obveščanje bi moralo biti odprto in pošteno. Postavljena morajo biti jasno definirana pravila o načinu rudarjenja, parametrih, času trajanja, uporabi… in potrošnik mora biti z njimi seznanjen. Večina uporabnikov se verjetno ne bi odločila za rudarjenje (opt out).

Uporabnikom je neprijetno ob dejstvu, da lahko računalnik predvidi njihove navade in interese. Zaskrbljeni so ob dejstvu, da lahko nekdo odkrije in pokaže napačne zaključke in rezultate. Spet drugi uporabniki pa v tem vidijo ugodnosti (direktno oglaševanje, finančne ugodnosti, popusti…) in se s takšnim načinom pridobivanja informacij strinjajo (opt in). Pomembno pri vsem tem je, da se uporabniku pove, kako so se podatki o njem uporabili in da se uporabnik sam odloči, ali bo sodeloval ali ne.

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

3.6 E-profiliranje

E-profiliranje je proces izgradnje podatkovne baze, ki vsebuje aktivnosti in lastnosti uporabnikov interneta, ki pa poteka preko zbiranja informacij, s sledenjem (monitoringom) s pomočjo uporabe piškotkov, kjer se zapisuje in klasificira obnašanje uporabnikov interneta. Tako se pridobi vzorec obnašanja uporabnikov, njegovo zanimanje in nakupovalne navade. Vse to se lahko shrani kot profil uporabnika v podatkovno bazo. 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 oblikovanja ponudbe in storitev ob obisku spletnih strani. Ti podatki so večinoma neosebni, lahko pa se povežejo s podatki, ki jih prostovoljno puščamo na internetnih straneh (ime, spol, starost, izobrazba…), elektronsko pošto, IP naslovom, demografijo, kar ustvari veliko natančnejši in bolj oseben profil uporabnika.

Profiliranje se uporablja predvsem za oblikovanje ponudbe in storitev spletnih strani, za osebno oglaševanje. Organizacije, ki se ukvarjajo s profiliranjem, trdijo, da je to le v dobro e-uporabnika oz. potrošnika, saj mu lahko ponudijo bolj osebno prilagojene storitve in proizvode glede na njegov profil. Kljub temu pa mnogi vidijo e-profiliranje kot vdor v njihovo zasebnost, saj se zbirajo in posredujejo osebni podatki brez uporabnikovega vedenja ali zavestne privolitve (Seničar, et al., 2003).

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). 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. 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 ali je na mestu nakupa prvikrat, 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. Amazaon.com se je na koncu potrošnikom tudi opravičil in jim dal možnost povrnitve preplačane vrednosti, če so uporabniki sumili, da so izdelek preplačali (Weiss, 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, 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).

Tehnologija danes omogoča organizacijam zbiranje informacij, izpeljanih iz neštetih podatkovnih baz, ki jih povezujejo med sabo ter tako gradijo izčrpne profile posameznikov, ki jih nato klasificirajo v različne grupe. Eden takšnih primerov v ZDA je Claritas, ki ima posameznike grupirane v 15 grup glede na lokacijo bivališča – od visoko elitnih četrti do najbolj ubožnih predelov mest. Te podatke Claritas prodaja za nizko ceno 65 dolarjev za tisoč imen (EPIC, 2004).

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

Profiliranje je do posameznika na videz prijazno, saj potrošnika potiska, kamor si sam želi, oziroma ga zalaga z dobrinami in vsebinami, ki ustrezajo njegovemu okusu in potrebam. Značilen primer so reklame, prilagojene zaznanemu okusu in predvidenim potrebam potrošnika. Velikokrat res nimamo možnosti izbire, dostikrat pa povsem prostovoljno vstopamo v ta sistem. Takšen primer so različne kartice zaupanja, kjer za majhne ugodnosti prostovoljno posredujemo osebne podatke in

kot navaja Kovačič iz sistema niti ne želimo izstopiti, saj nam na videz prinaša majhne popuste ali ugodnosti (Kovačič, 2003).

3.7 Prestrezanje 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.

Elektronska pošta se po internetu prenaša večinoma nešifrirano, kot navadno besedilo (plain text). Za napadalca ponavadi ne predstavlja prav težkega problema, saj je v nešifriranem sporočilu povsem enostavno iskanje določenih besed. Poleg tega imajo do elektronske pošte prost dostop upravitelji poštnih strežnikov in tudi upravitelji posredniških poštnih strežnikov, preko katerih se elektronska pošta prenaša. Pri prenosu elektronske pošte velja, da mora biti sporočilo s končnega in posredniškega poštnega strežnika izbrisano takoj, kot je bilo posredovano naprej, enako velja tudi za končni poštni strežnik uporabnika, razen če se uporabnik sam odloči, da bo sporočilo ohranil na svojem poštnem strežniku. 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. Pomembno je tudi ločevanje med prometnimi podatki, ki so nujni za prenos sporočila in zaračunavanje stroškov, ter osebnimi podatki in vsebino sporočila. S posebno programsko opremo oz. posebnimi nastavitvami je mogoče beležiti še veliko drugih podatkov, kot so število in velikost datotečnih prilog, uporabljeni nabor znakov, 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).

Kot ugotavlja Kovačič, je problem elektronske pošte predvsem v tem, da je tehnično videti kot razglednica, uporabniki pa jo uporabljajo kot zaprto pisemsko pošiljko. Kot zaprto pisemsko pošiljko jo obravnava tudi zakonodaja (Kovačič, 2003).

3.7.1 Nadzor elektronske pošte na delovnem mestu

Uporaba elektronske pošte na delovnem mestu je postala nezamenljiva: velikokrat nadomešča uporabo telefona, uporabo klasične pošte, ali zgolj hojo po stopnicah. Enostavno natipkamo sporočilo ter ga odpošljemo, pri tem se nam zdi, da je sporočilo osebno, da ga bo videl le naslovnik. Pozabljamo, da temu ni tako.

Marsikateri delodajalec kontrolira elektronska sporočila. Razlogi za to so različni, večinoma zaradi nevarnosti izdajanja poslovnih skrivnosti. Zaposleni sicer čutijo ta nadzor kot invazijo na njihovo zasebnost, vendar ameriška sodna praksa v tem pogledu pritrjuje delodajalcem, češ da gre za službeno pošto in ne zasebno. V Sloveniji takšen nadzor ni dovoljen oz. mora biti uslužbenec predhodno seznanjen z možnostjo nadzora in se mora z njim strinjati (Kovačič, 2003).

3.8 Neželena elektronska pošta ali smetje

Izraz smetje ali ang. spam (uporablja se tudi izraz unsolicited commercial e-mail (UCD), unsolicited bulk e-mail (UBE) ali junk mail) označuje nezaželena oziroma nenaročena elektronska sporočila, pri čemer gre večinoma za oglasna elektronska sporočila. Smetje je eden izmed resnih problemov interneta, saj so raziskave pokazale, da se količina takih sporočil veča in je leta 2003 obsegala že več kot 50% vseh sporočil. To bi celo utegnilo uničiti uporabnost elektronske pošte. Oglaševanje z nenaročeno elektronsko pošto je izredno poceni in se podjetjem splača že, če se odzove le peščica potrošnikov. Nekaterim se zdi ta način oglaševanja nemoteč, medtem ko drugi občutijo to kot nadlegovanje, ki jim povzroča velike preglavice, celo takšne, da so prisiljeni zamenjati poštni naslov. Smetje je zaradi možnosti velikih zaslužkov tudi eden izmed pomembnih dejavnikov za razmah kiberkriminala. A omejeno ni samo na elektronsko pošto, temveč so ga pošiljali tudi na USENET oz. prek interaktivnih sistemov za klepet po internetu (MSN, ICQ, itd. t. i. SPIM). V zadnjem času pa je priljubljena posebna oblika smetja, ko pošiljatelj dopisuje reklamne komentarje v t. i. spletne dnevnike (ang. blog). Čeprav smetje ne pomeni neposrednega vdora v zasebnost v sistemu nadzorovanja, pa ga lahko štejemo za poseg v pravico biti puščen pri miru, skratka v tisti del zasebnosti, ki posamezniku omogoča, da se umakne iz družbe. Neželena elektronska pošta je nelegitimna in nepoštena komunikacija, ki poteka v eno smer. Največja težava je, da je dejansko nemogoče odkriti pošiljatelja sporočila.

Nekateri poštni strežniki imajo namreč nameščene posebne programe, ki pošto pregledujejo in skušajo ugotoviti, ali je sporočilo okuženo z virusom oziroma ali gre za t. i. spam. Vsekakor velja, da programi ne smejo posredovati okužene ali spam pošte nobeni tretji osebi (Data Proteciton Working Party, 2000). Kadar so ti programi nameščeni brez soglasja ali celo vednosti uporabnikov, nastajajo tudi zanimiva pravna vprašanja, ali je to dopustno ali ne. Če je filtriranje (brisanje) spam pošte po merilih, ki jih uporabnik morda ni odobril, je to pravno že nekoliko bolj sporno. Kljub nekaterim pravnim prazninam pa imajo uporabniki elektronske pošte možnosti le-to zavarovati s kriptografijo.

Neželena in nenaročena elektronska pošta – »spam« poleg problema zasebnosti predstavlja tudi velik ekonomski problem. Po poročilu Ferris Research je neželjena elektronska pošta stala ameriška podjetja v letu 2003 10 bilijonov dolarjev v izgubljeni produktivnosti. Po neželenem vmešavanju na omrežju neželena elektronska pošta že prekaša viruse. Kot navaja poročilo (Protecting Privacy and Fighting Spam, 2006) neželena elektronska pošta ni nepomemben pojav, kajti samo v decembru 2003 je bilo v državah EU več kot polovica prometa elektronske pošte neželene. To pa že predstavlja masovno invazijo na zasebnost, prevaro potrošnikov, nenadzorovano gibanje škodljive vsebine, velike stroške za podjetja, zmanjšano produktivnost in zaviranje rasti informacijske družbe v celoti.

Najbolj občutljive so tiste informacije, ki jih lahko direktno povežemo s posameznikom. Elektronski poštni naslov spada v to kategorijo: enostavno in učinkovito lahko pridemo v kontakt z naslovnikom. Ko si tretja stranka pridobi naslov brez privolitve, pomeni to kršitev zasebnosti naslova. Cena takšne kršitve zasebnosti je različna med posamezniki, celotna cena pa je zelo visoka.

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

Danes pošiljajo že preko bilijon neželene elektronske pošte po vsem svetu, ne glede na to, ali bodo imeli od tega kakšen dobiček ali ne (neželeno elektronsko pošto pošiljajo ne glede na jezik, ne glede na razumevanje sporočila. Neželena elektronska pošta je mednarodni problem in edino skupna mednarodna »prekomejna« politika lahko razvije legalno orodje potrebno za uspešen boj proti njihovim pošiljateljem. Samo mednarodno koordinirana akcija je lahko uspešna v boju zoper neželeno elektronsko pošto.

3.9 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 (ang. robot, spider, worm). Najpogosteje so namenjeni zbiranju elektronskih naslovov, ki se kasneje uporabljajo pri pošiljanju nezaželene elektronske pošte. 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.

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

Neosveščenost uporabnikov interneta in podcenjeno tveganje v veliki meri še povečuje stopnjo ogroženosti. Za bolj lagodno življenje smo namreč pripravljeni razkriti marsikateri podatek, ki je lahko kasneje zlorabljen in predstavlja poseg v našo zasebnost.

Nekatere spletne strani prodajajo podatke o svojih uporabnikih kljub obljubi, da tega ne bodo storile. Spletni iskalnik AskJeeves je od spletne strani ETour.com odkupil bazo z osebnimi podatki 2,2 milijona piscev novic, kljub obljubi, ki jo je dal Etour

svojim uporabnikom, da osebni podatki v nobenem primeru, nikoli ne bodo posredovani naprej »tretji strani«. Baza je obsegala podatke o uporabnikovem imenu, elektronskem naslovu, starosti, spolu (Hinde, 2002).

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 uporabljajo v drugačne namene, kot naj bi se. Zbiranje podatkov lahko poteka preko registracije različnih programov (Kovačič, 2003).

3.10 Vdiranje v sisteme

Vdiranje v računalniške sisteme je eden izmed najbolj neposrednih napadov na zasebnost. Do njega sicer lahko pride zaradi malomarnosti pri postavitvi in vzdrževanju sistemov, npr. zaradi nepravilno nastavljenih pravil za dostop do datotek ali slabo napisanih programov (značilen primer so npr. spletni programi, ki ne preverjajo ukazov za delo z bazami), navadno pa gre pri vdiranju v sisteme bolj za sofisticirane načine iskanja varnostnih pomanjkljivosti in njihovo izkoriščanje. Praviloma to zahteva veliko računalniškega znanja, vendar pa se je v zadnjih letih začelo korenito spreminjati.

3.10.1 Trojanski konj

Trojanski konj je zlonamerni program, ki se za razliko od virusov, ne širi samodejno, niti ne more okuževati drugih datotek v računalniku. Trojanski konji se navadno »pretvarjajo«, da so povsem običajni programi (od tod tudi njihovo ime), njihove skrite funkcije pa so najbolj pogosto namenjene odpiranju t. i. stranskih vrat na žrtvinem računalniku, kraji gesel ali povzročanju druge škode.

Leta 1995 sta računalniška programerja Wietse Venema in Dan Farmer objavila na internetu program SATAN (Security Administrator's Tool for Analyzing Networks), ki po internetu ali lokalnem omrežju išče varnostne luknje v računalniškemu sistemu. Program je namenjen odkrivanju, ne pa tudi izkoriščanju varnostnih lukenj, avtorja pa sta ob njegovi brezplačni objavi na internetu zatrdila, da je namenjen predvsem upraviteljem računalniških sistemov za izboljšanje varnosti njihovega lastnega sistema. Tri leta pozneje, leta 1998, pa je skupina računalniških hekerjev, zbranih v skupini Cult of the Dead Cow, na svoji spletni strani objavila trojanskega konja Back Orifice, ki je namenjen oddaljenemu nadzorovanju računalnikov, na katerih teče operacijski sistem Windows. Back Orifice je sistem za oddaljeno upravljanje z računalnikom oziroma programski paket, ki na računalniku odpre t.i. stranska vrata (ang. back door), skozi katera sta napadalcu omogočeni oddaljeno nadzorovanje in upravljanje z računalnikom prek interneta, ne da bi lastnik tega nadzorovanega računalnika to opazil. Program je zelo preprost za uporabo, saj ne zahteva kakšnega posebnega računalniškega znanja, poleg tega pa je popolnoma brezplačen. Edini problem je le, kako podtakniti ta program na računalnik žrtve. Hkrati s pojavom programa Back Orifice se je na internetu pojavil tudi konkurenčni program NetBus, ki je prav tako namenjen oddaljenemu nadzorovanju računalniških

sistemov. Danes je na internetu brezplačno dostopnih čedalje več orodij za nadzorovanje in vdiranje v računalniške sisteme, ki od uporabnika ne zahtevajo skoraj nobenega znanja. (Kovačič, 2006)

3.10.2 Virusi

S pojmom računalniški virus včasih poljudno označujemo vse programe ali programske kode, namenjene povzročanju škode ali obremenjevanju računalniških sistemov, ki so se hkrati sposobni sami širiti, vendar brez natančno določenega cilja. Virusi pa niso nujno le destruktivni.

Maja 2000 je bivši direktor CIE R. James Woolsey opozoril na novo vrsto virusov – instruktivne viruse. Ti naj bi se širili čim bolj neopazno in za svoje delovanje uporabili kar najmanj zmogljivosti sistema, njihov namen pa naj bi bila kraja podatkov (recimo seznama elektronskih naslovov iz uporabnikovega adresarja), spreminjanje vsebine datotek ali elektronsko prisluškovanje (Kovačič, 2006).

V začetku leta 2003 se je razširil prvi računalniški virus, katerega namen ni bil samo širjenje in povzročanje škode, temveč pošiljanje nezaželene elektronske pošte. Virus W32.SoBig.E se je širil po računalnikih z nameščenim operacijskim sistemom Windows in jih spreminjal v t.i. zombije (Kovačič, 2006).

3.10.3 Vohunski programi

Včasih imajo programi že vnaprej vgrajene skrite nadzorovalne zmogljivosti. Pogosto so to tako imenovani vohunski programi (ang. spyware), ki zberejo neke podatke (največkrat s tržno vrednostjo, kot npr. elektronski naslov in brskalne navade), nato pa jih pošljejo na strežnik avtorjev programa. Za take programe se včasih uporablja tudi izraz E. T. aplikacije, ker potem, ko zberejo podatke, »pokličejo domov« (izraz se je razvil na podlagi zgodbe iz filma E. T.).

Med vohunske programe naj bi spadale tudi nekatere različice programov Real Player ter 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. Microsoft je to sicer zanikal, ni pa dvoma, da so tehnične možnosti za kaj takega obstajale. (Kovačič, 2006)

Vendar pa mehanizmi nadzora niso vgrajeni samo v proizvode manj znanih podjetij, pač pa tudi v najbolj razširjene računalniške aplikacije. Na začetku leta 1999 se je namreč pojavil makrovirus Melissa, FBI pa je avtorja uspelo izslediti v presenetljivo kratkem času. Glede na to, da je bil za pisanje virusa uporabljen skriptni jezik, ki je del MS Office okolja, je seveda takoj nastalo vprašanje, kako je FBI uspelo med milijoni uporabnikov MS Officea odkriti pravega avtorja. Izkazalo se je, da je dal Microsoft v Office 97 potihem vgraditi t. i. GUID, globalni univerzalni identifikator, ki se zapiše v vsaki 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. Zaradi tega so nastala resna vprašanja, ali ni mogoče takšno tehnologijo zlorabiti tudi v drugačne namene, ne samo za odkrivanje piscev virusov, pač pa, na primer,

tudi za odkrivanje političnih nasprotnikov. Tudi zato direktiva EU 2002/58 o obdelovanju osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij opozarja, da vohunski programi in skriti identifikatorji resno ogrožajo pravico do zasebnosti in zato določa, da smejo biti uporabljeni le v zakonite namene in z vednostjo uporabnikov (Možina 2002).

Poleg tega imajo današnji računalniški sistemi veliko varnostnih lukenj, za katere se sicer hitro najdejo ustrezni popravki, vendar si jih njihovi uporabniki ne namestijo dovolj hitro, včasih pa si jih sploh ne, ker zanje niti ne vedo. Ker so varnostne luknje navadno dobro dokumentirane (čeprav je res, da je prave informacije včasih težko najti), uporabniki pa popravkov ne namestijo, lahko od hekerjev, zasebnih podjetij in tudi državnih organov pričakujemo naraščanje vdorov in poskusov vdorov v računalniške sisteme.

O varnostnih luknjah v okolju Windows skoraj redno poročajo internetni časopisi, kot npr. Crypto-Gram (http: //www.counterpane.com/crypto-gram.html) ali Security Focus (http://www.securityfocus.com*),* veliko tovrstnih infomacij pa je dostopnih tudi na spletnih strežnikih podjetja Microsoft (http: //microsoft.com/technet/security/).

3.10.4 Roboti, pajki ali črvi

Roboti, pajki ali črvi (ang. spider, worm, harvester) so programi za zbiranje podatkov iz spleta, pogosto so namenjeni zbiranju elektronskih naslovov. Programi iščejo po spletnih straneh pa tudi po spletnih forumih, novičarskih skupinah in arhivih poštnih seznamov. Upravitelji, ki želijo takšno zbiranje preprečiti, sicer lahko določijo področje spletnega strežnika, kjer je vstop robotom prepovedan, vendar ni nujno, da se roboti teh navodil držijo. Zato se pri objavi nekaterih podatkov, predvsem elektronskih naslovov, mnogokrat uporabljajo različni triki, ki robote zmedejo tako zelo, da podatka niso več sposobni prepoznati kot elektronski naslov.

Roboti se obnašajo povsem kot običajni spletni brskalniki, mogoče pa jih je prepoznati po vrednosti posebne okoljske spremenljivke, ki vsebuje podpis spletnega brskalnika (USER_AGENT). Vendar pa ni nobenih tehničnih ovir, da se robot ne bi izdajal za povsem običajen spletni brskalnik.

4 TEHNOLOGIJE ZA BOLJŠE VAROVANJE ZASEBNOSTI

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 kadarkoli 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.

Razvoj tehnologij sicer že danes omogoča tudi zaščito zasebnosti, vendar bo v bodoče potrebno še več napora usmeriti v učinkovito varovanje zasebnosti. Kot navaja Hübnerjeva, predstavlja razvoj tehnologij za zaščito zasebnosti velik korak naprej, vendar to še ni zadosten pogoj za celovito zaščito posameznikove zasebnosti. Poleg ustrezne tehnologije je potrebno zagotoviti zaščito zasebnosti tudi:

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

(Fischer-Hübner, 2001).

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

Problem varnosti in s tem tudi zasebnosti namreč ni samo tehnični, pač pa tudi družbeni problem. To tudi pomeni, da bi se morali uporabniki računalnikov bolj zavedati nevarnosti različnih zlorab, predvsem pa, kako se proti njim kar najbolje zavarovati. Kljub temu da noben sistem ni stoodstotno varen, pa je s samozaščitnim ravnanjem mogoče varnost precej povečati. Predvsem se je treba zavedati, da varnost ni izdelek oziroma nekaj, kar lahko kupimo, pač pa je proces. Varnostno kulturo je treba razviti in gojiti neprestano. Pri tem si lahko veliko pomagamo že z razumnim ravnanjem, pa tudi s specializiranimi programi, ki so večinoma poceni, marsikateri izdelek pa je na internetu dostopen tudi povsem brezplačno.

Nove vrste tehnologij, tako imenovane tehnologije za boljšo zaščito zasebnosti (Privacy Enhancing Technologies – PETs), so bile ustvarjene z namenom povečevanja posameznikovega nadzora nad podatki, ki jih želijo razkriti v elektronskih transakcijah. Njihov namen je izenačiti moč med posameznikom in celoto 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):

1. anonimnost (ang. Anonymity*);* možnost uporabe spletnih storitev in virov, pošiljanje in sprejemanje elektronskih sporočil brez razkritja svoje identitete,
2. psevdonimnost (ang. Pseudonymity*);* možnost, da uporabnik pod psevdonimom uporablja spletne storitve in vire, pošilja in sprejema elektronska sporočila brez razkritja svoje identitete,
3. nepovezljivost (ang. 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 (ang. Unobservability*);* možnost uporabe spletnih storitev in virov brez nadzora tretje stranke.

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

Avtor poročila »The Voiding of Privacy« tehnologije za boljšo zaščito zasebnosti klasificira v tri kategorije (Stalder, 2002):

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):

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).*

4.1 Tehnologije zaščite na osebni ravni

4.1.1 Kriptografija (šifriranje)

“Kryptos logos” pomeni po grško skrita beseda. Kriptologija je veda, ki vključuje dva pojma: kriptografijo in kriptoanalizo. Kriptografija predstavlja pretvorbe podatkov v tajno – nečitljivo obliko s pomočjo kriptografskega algoritma. Nasprotni proces kriptografije oziroma šifriranju pa je kriptoanaliza, to je dešifriranje oziroma razkritje šifriranih podatkov, za kar pa je potrebno poznati kriptografski ključ (Kovačič, 2003).

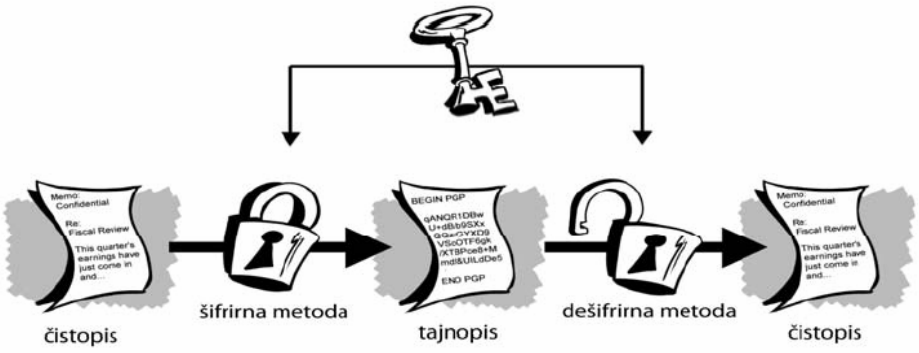
Kriptografija je ena izmed najbolj znanih in učinkovitih tehnik zaščite podatkov in zasebnosti. Zagotavlja zaupnost med udeleženci, ki želijo med sabo komunicirati. Sporočilo, ki ga pošiljatelj želi poslati, s pomočjo šifrirane metode zakrije (zašifrira) ter nato pošlje šifriran tekst. Če tak šifriran tekst prestreže napadalec, mu ne pove nič, teksta ne more dešifrirati, lahko samo spremlja promet. Prejemnik prejme šifriran tekst ter ga s pomočjo dešifrirane metode dešifrira ter tako dobi sporočilo, ki mu ga je poslal pošiljatelj.

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 s 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.

V kriptografiji imenujemo temeljno sporočilo čistopis (ang. cleartext, plaintext), zašifrirano pa šifropis ali tajnopis (kriptogram, ciphertext). Čistopis po nekem postopku spremenimo v tajnopis, pri tem pa upoštevamo neke vrednosti za parametre v šifrirnem algoritmu. Tem vrednostim pravimo ključ ali geslo. Sogovornika se morata torej dogovoriti o algoritmu in ključu, da si lahko pošiljata šifrirana sporočila. Z vidika šifrirnega in dešifriranega ključa poznamo dve vrsti kriptografije:

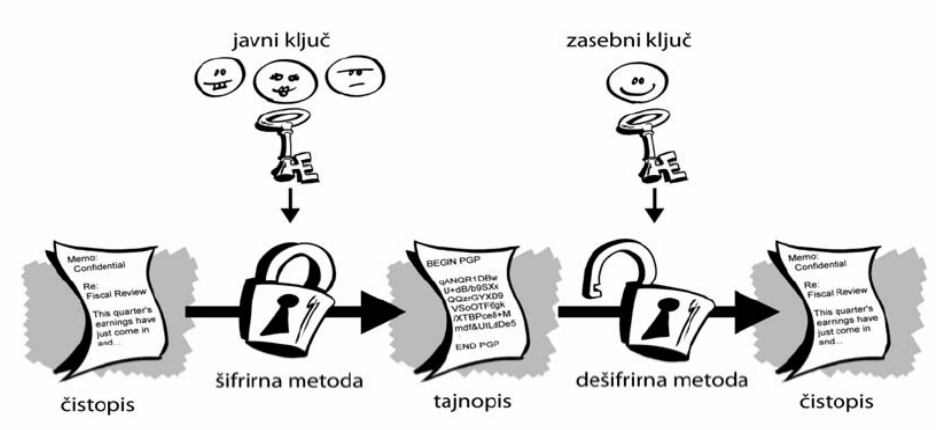
1. simetrično ali konvencionalno, ki za šifriranje in dešifriranje sporočila uporablja isti ključ (isto geslo - glavni problem: kako prenesti ključ do prejemnika, ne da bi ga tretja stranka prestregla), in
2. asimetrično ali šifriranje z javnim ključem, pri katerem je ključ za šifriranje različen od ključa za dešifriranje.

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.



Slika 1: Simetrična metoda šifriranja (Vir: How to PGP works, 2008)

Problem uporabe simetrične kriptografije v javnih omrežjih je izmenjava ključa. Vsak prejemnik šifriranega sporočila mora pri sebi imeti ključ s katerim je bilo sporočilo zaščiteno, da lahko sporočilo dešifrira. Zato si morajo udeleženci v komunikaciji pred prvo vzpostavitvijo zveze ključe izmenjati, najbolje osebno, če želijo skrivnost ohraniti zase. V današnjem času pa je tak postopek skoraj nemogoč, zato se simetrični algoritmi uporabljajo le v manjših zaključenih skupinah ali pa v kombinacijah z drugimi algoritmi, ki omogočajo varno izmenjavo ključev (Jerman-Blažič, 2002).



Slika 2: Asimetrična metoda šifriranja (Vir: How to PGP works, 2008)

Poleg simetričnih in asimetričnih algoritmov poznamo tudi zgostitvene algoritme, ki poljubno dolg niz znakov preslikajo v število fiksne dolžine, kar pomeni, da izračunajo t. i. prstni odtis tega niza znakov, kar je osnova za digitalni podpis. Z uporabno kombinacije kriptografskih metod, metod za digitalno podpisovanje in z uporabo potrdil, ki vsebujejo npr. čas nastanka, podatke o lastniku, rok veljavnosti ipd., lahko zagotovimo zaupnost, celovitost in overjanje sporočila (Kovačič, 2003).

Eden pomembnejših mejnikov v razvoju kriptografskih algoritmov predstavlja leto 1976, ko je inženir Sun Microsystemsa Whitfield Diffie skupaj z Martinom Hellmanom z Stanfordske univerze razvil asimetrično šifrirano shemo imenovano tudi sistem javnih ključev (Horniak, 2004).

Pri tem sistemu ključa za šifriranje in dešifriranje nista več enaka, pošiljatelj in prejemnik imata vsak par ključev: javnega, ki je javno objavljen in zasebnega, ki ga obdržita v tajnosti. Prednost te metode je v tem, da ni več potrebnih »tajnih kanalov« za distribucijo ključev.

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

4.1.2 Steganografija

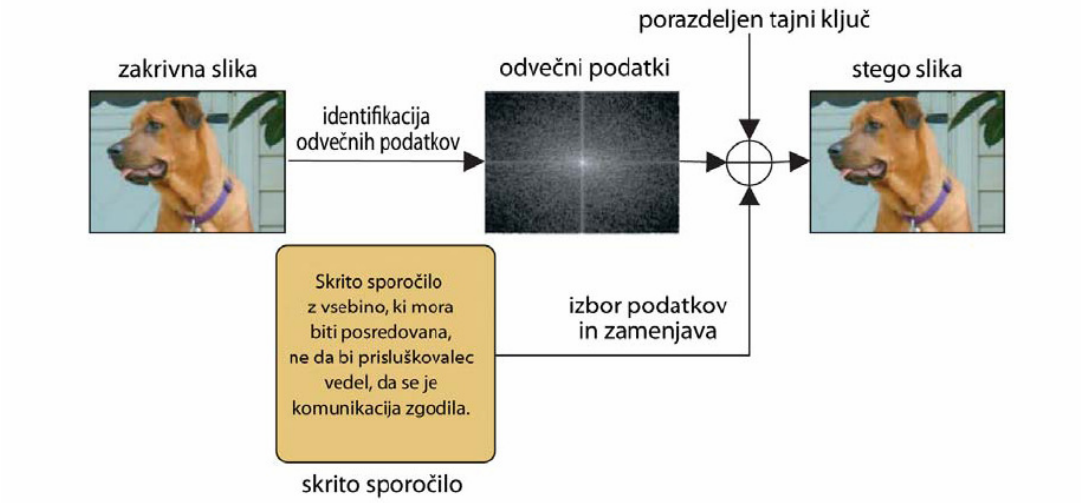
Steganografija je prav tako kot kriptografija zelo stara veda, poznana že iz antične Grčije in pomeni »zakrito pisanje«. Gre za sklop metod za skrivanje informacij v druge informacije. Sprva je bila steganografija le slab približek kriptografiji. Danes pa vse bolj pridobiva na popularnosti, predvsem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

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

Ponavadi pa samo šifriranje ni dovolj, saj uporabnik želi skriti tudi samo dejstvo, da so podatki šifrirani. To lahko stori s pomočjo steganografije; umetnosti skrivanja znakov znotraj samih znakov, kar pomeni, da so občutljive informacije shranjene znotraj popolnoma nedolžne datoteke. Tehnologija steganografije 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.

Obstajata dve varianti steganografskih sistemov glede na namen uporabe:
1. puščanje prstnih odtisov (fingerprinting): skrivanje informacij v datoteke, kjer izkoriščajo prazen prostor v datotekah (skrivanje serijskih številk),
2. digitalni vodni tisk: uporablja se za vstavljanje informacij o licenci, lastništvu, avtorskih pravicah…

Tajnost steganografskega procesa je odvisna od tajnosti steganografskega ključa.



Slika 3: Primer uporabe steganografije (Vir: Provos, Honeyman, 2003)

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

1. skrivanje podatkov v slikovne datoteke s pomočjo navideznega povečanja števila barv,
2. skrivanje podatkov v zvočne datoteke za človeško uho neopaznim popačenjem digitalne oblike zvoka,
3. skrivanje podatkov na neuporabljene sektorje disket in CD-jev;
4. Skrivanje podatkov v HTML datoteke,
5. skrivanje podatkov v ASCII datoteke (s pomočjo zamika kazalca za začetek datoteke),
6. s pomočjo programa, ki binarno datoteko pretvori v nesmiseln tekst, ta pa je statistično podoben tekstu v poljubnem naravnem jeziku (imeti moramo slovar za ta jezik) (Kovačič, 2009).

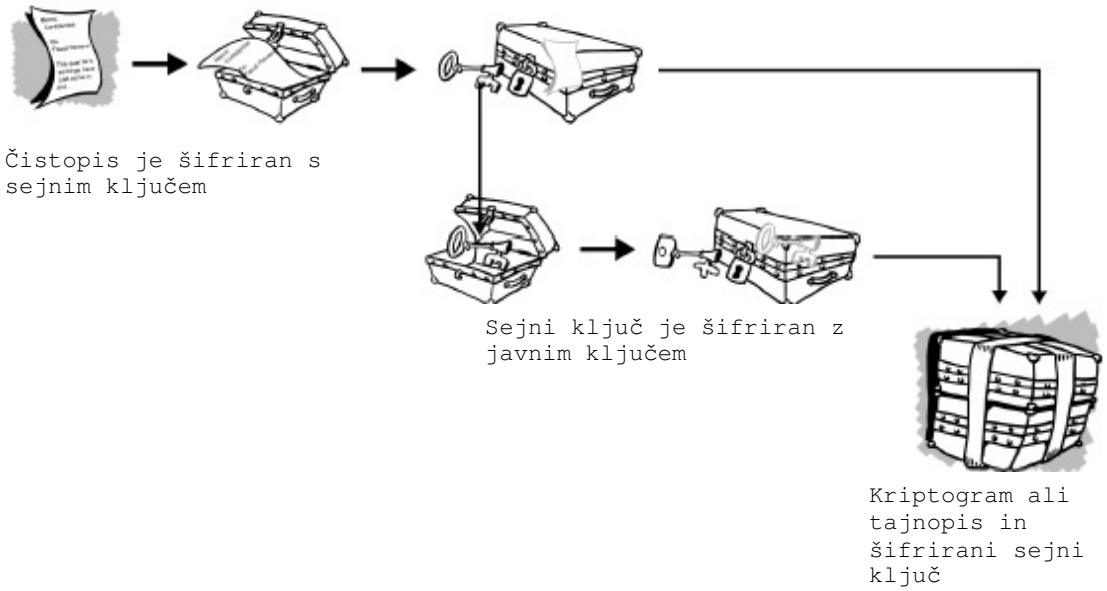
4.1.3 PGP (Pretty Good Privacy)

PGP je računalniški program, ki ga je leta 1991 napisal računalniški programer Phil Zimmerman in ki je namenjen za kodiranje vsebine datotek in elektronskih sporočil na osebnem računalniku. Je hibriden kriptosistem, ki združuje tako simetrično kriptografijo kot kriptografijo javnih ključev. To pomeni, da imata tako pošiljatelj, kot prejemnik vsak svoj par javni in tajni ključ. Javni ključ javno objavita, tajnega pa obdržita zase. Kodiranje poteka tako, da pošiljatelj sporočilo zakodira s prejemnikovim javnim ključem in svojim tajnim ključem. Prejemnik pa sporočilo lahko dekodira samo s pošiljateljevim javnim ključem in svojim tajnim ključem. Bazira na obstoječih standardiziranih algoritmih, kot so RSA, IDEA in MD5.

RSA algoritem je implementiran v kodiranje z javnim ključem, temelji na dejstvu, da je enostavno pomnožiti dve veliki praštevili, ter težko ti dve števili izluščiti iz produkta.

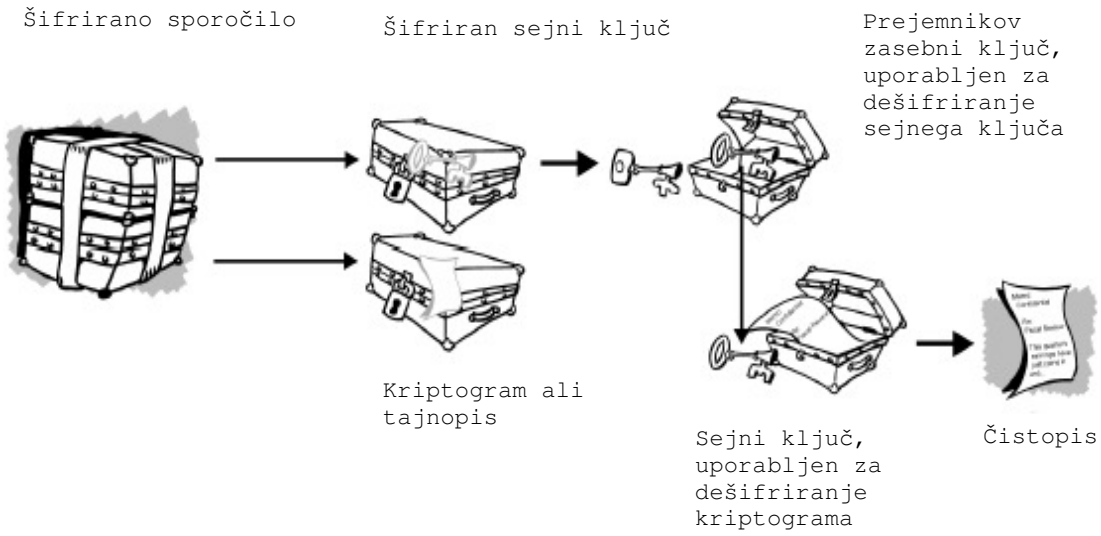
Primer delovanja programa PGP

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 ključ nato z varnim in hitrim simetričnim šifriranim algoritmom zakodira čistopis in nastane tajnopis *(ciphertext)*. Ko so podatki enkrat šifrirani, se sejni ključ zakodira s prejemnikovim javnim ključem in se skupaj s tajnopisom pošlje prejemniku.



Slika 4: Grafični prikaz šifriranja s programom PGP (Vir: How to PGP works, 2008)

Odkodiranje poteka v obratni smeri. Prejemnikova kopija programa PGP uporabi zasebni ključ prejemnika, s katerim odkodira sejni ključ, ki ga nato PGP uporabi za dešifriranje originalnega sporočila.



Slika 5: Grafični prikaz dešifriranja s programom PGP (Vir: How to PGP works, 2008)

Metoda šifriranja s PGP izkorišča prednosti dveh šifriranih metod: pripravnost asimetrične metode uporabe javnih ključev ter hitrost simetrične metode, s katero je zakodiran čistopis. Simetrična metoda je približno 1000 krat hitrejša kot metoda z uporabo javnih ključev. Uporaba javnih ključev pa rešuje problem distribucije ključev. Kombinacija teh dveh šifrirnih metod združuje pripravnost šifriranja z javnim ključem s hitrostjo simetrične kriptografije. V skupni uporabi sta učinkovitost in razpošiljanje ključev izboljšana brez žrtvovanja varnosti (How to PGP works, 2008).

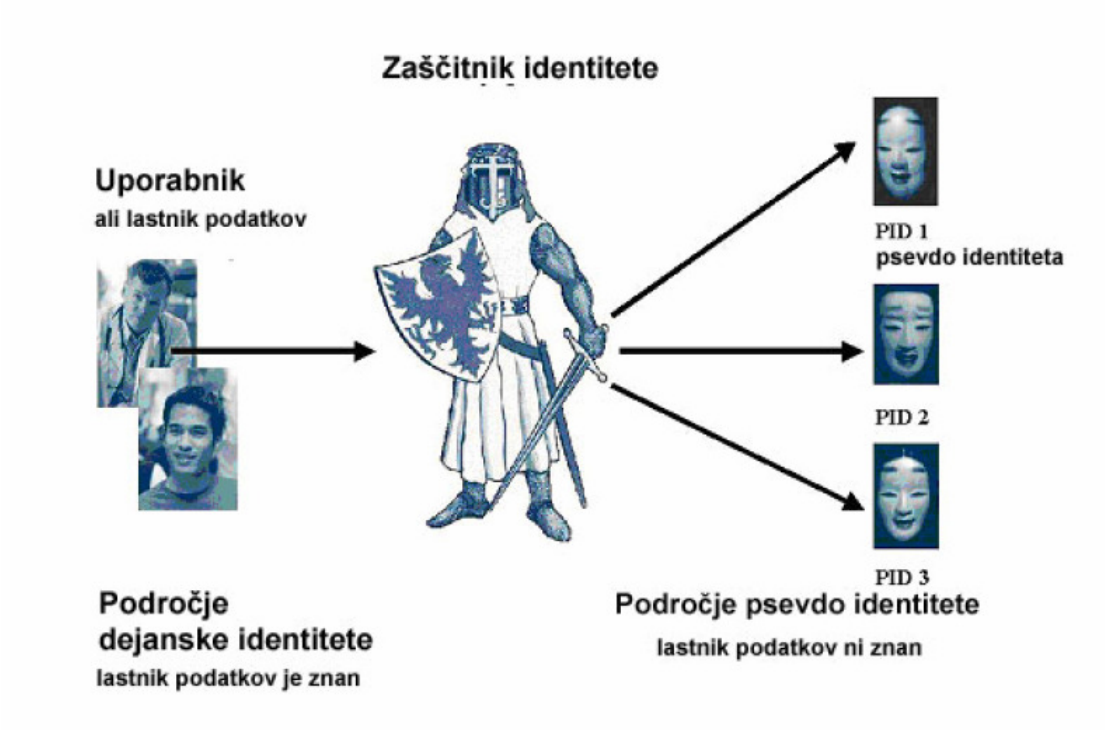
4.2 Tehnologije zaščite identitete

Zaščitnik identitete (ang. Identity Protector) 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):

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 et al.,2003).



Slika 6: Zaščitnik identitete (Vir: Blarkom et al. 2003)

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

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

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

Ker je zaščitnik identitete pod nadzorom uporabnika, lahko le ta poljubno dovoljuje razkritje svoje prave identitete nekaterim internetnim ponudnikom, drugim pa ne. Uporabnik tako lahko uporablja storitve in izvaja transakcije anonimno (z uporabo psevdo identitete). Ponudnik internetne storitve lahko sledi in zapisuje internetne aktivnosti le uporabnika s psevdo identitetami in ne uporabnika za dejansko

identiteto. S tem je ponudnikom storitev onemogočeno profiliranje dejanskih uporabnikov storitev.

Ponudnik storitev mora v nekaterih primerih imeti nadzor nad avtorizacijo, zato mora biti poučen o uporabnikovi pravi identiteti. Ker predstavlja zaščitnik identitete vmesni člen med uporabnikom in ponudnikom, mu morata obe strani zaupati. Zaščitnik osebnosti je narejen tako, da preprečuje prevare in nepravilno uporabo; ščiti uporabnikovo anonimnost, vendar jo lahko v določenih okoliščinah tudi razkrije, kot na primer internetnemu posredniku ali državnim organom.

Tehnike uporabljene za implementacijo zaščitnika identitete so lahko digitalni podpis, slepi digitalni podpis, digitalni psevdonim in zaupni centri (Seničar et al.,2003).

4.2.1 Zaupni centri

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.

Naloga zaupanih centrov (ang. Trust Centres) je vzpostaviti varen servis znotraj celotne informacijske strukture na način, da mu bodo zaupale vse vpletene strani: tako uporabniki kot tudi ponudniki storitev. Primerjamo ga lahko z notarjem: nevtralno, nevpleteno telo. Uporabnik mora zaupati, da bo ostala relacija med dejansko identiteto in psevdonimom tajna. V primeru zakonitega razkritja identitete mora biti uporabnik nemudoma obveščen o tem, kdo in zakaj bo razkril njegovo identiteto. Ponudnik pa mora zaupati zaupnemu centru, da bo uporabnikova dejanska identiteta v posameznih, dogovorjenih primerih razkrita. 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. 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. Zaupni centri morajo biti nevtralni in neodvisni ter ne smejo biti ogroženi zaradi nasprotja interesov (Seničar et al., 2003).

Glavne naloge zaupnih centrov so upravljanje s ključi (generiranje, shranjevanje, distribucija ključev), izdaja ter upravljanje s certifikati, naloga pooblaščenca (zaupnika) ter servisne funkcije (posredovanje informacij kot je seznam ključev, časovnih žigov, informacije o overovljenih, opazovanja na varnostne kritične dogodke…).

4.2.2 Anonimni strežniki

Anonimni strežniki omogočajo uporabnikom anonimni dostop do internetnih strani. Strežnik predstavlja neke vrste pregrado med računalnikom in internetom. Princip delovanja je enostaven: sklene se pogodba z organizacijo, ki ji zaupamo (zaupati ji morajo tako internetni uporabniki kot tudi komercialne organizacije).

Zahteva, ki jo pošljemo v internet, gre preko anonimnega strežnika, ki jo transformira tako, da končna destinacija ne more določiti izvora - zahteva, ki je prispela do končne destinacije vsebuje samo IP naslov anonimnega strežnika, uporabnikovega pa ne. V skupino anonimnih strežnikov lahko prištevamo tudi proxy strežnike in požarne zidove, ki prav tako predstavljajo neke vrste pregrado med računalnikom in internetom. Komunikacija je dovoljena samo pod določenimi pogoji. Proxy strežnik je lahko nastavljen za blokiranje kolačkov, neželeno pošto…, požarni zidovi pa onemogočajo nedovoljen dostop do računalnika (Seničar et al., 2003).

Ena izmed definicij pravi, da 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.

Eno izmed najstarejših podjetij s pomočjo storitve anonimnega strežnika je Anonymizer, ki obstaja že od leta 1995. Pri uporabi njihovih anonimnih strežnikov je IP naslov končnega uporabnika skrit, tako je onemogočeno logiranje spletnih strani, sledenje oglaševalcev, hekerskih napadov, monitoringa s strani ponudnikov internetnih strani ali delodajalcev, filtrirajo se piškotki, spletni hrošči, virusi ter ostale grožnje zasebnosti, kot so kraje identitete, neželeno oglaševanje… Podjetje nezadržno raste, od leta 2001 je tudi dobičkonosno; imajo preko 100.000 predplačniških uporabnikov; preko milijon mesečnih uporabnikov ter od leta 1995 preko štiri bilijone zaščitenih pogledov spletnih strani (Anonymizer, 2009).

Naslednji primer zaščite z anonimnim/psevdonimnim strežnikom je programska rešitev Freedom podjetja Zeroknowledge iz Montreala. Freedom je tehnologija, ki omogoča uporabniku interneta da ustvari 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 et al., 2003).

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).

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, 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. 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)

4.2.3 Ponovni pošiljatelj

Uporabniki pošiljajo sporočila preko »remailerja«, ki sporočilu odreže identifikacijske informacije ter ga opremi s psevdonimom. Za prejemnika elektronskega sporočila ostane pošiljateljev elektronski naslov neznan, ni pa neznan za operaterja ponovnega pošiljatelja. Odgovor prejme pošiljatelj prav tako preko »remailerja«. Stopnja zasebnosti je odvisna od zaupanja, ki ga imamo do servisa ter njihove varnostne tehnike. Za boljšo zaščito anonimnosti lahko uporabniki sporočilo zakodirajo ter ga pošljejo preko verige ponovnih pošiljateljev. Najnovejša različica »re-mail« tehnologije je t.i. Mixmaster, ki omogoča zaščito pred prisluškovanjem ter pred napadi pri odgovoru na pošto (Seničar et al., 2003).

Ponovni pošiljatelji (ang. re-mailer) so programi, ki sprejemajo elektronska sporočila od pošiljateljev ter jih po preoblikovanju pošljejo naprej prejemnikom, tako da le ta ne more ugotoviti identitete pošiljatelja. Najbolj enostavna različica takšnih programov so t.i. »Type I« ali »Cypherpunk« ponovni pošiljatelji (Stalder, 2002). 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 et al.,2003).

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 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).

Najnovejša in najsodobnejša različica *re-mailer* tehnologije je t.i. Mixmaster, ki omogoča zaščito pred prisluškovalnimi napadi, 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 in izboljšan sistem za prestrezanje sporočil. Tehnologija Mixmaster temelji na »varnosti v številkah«, 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, z namenom skrivanja originalnega sporočila (Fischer-Hübner, 2001).

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 verigi odgovornega bloka razkriti, če bi nekdo želel odkriti originalen e-naslov ustvarjen z *newnym* strežnikom (Fischer-Hübner, 2001).

4.2.4 Slepi digitalni podpis

Slepi digitalni podpis (ang. Blind digital signature) je samo ena od različic digitalnega podpisa, ki zagotavlja uporabnikovo anonimnost. 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.

Razlika med navadnim digitalnim podpisom in slepim digitalnim podpisom ni v samem podpisu, temveč v dokumentu, ki je bil podpisan. Ko nekdo podpiše dokument z digitalnim podpisom, pozna vsebino dokumenta, ko pa nekdo podpiše dokument s slepim digitalnim podpisom, vsebine dokumenta ne pozna, oziroma pozna samo del vsebine. Podpisniki so v tem primeru posebne agencije ali notariati, ki za vsebino dokumenta ne odgovarjajo. Slepi podpis deluje na ta način: uporabnik prinese dokument notariatu; pri tem ne želi, da bi kdor koli, vključno z notarjem, poznal vsebino dokumenta. Dokument je obdan z ovojem, del dokumenta pa je viden. Na vidni del dokumenta da notar pečat, ki dokazuje avtentičnost dokumenta. Kadar se uporablja digitalni podpis, zamenjajo ovoj in pečat šifrirane tehnike. Uporabnik šifrira digitalni dokument, ta dokument pa potem s svojim digitalnim podpisom podpiše notar. Podpis zagotavlja avtentičnost dokumenta.

Druga 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. Slepi digitalni podpis se uporablja v plačilnem sistemu poznanem kot elektronski denar *(Ecash),* kot časovni žig *(timestamping)* (Seničar et al., 2003).

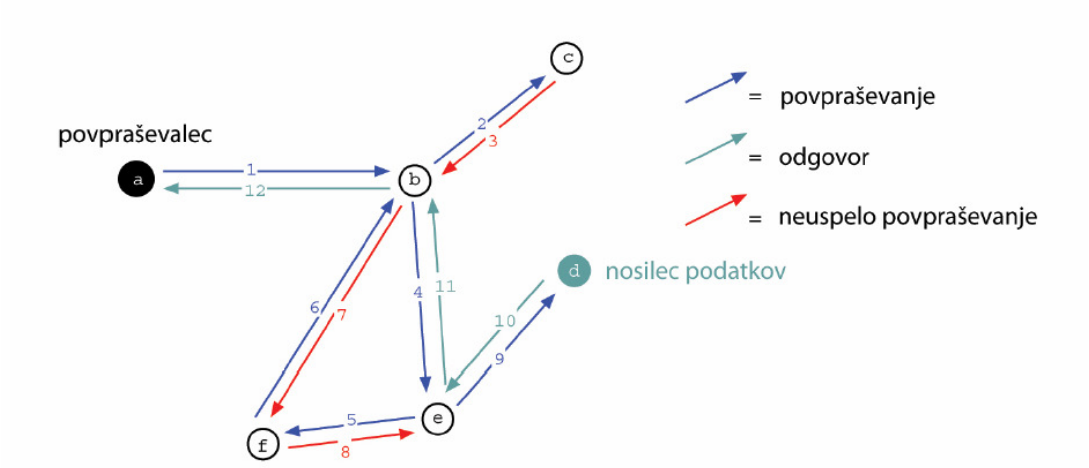
4.3 Tehnologije zaščite z neizsledljivostjo

4.3.1 Omrežje Freenet

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

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

Primarni namen Freeneta je zagotoviti zaščito anonimnosti povpraševalcev ter vsebine povpraševanj. Zasebnost je ohranjena z uporabo različice mix-net sheme za dosego anonimnosti komunikacije. Namesto direktno od pošiljatelja k prejemniku sporočilo potuje skozi verigo vozlišč, v katerem je vsak link posebej šifriran, vse dokler sporočilo ne doseže končnega prejemnika. Vsako vozlišče pozna samo svojega neposrednega soseda v verigi, zato je lahko končna točka kjerkoli v omrežju vozlišč, ki neprenehoma izmenjujejo nečitljiva sporočila. Niti vozlišče neposredno za pošiljateljem ne more vedeti ali je njegov predhodnik resnični pošiljatelj ali samo prenaša sporočilo z drugega vozlišča. Prav tako za naslednje vozlišče ne more vedeti ali je to že pravi prejemnik ali pa bo poslal sporočilo naprej.



Slika 7: Povpraševanje v sistemu Freenet (Vir: Clarke et al., 2002)

Takšna ureditev ne ščiti samo producenta (povpraševalca) ter uporabnika informacije (na začetku verige), temveč tudi nosilca informacije oz. podatkov (na koncu verige) (Clarke at al., 2002).

Freenet je sistem, ki omogoča nastajanje in ohranitev informacij na internetu, ne da bi nas skrbela cenzura. Omogoča prost pretok podatkov, svobodno širjenje misli, idej in mnenj. »Edina pot do demokracije je, da se vladam onemogoči kontrola nad državljani. Dokler bo vse, kar vidimo in slišimo, filtrirano, ne bomo resnično svobodni« (Clarke et al., 2002). Clarke se v svoji filozofiji dotika tudi problema zaščite intelektualnih in avtorskih pravic. Jedro problema zaščite intelektualne pravice vidi v uveljavljanju zahteve po monitoringu komunikacij. Če je nadzorovano vse, kar kdo reče, svobode govora ni. To pa je razlog, da Freenet onemogoči uveljavitev zakona o zaščiti intelektualne lastnine.

Freenet je nastal kot raziskovalni projekt leta 1997 Iana Clarka iz Edinbruške Univerze. Leta 1999 je bila programska koda kot začetek projekta odprte kode *(open source project)* postavljena na splet. Danes je na voljo programska verzija 0.7, kar pomeni, da je projekt še vedno 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):

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 protivladno 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 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 preslikanih 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, ki prevede računalniško berljive naslovne številke v prijazna in lahko uporabna imena. To povzroči očitno kontrolo, ki jo trenutno upravlja ICANN (Stalder, 2002).

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

Ena od rešitev, ki jih ponuja sistem Freenet, se imenuje porazdeljeni priročni spomin. Priročni spomin so trenutno shranjeni podatki, ki jih ima vsak spletni brskalnik. V Freenet modelu vsak vključen računalniški odjemalec 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. 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):

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 izvirnika.

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 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. 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).

Sistem Feenet 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. 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 Sistem Crowds

Crowds je sistem, ki zaščiti zasebnost med brskanjem po spletu, saj preprečuje spletnim strežnikom pridobivanje informacij o uporabniku. Njegov glavni cilj je narediti navigiranje anonimno, s čimer bo mogoče skriti informacije o uporabniku, spletne strani, ki jih je ta obiskal, ter vsebino, ki jo je pridobil od spletnih strežnikov.

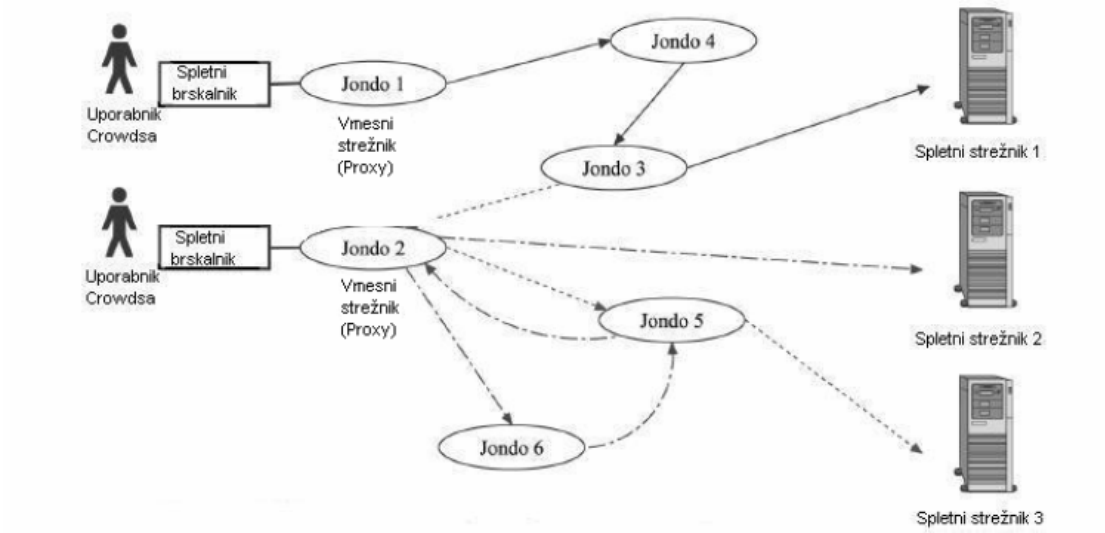
Sistem Crowds grupira uporabnike v velike, geografsko diverzificirane skupine in v njihovem imenu izdaja zahtevke po informacijah. Sistem deluje na način »pomešaj se v gnečo«, kar pomeni skrivanje akcij enega uporabnika v akcijah mnogih in tako onemogoči spletnemu strežniku definirati izvor zahteve. 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 izvirnik zahtevka (Seničar et al., 2003).

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:

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.

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



Slika 8: Delovanje sistema Crowds (Vir: Gritzalis, 2004)

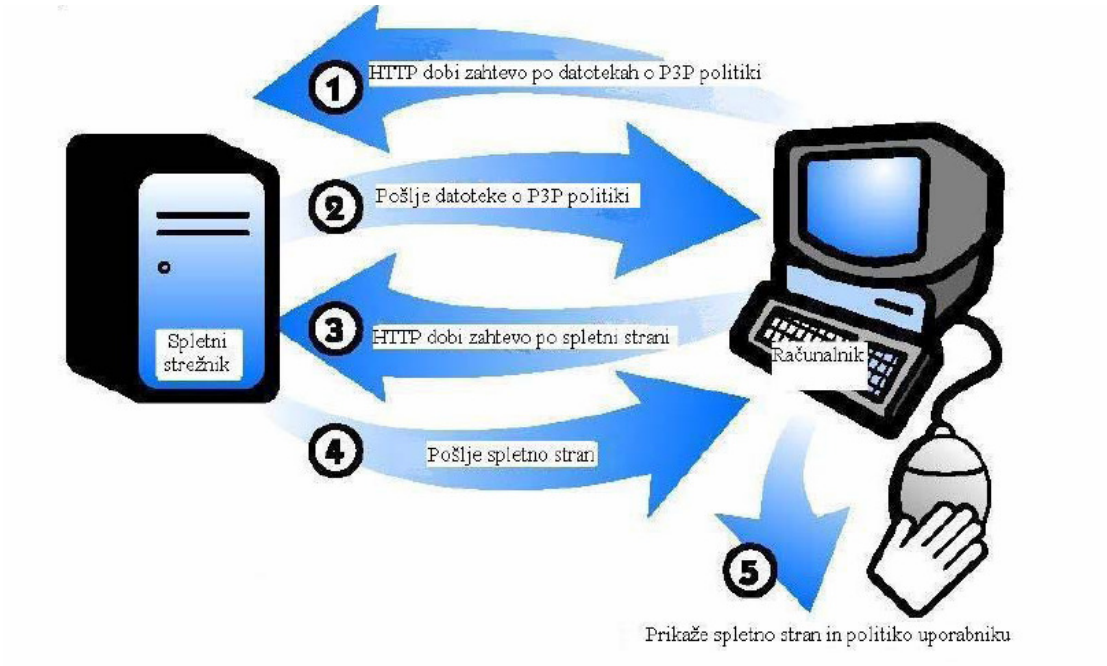
Sistem Crowds pomaga zagotoviti zasebnost dostopa do spleta, ne da bi lahko spletne strani ugotovile, s katerega računalnika smo dostopili. Bazira na ideji, da lahko član množice ostane anonimen in da lahko skrije svoje aktivnosti v aktivnosti drugih članov te množice, to pomeni: skriti svojo aktivnost znotraj aktivnosti drugih udeležencev. Specifični protokol prepreči spletnemu strežniku zapisovanje kakršnih koli informacij (npr. domensko ime, uporabnikov IP naslov, uporabnikovo računalniško platformo itd.), ki bi se lahko uporabile za identifikacijo uporabnika. Udeležencem sistema tako ni potrebno zaupati še neki tretji stranki, ki bi mu zagotavljala anonimnost. Vsak uporabnik kontaktira z osrednjim strežnikom ter

sprejme participacijski list “crowd”. Uporabnik nato prenaša svoje povpraševanje preko naključno izbranega vozlišča v sistemu crowd. Na osnovi prejetja zahteve vsakega vozlišča se naključno žreba žeton in odloči, ali gre povpraševanje še naprej skozi množico (crowd) ali pa se pošlje končnemu prejemniku. Odgovor je poslan nazaj uporabniku preko poti ustanovljene z zahtevo skozi množico “crowd” (Seničar et al., 2003).

4.4 Tehnologije za zaščito zasebnosti s privolitvijo

4.4.1 Platforma P3P

P3P je standard obveščanja uporabnika o zbiranju osebnih informacij ob obisku spletne strani, ki ga je izdelala organizacija W3C *(World Wide Web Consortium)*. Lahko bi ga tudi definirali kot standarden niz vprašanj, ki celovito pokriva politiko zasebnosti. 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.



Slika 9: Delovanje P3P tehnologije (Vir: P3P, 2006)

P3P standard je XML dokument, 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 pridobivanje 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. 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.

V poročilu »Prety poor privacy« ugotavljajo problematiko v zvezi z uporabo protokola P3P v tem, da prihaja do podobne situacije kot pri piškotkih: če zavračaš piškotke v celoti, potem skoraj ni več strani, ki bi jo lahko obiskal. Podobno je pri nastavitvah P3P. Uporabniki, ki so zelo zaskrbljeni glede svoje zasebnosti in si nastavijo P3P na visoko stopnjo zaščite ter blokirajo strani, ki tem zahtevam ne ustrezajo, potem skoraj ni strani, ki bi jo lahko obiskali. Da se uporabnik izogne takšnim situacijam, si nastavi stopnjo zaščite na minimum, s tem mu je omogočen dostop do vseh strani, vprašljivo pa postane varovanje zasebnosti.

Platforma P3P omogoča komunikacijo spletne strani z uporabniki glede njihove politike varovanja zasebnosti, toda to še ni zagotovilo, da bodo spletne strani tej politiki zasebnosti res tudi sledile (Cranor, 2003).

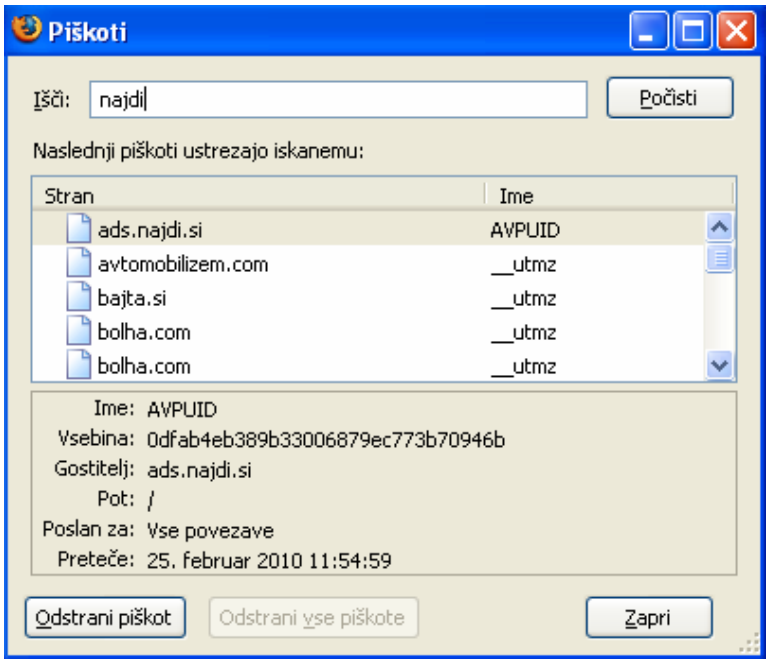
Obstaja kar nekaj orodij za brskanje po spletu z implementacijo P3P standarda, npr. brskalnika Netscape in Microsoft Explorer, ter samostojni program AT&T Privacy Bird (Seničar et al., 2003).

4.4.2 Upravitelj elektronskih piškotkov

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. Poleg tega so v datoteki piškotka zajeti podatki o naslovu računalnika, življenjska doba piškotka, identifikacijska številka, pogosto pa vsebuje tudi podatke, ki se nanašajo na uporabnika: ime, čas obiska strani, geslo… 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.

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



Slika 10: Upravitelj piškotkov

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 (Working Party on Information Security and Privacy, 2002):

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.

Piškotki lahko vsebujejo tudi občutljive osebne podatke in zaradi tega predstavljajo grožnjo zasebnosti. Grožnje ne predstavlja samo sledenje uporabniku ter ugotavljanje njegovih navad, nevarnost predstavlja tudi prestrezanje piškotkov ter vdor v uporabnikov računalnik. Uporabnik ponavadi nima pogleda nad stopnjo ter načinom zaščite piškotkov pri samem prenosu ter shranjevanju (Seničar et al., 2003).

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. 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 (Kovačič, 2000).

5 SKLEP

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

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

Internet omogoča zbiranje velikanskega števila podatkov, tudi osebnih. S sodobnimi tehnologijami lahko nepovezane podatke združujejo, predelujejo ter ustvarjajo povsem nove baze podatkov, ki jih uporabljajo v druge namene, kot pa so bili prvotno zbrani. Večinoma se to dogaja brez vednosti in privolitve posameznika, na katerega se podatki nanašajo. Zbiranje in povezovanje podatkov, sledenje, video nadzor, profiliranje, rudarjenje, nadlegovanje preko elektronske pošte in uporaba biometričnih metod so grožnje, ki jih moramo spoznati, se z njimi soočiti ter jih sprejeti kot neizbežno dejstvo, šele nato se jih bomo lahko tudi uspešno ubranili.

Različne mednarodne institucije si prizadevajo zajeziti val poseganja v zasebnost ljudi in zaščititi potrošnike in državljane pred nedovoljenimi posegi v zasebnost. Pomembno vlogo pri tem imajo tudi države s svojo politiko ter ustrezno zakonodajo glede človekovih pravic in varovanja podatkov. Zakonodaja mora uravnotežiti dva interesa: prost pretok podatkov (informacij) na eni strani ter spoštovanje zasebnosti posameznika na drugi strani.

Z razvojem informacijskih tehnologij so se tako pojavili tudi prvi zakoni v zvezi z zaščito zasebnosti. Zaradi globalizacije informacijske izmenjave pa je pomemben razvoj mednarodnih meril oziroma principov varovanja podatkov in zasebnosti. Evropska zakonodaja o zaščiti podatkov zahteva od upravljalcev osebnih podatkov implementacijo takšne tehnologije, ki bo zaščitila osebne podatke pred uničenjem, izgubo, zlorabo in nedovoljenim dostopom. Pri tem je potrebno razlikovati pojma varnost in zasebnost, ki ju mnogokrat kar enačimo. Res je, da sta varnost in zasebnost dostikrat povezana, se prekrivata, velikokrat pa prihaja tudi do nasprotij – predvsem pri pojmovanju skupinske varnosti in individualne zasebnosti. Za dosego skupinske varnosti je lahko ogrožena zasebnost posameznika. To se dogaja predvsem po 11. septembru 2001, ko se je v imenu javne varnosti povečal in se še povečuje nadzor države nad državljani.

Pri kreiranju novih tehnologij ni potrebno pozornost usmeriti le na varnost podatkov, temveč tudi na varovanje zasebnosti in zaupnost podatkov. To vrsto tehnologij imenujemo tehnologije za boljše varovanje zasebnosti. S pomočjo te tehnologije naj bi vpeljali osnovne principe zasebnosti v zakonito obdelavo podatkov.

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 onemogoča določanje lokacij shranjene vsebine in tako zagotavlja 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.

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

Uporabniki interneta velikokrat popolnoma zavestno in prostovoljno izdajo svoje osebne podatke. Včasih res nimajo izbire, če želijo priti do določene vsebine, se pač odločijo za razkritje, velikokrat pa razkrijejo podatke zgolj za kakšno majhno ugodnost, kakšno nagrado ali popust pri nakupu. Svoje podatke v obliki elektronskih odtisov (t. i. electronic footprints) uporabniki razkrivajo tudi nehote, neprostovoljno. Do tega prihaja predvsem s sodelovanjem v različnih forumih in spletnih klepetalnicah, kjer se uporabniki niti ne zavedajo, da izdajajo tudi osebne podatke, ki se nekje beležijo in lahko ostanejo zapisani in dostopni še mnoga leta. Uporabniki so različni, nekateri bi za manjšo ugodnost takoj razkrili svoje ime, svoj elektronski naslov, skoraj vse osebne podatke, spet drugi želijo anonimnost, uporabljajo ponovne pošiljatelje, blokirajo kolačke. Pomembno je, da so uporabniki obveščeni, da vedo kaj kdo o njih zbira, zakaj in kaj počne s temi podatki in imeti morajo možnost izbire.

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

V prihodnosti se pričakuje vedno večja grožnja s strani interneta, zato je treba temu področju posvetiti veliko pozornost. Poskrbeti bo potrebno za neprestano izobraževanje in seznanjanje z novimi grožnjami, da bomo kos vedno novim napadom, ki pretijo z interneta. Vendar pa samo tehnična znanja, brez osveščanja uporabnikov, ne bodo zadostovala, saj bo prav od našega ravnanja odvisna naša zasebnost. Problem nadzora države in drugih institucij se stopnjuje, zato moramo kar najhitreje poskrbeti za obvarovanje pred neželenim nadzorom in obdržati svobodo, ki nam je trenutno dana na internetu.

6 LITERATURA IN VIRI

6.1 Literatura

- Bernik, I.: Razvoj sistema za zvezno simulacijo v C++, Diplomsko delo visokošolskega študija, Kranj 1996.
- Blarkom et at.: Handbook of Privacy and Privacy-Enhancing Technologies. The case of Intelligent Software Agents. Blarkom G.W., Borking J.J. Olk J.G.E., Haag: PISA Consortium, 2003.
- Clarke I., et al.: Protecting Free Expression Online with Freenet. Miller S.G., Hong T.W., Sandberg O., Wiley B. New York: Institute of Electrical and Electronics Engineers, 2002.
- Cranor L.F.: The role of Privacy Enhancing Technologies. Considering Consumer Privacy. Washington: Center for democracy and technology, 2003.
- Čebulj, J.: Varstvo informacijske zasebnosti v Evropi in Sloveniji. Ljubljana: Inštitut za javno upravo pri Pravni fakulteti v Ljubljani, 1992.
- Data Protection Working Party: Privacy on the Internet – An Integrated EU Approach to On-line Data protection. Bruselj: The European Commision, 2000.
- Fischer-Hübner S.: Privacy Enhancing Technologies, Karlstad: Department of Computer Science, Karlstad University, 2001.
- Graham I.: Putting Privacy in Context: An overview of the Concept of Privacy and of Current Technologies. Toronto: Centre for Academic Technology Information Commons University of Toronto, 1999.
- Horniak V.: Privacy of Communication – Ethics and Technology. Master thesis. Vasteras: Department of Computer Science and Engineering Malardalen University, 2004.
- Hinde S.: The Perils of privacy. Computer&Security, 2002.
- Jerman Blažič, B.: Elektronsko poslovanje na internetu. Ljubljana: Gospodarski vesnik, 2001.
- Kovačič M.: Nadzor in zasebnost v informacijski družbi, Mirovni inštitut, Ljubljana 2006.
- Kovačič M.: Zasebnost na internetu, Mirovni inštitut, Inštitut za sodobne družbene in politične študije, Zbirka politike, Ljubljana, 2003.
- Kovačič M.: Zasebnost v informacijski družbi. Diplomsko delo. Ljubljana: Fakulteta za družbene vede, Univerza v Ljubljani, 2000.
- Možina D.: Se Evropa odreka zasebnosti v korist varnosti. Pravna praksa 21 (2002), št. 43, priloga Informatika in pravo, 2002.
- Možina D.: Varstvo osebnih podatkov na internetu – cookie: piškotek ali Veliki brat, Pravna praksa, informatika in pravo, Ljubljana, 2000.

- Seničar et al.: Privacy Enhancing Technologies – approaches and development. Seničar Vanja, Jerman Blažič Borka, Klobučar Tomaž, Ljubljana: Laboratory for Open Systems and Networks, Inštitut Jože Štefan, 2003.
- Stalder F.: The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy. B.k.: Sociological Research Online, 2002.
- Verdovnik I., Bratuša T.: Hekerski vdori in zaščita, Založba Pasadena, Ljubljana, 2005.
- Working Party on Information Security and Privacy: Inventory of Privacy Enhancing Technologies (PETs). Paris: Organisation for Economic Co-operation and Development, 2002.

6.2 Viri

- Anonymizer: [URL: http://www.anonymizer.com/], (12.1.2009).
- Banisar D.: Privacy & Human Rights 1999. Washington: Electronic Privacy Information Center; London: Privacy International. [URL: http://www.privacyinternational.org/survey/index99.html], (1.9.1999).
- Direktiva 95/46/ES Evropskega parlamenta in sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov. Luksemburg, 24. oktobra 1995.
- Direktiva 2002/58/ES Evropskega parlamenta in Sveta o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij. Bruselj, 12. julija 2002.
- EPIC: Privacy and Consumer Profiling. [URL: http://epic.org/privacy/profiling/default.html], (13.10.2004).
- Gritzalis S.: Enhancing Web privacy and anonymity in the digital era. B.k.: Information Management & Computer Security, Emerald Group Publishing Limited, Vol. 12, No. 3, str. 267, 2004.
- How to PGP works: [URL: http://www.pgpi.org/doc/pgpintro/] (8.12.2008).
- Kovačič M.: Mehanizmi varovanja zasebnosti v informacijski družbi, [URL: http://www.ljudmila.org/matej/zasebnost/zasebnost.html], (22.12.2008).
- Kovačič M.: Steganografija ali kako nevidno kodirati sporočila, [URL: http://www.ljudmila.org/matej/privacy/kripto/stego.html], (12.1.2009).
- P3P. [URL: http://www.w3.org/P3P/brochure/full-brochure.pdf], (10.12.2006).
- Protecting Privacy and Fighting Spam: [URL: http://ec.europa.eu/information_society/doc/factsheets/024-privacy-and-spam-en.pdf], (24.1.2006).
- Provos N., Honeyman P.: Hide and Seek: An Introduction to Steganography. IEEE Security&Privacy, New York, maj/junij 2003.

- The Free Network Project: [URL: http://freenetproject.org/], (13.3.2009).
- Weiss T. 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).
- Working party on cooperation in criminal metters. Brussels. Council of the European union, 24. February 2005.
- Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/2007).
- Zakon o elektronskih komunikacijah (Uradni list RS, št. 13/2007).
- Železnikar J.: Zasebnost na internetu. [URL: http://www.mladina.si/dnevnik/18868/], (18.4.2002).

6.3 Kazalo slik