FAKULTETA ZA INFORMACIJSKE ŠTUDIJE
V NOVEM MESTU

DIPLOMSKA NALOGA

# VARNOST PODATKOV SPLETNIH UPORABNIKOV: GOOGLOVA POLITIKA ZASEBNOSTI

Mentor: doc. dr. Dušan Caf

Novo mesto, oktober 2012 Jure Pintar

# IZJAVA O AVTORSTVU

Podpisani Jure Pintar, študent FIŠ Novo mesto, v skladu z določili statuta FIŠ izjavljam:

- da sem diplomsko nalogo pripravljal samostojno na podlagi virov, ki so navedeni v diplomski nalogi;
- da dovoljujem objavo diplomske naloge v polnem tekstu, v prostem dostopu, na spletni strani FIŠ oziroma v digitalni knjižnici FIŠ:
  - **takoj**,
  - po preteku 12 mesecev po uspešnem zagovoru,
  - ne dovoljujem objave na spletni strani oziroma v elektronski knjižnici FIŠ zaradi prepovedi organizacije, v sklopu katere je bil pripravljen empirični del naloge;
- da je diplomska naloga, ki sem jo oddal v elektronski obliki, identična tiskani verziji;
- da je diplomska naloga lektorirana.

V Novem mestu, dne 25. oktober 2012 Podpis avtorja:

## POVZETEK

Informacijsko-komunikacijska tehnologija je v današnjem svetu močno prisotna, brez nje bi svet obstal ali postal neuporaben. Internet ima velik vpliv na dogajanje v družbi. Prinaša mnogo koristi, je hitro in globalno dostopen, prinaša pa tudi mnogo slabosti, saj je zasebnost posameznika v informacijski družbi ogrožena. S pojavom spletnih socialnih omrežij je internet postal zakladnica osebnih podatkov posameznikov, s katerimi upravljajo ponudniki tovrstnih storitev, ki izkoriščajo osebne podatke za drugoten namen, kot so bili prvotno zbrani.

Na tem področju je bilo potrebno urediti zakonodajo, ki bi varovala posameznike pred nepooblaščenim dostopom in ščitila njihovo zasebnost. Google je v prehodu v leto 2012 najavil veliko spremembo njihove politike zasebnosti, s katero zelo posega v zasebnost posameznika.



**KLJUČNE BESEDE:** Zasebnost na internetu, zakonodaja, varstvo osebnih podatkov, Google, politika zasebnosti, varnost na internetu.



## ABSTRACT

Information Communication Technology is extremely present nowadays and without it, the world would stop and become useless. Internet has a great influence on what is going on in the society. It brings a lot of advantages, since it is fast and globally accessible, but it also brings many disadvantages, because the individual's privacy in the information society is threatened. With the appearance of social networks, the internet has become the treasury of individuals' personal data, which the providers of such services manage with, who use personal data for a different intention that were originally gained.

The legislation had to be arranged on this field, which would protect individuals from unauthorized access and protect their privacy. In the beginning of the year 2012, Google has announced a big change in their privacy politics, which it interferes a lot with individual's privacy.



**KEY WORDS:** Privacy on the internet, legislation, protection of personal data, Google, privacy policy, security on the internet.

# KAZALO

# 1 UVOD

## 1.1 Raziskovalni problem

Internet je široko razširjen medij komunikacije, ki se uporablja na različnih področjih vsakdanjega življenja. Med uporabniki je zelo priljubljen, hitro – predvsem globalno – dostopen in za marsikoga predstavlja nepogrešljiv del vsakdana. Uporabniki imajo od interneta ogromno koristi, saj so v vsakem trenutku v stiku z ostalim svetom in lahko počnejo praktično karkoli. Tako kot ima vsaka stvar dve strani, ima tudi internet poleg pozitivnih svojo negativno stran. Zaradi tesne povezave z uporabnikom vse bolj v ospredje prihaja vprašanje varnosti uporabnikov na internetu.

V zadnjem času smo priča, zaradi dobrega glasu in oglaševanja, ogromnemu pojavu spletnih socialnih omrežij. Slednja s svojo iznajdljivostjo in spretnostjo zlahka zavedejo uporabnike na ta način, da le-ti svoje podatke redno pošiljajo na internet in tako skrbijo, da so njihovi javni profili čim bolj polni s podatki. Dostop do teh podatkov pa ima vse več institucij in posameznikov, kar lahko ob zlonamerni uporabi privede do njihove uporabe v druge namene, kot so bili prvotno namenjeni. Velike količine podatkov prav pridejo velikim korporacijam, katere nato kupujejo te podatke, to pa je z vidika etike in morale sporno. Dobljene podatke s pridom izkoriščajo za oglaševanje uporabniku priljubljene vsebine. Zavedajo se namreč, da je oglaševalski trg zaradi tovrstnih potez izjemno dobičkonosen.

Vodilno na področju obvladovanja interneta je prav gotovo ameriško podjetje Google, ki s svojo politiko zasebnosti v javnosti dviguje veliko prahu, na posameznih točkah pa nevarno posega v pravice posameznika. Še posebej je na udaru nova politika zasebnosti, ki jo je Google najavil 24. januarja 2012 in uvedel 1. marca 2012.

Diplomska naloga obravnava problem varnosti spletnih uporabnikov in njihovih osebnih podatkov. Dandanes je tema varnosti uporabnikov interneta eden izmed ključnih problemov sodobne družbe, saj vsakodnevno prihaja do številnih zlorab, povezanih z osebnimi podatki posameznika. Napadalci izkoriščajo pomanjkljivosti varnostnih sistemov podjetij, kjer se dokopljejo do številnih podatkov, ki jih posameznik objavi na internetu.

V nalogi sem se osredotočil na podjetje Google in na njegovo novo politiko zasebnosti ter pogojev uporabe storitev, saj velja za zakladnico osebnih podatkov.

### *1.1.1 Cilji naloge*

Pričakujem, da so v novem Googlovem pravilniku zasebnosti pomanjkljivosti ter da je uporabniku slabo razumljiv, da je vsaj na eni točki v nasprotju z Evropsko zakonodajo. Pričakujem tudi, da je sestavljen preveč pavšalno – predvidevam, da v tolikšni meri, da se v nasprotju s starejšimi različicami, ki so bile redno obnovljene, kar nekaj let ne bo spremenil tako, da bi sledil uporabnikovim zahtevam in aktivnostim. Zanimivo bo videti tudi, ali obstajajo primeri, kjer so bili uporabnikovi podatki izrabljeni in njegove pravice kršene z vdiranjem v zasebnost.

### *1.1.2 Namen naloge*

Namen diplomske naloge je ugotoviti, kako varni so podatki uporabnikov, ko so enkrat na internetu. Zanima me, kako je urejena zakonodaja na področju varnosti osebnih podatkov v Evropi in kako v Združenih državah Amerike, ali Google z novo politiko zasebnosti res grobo posega v pravice posameznika, kot to trdijo mnogi, ali pa je za to kriva le naivnost uporabnikov, ki tolerirajo početje Googla in v želji po uporabi njihovih storitev, ki so sicer brezplačne, brez slabe vesti vnašajo ogromne količine informacij o sebi. Kakšna je nova politika zasebnosti, ki je bila uvedena s 1. marcem 2012 oziroma v čem se razlikuje od stare? Za konec pa še kritični pogled na Googlovo politiko zasebnosti – ali se Google v čem razlikuje v primerjavi s konkurenčnimi podjetji?

## 1.2 Struktura naloge

Naloga je sestavljena iz teoretskega dela, ki sem jo razdelil na šest delov:

- zasebnost in pravica do zasebnosti,
- varnost osebnih podatkov,
- primerjava zakonodaje v Sloveniji, Evropski uniji in v Združenih državah Amerike,
- podjetje Google,
- primerjava stare Googlove politike zasebnosti z novo,
- varnost na internetu in vidiki zasebnosti.

Pravica do zasebnosti je ena izmed temeljnih človekovih pravic in jo je kot takšno težko postaviti v okvir ene same definicije. Opisal sem, kako tesno sta med seboj povezana pojma internet in zasebnost ter katere grožnje in kakšna tveganja predstavlja internet. Nadalje sem opisal sestavine, vrste in grožnje zasebnosti, ki jih označujejo številni avtorji, ter zgodovinski razvoj zakonodaje na tem področju.

Varnost osebnih podatkov je v diplomski nalogi podkrepljena z zakonodajo na tem področju v Sloveniji, v Združenih državah Amerike in v Evropski uniji. V tem delu sem predstavil še sporazum Safe Harbor, ki sta ga dosegli EU in ZDA.

V nadaljevanju sem predstavil podjetje Google, kakšni so bili prvi koraki podjetja, težave, s katerimi sta se srečevala soustanovitelja in kaj je podjetju omogočilo rast in razvoj. V nadaljevanju sem s primerjalno analizo primerjal staro Googlovo politiko zasebnosti z novo, za konec pa opisal še varnost na internetu oziroma vidike zasebnosti na internetu, kjer so podani odgovori na vprašanja, kako naj se uporabnik zaščiti oziroma kako naj ravna, da bo čim bolj zaščitil svojo zasebnost.

### 1.3 Hipoteze

Skladno z namenom in cilji diplomske naloge sem si postavil naslednje hipoteze:

1. Delež populacije, ki se zaveda nevarnosti in tveganj pri uporabi interneta, je majhen.
2. Zakonodaja na področju varstva osebnih podatkov je v posameznih državah zelo različna.
3. Google močno posega v zasebnost posameznika.
4. Nova Googlova politika zasebnosti je v nasprotju z zakonodajo v EU.
5. Za varnost na internetu lahko uporabnik največ stori sam.

### 1.4 Metodologija

Diplomska naloga je sestavljena samo iz teoretskega dela, kjer sem analiziral ključne pojme, ki se pojavljajo v diplomski nalogi. Nadalje sem s primerjalno metodo primerjal zakonodajo na področju varnosti osebnih podatkov v Sloveniji, v EU in v ZDA, v osrednjem delu naloge pa sem primerjal staro Googlovo politko zasebnosti z novo.

# 2 INTERNET IN PRAVICA DO ZASEBNOSTI

Internet je postal široko razširjen medij komunikacije, ki se uporablja na različnih področjih vsakdanjega življenja (Praprotnik 2003, str. 5).

Internet je del današnjega vsakdana, brez katerega si življenja ne moremo predstavljati. V svetu je postal nepogrešljiv, koristen, poučen, a hkrati tudi vsebuje nevarnosti in neprijetnosti. Nevarnosti niso povezane le z virusi, neželeno elektronsko pošto, temveč tudi s potencialno škodljivimi nelegalnimi vsebinami, kakršni sta lahko predvsem zloraba osebnih podatkov in bančnih kartic (Kovačič in drugi, 2008).

Za začetek je potrebno razumeti razlike med varstvom in zaščito podatkov na internetu. Medtem ko se varstvo podatkov nanaša na varovanje pomembnih podatkov, se zaščita podatkov nanaša na pravice posameznika in zaščito njegovih osebnih podatkov. To je še posebej pomembno na poti v informacijsko družbo, kjer ne smejo biti ovirane pravice posameznika do njegovih podatkov (Kovačič in drugi 2008, str. 10).

Odbor Evropske unije za varstvo osebnih podatkov in zasebnost v svojem poročilu *Privacy on the internet: An integrated EU Approach to On-line Data Protection* opozarja, da je internet »odprt javni sistem, ki deluje po tehnično znanih protokolih in katerega tehnična in programska konstrukcija sta primarno usmerjeni na izmenjavo informacij in ne na zagotavljanje zaupnosti in tajnosti teh informacij. To obenem omogoča vsakomur z minimalnim tehničnim znanjem, da najde in uporabi vrsto programskih orodij, namenjenih prestrezanju, nadzoru in razkrivanju podatkov, ki se pretakajo po internetu.« (European Union v Makarovič in drugi 2003, str. 102).

Lastnosti, zaradi katerih je internet po mnenju Jančič Bogatajeve in drugih (2007, str. 23) zanimiv s pravnega, ekonomskega in širše družbenega vidika, so tri. Prva je paketni način komunikacije, kar pomeni, da komunikacija po internetu poteka s prenašanjem zaporedij informacijskih paketov, ki podatke prenesejo do cilja po optimalni prosti poti. Druga lastnost je decentralizacija, kar pomeni, da internet nima ene same središčne točke, s katere bi ga bilo mogoče upravljati, temveč se lahko poljubno širi z vključevanjem novih strežnikov, usmerjevalnikov in uporabnikov. Tretja lastnost je globalna razširjenost in brezmejnost, kar pomeni, da internet ignorira državne meje, saj tehnološko praviloma ne pozna razlike med domačo in čezmejno komunikacijo ter obe omogoča v povsem enakovredni obliki. Posledično je internet idealno okolje za globalno širjenje znanja in mej.

Povsem preprosto teorijo o internetu je med drugim postavil tudi profesor s hardvarske univerze, H. T. Kung, ki je na harvardski konferenci *The Internet & Society* dejal, da internet prinaša edinstveno moč tako posameznikom kot tudi organizacijam. Internet ni omejen v smislu, da bi bil dostopen samo bogatim in vplivnejšim. Ljudje lahko uporabljajo domače spletne strani, na drugi strani ga organizacije uporabljajo za oglaševanje svojih produktov in storitev s potencialom, da le-te vidi na milijone ljudi v vsakem trenutku (O'Reilly, 1997).

Profesor Kung meni, da lahko internet označimo kot informacijsko tehnologijo, za katero je značilno, da se za razliko od drugih tehnologij samoizboljšuje. Ta proces ponazori s primerom, da takoj ko je zgrajen hitrejši računalnik, so v ozadju že narejeni načrti za novega, še boljšega. Hkrati poudarja, da bodo končni uporabniki interneta vedno sledili boljšim zahtevam in da ima internet velik vpliv na družbo (O'Reilly, 1997).

S pojmom internet je tesno povezan tudi pojem zasebnost oziroma pravica do zasebnosti vsakega posameznika na internetu. Makarovič in drugi (2003, str. 101) menijo, da vprašanje zasebnosti v tako imenovani informacijski družbi predstavlja enega ključnih pravnih, sociooloških, filozofskih in etičnih vprašanj sodobne družbe. Ob vrsti pozitivnih vidikov in do pred nekaj desetletji ne slutenih možnostih, ki jih omogočata razvoj tehnologije v informacijski družbi in predvsem globalno računalniško omrežje, prinaša ta tehnološki razvoj veliko nevarnost – počasno, a gotovo oženje življenjskega prostora ene izmed temeljnih človekovih pravic, to je pravice do zasebnosti.

Pravica do zasebnosti je sicer zelo širok pojem. Rovšek (2005) jo razume kot pravico, ki je človeku prirojena, ki jo instinktivno čuti, ne da bi jo znal natančneje definirati.

Informacijska družba predstavlja velik napredek, hkrati pa tudi vse večjo grožnjo človeku in njegovi zasebnosti (Kovačič, 2003). Čebulj (1992, str. 16) meni, da informacijska zasebnost posameznika ni postala ogrožena šele z uvedbo informacijskih tehnologij in računalniško vodenih zbirk osebnih podatkov, temveč jo je ta samo potencirala in privedla do tega, da so se ljudje začeli te nevarnosti veliko bolj zavedati kot v času ročno vodenih evidenc.

V kompleksni moderni družbi je potreba po organiziranosti in s tem po zbiranju informacij o posameznikih vsak dan večja, posledica tega pa je ogroženost zasebnosti (Kovačič 2000, str. 1019).

Praprotnik (2006) pravi, da se je z vse večjo rastjo interneta ter elektronskega poslovanja 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 nastavljene.

Meje med zasebno in javno sfero v svetu skorajda ni več, nova tehnologija omogoča različne vrste posegov v zasebnost posameznikov. Varstvo pravice do zasebnosti tako postaja ena najbolj kritičnih točk borbe med državo, delodajalcem, družbo in posameznikom. Zato veliko vlogo na tem področju igra pravna ureditev zasebnosti (Makarovič in drugi 2003). Zaradi neobstoja mej med zasebno in javno sfero je s tem, po mnenju Kneza (2009), odločanje posameznika o odkritju njegovih osebnih podatkov zelo oteženo. Osnovna elementa zaščite in varovanja zasebnosti sta kontrola meje med zasebno in javno sfero ter možnost odločanja, katere informacije in pod kakšnimi pogoji le-te posameznik lahko odkrije. V tehnologijah za izboljšanje zasebnosti so uporabljena nekatera orodja, s katerimi sta omogočena kontrola in nadzor meje med zasebno in javno sfero.

Kanadski akademik Marshall McLuhan je trdil, da današnji mediji premagujejo tiranijo besedila nad našimi mislimi in čuti. Njegov pregovor pravi, da je medij nekakšno sporočilo. S tem je priznaval in slavil nove komunikacijske tehnologije, ki imajo moč, da lahko povzročijo velike spremembe. Njegove besede namreč vsebujejo tudi svarilo o grožnji, ki jo ta moč predstavlja in o tveganju, da se zanjo ne zmenimo (Carr, 2011).

Nadalje je McLuhan razumel, da ljudi vsakič, ko se pojavi nov medij, prevzamejo informacije oziroma vsebino, ki jih prenaša. Ne glede na to, kako osupljiva je tehnologija medija, slednja vselej izgine v senci tistega, kar prenaša in to so dejstva, zabava, navodila in pogovori. Vsebina medija dolgoročno gledano ne vpliva tako močno na naše razmišljanje in dejanja kot medij sam. Priljubljen medij predstavlja naše okno v svet in tako oblikuje, kaj in kako vidimo in nas sčasoma, če ga dovolj pridno uporabljamo, spremeni kot posameznike in družbo (Carr, 2011).

Po mnenju Makaroviča in drugih (2003, str. 102), poglaviten razlog za ogroženost zasebnosti v internetu predstavlja prav tehnologija, na kateri internet temelji. Pri tem daje velik pomen pomembnosti rezultatom raziskav, ki kažejo, da so uporabniki interneta izrazito neosveščeni oziroma podcenjujejo tveganje, ki ga uporaba interneta predstavlja s stališča varnosti osebnih

podatkov in zasebnosti ter so pripravljeni pristati nanj zgolj zaradi lagodnejšega (potrošniškega) življenja.

Odbor Evropske unije za varstvo osebnih podatkov je v zaključku svojega poročila *An Integrated EU Approach to on-line data protection* (European Union v Makarovič 2003, str. 103) opozoril na nekatere težnje in tveganja v zvezi z internetom in s pravico do zasebnosti, ki bodo v prihodnjih letih eden ključnih izzivov pravnega urejanja Evropske unije. Ugotovitve so sledeče:

- vsestranski razvoj interneta bo še naprej skokovito naraščal (tako v smislu tehnične dovršenosti, števila uporabnikov, elektronskega poslovanja kot novih vrst storitev, ki jih bo ponujal);
- podjetja bodo še naprej težila k temu, da svojo ponudbo čim bolj približajo interesom, navadam in potrebam posameznikov ali posameznih skupin – to pa zahteva profiliranje uporabnikov interneta s samodejno obdelavo osebnih podatkov;
- razvoj tehnologije bo še olajšal sledenje uporabniku interneta in njegovim navadam (npr. z mobilno telefonijo), olajšal pa bo tudi dostopnost do prikritega zbiranja osebnih podatkov;
- povečana dostopnost osebnih podatkov odpira vrata vrsti morebitnih sekundarnih zlorab teh podatkov, ki presegajo (dovoljene) okvire prvotnega zbiranja;
- vse omenjeno prinaša nova tveganja s stališča pravice do zasebnosti, še posebej če so podatki v rokah enega podjetja ali majhnega števila podjetij ali posameznikov.

Po navedbah Makaroviča in drugih (2003, str. 103) ta opozorila o tveganjih uporabe interneta niso nova, vendar so v ospredju izključno z vidika omogočanja večjega državnega nadzora nad internetnimi uporabniki, saj so ljudje v želji po varnosti pripravljeni sprejeti precej večja pooblastila varnostnih in obveščevalnih služb. Kljub temu pa z vidika varstva zasebnosti, s pomočjo kriptografije, lahko občutno zmanjšamo možnost neupravičenih, neutemeljenih in protiustavnih posegov v zasebnost uporabnikov interneta.

Vstop v informacijsko družbo močno vpliva na dosedanji način človekovega življenja in dela. Informacija je postala temelj nadaljnjega razvoja družbenega sistema in celotno delovanje človeka je danes osredotočeno okoli zbiranja, predelave in posredovanja informacij. Ogromna količina podatkov in informacij o posamezniku in njihovo enostavno obvladovanje z informacijsko tehnologijo daje imetnikom velikansko moč. Posameznik ni bil še nikoli tako ogrožen v svoji informacijski zasebnosti, kot je danes (Čebulj 1992, str. 3).

# 3 DEFINICIJA ZASEBNOSTI IN OSEBNIH PODATKOV

## 3.1 Zasebnost

Zasebnost je temelj človeškega dostojanstva, ki vsebuje dve ključni vrednoti, in sicer svobodo združevanja ter svobodo govora. V moderni družbi je vprašanje zasebnosti postalo eno od najbolj pomembnih vprašanj človekovih pravic (Banisar in Davies, 1999).

Zasebnost je tudi osnovna človekova pravica. Generalna skupščina združenih narodov je 10. decembra 1948 razglasila *Splošno deklaracijo človekovih pravic*, ki pravi, da »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.«

Širina in večdimenzionalnost pojma zasebnost onemogočata postavljanje le-te v okvir ene same definicije. Izmed vseh človekovih pravic je ravno zasebnost, po mnenju Banisarja in Daviesa (1999), eden izmed najtežje opisljivih in definiranih pojmov. Tudi Cvetko (1999, str. 16) meni, da enotne opredelitve zasebnosti ni. Podobnega mnenja je tudi Gutwirth (v Kovačič 2006, str. 12), ki poda vzroke, zakaj univerzalne definicije zasebnosti in pravice do zasebnosti ni. Vzroke išče predvsem v njenem subjektivnem pojmovanju, da je relativna in kontekstualna. Vsakdo ima drugačna pričakovanja glede zasebnosti in ta se spreminjajo tudi glede na družbeni kontekst. Dejstvo je tudi, da ima ta pojem za vsakogar drugačen pomen. Zato preveč natančno definiranje zasebnosti ni zaželjeno.

Lampe (2004) bi zasebnost najenostavneje pojmoval kot nekaj, kar ni javno in kar posameznik noče nameniti javnosti. Včasih jo nameni le določenim osebam ali pa še tem ne.

Cvetko (1999, str. 23) se sprašuje predvsem o tem, kaj v zasebnost sploh spada. V zasebnost spada vse, kar se nanaša na posameznika, zato se lahko njegov obseg po potrebi spreminja oziroma širi. Kljub temu jo isti avtor (1999, str. 16) razume kot pravico do osebnega življenja, ki vsakomur omogoča tak razvoj osebnosti, kot si ga sam določi in ga tudi varuje pred posegi tretjega v njegovo zasebno področje.

Graham (1999) meni, da zasebnost nima pomena, razen če gre za informacijo zaupne narave in če je meja med zasebno in javno sfero dobro definirana. Zasebnost povezuje s štirimi pojmi in sicer: svoboda, javno, zasebno, skrivnost. Ti koncepti so medsebojno povezani in jih ni mogoče ločiti.

Banisar in Davies (1999) v poročilu *Privacy and Human Rights* ugotavljata, da se opredelitve zasebnosti med seboj močno razlikujejo glede na razmere in okolje. V mnogih državah je zasebnost povezana z zaščito podatkov in področjem ravnanja z osebnimi podatki. Zasebnost lahko torej razumemo predvsem v smislu, kako daleč lahko družba posega v pravice posameznika.

Nekateri avtorji navajajo tri sestavine zasebnosti. Prvo označujejo kot zasebnost v prostoru, ki se nanaša na željo posameznika, da ima možnost biti sam, torej ločen od fizične prisotnosti drugih ljudi. Zasebnost osebnosti se nanaša na svobodo misli, opredelitve in izražanja. Zadnja sestavina je informacijska zasebnost, ki se jo veliko zanemarja, saj je njeno bistvo v želji posameznika, da obdrži informacije o sebi, ker noče, da bi bili z njimi seznanjeni drugi (Kraemer in King v Čebulj 1992, str. 7).

Banisar in Davies (1999) ločita štiri vrste zasebnosti, in sicer:

- **informacijsko zasebnost,** ki vključuje vzpostavitev pravil glede zbiranja in obdelave osebnih podatkov, kot so podatki o kreditih in zdravstvu;
- **zasebnost telesa,** ki se nanaša na fizično zaščito ljudi in proti postopkom, da se na njih izvaja testiranje zdravil;
- **zasebnost komunikacij,** ki zajema varnost in zasebnost pošte, telefona, elektronske pošte in drugih oblik komuniciranja;
- **prostorsko zasebnost,** ki se nanaša na omejevanje vdiranja v posameznikov življenjski prostor.

V sodobni družbi sta najbolj ogroženi informacijska zasebnost in zasebnost komunikacij (Kovačič, 2003).

Banisar in Davies (1999) ugotavljata, da globalizacija, konvergenca med tehnologijami in multimedialnost močno ogrožajo zasebnost. Ti trendi namreč odstranjujejo geografske omejitve pri pretoku podatkov, tehnologije so med seboj čedalje bolj povezljive in podatki v določeni obliki se hitro lahko spremenijo v drugo obliko. Zato so vsi ti procesi po mnenju Kovačiča (2003, str. 34) privedli do potrebe po učinkoviti zakonodaji za zaščito zasebnosti, ki ga danes skoraj vsaka država na svetu priznava v ustavi, se pa po posameznih državah razlikuje obseg priznavanja te pravice.

Ustava Republike Slovenije (2012) opredeljuje v členih od 35. do 38. varstvo pravic zasebnosti in osebnostnih pravic, nedotakljivost stanovanja, varstvo tajnosti pisem in drugih občil ter varstvo osebnih podatkov.

Začetki zakonodaje, ki ščiti zasebnost, segajo v leto 1361, ko je zakon *Justice of the Peace Act* predvidel kazni za osebe, ki so skrivaj opazovale druge posameznike ali jim prisluškovale. Leta 1765 je britanski lord Camden protestiral, ker so preiskovalci želeli vstopiti v njegovo hišo in zaseči neke listine. Švedski parlament je leta 1776 sprejel *Zakon o dostopnosti javnih zapisov*, ki je določal, da morajo biti vsi podatki, ki jih zbere država, uporabljeni izključno za zakonite namene. Leta 1792 je bilo v *Deklaraciji o človekovih pravicah* zapisano, da je privatna lastnina nedotakljiva in sveta. Francija je leta 1858 prepovedala objavo zasebnih podatkov in zanje določila stroge kazni (Banisar in Davies, 1999).

Skozi različna obdobja so nastajale različne definicije, ki so bile odvisne od mnogih dejavnikov: kulture, okolja, zgodovinskega dogajanja, pa tudi stopnje razvoja naroda nasploh. Zatorej lahko zasebnost razumemo kot interdisciplinaren pojem, upoštevajoč zakonski, politični in sociološki vidik (Praprotnik, 2006).

Tako se je ena prvih definicij izoblikovala ob koncu 18. stoletja, in sicer v ZDA. Ameriška pravnika Warren in Brandeis (v Kovačič, 2003) sta zasebnost opredelila kot pravico posameznika, da se ga pusti pri miru. Vendar pa ta definicija, po mnenju Čebulja (1992), za sodoben družbeni sistem prav gotovo ni povsem ustrezna, saj najpomembnejšo značilnost in podlago za delovanje predstavljajo informacije. Tako se danes ta pravica opredeljuje kot pravica posameznika, da zahteva, da se podatki in informacije o njegovih zasebnih razmerjih ne sporočajo komurkoli.

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 oblikovanje ustrezne zakonodaje za zaščito zasebnosti v drugih državah izvajajo danes Direktive Evropske unije.

Obstajajo trije glavni razlogi, zakaj države sprejemajo zakonodaje, ki urejajo področje varovanja zasebnosti in osebnih podatkov (Banisar in Davies, 1999):

- **odprava krivic iz preteklosti:** številne države, zlasti v srednji Evropi, Južni Ameriki in Južni Afriki sprejemajo zakone za odpravo kršitev zasebnosti, ki so nastale v prejšnjih avtoritarnih režimih;

- **spodbujanje elektronskega poslovanja:** v mnogih državah se razvija zakone, s katerimi se vsi podatki o posamezniku oziroma državljanu centralizirajo in so za posamezno državo dostopni na enem mestu;
- **skladnost evropske zakonodaje:** večina držav sprejema zakone, ki temeljijo na Konvenciji Sveta Evrope in Evropske unije, Direktive o varstvu podatkov.

Pravno so največja nevarnost pri zbiranju podatkov zlasti nenatančnost, napačnost, nepopolnost ali neažurnost zbranih podatkov (Čebulj v Kovačič, 2003).

### 3.2 Pojmovanje zasebnosti skozi čas

Skozi različna obdobja zgodovine je pojem zasebnosti imel različen pomen (Knez, 2009). V času prvih skupnosti je človek čutil potrebo po zasebnosti, biti sam, biti nemoten, biti brez javne pozornosti (Graham, 1999).

Kulturna in družbena zgodovina nas učita, da v času manj razvitih družb zasebnost ni imela velikega pomena. Zasebnost je imela pomen v fizičnem umiku na varno lokacijo, stran od skupnosti, izogibanju le-ti, svobodo pred vdori v človekov prostor. Kasneje je pridobila tudi na družbenem pomenu v obliki temeljne človekove pravice (Graham, 1999).

Sodoben pogled zasebnosti zahteva, da sta javna in zasebna sfera dobro ločeni. Manj razvite skupnosti tega niso razlikovale, saj so bile bolj skupne in ne dovolj strukturirane (Graham, 1999). Med te družbe lahko uvrstimo Eskime ali ameriške indjske družbe. Tu meja med javnim in zasebnim ni obstajala, saj so pogosto vsi vedeli vse in nihče ni ostal anonimen (Horniak, 2004). Rezultat tega je nejasno definirana meja med javno in zasebno sfero. Jasno pa je, da so imele družbe in podjetja moč, s katero so posegali v zasebno sfero človeka (Graham, 1999).

Različne študije kažejo, da je zasebnost medkulturna in univerzalna ter ni značilna samo za človeka. Alan Westin je ugotovil, da se tudi živali v določenih trenutkih zatečejo v samoto. Na obstoj zasebnosti kaže tudi njihovo branjenje lastnega teritorija (Wagner De Cew v Kovačič, 2006).

Zasebno sfero poznajo različne kulture in družbe. Na to kažejo nekatere navedbe v Bibliji, Koranu, judovski tradiciji, antični Grčiji in starodavni Kitajski (Laurant v Kovačič, 2006). Graham (1999, str. 6) navaja, da sta družbi antične Grčije in Kitajske imeli dobro razvit koncept javno in zasebno, ki se je pojmovala kot izraz lastninske pravice.

Kovačič (2006, str. 11) meni, da je zasebnost na zahodu nastala v času kapitalizma, nekoliko jasneje pa se je začela izražati ob nastanku univerzalnih človekovih pravic.

Sprva katoliške cerkve in kraljeve oblasti zasebnosti niso obravnavale kot družbeni problem. Imele so moč in zagotavljale stabilnost. Družba je bila izrazito stratificirana, kjer so kleriki in kraljeve oblasti veljali za najvišji sloj družbe, kmetje pa so bili označeni kot nižji sloj družbe. Le-ti niso imeli veliko pravic, še posebej ne pravice do zasebnosti (Horniak, 2004).

Stvari so se spremenile v obdobju razsvetljenstva v poznem 17. stoletju, ko so se ljudje začeli zavedati in razmišljati o pravici do zasebnosti. Ljudje so začeli razumevati, da so njihova izkustva pomembna in rezultat tega so bila nova spoznanja. Obdobje razsvetljenstva je spremenilo posameznikov pogled na njegove pravice in položaj, ki ga zaseda v družbi (Horniak, 2004).

Za obdobje 18. stoletja je značilna krepitev merkantilizma in buržuazije ter prevzem nadzora nad ekonomijo, ki je bil prej v rokah kraljevih oblasti in klerikov. Buržuazija je prevzela nadzor nad ekonomijo v družbi in si tako pridobila tudi politično moč. S politično močjo so pridobili tudi privilegije in pravice. Za ohranitev tega 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).

Čim je družba postajala bolj struktirirana, je vprašanje zasebnosti šele v 19. stoletju postajalo čedalje večji družbeni problem (Graham, 1999).

V prehodu na 20. stoletje se je pravica do zasebnosti spremenila skupaj s pojavom računalniške tehnologije, shranjevanjem podatkov in informacij v računalniških strežnikih in podatkovnih bazah. Vlade, ki so imele podatke o državljanih, so jih varovale kot tajne, le-to pa je vodilo v spremembo zakonodaje, s katero bi državljani imeli vpogled v to, katere podatke shranjuje vlada o posamezniku in na kakšen način jih lahko uporabi. Ljudje so hkrati zahtevali tudi dopolnitev zakonodaje, s katero bi bili njihovi osebni podatki varovani na način, da do njih ne bi dostopale velike korporacije in le-ti ne bi bili zlorabljeni (Horniak, 2004).

### 3.3 Varstvo osebnih podatkov

S pojmom pravica do zasebnosti vsakega posameznika je tesno povezan tudi pojem varovanje osebnih podatkov. Ta pravica se je razvila s pojavom in razvojem tehničnih sredstev, ki

omogočajo avtomatsko obdelavo podatkov, kar je tako poseglo v pravico do zasebnosti posameznika, da je pravica postala še bolj ranljiva in ogrožena. Pravico do varovanja osebnih podatkov se pogosto označuje za enega od vidikov pravice do zasebnosti, in sicer kot informacijsko zasebnost (Koman Perenič, 2009).

Generalni direktorat za pravosodje, svobodo in varnost (2010) definira osebni podatek kot vse informacije, ki se nanašajo na posameznika in s pomočjo katerih je mogoče neposredno ali posredno ugotoviti identiteto posameznika, npr. ime, priimek, telefonska številka, e-poštni naslov, kraj in datum rojstva itd.

Po navedbah Kovačiča (2000) se je država vedno trudila zbirati osebne podatke o posameznikih, vendar v preteklosti ni bilo na voljo ustrezne tehnologije, ki bi osebne podatke procesirala, klasificirala in povezovala, ne nazadnje pa tudi avtomatsko zbirala. To se je spremenilo z razvojem informacijsko-komunikacijske tehnologije (IKT), ki zaznamuje moderno družbo.

Iz pravnega vidika za posameznika pomenijo največjo nevarnost v zvezi z zbiranjem osebnih podatkov nenatančnost, napačnost, nepopolnost ali neažurnost zbranih podatkov (Čebulj v Kovačič, 2000).

»Najboljša zaščita ni ta, da oni (država) vedo manj o nas, pač pa da mi vemo več o njih: da vemo, kaj vedo o nas in kako te informacije o nas uporabljajo.« (Mellors v Raab 1997, str. 158).

Osebni podatki so dandanes, v dobi interneta, ena najbolj občutljivih tem, saj vseskozi prihaja do zlorabe le-teh in posredovanj v namene, za katera prvotno niso bile mišljene. Do zlorab prihaja zaradi različnih vzrokov. Največkrat želijo napadalci, ki jih z drugim izrazom lahko imenujemo tudi hekerji, pokazati ali dokazati velikim korporacijam, kako ranljivi so njihovi varnostni sistemi oziroma, da njihovi varnostni sistemi niso dovolj dobro zaščiteni in se najdejo pomanjkljivosti. Kot drugi razlog lahko upoštevamo željo po zaslužku, saj nekatere korporacije kljub zatrjevanju, da so njihovi varnostni sistemi dovolj dobri, te podatke namenoma izgubijo ali jih prodajo tretjim osebam, katere nato posamezniku med brskanju po internetu z oglasi prikazujejo uporabniku priljubljene vsebine. Med razloge bi lahko uvrstili tudi zgolj škodoželjnost napadalcev, saj ti z vdiranjem v uporabnikovo elektronsko pošto ali njegovim internetnim profilom, bodisi gre za izjemno priljubljeni Facebook bodisi za

LinkedIn ali nenazadnje tudi Twitter, povzročijo, da uporabnika z neprimernimi vsebinami očrnijo pred celotno javnostjo.

V času pisanja te diplomske naloge se je zgodilo več zlorab osebnih podatkov. Tako je po navedbah Huša (2012) hekerska skupina D33ds Company v juliju 2012 napadla ameriško podjetje Yahoo! in njegovo storitev Yahoo! Voices, s katerim so pridobili več kot 450.000 uporabniških imen in gesel njihovih uporabnikov. Napadalci so zapisali, da so z napadom želeli svetu pokazati in hkrati opozoriti podjetje Yahoo! na njihovo malomarno varnost sistema.

Le nekaj dni za tem se je zgodil nov napad, tokrat sta bila na udaru Android Forums in Nvidia. Napadalci so s kompromitiranjem strani Android Forums pridobili uporabniška imena, elektronske naslove, IP naslove in zgoščene vrednosti gesel. Pri tem so prizadeli več kot milijon njihovih članov. Kot glavni razlog so navedli zaslužek, saj so želeli pridobiti čim več elektronskih naslovov, ki bi jih lahko nato preprodali vsiljivcem, le-ti pa bi uporabniku pošiljali neželene vsebine. Še huje je bilo s skupina Nvidia, saj so ji napadalci, poleg uporabniškim imen, elektronskih naslovov in zgoščenih vrednosti gesel odtujili še javne informacije v profilu uporabnika, kot so njegovo ime, starost, lokacija itd. (Huš, 2012b).

Zgoraj opisana primera sta le dva odmevna napada na podjetji, ki sta se zgodila v času pisanja diplomske naloge. Takšnih in podobnih napadov je še več, dogajajo se vsakodnevno, vsi ti napadi pa imajo skupno nit in to je, da izkoristijo ranljivosti sistema, odtujijo podatkovne baze, elektronske naslove in druge pomembne, zaupne dokumente.

### *3.3.1 Razvoj varstva osebnih podatkov*

Varstvo osebnih podatkov se je v zadnjih letih osamosvojilo kot posebno področje varstva človekovih pravic v okviru širše pravice do zasebnosti (Rovšek 2005, str. 64). Potreba po varstvu zasebnosti se je pojavila zaradi prisluškovanj in podobnih vdorov v zasebnost posameznikov. Pravica do varstva osebnih podatkov se je začela uveljavljati precej pozno, saj je večino novodobnih kršitev zasebnosti omogočil šele razvoj nove tehnologije. Pred iznajdbo različnih naprav in uporabo računalniških baz je bil posameznik lahko skorajda prepričan, da njegovi osebni podatki ne bodo zlorabljeni, saj so bile informacije o posameznikih pogosto raztresene in težko dostopne. Zato je bilo na tem področju potrebno sprejeti zakonodajo, ki bo posameznikom nudila varstvo in jim zagotavljala ustrezne pravice, hkrati pa omogočala uporabo osebnih podatkov tistim subjektom, ki so upravičeni do zbiranja in obdelovanja le-teh (Musar Pirc in drugi 2006, str. 13).

V Evropi so bili prvi zakoni o varstvu osebnih podatkov sprejeti v sedemdesetih letih prejšnjega stoletja. Prva je zakon sprejela Švedska, in sicer leta 1973. Podobne zakone so kmalu za Švedsko sprejele še Grčija, Madžarska, Francija in Finska. Nekoliko kasneje, leta 1984, sta se jim pridružili še Velika Britanija in Severna Irska. V devetdesetih letih so tovrstno zakonodajo drugo za drugo sprejele tudi takratna Zvezna republika Nemčija, Slovaška, Avstrija, Danska, Italija, Norveška in druge države. Po prehodu v novo tisočletje so jo usklajevale z določbami *Evropske Direktive 95/46/EC* (Musar Pirc in drugi 2006, str. 13).

*Direktiva 95/46/EC* je bila *Direktiva o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku teh podatkov*, ki jo je sprejela Evropska unija 24. oktobra 1995 (Rovšek, 2005).

V Republiki Sloveniji smo pravico do varstva osebnih podatkov kot posebno človekovo pravico na ustavni ravni prvič opredelili z amandmajem XLIV iz leta 1989 k takratni ustavi (Rovšek, 2005).

## 3.4 Zakonodaja na področju osebnih podatkov

### *3.4.1 Zakonodaja v Sloveniji*

Slovenija je bila med prvimi, ki je v ustavo zapisala pravico do varstva osebnih podatkov (Rovšek, 2005). Prvi zakon s področja varstva osebnih podatkov v Republiki Sloveniji je bil *Zakon o varstvu osebnih podatkov* (Ur. l. RS, št. 8/1990). Temeljni cilj zakona je bil urediti varstvo osebnih podatkov in pri tem določiti pravice, načela in ukrepe, s katerimi se preprečujejo nezakoniti in čezmerni posegi v nedotakljivost človekove osebnosti, ki so lahko posledica zbiranja, obdelave, shranjevanja in posredovanja osebnih podatkov ter njihove uporabe (Bogataj, 2002). Ta zakon je bil po navedbah Rovška (2005, str. 65) sprejet 7. marca 1990 in je bil eden izmed prvih zakonov sprejetih v Evropi, hkrati pa poudarja, da četudi je bila Slovenija med prvimi v Evropi pri sprejetju zakonov, je zelo dolgo usklajevala svojo zakonodajo z *Direktivo 95/46/EC*.

Leta 1999 je bil sprejet nov zakon na tem področju, in sicer *Zakon o varstvu osebnih podatkov*, ki se je imenoval ZVOP-A (Musar Pirc in drugi, 2006), državni zbor pa ga je sprejel 8. julija istega leta (Ur. l. RS, št. 59/1999) zaradi približevanja Evropski uniji in zahtev Direktive Evropskega parlamenta ter Sveta o zaščiti posameznikov pri obdelavi osebnih podatkov in o prostem gibanju takih podatkov (Bogataj, 2002).

Omenjeni zakon ni bil v celoti skladen z Direktivo, saj po mnenju predstavnikov Evropske unije ni zagotavljal neodvisne institucije za nadzor nad varstvom osebnih podatkov. Zaradi tega je Državni zbor Republike Slovenije 26. junija 2001 sprejel novelo zakona ZVOP-A (Ur. l. RS, št. 57/2001). Glavni namen novele je bil vzpostavitev neodvisnega nadzorstva nad izvajanjem določb zakona (Bogataj, 2002).

Slovenski zakon se je Evropski Direktivi približal s sprejetjem novega zakona ZVOP-1 (Musar Pirc in drugi, 2006), ki je bil sprejet 23. julija 2004 (Ur. l. RS, št. 86/2004) (Uradni list Republike Slovenije, 2012). Leta 2005 je bila tako ustanovljena manjkajoča institucija, in sicer nov državni organ, Informacijski pooblaščenec, ki je kot neodvisen državni organ pristojen tudi za nadzor nad varstvom osebnih podatkov (Musar Pirc in drugi, 2006).

Po navedbah Kovačiča (2006, str. 78) ima zgoraj omenjena Direktiva nekaj pomembnih določil, med drugim se ne nanaša samo na živeče posameznike, dovolj široko definira obdelavo osebnih podatkov, posebno pozornost namenja obdelavi občutljivih osebnih podatkov. Kot je omenjeno že zgoraj, v Sloveniji to vlogo opravlja Informacijski pooblaščenec, medtem ko v Evropi za to skrbijo specializirane agencije in komisarji, ki morajo imeti določeno stopnjo pooblastil.

Slovenska ustava opredeljuje varstvo osebnih podatkov kot posebno pravico v 38. členu, ki pravi: »Zagotovljeno je varstvo osebnih podatkov. Prepovedana je uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja. Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon. Vsakdo ima pravico seznaniti se z zbranimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi.« (Ustava Republike Slovenije, 2012).

V Sloveniji se z *Zakonom o varstvu osebnih podatkov* (ZVOP-1, 2004) določajo pravice, obveznosti, načela in ukrepi, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v informacijsko zasebnost in dostojanstvo posameznika pri obdelavi osebnih podatkov, varovanju zbirk, obdelavi in uporabi le-teh. Za vsakega posameznika velja načelo prepovedi diskriminacije, kar pomeni, da je vsakemu posamezniku zagotovljeno varstvo osebnih podatkov, ne glede na njegove osebne okoliščine.

Osebni podatek se v zakonu definira kot podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen, njihova obdelava pa je niz delovanj, ki so avtomatizirano obdelani

s sredstvi informacijske tehnologije. Zbirka osebnih podatkov je strukturiran in organiziran niz podatkov, ki vsebuje vsaj en osebni podatek.

Osebni podatki morajo biti pridobljeni in obdelani na zakonit in pošten način. Zbirajo se lahko le za določene in zakonite namene, biti morajo ustrezni in po obsegu primerni namenu, za katerega se zbirajo in obdelujejo. Vsi podatki morajo biti točni in ažurni, za točnost osebnih podatkov pa lahko upravljalec le-teh pred vnosom v zbirko osebnih podatkov preveri z vpogledom v ustrezno javno listino posameznika, na katerega se podatki nanašajo. Osebni podatki se smejo hraniti le dokler je to potrebno, po izpolnitvi namena obdelave pa se zbrišejo, uničijo ali anonimizirajo, če niso opredeljeni kot arhivsko gradivo.

Posameznik ima po tem zakonu številne pravice do seznanitve z njegovimi osebnimi podatki.

Omeniti velja dve glavni pravici, in sicer, da se vsakemu posamezniku na njegovo zahtevo omogoči vpogled v katalog zbirke osebnih podatkov, kjer lahko posameznik preveri, kateri podatki so vsebovani v tej zbirki, pridobi lahko tudi seznam uporabnikov, katerim so bili posredovani njegovi osebni podatki, kdaj so bili posredovani, na kakšni podlagi in za kakšen namen, hkrati pa ima tudi pravico do dopolnitve, popravka, blokiranja ali izbrisa, v kolikor dokaže, da so ti podatki nepopolni, netočni, neažurni ali zbrani in obdelani na nezakonit način.

Osebni podatki posameznika se lahko posredujejo tudi drugim upravičenim uporabnikom proti plačilu. V kolikor gre za uporabo osebnih podatkov v zgodovinske, statistične in znanstveno-raziskovalne namene, je posredovanje brezplačno. Upravljalec osebnih podatkov mora v tem primeru zagotoviti tudi sledljivost podatkov, tako da je lahko kadarkoli pozneje mogoče ugotoviti, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni podlagi.

Podatki se lahko posredujejo tudi za namene ponujanja blaga, storitev, zaposlitev, telefonskih klicev, elektronske pošte in drugih telekomunikacijskih storitev, saj sodobna potrošniška družba vsebuje vse več neposrednega trženja. Pomembno pa je, da se ti podatki lahko posredujejo le, če so bili zbrani iz javno dostopnih virov. Za namene neposrednega trženja se lahko uporabljajo le osebno ime, naslov prebivališča, telefonska številka in elektronska pošta. Lahko pa posameznik s pisnim obvestilom zahteva, da se njegovi podatki za namen neposrednega trženja trajno ali začasno prenehajo uporabljati.

V druge države, tako imenovane tretje države – to so države, ki niso članice Evropske unije ali Evropskega gospodarskega prostora, se lahko posredujejo osebni podatki zgolj ob izdani

odločbi Informacijskega pooblaščenca, da tretja država zagotavlja ustrezno raven varstva osebnih podatkov.

V kolikor gre za videonadzor nad posameznikom, kar je dandanes skoraj povsod v uradnih, službenih ali poslovnih prostorih, v prostorih večstanovanjskih stavb itn., mora izvajalec na vidnem mestu objaviti obvestilo, da se izvaja videonadzor nad posameznikom. Ta metoda se običajno uporablja za varnost ljudi in premoženja, nadzora vstopov in izstopov v prostore. V tem primeru videozbirka osebnih podatkov v glavnem obsega posnetek posameznika, datum in čas vstopa v prostor in izstopa iz njega.

Tretji način je biometrija. Biometrične značilnosti imajo vsi posamezniki, to so telesne, fiziološke in vedenjske značilnosti. So edinstvene in nespremenljive in je možno z njimi identificirati posameznika s pomočjo prstnih odtisov, obraza, ušesa, deoksiribonukleinske kisline (DNK) ipd. (ZVOP-1, 2004).

Z uporabo biometrije se identificira posameznika oziroma preveri njegovo identiteto. Biometrija se čedalje bolj uveljavlja na letališčih, zelo pogosto pa je uporabljena recimo v policiji in kriminalistični policiji, saj s to metodo lahko odkrijejo posameznike, ki so storili kazniva dejanja.

### *3.4.2 Zakonodaja v ZDA*

V ZDA je zakonodaja na področju varovanja osebnih podatkov z našega vidika precej problematična. Kovačič (2006, str. 54) navaja, da ni moč upravičeno pričakovati zasebnosti, saj so zbirke osebnih podatkov v ZDA večinoma vse pod nadzorom oziroma v lasti tretjih oseb in podjetij.

Zasebnost oziroma pravica do zasebnosti v ZDA ni ustavna pravica, saj je ustava sploh ne omenja (Movius in Krup, 2009).

Prvi zakon, ki se dotika pravice do zasebnosti, je nastal leta 1974, ko je bil sprejet zakon o zasebnosti, in sicer *Privacy Act of 1974*, ki vsebuje omejitve pri razkrivanju osebnih podatkov za praktično katerokoli rabo. V grobem ta zakon prepoveduje razkritje posameznikovih osebnih podatkov, poleg tega pa določa, da smejo vladne agencije zbirati samo nujne in relevantne osebne podatke, osebne podatke v največji možni zbirati neposredno od posameznika, skrbeti za točnost in popolnost osebnih podatkov ter zagotoviti tehnične in administrativne postopke za zaščito osebnih podatkov. Poleg zakona Privacy Act v ZDA velja omeniti še zakon o svobodi informacij, to je zakon *Freedom of Information Act*, katerega

poglavitni namen je zagotavljati nadzor javnosti nad delovanjem vlade. Zakon določa, da ima vsakdo pravico do dostopa do kateregakoli zveznega dokumenta, razen v nekaterih primerih, med drugim je omejen dostop do osebnih in medicinskih ali podobnih dosjejev, katerih razkritje bi pomenilo očiten nepooblaščen poseg v zasebnost posameznika ter v primeru kazensko-preiskovalnih zadev, ko gre pričakovati, da bi objava dokumentov povzročila nepooblaščen vdor v posameznikovo zasebnost (Kovačič, 2006).

Privacy Act iz leta 1974, ki je v veljavi od 27. septembra 1975, je zbirka kodeksov poštenega ravnanja z osebnimi podatki, ki skuša nadzorovati zbiranje, hranjenje, uporabo in širjenje osebnih podatkov s strani zveznih izvršnih agencij. Kljub temu pa so ga njegov netočen zapis, omejena zakonodajna zgodovina in dotrajani napotki zaznamovali kot težaven statut za razumevanje in uporabo. Tudi po več kot 35-ih letih administrativne in sodne analize, številni problemi zakona ostajajo nerešeni in neraziskani (The United States Department of Justice, 2010).

Zakon Privacy Act vsebuje pet temeljnih načel, ki jih morajo kot kodeks poštenega ravnanja s podatki upoštevati vse zvezne agencije (Privacy Act of 1974, 2003):

- vlada ne bi smela hraniti nobenih tajnih podatkov;
- posameznikom bi moral biti omogočen vpogled v to, katere informacije se zbirajo o njih in kako so uporabljene;
- osebni podatki, ki so shranjeni v določen namen, se ne smejo uporabljati v drugotne namene brez predhodnega pisnega soglasja osebe, katere se ti podatki tičejo;
- posameznikom mora biti omogočeno, da popravijo ali razjasnijo informacije o njih;
- organizacije, ki hranijo ali uporabljajo osebne podatke, morajo biti odgovorne za verodostojnost podatkov in preprečiti vsakršno zlorabo.

V ZDA se zakonoska regulativa Privacy Act nanaša zgolj na javni sektor, velja za zvezno vlado in njene agencije, medtem ko za zasebni sektor zakonodaja ne velja, saj ima velik odpor do sprejetja take zakonske regulative (Raab 2004, str. 8). V praksi to pomeni, da za podjetja taka zakonska regulativa ne velja, pa tudi podjetja se tej zakonodaji upirajo. Na področju varovanja osebnih podatkov so ubrale laissez-faire pristop (Nijhawan Raj 2003, str. 940), ki pomeni bolj svoboden pristop k zakonodajnemu urejanju. Zakon ni nastal kot potreba po nujnem urejanju tega področja, temveč bolj po slučaju, tako pravi Wafa (2009). Kovačič (2006) omenjeno trditev podkrepi z navedbo, da je urejanje zasebnosti partikularno urejeno v različnih zakonih, ki so večinoma nastali kot odziv na kakšen javno odmeven primer.

Nijhawan Raj (2003) navaja, da bi sprejetje take zakonodaje na področju varovanja osebnih podatkov, ki bi bila močno regulirana in nadzorovana s strani vlade, imela negativen vpliv na svoboden pretok informacij v ekonomiji, ki je bistvenega pomena za poslovanje ameriških podjetij. Interes podjetij je, da od posameznika pridobivajo osebne informacije in jih uporabljajo v tržne namene.

Ameriški pristop do regulacije zasebnosti je v primerjavi z Evropsko unijo težko primerjati, saj so ključne vrednote, ki zadevajo posameznikovo zasebnost preko interneta, neenakovredne. Oba politična sistema priznavata zasebnost potrošnikov (Nijhawan Raj, 2003).

Nasprotno od Evropske unije, se ZDA ravnajo po trgu – samostojno urejajo in določajo predpise o internetni zasebnosti. Američani si ne želijo, da bi se vlada vpletala v njihove pravice zasebnosti. V splošnem, se tudi ameriška vlada skuša čim manj vpletati v pravice zasebnosti in preferira čim manj premostitvenih zakonov (Nijhawan Raj, 2003).

Kot navajata Levin in Nicholson Jo (2005), ZDA nimajo enotnega zakona, ki bi urejal področje varovanja osebnih podatkov, temveč imajo množico drugih zakonov, ki jih je potrebno upoštevati tako na področju ZDA kot tudi na področju posameznih zveznih držav.

ZDA se zavedajo, da je pomembno, da je zasebnost varovana, če želijo, da se trgovanje na spletu razvija, zato to še naprej same urejajo znotraj posameznih industrij. Ameriška perspektiva je bila povzeta v Clinton/Gore 1997 *Framework for Global Electronic Commerce*, v katerem je poudarek na tem, da bi moral zasebni sektor vzeti ključno vlogo v internetnem trgovanju in obvladovanju nad njim. Zatorej je ta sestavek vzpodbujal samostojne rešitve za zagotavljanje zasebnosti, internetno trgovanje pa je bilo prepuščeno samostojni regulaciji, kolikor je bilo to možno zagotoviti. Vsekakor je bilo to bolj po godu večini podjetij, kot pa da bi poslovali pod diktirko vlade. Stremeli so k regulaciji preko različnih mehanizmov, kot so predpisi v stroki ipd. (Fromholz v Movius in Krup, 2009).

Ta pristop do zasebnosti podatkov je v nasprotju s tistim v Evropski uniji. Medtem ko je v Evropski uniji odgovornost vlade varovati pravico do zasebnosti prebivalcev, v ZDA ne oblikuje informacijske zasebnosti zakon ali pravo, temveč trgi in samostojna regulacija. V Evropski uniji je zasebnost vzeta za temeljno pravico, v ZDA pa z zasebnostjo ravnajo kot z blagom, ki ga nadzoruje trg in je vpet v ekonomske vode (Kobrin v Movius in Krup, 2009).

### *3.4.3 Zakonodaja v Evropi*

V Evropi je pristop k zakonodaji na področju varovanja osebnih podatkov v primerjavi z ZDA diametralno nasproten, saj se za razliko od ZDA Evropa poslužuje strogega zakonodajnega urejanja tega področja (Nijhawan Raj 2003, str. 940). Tu po navedbah Kovačiča (2006) zakon velja tako za zasebni kot tudi za javni sektor.

Evropska unija se poslužuje tako imenovane centralizacije zakonodaje – zakonodaje, ki velja za vse države članice Evropske unije. V ta namen so sprejeli *Direktivo 95/46/EC*. Omenjena Direktiva je bila že večkrat spremenjena zaradi nenehnih posodobitev na tem področju, saj je bilo potrebno z uvedbo nove tehnologije zakonodajo uskladiti tudi s hrambo elektronskih podatkov in zaščito zasebnosti na področju elektronskih komunikacij (Wafa, 2009).

Evropska zakonodaja daje vladi hkrati tudi veliko večjo kontrolo nad osebnimi podatki državljanov (Nijhawan Raj 2003, str. 941).

V večini evropskih držav veljajo naslednje pravice (Sullivan, 2006):

- posamezniku informacija ne sme biti odvzeta brez njegovega dovoljenja, pravico ima do vpogleda in popravkov podatkov;
- podjetja, ki obdelujejo osebne podatke, morajo imeti registrirano dejavnost;
- delodajalec ne sme brati delavčevih zasebnih elektronskih pisem;
- osebne informacije ne smejo biti posredovane tretjim osebam brez izrecnega dovoljenja s strani tistega, katerega podatki se tičejo;
- prodajalci ob izhodu nimajo dovoljenja, da prosijo nakupovalca za njegovo telefonsko številko.

Razlikujoče norme zasebnosti v ZDA in Evropski uniji lahko vidimo kot rezultat temeljnih razlik med vlogo vlade in tržnega sektorja. Širše gledano zahteva evropski pristop tesno sodelovanje med trgom in politiko za dosego javnih dolžnosti. Vlado vidijo kot aktivnega partnerja v sodelovanju z večjimi industrijskimi akterji, ki združeno razpravljajo o urejevalnih in javnih interesih ter strategijah, kako jih doseči. Nadalje, evropski odločevalci so vedno videli socialne probleme kot širšo vlogo za državo. Nasprotno pa so ZDA dajale večji pomen bolj svobodnim pristopom k odločanju in poudarile vlogo zasebnih akterjev ter tržnih sil (Farrell v Movius in Krup, 2009).

Bach (v Movius in Krup, 2009) navaja, da evropski podvigi, da bi uredili zasebnost, izvirajo iz njihovega koncepta zasebnosti. Državljani Evropske unije jemljejo pravico do zasebnosti

kot temeljno pravico, ki jo mora zagotavljati posamezna država. V številnih evropskih državah je pravica do zasebnosti, za razliko od ZDA, ustavna pravica in tudi v Evropski konvenciji za varovanje človekovih pravic in temeljnih svoboščin.

Svet Evrope, ki je bil ustanovljen takoj po drugi svetovni vojni, se je še istega leta lotil problema osebnih informacij. Zgodnji poskusi so s časom privedli do konvencije *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data*, ki je bila sprejeta leta 1980. Konvencija je ustvarila osnovna načela zasebnosti in podala obrazec državam, ki varstva zasebnosti niso imela zakonsko urejenega (Levin in Nicholson Jo, 2005).

Iz istega dela lahko razberemo, da načela za avtomatsko obdelane osebne podatke zahtevajo, da:

- so pridobljeni in obdelani pošteno in v skladu z zakonom;
- so shranjeni v točno določene in legitimne namene;
- niso uporabljeni na način, ki ni skladen s temi nameni;
- so ustrezni, ključni in pravega obsega v razmerju do namena, za katerega so zbrani;
- so točni in, če je potrebno, ažurirani;
- so ohranjeni v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo toliko časa, kolikor je potrebno za namen, za katerega so podatki shranjeni;
- so zaščiteni s primernimi varnostnimi ukrepi;
- so dostopni posameznikom na vpogled, da se preveri verodostojnost informacij in omogoči popravljanje, v kolikor je to potrebno.

Na tem mestu se lahko vprašamo, zakaj prihaja do takih razlik pri varovanju zasebnosti v Evropi in v ZDA. Kovačič (2006, str. 72) na omenjeno vprašanje odgovarja, da je verjetnost, da je k razvoju varstva informacijske zasebnosti v Evropi pripomogla tudi negativna izkušnja totalitarnih režimov, ki jih ZDA nikoli niso izkusile tako zelo in na tak način kot Evropa.

V Evropi je večina držav podpisala in ratificirala mednarodne akte, ki urejajo varstvo zasebnosti. Najpomembnejši med njimi so *Splošna deklaracija človekovih pravic, Mednarodni pakt o državljanskih in političnih pravicah* ter *Evropska konvencija o varstvu človekovih pravic in mednarodnih svoboščin* (Kovačič 2006, str. 72–73).

Pri obdelavi osebnih podatkov ima posameznik pravice, da je jasno in razumljivo obveščen, da se njegovi osebni podatki obdelujejo, da ima dostop do lastnih podatkov in popravkov morebitnih napačnih ali nepopolnih podatkov, da v nekaterih primerih na zakonski podlagi ugovarja obdelavi in da od upravljalca podatkov prejme odškodnino za morebitno škodo, ki jo je posameznik utrpel, v kolikor bi prišlo recimo do zlorabe podatkov (Generalni direktorat za pravosodje, svobodo in varnost, 2010).

Isti vir tudi navaja, da mora upravljalec osebnih podatkov (bodisi gre za subjekt javnega bodisi zasebnega sektorja) izpolniti obveznosti, med katere sodijo zagotavljanje, da se pravice posameznika spoštujejo, da se podatki zbirajo samo za določene, posebne in zakonite namene, da so točni in ažurni ter da se ne hranijo dlje, kot je potrebno, da so izpolnjena merila za zakonito obdelavo podatkov (npr. da posameznik da soglasje ali podpiše pogodbo), zaupnost obdelave, varnost in zagotavljanje, da v primeru prenosa podatkov v države zunaj Evropske unije te države jamčijo ustrezno raven varstva.

### 3.5 Sporazum »Safe Harbor agreement«

Do sedaj smo spoznali, da sta si Evropa in ZDA na področju zakonodaje varstva osebnih podatkov različni. V kolikor vprašanja raznolikosti zakonodaje med tema dvema skupnostima ne bi rešili, bi taka urejenost povzročala težave pri poslovanju med državami, če poudarimo že znano dejstvo, da je svet globalen, kjer internet ne pozna meja in posledično tu velja prost pretok informacij. Po navedbah Kovačiča (2006, str. 79) Evropska Direktiva prepoveduje iznos osebnih podatkov v države, v katerih ni ustrezne zaščite informacijske zasebnosti. To vpliva na zakonodaje držav, ki niso članice Evropske unije. Po slovenskem Zakonu o varstvu osebnih podatkov (ZVOP-1) iz leta 2004 iznos osebnih podatkov v ZDA ni bil dovoljen, saj niso imele v celoti niti delno zagotovljene ustrezne ravni varstva osebnih podatkov.

To se je spremenilo po odločbi št. 0601-2/2010/5 z dne 26. 11. 2010, ko so se ZDA uvrstile na seznam tretjih držav kot država, ki zagotavlja ustrezno raven varstva osebnih pdoatkov v delu, ko gre za iznos osebnih podatkov organizacijam, ki delujejo po načelih varnega pristana (angl. Safe Harbor) (Informacijski pooblaščenec Republike Slovenije).

Konec devetdesetih let je skoraj prišlo do zaustavitve trgovanja med Evropo in ZDA po sprejetju te Direktive. Prišlo je do konfliktov med njima, saj ZDA niso izpolnjevale kriterijev, ki jih je postavila Evropska unija (Sullivan, 2006). ZDA so hkrati ta določila Evropske unije kritizirale, saj so menile, da so neprimerna in nezdružljiva s postopki v resničnem svetu (Kovačič 2006, str. 79).

Omejitve pretoka osebnih podatkov bi utegnile škodovati ameriškemu gospodarstvu (Kovačič 2006, str. 79). Sullivan (2006) navaja, da so se dvoletna pogajanja med Evropo in ZDA končala s posebnim sporazumom, imenovanim *Safe Harbor Agreement.* Ta sporazum predvideva overjanje ameriških podjetij, ki bo po taki overitvi lahko prejemala osebne podatke iz držav članic Evropske unije (Laurant v Kovačič, 2006).

Sporazum Safe Harbor sta ZDA in Evropa podpisale leta 2000 (Wafa, 2009), s podpisom pa se podjetja v ZDA strinjajo, da spoštujejo osnovna načela zasebnosti osebnih podatkov, ki jih navaja Evropska Direktiva o varstvu osebnih podatkov (Schriver, 2002).

Uporaba načel Safe Harbor (načel varnega pristana) v praksi torej pomeni, da je organizacija, ki želi prenesti osebne podatke organizaciji v ZDA ali v Evropsko unijo, ki se je tem načelom zavezala, najprej zavezana nacionalni zakonodaji, da zagotovi, da se podatki obdelujejo pravično in zakonito (Informacijski pooblaščenec Republike Slovenije).

Po navedbah istega avtorja načela varnega pristana določajo, da mora organizacija posameznike obvestiti o namenu zbiranja in uporabe njihovih osebnih podatkov. Prav tako mora posameznikom ponuditi možnost izbire o tem, ali se bodo njihovi osebni podatki razkrili tretji stranki ali se bodo uporabili za namen, ki je različen od tistega, s katerim so bili zbrani. Zavezanost načelom tako ščiti osebne podatke pred nepooblaščeno uporabo in določa, pod kakšnimi pogoji sme organizacija posredovati osebne podatke tretji osebi.

V kolikor se organizacija zaveže k upoštevanju načel varnega pristana, mora le-to javno razglasiti v svojih politikah zasebnosti oziroma politikah varnosti podatkov.

Ministrstvo za trgovino v ZDA (angl. Export Goverment) opozarja, da organizacije niso zavezane pristopiti k načelom sporazuma Safe Harbor, ampak da je njihova priključitev k temu prostovoljna. Organizacije lahko k načelom pristopijo na različne načine (Schriver 2002; Nijhawan Raj 2003; Regan 2003; Export Goverment 2009).

Isti avtorji omenjajo 7 principov, na katere se nanašajo mednarodni Safe Harbor principi (angl. International Safe Harbor Privacy Principles). Ti principi se nanašajo na:

- **Obveščanje:** organizacija mora obvestiti posameznike o namenu, za katere zbira in uporablja podatke o njih, kako stopiti v stik z organizacijo, če ima posameznik kakršno koli vprašanje ali pritožbo, katere so te tretje osebe, katerim bi posredovala podatke. To obvestilo mora biti za uporabnika jasno in nedvoumno še preden

organizacija posreduje podatke ali jih uporablja za druge namene, kot je bilo prvotno mišljeno.

- **Izbira:** organizacija mora dati posamezniku na voljo možnost izbire, ali bo dovolil posredovanje osebnih podatkov tretji osebi in uporabo podatkov za drug namen, kot so bili prvotno zbrani, ali ne. Občutljive podatke, kot so osebno zdravstveno stanje, rasna ali etična pripadnost, politična mnenja, verska ali filozofska prepričanja, članstvo v sindikatih in podatki o spolni usmerjenosti posameznika morajo posamezniki izrecno potrditi, ali jih lahko organizacije posredujejo tretjim osebam in uporabijo za drugoten namen, kot so bili sicer zbrani, ali ne. V vsakem primeru mora organizacija obravnavati kot občutljiv podatek vsak podatek, ki je bil prejet od tretjih oseb, kadar tretja oseba obravnava in opredeljuje podatek kot občutljiv.
- **Nadaljnji prenos:** za razkritje podatkov tretji osebi mora organizacija upoštevati prvi dve načeli, načeli obveščanja in izbire. Podatke lahko posredujejo naprej le tistim, ki zagotavljajo ustrezno zaščito, kot jo zahtevajo ti principi. Če organizacija ne izpolnjuje teh zahtev, potem ni odgovorna, kadar tretja oseba, kateri prenese te podatke, obdela na tak način, ki je v nasprotju z omejitvami in dogovori. Razen če se organizacija ne dogovori drugače in je vedela, da jih bo tretja oseba uporabila na drugačen način, ali če organizacija ne sprejme primernih ukrepov, ki bi preprečila te možnosti.
- **Varnost:** organizacije, katere osebne podatke ustvarjajo, vzdržujejo, uporabljajo ali razširjajo, morajo sprejeti ustrezne preventivne ukrepe, s katerimi zagotavljajo zaščito pred izgubo, zlorabo, nepooblaščenim dostopom, razkritjem, spreminjanjem in uničenjem.
- **Neokrnjenost podatkov:** v skladu z načeli morajo biti osebni podatki relevantni za namen uporabe, za katerega se zbirajo. Organizacija ne sme obdelovati osebnih podatkov na način, ki je nezdružljiv z nameni, za katere so bili zbrani. Organizacija mora sprejeti ustrezne ukrepe za zagotovitev, da so podatki zanesljivi, točni, popolni in trenutni.
- **Dostop:** posameznik mora imeti dostop do osebnih podatkov, ki jih zbira organizacija o njem in imeti možnost, da jih popravi, spremeni ali izbriše, kadar niso točni, razen v primeru, ko bi dostop povzročil ogroženost posameznika.
- **Uveljavitev:** učinkovita zaščita zasebnosti mora vsebovati mehanizme za zagotavljanje skladnosti s temi načeli in sankcije za organizacije, če tem načelom ne sledijo.

Na račun tega sporazuma je slišati precej kritik. Laurant (v Kovačič 2006, str. 79) tako navaja, da sporazum predvideva samo-certificiranje, saj je tako imenovani status sporazuma podeljen že s tem, ko se podjetje obveže, da bo spoštovalo načela o zaščiti zasebnosti. Schriver (2002) navaja, da so ZDA Evropi očitale preveliko samoregulacijo, hkrati pa naj bi bil sporazum preveč strog do podjetij v ZDA. Ravno nasprotno so se v Evropi zbali, da je sporazum premalo strog.

Hübner (v Praprotnik, 2006) vidi pomanjkljivosti zgoraj opisanih principov v tem, da ni zahteve glede prekomernosti zbirk, dolžine shranjevanja in anonimnosti. Ni tudi možnosti pritožbe neodvisnemu organu, nadaljni prenos temelji na strinjanju tretje stranke glede zaščite podatkov.

Nijhawan Raj (2003) je v začetku veljavnosti sporazuma videl tri glavne ovire, zaradi katerih se podjetja niso takoj odločala za pristop k temu sporazumu. Mednje uvršča stroške, ki bi nastali ob priključitvi k sporazumu, vključitev sodne veje oblasti in dejstvo, da je bilo v začetku zelo malo podjetij, ki je pristopilo k temu sporazumu.

Kritiki v ZDA menijo, da načela sporazuma posegajo v pravice posameznikov in pod vprašaj postavljajo ameriško suverenost. Hkrati se potrošniki čutijo diskriminirani v primerjavi z Evropejci, saj naj bi sporazum državljanom v Evropi nudil veliko večjo zaščito pred kršitvami njihovih pravic do zasebnosti s strani ameriških podjetij, kot jo nudi njihovim lastnim potrošnikom (Regan, 2003).

Evropski kritiki menijo, da sporazum ne nudi zadostne zaščite evropskim državljanom, saj se zanaša na samoregulacijski sistem, ki je v ZDA neuspešen (Regan, 2003).

Danes je število podjetij, ki so pristopila k sporazumu Safe Harbor, ogromno – po navedbah Ministrstva za trgovino v ZDA več deset tisoč(Export Goverment, 2009).

Z vidika diplomske naloge je zanimivo podjetje Google, ki k sporazumu Safe Harbor sprva ni pristopilo, vendar je po navedbah Ministrstva za trgovino v ZDA (Export Goverment, 2009) pristopilo prvič leta 2005 in nato še 2011. Google je izkoristil tako imenovani člen, ki omogoča organizacijam, da pristopijo k sporazumu na različne načine. Osebne podatke zbira in jih ročno obdeluje, vir teh podatkov pa so ljudje sami.

Google se v začetku, tako navaja Kovačič v Žbogar (2009), ni obvezal k odgovornosti za varnost podatkov svojih uporabnikov, temveč je v splošnih pogojih uporabe njihovih storitev

uporabnike seznanil s tem, da se »strinjajo s prenosom svojih osebnih podatkov v ZDA ali katerokoli drugo državo, kjer ima Google svoje podružnice«.

Za Google pristop k sporazumu Safe Harbor danes pomeni, da uporabniki Googlovih storitev, tako v Evropi kot v ZDA, dobijo ne le enako raven njihovih storitev, temveč tudi enako raven varstva zasebnosti. Hkrati je za podjetje zasebnost ključni dejavnik za uspeh na globalnem trgu (Google Policy Europe, 2011).

V okviru samoregulacije Google upošteva načela Safe Harbor med ZDA in Evropo, kot jih je določilo Ministrstvo za trgovino v ZDA v zvezi z zbiranjem, uporabo in shranjevanjem osebnih podatkov iz držav članic Evropske unije. Google se je zavezal, da upošteva načela zasebnosti Safe Harbor o obveščanju, izbiri, nadaljnem prenosu, varnosti, celovitosti podatkov, dostopu in uveljavljanju (Google, 2012).

Med države, iz katerih Google pridobiva osebne podatke, po podatkih Ministrstva za trgovino v ZDA (Export Goverment, 2009) sodijo: Avstrija, Belgija, Bolgarija, Ciper, Češka, Danska, Estonija, Finska, Francija, Grčija, Irska, Islandija, Italija, Latvija, Liechenstein, Litva, Luksemburg, Madžarska, Malta, Nemčija, Nizozemska, Norveška, Poljska, Porgualska, Romunija, Slovaška, **Slovenija,** Španija, Švedska, Švcia in Združeno kraljestvo Velike Britanije.

# 4 PREDSTAVITEV PODJETJA GOOGLE

»The world has been Googled. We don't search for information, we 'Google' it.« (Auletta, 2009). S temi besedami lahko opišem celotno zgodbo podjetja Google.

Google Inc. je ameriško multinacionalno podjetje, ki se nahaja v kraju Mountain View v zvezni državi Kalifornija. Google zagotavlja internetne storitve in produkte, vključno s svojim spletnim iskalnikom na internetu, računalništvom v oblaku, programsko opremo in s tehnologijo oglaševanja. Kot navaja Ruter (2007), podjetje ponuja vrsto uporabnih in večinoma brezplačnih orodij za poslovnega in vsakodnevnega uporabnika. V času pisanja te diplomske naloge so septembra dopolnili 14. let delovanja.

Podjetje je najbolj znano po svojem spletnem istoimenskem iskalniku, ki z vrhunskim algoritmom PageRank omogoča, da želene rezultate uporabnik najde zelo hitro. Sicer pa je podjetje nastalo kot rešitev za iskanje po internetu. Iskanje je še danes ena od glavnih dejavnosti, saj mu namenjajo največ razvojnih sredstev. Njihova logika temelji na pravilu, da

lahko uporabnik s hitrejšim in boljšim iskanjem vedno najde to, kar želi in to kadar koli in kjer koli (Google, 2012).

## 4.1 Zgodovina

Podjetje je bilo ustanovljeno 4. septembra 1998 (Google, 2012), ko sta se na ameriški univerzi v Stanfordu med doktorskim študijem spoznala njegova ustanovitelja, Larry Page in Sergey Brin (Skrt, 2004). Pri tem velja omeniti še dva pomembna datuma, ki sta povezana z začetki podjetja. Po navedbah Huša (2011) je bila njegova domena zakupljena 15. septembra 1998, povsem samovoljno pa so si izbrali datum 27. september, na katerega praznujejo rojstni dan.

Leta 1995 je Brin s strani Univerze v Stanfordu dobil nalogo, da le-to razkaže Pageu. Na njunem prvem srečanju se nista strinjala skoraj o ničemer (Google, 2012). Tudi Vise in Malseed (2005, str. 13) sta potrdila, da sta bila zelo različni osebnosti. Kljub temu sta hitro ugotovila, da imata podobne interese na raziskovalnem področju. Gre za področje pridobivanja in iskanja relevantnih informacij med ogromno količino podatkov (Skrt, 2004).

Larry in Sergey sta nesporazume hitro pozabila, pomembno vlogo v njuni raziskovalni dejavnosti pa je igral profesor na stanfordski univerzi, Dr. Terry Winograd, ki je Pagea opogumil in mu svetoval, naj se ukvarja s svetovnim spletom – internetom (Scott, 2008). Tako sta Page in Brin januarja 1996 začela sodelovati na razvoju internetnega iskalnika (Google, 2012), ki bi najdene rezultate iskanja rangiral tako, da bi višje na seznamu zadetkov uvrstili tiste strani, na katere se sklicujejo več drugih spletnih strani (Škrt, 2004). Iskalnik sta sprva poimenovala BackRub, ker je imel zmožnosti analiziranja povratnih povezav do določenih spletnih strani z namenom ugotavljanja njihove popularnosti. Osnova, ki sta jo razvila, je nekaj let kasneje pripeljala do razvoja PageRank sistema, ki ga Google pri iskanju in razvrščanju zadetkov uporablja še danes.

Po testnih verzijah iskalnika BackRub sta se ustanovitelja odločila za drugo ime. Izmed najrazličnejših možnosti sta se odločila za besedo google (Google, 2012). Prvič je o tem, zakaj sta za ime iskalnika izbrala ravno to besedo, Sergey spregovoril šele dve leti kasneje v svojem intervjuju za Washington Post. Dejal je, da je beseda google izpeljanka iz matematičnega termina za veliko število »googol«, kjer številu 1 sledi 100 ničel (Scott, 2008). Odločitev za takšno besedo je povsem razumljiva in logična, saj je poglavitna naloga iskalnika organizacija neskončne količine podatkov, ki se nahajajo na svetovnem spletu (Škrt, 2004).

Sprva sta bila Sergey in Larry do imena iskalnika skeptična, saj sta menila, da je neprimerno oziroma v nasprotju s tistim, kar je Dr. Winograd svetoval Larryu, to je raziskovanje svetovnega spleta (angl. World Wide Web). Kljub temu sta to ime ohranila in kmalu je iskalnik postal številka ena za iskanje po internetu (Scott, 2008).

### *4.1.1 Zagon podjetja*

Sprva sta oklevala ali bi sploh ustanovila podjetje, saj sta, kot navaja Scott (2008), iskala potencialne investitorje, ki bi z njima sodelovali. Z njuno iskalno tehnologijo pridobivanja najpomebnejših informacij sta želela premagati obstoječo konkurenco. Mnogi investitorji niso bili zainteresirani za sodelovanje, saj niso videli, da je povpraševanje po učinkovitem iskalniku na trgu resnično. Zato sta se odločila, da stopita na samostojno pot.

Leta 1998 sta prek profesorja na Univerzi v Stanfordu, Davida Cheritona, spoznala Andya Bechtolsheima (Vise in Malseed, 2005), soustanovitelja podjetja Sun, ki je njunemu podjetju napisal ček v vrednosti $100.000 (Google, 2012). Andy je po ogledu njune verzije iskalnika dejal, da je ideja spletnega iskalnika odlična in da sta razvila boljši način iskanja pomembnih informacij na internetu (Vise in Malseed, 2005).

Zgodba se je pričela z ureditvijo delovnih prostorov, odprtjem bančnega računa, kamor sta ustanovitelja položila znesek, ki jima ga je nakazal Andy, ter denar, ki sta ga zbrala s pomočjo prijateljev in sorodnikov ter nadaljevala z zaposlitvijo prvega zaposlenega in z oddajo vloge v Kaliforniji za registracijo podjetja.

## 4.2 Uspešnost podjetja

Ni skrivnost, da je Google daleč najuspešnejši iskalnik na svetu. Vprašanje, ki se mi samo po sebi postavlja pri tem pa je, zakaj je podjetje tako uspešno v prierjavi z drugimi in kaj ga naredi tako uspešnega, da se njegova rast še ne ustavi? Številni avtorji imajo svoje poglede in odgovore na vprašanja, v večini pa so si odgovori med seboj zelo podobni. Prvi odgovor poda Škrt (2004), ki med poglavitne prednosti uvršča enostavnost in učinkovitost iskanja ter preprost uporabniški vmesnik. Poleg naštetega pa tudi dejstvo, da je Google ves denar vložil v razvoj iskalnika in ne toliko v oglaševanje.

Glavni uspeh Googla temelji tudi na preprosti zamisli. Dosedanji iskalniki so za razvrščanje rezultatov uporabljali neučinkovite algoritme, ki uporabnikom večinoma niso postregli z želenimi rezultati. Page in Brin sta se domislila rešitve razvrščanja rezultatov glede na število povezav na določeno stran, in sicer več kot je povezav na določeno spletno stran, bolj je le-ta

popularna in s tem se stran tudi višje prikaže na seznamu zadetkov. Algoritem se je izkazal za odličnega in rast Googla se je pričela (EnaA magazin – DNE Tehno, 2012).

Drugi odgovor na zgornje vprašanje poda stran Wesearch.org. Glavni razlog uspešnosti podjetja Google je v tem, da podjetje zagotavlja daleč najboljše iskalne rezultate, po katerih poizvedujejo uporabniki interneta. Cilj podjetja je vedno bil in še vedno je nekaj, k čemur nenehno stremijo – to, da uporabnik dobi tisto, kar išče. Zato nenehno posodabljajo iskalne algoritme, ki zagotavljajo, da bodo iskalni rezultati najboljši in najbolj relevantni. To je le en razlog, zakaj so na področju iskalnikov vedno korak ali dva pred konkurenco.

Ista stran nadalje navaja, da je razlog za uspešnost podjetja tudi investiranje v tehnologijo. V iskalne algoritme vložijo zelo veliko denarja, zaradi katerega so ti boljši, kot bi bili sicer. Nadalje so v podjetju iznašli pravo pot, kako z iskalnimi poizvedbami zaslužiti denar. To jim omogoča tehnologija Adwords, s katero podjetja kupujejo prazen prostor med iskalnimi rezultati. To pomeni, da se uporabniku pri iskanju pojavljajo tudi oglasi teh podjetij. Oglaševalski trg pa je danes ena najbolj dobičkonosnih dejavnosti.

Dodaten vidik uspešnosti se kaže tudi v tem, da so v podjetju zgradili eno najbolj prepoznavnih blagovnih znamk v svetu. Dejstvo je, da Google ni samo ime podjetja, ampak je tudi beseda, ob kateri vsakdo dobi asociacijo za spletno iskanje in številne druge storitve.

Lenzie (2010) poleg zgoraj navedenih dejstev med uspešnost uvršča tudi zaposlene v podjetju, ki imajo unikatno delovno okolje, ki jih spodbuja k razvoju novih idej. Na drugi strani Hopkinson (2009) uspešnost podjetja vidi v štirih glavnih dejavnikih:

- znamka ali brand,
- številni izdelki in produkti,
- pomanjkanje konkurence in
- uspešnost iskalnih poizvedb.

Po mnenju Batemana (2012) so pomemben vidik uspešnosti tudi povratne informacije uporabnikov, zato je pomembno, da poslušajo uporabnike in se jim kar se da prilagodijo.

Uspešnost podjetja se kaže tudi v tem, da so njihovi izdelki in storitve v večini brezplačne. V podjetju skušajo le-te prilagoditi uporabnikom in jim izboljšati uporabniško izkušnjo. Hkrati vlagajo v gradnjo nove in posodobitev obstoječe infrastrukture, sklepajo številna partnerstva z drugimi podjetji (AOL, Mozilla, Yahoo!, Apple, Microsoft, itd.), poleg naštetega odpirajo

pisarne in predstavništva po vsem svetu in se tako še približajo svojim uporabnikom, prirejajo tekmovanja v ranljivosti varnostnega sistema, kjer ponudijo visoke nagrade tistim, ki vdrejo in najdejo pomanjkljivosti v varnostnem sistemu podjetja. Nadalje podjetje redno skrbi, da so njihovi izdelki in storitve dostopne čim širši populaciji sveta s številnimi jezikovnimi vmesniki, svoje inovacije zaščitijo s patenti, velik poudarek pa dajejo tudi zadovoljstvu zaposlenih.

Menim, da uspeh podjetja tiči tudi v tem, da Google ni podjetje, ki bi se moralo prilagajati spremembam na trgu, temveč oni povzročijo spremembe, katerim se morajo ostali prilagajati. Na ta način obvladujejo svetoven splet.

Neglede na uspešnost podjetja in dejstvo, da velja danes za eno največjih tehnoloških podjetij, pa EnaA Magazin v svojem članku (2012) navaja, da je Google z rastjo postajal tudi vedno bolj okoren in izgubil del zagnanosti, ki je bila prvih 10 let njegovo gonilo razvoja. Danes njihove poteze zaznamuje tipična kapitalistična preračunljivost in ne toliko inovacije, kar je v trenutnih razmerah dobro za podjetje, mnogo manj pa za njegove uporabnike.

# 5 POLITIKA ZASEBNOSTI PODJETJA GOOGLE

»One policy, one Google experience« oziroma »En pravilnik, eno doživetje Googla«. Tako se glasi uvodni stavek nove politike zasebnosti in pogojev storitev, ki ju je podjetje Google spremenilo in uvedlo z dnem 1. marec 2012 (Google, 2012).

## 5.1 Načela zasebnosti

Preden obravnavam politiko zasebnosti podjetja in pogoje uporabe, je potrebno narediti kratek pregled tudi pri načelih zasebnosti. Vsi omenjeni predpisi so zelo pomembni za slehernega uporabnika storitev, saj z njimi podjetje določa, pod kakšnimi pogoji lahko uporabnik uporablja storitve in po katerih pravilih se mora ravnati. Teoretično bi jih moral prebrati vsak uporabnik, preden prične uporabljati storitve ali izdelke nekega podjetja, in sicer (1), da se seznani, kako podjetje zagotavlja varnost in zasebnost uporabnika, (2) katere osebne podatke potrebuje in zakaj jih potrebuje, (3) s kakšnim namenom jih zbira in obdeluje, (4) kakšne so obveznosti podjetja do uporabnika in obratno ter (5) kaj uporabnik sme oziroma česa ne sme početi pri uporabi teh izdelkov in storitev. V praksi pa to stori le redkokdo, saj so v večini predpisi prepredeni s pravniško terminologijo, so zelo dolgi in za marsikoga tudi zamudni. Večina ljudi vedno sprejme vse mogoče, samo da bi lahko začeli uporabljati določene storitve.

Načela zasebnosti podjetja, za razliko od politike zasebnosti in pogojev uporabe, se v vseh teh letih niso posebej spreminjala, saj se jih podjetje drži že od svojega samega začetka.

Osnovno poslanstvo podjetja je organiziranje informacij vsega sveta. Izdelki so inovativni in v koraku s časom. Njihova načela zasebnosti so vodilo pri odločitvah na vseh ravneh podjetja, da zavarujejo uporabnike pri njihovi uporabi. V ta namen ima Google definiranih 5 načel zasebnosti (Google Privacy Principles, 2012):

- **Podatke želijo uporabiti, da uporabnikom ponudijo uporabne izdelke in storitve:** na podlagi podatkov, ki jih dobijo od uporabnikov, razvijajo storitve in izdelke po meri uporabnika, saj s tem zagotavljajo izboljšanje funkcij in varnosti izdelkov.
- **Izdelke razvijajo po strogih standardih in postopkih zagotavljanja zasebnosti:** z različnimi orodji omogočajo uporabnikom urejanje osebnih podatkov na preprost in dostopen način. Spoštujejo zakonodajo, ki ureja zasebnost.
- **Zbiranje osebnih podatkov poteka pregledno:** sledijo načelu, da mora posamezen uporabnik vedeti, kateri podatki se zbirajo o njem in s katerimi podatki prilagajajo storitve. Izdelek *Google Nadzorna plošča* odgovori uporabniku na vprašanje »Kaj Google ve o meni?« Tu se nahajajo vsi podatki, ki jih je uporabnik vnesel in shranil v svoj račun, hkrati pa mu omogoča urejanje in brisanje teh podatkov.
- **Uporabnikom želijo ponuditi smiselne možnosti izbire pri varovanju zasebnosti:** uporabnikom zagotavljajo nadzor nad njihovimi osebnimi podatki z nekaterimi orodji za zagotavljanje zasebnosti. Tako lahko uporabniki šifrirajo promet med računalnikom, ki ga uporabljajo, in Googlom, zasebno brskajo po spletu v nevidnem načinu (to možnost ponujajo praktično vsi brskalniki v svojih nastavitvah), brišejo zgodovino iskanja, izvažajo osebne podatke iz Googlovih izdelkov, izklopijo prilagojeni način iskanja glede na njihove predhodne aktivnosti in podobno.
- **Skrbno varujejo zbrane podatke:** zavedajo se odgovornosti za varovanje podatkov, ki jim jih zaupajo uporabniki. Na tem področju sodelujejo s številnimi uporabniki, razvijalci in zunanjimi strokovnjaki za varnost. Njihovi samodejni pregledovalniki ščitijo uporabnike pred zlonamerno programsko opremo, prevarami, poneverbami in neželeno elektronsko pošto. V primeru težav z računom ali sumničavostjo, da so bili njihovi podatki zlorabljeni, lahko svoje težave sporočijo ustrezni podporni službi Googla, ki bo preverila vzrok težav in jih skušala odpraviti.

## 5.2 Pogoji uporabe storitev

### *5.2.1 Primerjalna analiza starih pogojev uporabe storitev z novimi*

Že prvi pogled na oba dokumenta nazorno pokaže, da je novi dokument pogojev storitev znatno krajši, preglednejši in bolj razumljiv od starih pogojev.

V uvodni točki dokumenta (Google Terms of Services, 2012) bistvenih razlik ni, saj oba natančno definirata, kdo zagotavlja izdelke in storitve podjetja Google in kje je glavni kraj poslovanja podjetja. Oba tudi uporabnike pozivata, naj pazljivo preberejo pogoje uporabe storitev. Opaziti je, da so stari pogoji bistveno težje razumljivi, saj vsebujejo številne odstavke, ki so si na tak ali drugačen način podobni in so razvlečeni do te mere, da je uporabniku iz odstavka v odstavek manj jasno, o čem sploh pogoj govori. Včasih se je Google poleg splošnih pogojev posluževal tudi dodatnih pogojev, ki so skupaj tvorili pravno zavezujoč sporazum med končnim uporabnikom in Googlom, v primeru nasprotij med tem, kar določajo dodatni pogoji in tem, kar določajo splošni pogoji pa so prednost imeli dodatni pogoji. Novi tako izčrpne definicije ne navajajo, niti ne definirajo, kateri pogoji imajo prednost pred katerimi v primeru nasprotij, čeprav tudi v novih pogojih veljajo tako splošni kot tudi dodatni (npr. nekatere vsebine na YouTube zahtevajo tudi starost uporabnika). Glavna razlika je predvsem v tem, da je v starih pogojih to razloženo skozi štiri odstavke, v novih pa zgolj v enem samem.

Drugi člen starega dokumenta se nanaša na sprejem pogojev, kjer je bilo potrebno za uporabo storitev obvezno strinjanje s pogoji uporabe, v nasprotnem primeru pa se teh storitev uporabnik ne sme posluževati. Navedli so, na kakšne možne načine se je lahko uporabnik strinjal s pogoji in na kakšne načine jih ni smel uporabljati. Včasih je tako veljalo, da uporabnik ni smel uporabljati storitev, če (1) še ni dosegel starosti, ki jo je zakon določal za pridobitev poslovne sposobnosti in (2) če mu je po zakonih ZDA ali drugih držav, vključno z državo, kjer je imel stalno prebivališče, bil prepovedan dostop do uporabe teh storitev. Novi pogoji ne navajajo niti starostne omejitve, niti zakonske ne. Strinjanje s pogoji je povsem zadosti.

Pri tem je zanimivo dejstvo, da stari pogoji sploh niso definirali, kaj je potrebno imeti za uporabo Googlovih storitev. Za uporabo večine Googlovih izdelkov in storitev uporabnik namreč potrebuje Google račun. Med osnovne storitve denimo sodijo elektronska pošta (Gmail), koledar (Calendar), blog (Blogger), fotografije (Picasa), prostor v oblaku za shranjevanje datotek in kreiranje dokumentov, preglednic, predstavitev (Drive), klepet s

prijatelji (Chat) in tako dalje. Obstajajo tudi nekatere osnovne storitve, ki ne potrebujejo Google računa. Mednje sodijo iskalnik, iskalnik slik, zemljevidi, prevajalnik in drugi. Na drugi strani novi pogoji jasno in nedvoumno razložijo, da je za nekatere storitve potreben Google račun, ki ga uporabnik pridobi tako, da odpre svoj Google račun ali pa mu ga dodeli skrbnik, npr. delodajalec ali izobraževalna ustanova. Hkrati novi pogoji tudi jasno povedo, da lahko v tem primeru veljajo tudi dodatni pogoji, kjer lastnik dostopa do uporabnikovega računa.

Naslednja zanimiva točka pogojev se nanaša na zagotavljanje storitev, kjer so stari pogoji navajali, da bodo uporabniku nekatere storitve v imenu podjetja Google zagotavljale njegove hčerinske in povezane družbe. Poleg tega se je uporabnik moral strinjati in zavedati dejstva, da se Google nenehno posodablja, oblika in narava storitev se spreminjata in to brez predhodnega obvestila končnega uporabnika. Novi pogoji ne omenjajo družb, ki jih pooblašča Google, temveč uporabljajo enotno družbo Google; kar pa se tiče posodabljanj storitev, uporabnike sedaj predhodno obveščajo o spremembah. Tako so bili vsi uporabniki leta 2011 deležni velike Googlove posodobitve celotne grafične podobe, kjer je Google za vse izdelke in storitve poskrbel z novim izgledom. Še preden je celoten Google prešel na nov izgled, so uporabnikom ponudili možnost izbire:

- takojšen prehod na nov izgled ali
- postopen prehod na nov izgled.

S prehodom na nov izgled so povzročili precejšen kaos na globalnem spletu, saj se ljudje novega izgleda niso mogli navaditi. Kritike so letele na njegovo nepreglednost, mnogi pa niso mogli razumeti, zakaj so šli spreminjati nekaj, na kar so se ljudje dodobra že navadili. S tem je Google uporabil tako imenovano sistemsko spremembo 1. reda, ki prisili uporabnike, da uporabljajo te storitve in izdelke v novi preobleki zato, ker jih morajo. Le redki uporabniki pa so videli v tem prednosti pred starim izgledom. Sprva so uporabnikom še nudili možnost postopnega navajanja na nov izgled, po nekaj mesecih pa so to možnost ukinili in od takrat naprej prehod na stari izgled ni več dostopen.

Uporaba storitev je bila v starih pogojih zelo slabo razložena, saj se je Google na nekaterih točkah začel podvajati, hkrati pa je po odstavkih našteval, s čim vse se mora uporabnik strinjati in s čim ne. Na drugi strani je v novih pogojih enostavno razloženo, da se storitev ne sme zlorabiti, da se do njih lahko dostopa le preko veljavnega uporabniškega vmesnika, da uporabnik ne sme na kakršen koli način pridobiti izvorno programsko kodo, za razliko od

starih pa je Google v novih pogojih dodal še možnost, da lahko vedno in kadar koli pregledujejo uporabnikovo vsebino, s čimer že posegajo v njegovo zasebnost.

Vsak uporabnik je odgovoren za vsebino, ki jo pusti pri Googlu oziroma za podatke, ki jih vnaša. Področje zasebnosti in avtorskih pravic včasih ni bilo dobro urejeno, saj Google ni povsem priznaval intelektualne lastnine, bolj kot ne si je uporabnikovo lastnino lahko tudi prilastil, poleg tega tudi ni dobro zaščitil uporabnika pri žaljivi ali sporni vsebini, temveč je vso odgovornost pripisal izključno uporabniku. Danes je to področje nekoliko drugače urejeno, saj se Google drži reka »Kar je v vaši lasti, tudi ostane vaše«, vendar s to razliko, da danes, ko uporabnik prenese kakršno koli vsebino, Googlu še vedno podeli pravico, da uporablja preneseno vsebino, vendar za omejen namen delovanja. Ta namen je razvoj novih in izboljšava obstoječih storitev.

Oba dokumenta preideta na isto temo v členu programske opreme, kjer še danes velja, da ima Google vso pravico, da se programska oprema, ki jo uporabnik uporablja, samodejno posodobi. Na ta način zagotavljajo, da so uporabniki v koraku s časom in da imajo vedno na voljo najnovejšo različico programske opreme. Za razliko od starih pogojev se je Google čedalje bolj pričel zavedati tudi odprtokodnosti, saj je temu namenjal velik del pozornosti. Uporabnikom je dal na voljo odprtokodno licenco, ki pa jo je uporabnik lahko naprej razvijal.

Kadar je uporabnik želel prenehati uporabljati storitve podjetja Google, se je le-ta včasih posluževal dveh metod, in sicer s pisnim obvestilom podjetju ali z zaprtjem računov za vse storitve, ki jih je uporabljal. Google je lahko tudi enostransko prekinil pravni sporazum z uporabnikom, če je ugotovil, da je le-ta kršil katero koli določbo pogojev, ali če je Google prenehal z nadaljnim zagotavljanjem storitev v tej državi, ali pa če trg tega preprosto ni več dopuščal. Danes za prenehanje uporabe njihovih storitev ni potrebno pisno obvestiti nikogar, temveč se v nastavitvah računa pobriše vse podatke povezane z računom in račun zapre. V primeru, da bo Google nekatere storitve ukinil ali uvedel, to stori tako, da predhodno obvesti uporabnika. Praksa ukinjanja nekaterih storitev, tistih, ki niso več aktualne, je taka, da Google običajno šele leto ali dve leti po obvestilu storitev ukine, hkrati pa uporabniku vedno ponudi možnost alternative. Pri tem mi je zanimivo tudi dejstvo, da Google ne omogoča odprtja istega računa, v kolikor je bil enkrat že zaprt.

Za konec velja omeniti še dvoje – najprej o izključevanju jamstev in omejitvi odgovornosti. Po obeh pogojih, tako starih kot novih, Google zagotavlja storitve po načelu »Take, kot so«, ne dajejo jamstva glede vsebine v storitvah in posameznih funkcij, ki so na voljo v storitvah,

ter glede njihove zanesljivosti, razpoložljivosti, hkrati tudi ne zagotavljajo, da bo uporaba storitev zahtevala potrebam uporabnika, da bo nemotena, pravočasna, varna in brez napak ter da bodo popravljene napake pri delovanju ali funkcionalnosti storitev. Nadalje se Google odpoveduje tudi kakršni koli odgovornosti za škodo, bodisi izgubi dobička, prihodkov, podatkov itd., ki jo utrpi uporabnik.

V primeru poslovne uporabe storitev (to navajajo zgolj novi pogoji) bo Google poravnal vso škodo v zvezi s kakršnim koli tožbenim zahtevkom, ki izhaja iz uporabe storitev ali s kršitvijo teh pogojev.

Eden izmed zadnjih členov še pravi, da je včasih veljalo, da so vse spore, ki izhajajo iz teh pogojev ali storitev oziroma so povezani z njim, urejala pristojna sodišča v Angliji. Danes se sodi po zakonih zvezne države Kalifornije v ZDA in vsi zahtevki se bodo reševali izključno na zveznih ali državnih sodiščih okraja Santa Clara v Kaliforniji, ZDA.

### 5.3 Nova politika zasebnosti

Novo politiko (z drugimi besedami tudi pravilnik) zasebnosti (Google Policy Privacy, 2012) je Google napovedoval dolgo časa, sprejel pa jo je s 1. marcem 2012. Mnogi varuhi človekovih pravic, Evropska komisija in številni strokovnjaki za zasebnost na internetu so jo sprejeli s številnimi dvomi, saj menijo, da nova politika zasebnosti močno posega v zasebnost posameznika.

Na Googlu lahko uporabnik praktično počne kar koli. Njihove storitve imajo številne namene, od iskanja, deljenja podatkov z drugimi, komunikacije ali ustvarjanja nove vsebine. Google vseskozi poudarja, da je ključen namen nove politike zasebnosti doseči zgolj to, da lahko na podlagi uporabniških osebnih podatkov še izboljšajo uporabniško izkušnjo, izboljšajo storitve in uporabniku prikazujejo ustreznejše rezultate iskanja in oglase. Pravilnik vsebuje tri ključne elemente, in sicer (1) katere podatke podjetje zbira in zakaj jih zbira, (2) kako uporabljajo zbrane podatke in (3) možnosti dostopa ter urejanja podatkov.

Podjetje vseskozi trdi, da je zasebnost uporabnika zanje na prvem mestu. Podatke zbirajo na dva načina. Prvi način je, da od uporabnika zahtevajo nekatere osnovne podatke, ko le-ta ustvari svoj račun na Googlu. Med obvezne podatke sodijo ime, priimek, elektronski naslov, starost. Po želji lahko uporabnik naloži še svojo fotografijo. V kolikor želi uporabnik svoje podatke (npr. fotografije, statuse ipd.) deliti z drugimi osebami, mora za skupno rabo ustvariti javno viden Google Profil. Drugi način zbiranja podatkov pa je pridobivanje podatkov

medtem ko uporabnik uporablja njihove storitve. Kadar uporabnik obišče neko spletno mesto, Google izve podatke o napravi, s katero dostopa do Googlovih storitev (npr. model strojne opreme, različica operacijskega sistema, informacije o omrežju ipd.), hkrati pa te podatke poveže z uporabniškim Google računom.

Nadalje so tu dnevniški podatki, ki jih Google shranjuje v svojih strežnikih. Mednje sodijo podatki o tem, kako je uporabnik uporabljal storitev, kakšne iskalne poizvedbe je iskal, ura in datum poizvedb, naslov IP številke, podatki o aktivnosti sistema, vrsti brskalnika, jeziku brskalnika, piškotkih in tako dalje. Google lahko tudi zbira in obdeluje podatke o dejanski lokaciji, kjer se uporabnik nahaja s pomočjo GPS sistema. Lokacijo uporabnika lahko dobijo tudi z različnimi tehnologijami, kot so senzorski podatki uporabnikove naprave, na podlagi katerih je mogoče pridobiti informacije o dostopnih Wi-Fi točkah in baznih postajah v bližini. Google hkrati beleži tudi zgodovino iskanja uporabnika in tako ustvarja neverjetno veliko bazo podatkov o uporabniku.

Vse podatke, ki jih zberejo v svojih storitvah, uporabljajo za zagotavljanje, vzdrževanje, zaščito in izboljšanje teh storitev, za razvoj novih ter varovanje Googla in njihovih uporabnikov. Pridobljene podatke uporabljajo zato, da lahko uporabniku ponudijo prilagojene vsebine, torej tisto, kar uporabnika zanima oziroma kar uporabnik preferira. Tako uporabniku prikazujejo tiste oglase, ki ga zanimajo in jim vrne ustreznejše iskalne rezultate.

V primeru, da uporabnik kontaktira podporno službo podjetja vodijo celotno evidenco komunikacije, ki jim pomaga pri reševanju morebitnih težav. Elektronski naslov uporabnika uporabljajo za obveščanje o storitvah, npr. ukinjanju nekaterih storitev, uvajanju novih, skratka o spremembah, ki se dogajajo. Uporabnikovo ime uporabljajo v vseh storitvah, ki jih ponujajo. Tako je omogočeno, da ima uporabnik za vse Googlove storitve na voljo le en Google račun, v katerega se stekajo vsi podatki tistih storitev, ki jih uporabnik uporablja.

S piškotki želijo izboljšati uporabniško izkušnjo v smislu, da shranijo jezikovne nastavitve uporabnika, da lahko v prihodnje ponudijo isto storitev v izbranem jeziku. V podjetju pa so se obvezali, da s piškotki ne bodo povezovali občutljive kategorije, npr. podatke povezane z raso, vero, zdravjem in druge.

Osebne podatke iz ene storitve lahko združijo s podatki iz druge storitve, saj s tem omogočajo lažjo skupno rabo z ljudmi, ki jih uporabnik pozna. Za povezovanje podatkov izrecno

zaprosijo soglasje uporabnika. Tudi za uporabo podatkov v namene, ki niso opisani v tem pravilniku, bodo zaprosili za soglasje.

Google potrebuje za obdelavo ogromnih količin osebnih podatkov tudi zmogljive strežnike po vsem svetu. Tako nova politika določa tudi, da lahko osebne podatke uporabnika obdelujejo v drugi državi, v kateri uporabnik prebiva.

Vsak uporabnik ima na voljo nekatere storitve, s katerimi lahko nadzoruje svoje osebne podatke. Seveda te ne omogočajo vpogleda in nadzoa nad popolnoma vsemi podatki, vendar le na nekatere vrste podatkov, povezanimi z uporabniškim računom. Nadalje ima možnost urejati tudi nastavitve oglasov, katere kategorije zanimajo posameznika, nastavitve, kdo vse lahko vidi profil posameznika in s kom vse lahko daje v skupno rabo svoje podatke.

V kolikor uporabnika skrbi za svoje podatke in se želi izogniti temu, da bi Google zbiral njegove podatke, lahko tudi onemogoči piškotke v brskalniku. S tem pa ne bo dosegel veliko, saj je Google sprogramiran tako, da številne storitve brez omogočenih piškotov ne bodo delovale pravilno. S tem prav za prav uporabnik popolnoma ničesar ne pridobi, čeprav mu Google to možnost ponuja.

Še večji poseg v zasebnost so podatki, ki jih uporabnik da v skupno rabo. S tem uporabnik dokončno izbriše svojo zasebnost, saj podatke daje v javno skupno rabo, ki jih indeksirajo iskalna orodja. Tako lahko kdor koli najde tega uporabnika in vidi njegove podatke.

Vsak uporabnik mora tudi skrbeti, da so njegovi podatki točni in ažurni. Teoretično je možno tudi poslati lažne podatke, vendar Google lahko slej kot prej z naprednimi tehnologijami odkrije prevarante. Še eden izmed številnih posegov v zasebnost je telefonska številka uporabnika, ki jo Google želi z namenom, da bi uporabnika zaščitil pred nepooblaščenim dostopom v njegov uporabniški račun. S telefonsko številko Google namreč želi uporabniku ponuditi možnost dvostopenjske prijave v njegov račun. Če številke ne pozna, potem se ne more prijaviti v račun.

V novem pravilniku zasebnosti je omogočeno, da si Google celo izmenjuje uporabnikove osebne podatke z drugimi družbami, organizacijami in posamezniki zunaj Googla pod pogojem, da pridobijo izrecno soglasje uporabnika ali soglasje skrbnika domene. Predvsem pri slednjem vidim nov poseg v zasebnost posameznika, saj so skrbniki domene ljudje v organizaciji ali ustanovi, ki uporabljajo Google Apps. V kolikor je uporabnik del te

organizacije in uporablja to storitev, ima le-ta dvojno skrb. Ne samo da ga nadzoruje Google, nadzoruje ga tudi skrbnik te domene.

Google si izmenjuje uporabnikove osebne podatke tudi za zunanjo obdelavo in zaradi zakonskih razlogov. Za zunanjo obdelavo pošljejo podatke svojim odvisnim družbam ali zaupanja vrednim podjetjem, da v njihovem imenu obdelajo uporabnikove osebne podatke skladno s pravilnikom o zasebnosti. Med zakonske zahteve pa spadajo npr. zahteve državnih organov, vlade, odkrivanje, preprečavanje goljufij, varnostnih ali tehničnih težav, zaščita pred kršitvijo pravic in podobne.

Pri tem Google postreže z zanimivo statistiko, koliko zahtev državnih organov, vlade, agencij ipd. prejmejo v podjetju za posredovanje osebnih podatkov. V šestmesečnem obdobju julij–december 2011 so prejeli največ, kar 6.321 zahtev v ZDA, najmanj pa iz Nizozemske, ki je zahtevala le 37 prošenj. Slovenija, sodeč po seznamu, še ni zahtevala posredovanja osebnih podatkov (Google Transparency Report: User Data Request, 2012).

Google si prizadeva tudi za varnost podatkov, ki jih hranijo. Za varnost skrbijo s šifrirano povezavo med odjemalcem in strežnikom, to je protokol, imenoval Secure Sockets Layer (SSL),ki omogoča preverjanje v dveh korakih, pri dostopu do Google računa, funkcija varnega brskanja v brskalniku Chrome, dostop do osebnih podatkov dovoljuje le svojim zaposlenim, pogodbenim sodelavcem in posrednikom, ki jih zavezujejo stroge pogodbene obveznosti glede zaupnosti.

### 5.4 Stara politika zasebnosti

Stara politika zasebnosti je veljala od leta 2000, ko je Google izdal svoj prvi pravilnik, pa vse do začetka leta 2012. Skozi vsa ta leta se politika vsebinsko ni veliko spreminjala kot v primeru sprejetja povsem nove, temveč je bila deležna zgolj nekaterih posodobitev. S primerjalno analizo želim povzeti nekatere ključne informacije, ki so veljale vsa ta leta, dokler ni bila sprejeta povsem nova politika zasebnosti.

V tistih letih je za vsako storitev veljal svoj pravilnik, le-teh je bilo več kot 60, s čimer ni bilo zagotovljenega pregleda nad vsemi storitvami. Tako se je moral uporabnik za vsako storitev, ki jo je želel uporabiti, posebaj strinjati s pogoji uporabe in politiko zasebnosti. Danes je to potrebno storiti le enkrat – ko se prijaviš v Google Račun.

Včasih se je Google držal načel varnega pristana (v tej diplomski nalogi sporazum Safe Harbor), vendar le za načela, ki so veljala v ZDA in je bil prijavljen v program varnega

pristana Ministrstva za trgovino v ZDA (Export Goverment). Kasneje so začeli upoštevati tudi načela med ZDA in Evropsko unijo ter načela med ZDA in Švico.

Ena izmed precej uporabnih zadev je bila tudi ta, da za številne storitve ni bilo potrebno ustvariti Google računa, posledično s tem ni bilo potrebno posredovati osebnih podatkov. Danes veliko storitev zahteva Google račun, zato je tudi podatkov veliko več. Stara politika tudi ni povezovala uporabniških podatkov z drugimi računi. V primeru, da je imel uporabnik odprt račun pri Googlu, mu je le-ta omogočil, da si je privzeto pregledoval elektronsko pošto, koledar, in ostale. V primeru, da je želel uporabiti katero drugo Googlovo storitev, npr. gledanje videoposnetkov in poslušanje glasbe na YouTube ali na katero koli drugo storitev, se je moral posebej registrirati na ta portal. Danes tega ni potrebno storiti, saj je z enim računom možen dostop do vseh storitev.

Obe politiki si prvič prideta skupaj v točki zbiranja podatkov. Včasih so podatke zbirali tako, da je za nekaj podatkov poskrbel uporabnik sam, ko je uporabljal Googlove storitve, za preostali del podatkov pa je poskrbel Google, ki je med uporabljanjem storitev od uporabnika pridobival številne podobne informacije, kot so bile opisane že v novi politiki zasebnosti (piškotki, dnevniške informacije, lokacija ipd.). Da pa stvar v tej točki ne bi izgledala tako enostavna, je ena izmed ključnih razlik ta, da včasih uporabnik ni imel možnosti, da bi mu Google prikazoval vsebine, ki jih uporabnik preferira, hkrati pa uporabnik ni imel možnosti deljenja podatkov oziroma dajanja podatkov v skupno rabo z drugimi ljudmi. To je tudi pomenilo, da uporabnik ni imel javnega profila na Googlu in da se njegovi podatki niso indeksirali z iskanjem po svetovnem spletu. Vse to izhaja iz razloga, da so Googlu spodleteli številni poizkusi s prisotnostjo na socialnih omrežjih z lastno storitvijo. Google Buzz in Google Wave sta po nekaj tednih hitro postala zgodovina in bila poslana na ukinitev, novi poizkus Google+ se zaenkrat še drži, vendar tudi ta še ni dosegel priljubljenosti, kot jo ima npr. Facebook.

Tako stara kot nova politika zasebnosti si skupaj prideta tudi v točkah namena zbiranja in uporabljanja pridobljenih podatkov, izmenjave podatkov z drugimi družbami ali posamezniki, pa tudi možnosti izbire, s katerimi lahko uporabnik upravlja in pregleduje, katere osebne podatke Google o njemu zbira.

Ne samo, da je stara politika zelo obsežna, slabo razumljiva in razpršena na več kot 60 različnih politik, v njej opazim še dve pomankljivosti. Prva je dejstvo, da ni jasno opredeljeno, na kakšen način je Google skrbel za varnost podatkov. Omenjala je le ustrezne

varnostne ukrepe, s katerimi so ščitili podatke pred nepooblaščenim dostopom, ne navaja pa, kateri so ti varnostni ukrepi sploh bili. Kot druga pa je dejstvo, da ni ponujala možnosti dvostopenjske prijave v račun oziroma dvostopenjske verifikacije. Četudi je res, da s telefonsko številko, kot jo zahteva nova politika, Google pridobi še en osebni podatek več, vendar je v tem primeru lahko uporabnik zagotovo prepričan, da mu napadalec ne bo tako zlahka vdrl v njegov osebni račun, kot bi lahko pred uvedbo telefonske številke za prijavo v račun.

### 5.5 Kritični pogledi na Googlovo politiko zasebnosti

Prvi kritični pogled na novo Googlovo politiko zasebnosti je podala Francoska komisija za informatiko in svoboščine (CNIL), ki očita Googlu, da z novo politiko krši *Evropsko Direktivo 94/46/EC*, ki se nanaša na varovanje osebnih podatkov in prost pretok teh podatkov. Menijo namreč, da v novi politiki ni mogoče jasno videti, za katere namene se bodo zbirali osebni podatki, temveč je namen zbiranja osebnih podatkov preveč splošno definiran. Za povprečnega uporabnika, ki bere nov pravilnik, to pomeni, da le-ti ne morejo razlikovati, kateri podatki so trenutno pomembni za uporabo določene Googlove storitve. Nadalje trdijo, da dejstvo, da Google obvešča uporabnike o tem, česa ne bo storil s podatki, ni zadosti za zagotavljanje splošnih informacij. Zahtevajo, da bi moral Google dopolniti obstoječe informacije s specifičnim namenom uporabe informacij, ki jih zbirajo. CNIL je zaskrbljen tudi nad povezovanjem podatkov iz različnih storitev, saj menijo, da je zelo težko natančno vedeti, kateri podatki so s kakšnim namenom združeni s posamezno storitvijo. CNIL in EU imata pomisleke in izražata zaskrbljenost nad novo Googlovo politiko zasebnosti (CNIL, 2012).

Tudi Evropska komisarka za pravosodje, Viviane Reding, pravi, da nova politika krši evropsko zakonodajo, saj se pri njeni implementaciji niso posvetovali z javnostjo in ne deluje v skladu z načelom preglednosti in omogoča deljenje podatkov s tretjimi osebami, ne da bi uporabniki imeli možnost odjave (opt-out). Tudi nova evropska uredba o varovanju osebnih podatkov, katere osnutek je bil predstavljen 25. januarja 2012, pa je v celoti v nasprotju z Googlovo politiko (Huš, 2012c).

V Sloveniji je svoj pogled predstavila tudi informacijska pooblaščenka Nataša Pirc Musar, ki meni, da je z novo politiko zasebnosti zelo težko preprečiti pojav zlorabe osebnih podatkov za druge namene. Pravi tudi, da nov pravilnik nevarno posega ali celo presega meje sorazmernosti, ki je eno izmed temeljnih načel v slovenski zakonodaji Zakona o varstvu

osebnih podatkov (ZVOP-1). Problem, ki ga vidi, je tudi v tem, da se po slovenskem zakonu lahko osebni podatki v zasebnem sektorju obdelujejo bodisi na podlagi zakona bodisi na podlagi osebne privolitve. Google pa svojega sedeža nima na območju Republike Slovenije, območju, na katerem je za nadzor nad obdelavo osebnih podatkov pristojen Pooblaščenec (Informacijski pooblaščenec Republike Slovenije).

Zgoraj napisane kritike so bili prvi komentarji na bežen pregled nove politike zasebnosti, še preden so nadzorni organi Evropske unije izvedli preiskavo zoper podjetja Google. V času pisanja te diplomske naloge je bilo sprva potrebno na podrobnejše informacije o tem, ali krši Evropsko zakonodajo, kot trdita CNIL in Evropska komisija, še počakati. Nadzorni organi za varstvo podatkov v EU (v okviru Delovne skupine iz člena 29, ki povezuje evropske nadzorne organe za varstvo osebnih podatkov) v zvezi z Googlovo novo politiko zasebnosti še izvajajo preiskave o tem, ali Google obdeluje podatke skladno z veljavnimi pravili in pri tem spoštuje pravico posameznikov, da se njihovi podatki obdelujejo na zakonit, korekten in preglede način (Parlamentarna vprašanja Evropskega parlamenta, 2012).

Zgodba je prvi epilog dobila sredi meseca oktobra, ko so evropski nadzorniki s skupnim pismom Google pozvali, naj upošteva priporočila in sprejme ukrepe za zavarovanje osebnih podatkov in zasebnosti evropskih uporabnikov (Informacijski pooblaščenec Republike Slovenije). Rezultati teh priporočil so opisani v naslednjem poglavju.

### *5.5.1 Evropski nadzorniki o Googlovi politiki zasebnosti*

Evropski nadzorniki (v besedilu tudi kot nadzorniki, pooblaščenci, delovna skupina) so v svojem skupnem pismu *Letter to Google Privacy Policy* (Article 29 Data Protection Working Party, Letter 2012), ki ga je podpisalo 24 pooblaščencev iz držav EU (podpisali ga niso le grški, romunski in litovski pooblaščenci) izrazili pomisleke o novi Googlovi politiki zasebnosti in izdali nekaj priporočil.

Google izvaja več postopkov obdelave osebnih podatkov v okviru zagotavljanja svojih storitev. Nadzorniki so identificirali tri tipe uporabnikov teh storitev:

- aktivni uporabniki (Gmail, GooglePlay, Docs, Google+ itd.),
- neaktivni uporabniki (Iskanje, Zemljevidi, YouTube itd.),
- pasivni uporabniki (DoubleClick, Analytics, '+1' gumb itd.).

V pismu in v priporočilih *Recommendation to Google Privacy Policy* (Article 29 Data Protection Working Party, Recommendations 2012) so informacijski pooblaščenci 24-ih

držav članic Evropske unije ugotovili, da je Google izvajal aktivno oglaševalsko kampanjo, kjer je uporabnike preko različnih informacijskih orodij (pošiljanje e-pošte, pojavna okna itd.) obveščal o spremembah in uvedbi nove politike zasebnosti. Ugotavljajo, da je nova politika zasebnosti v neskladju z *Direktivo o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov*, saj ne spoštuje obveznosti obveščanja, ki je določena v Oddelku IV te Direktive.

Podjetju očitajo, da so politiko implementirali brez predhodnih razgovorov in posvetovanj z varuhi človekovih pravic, nadzorniki, ki opravljajo nalogo varovanja zasebnosti in osebnih podatkov. Četudi Google pojasnjuje, da se njihova politika ne razlikuje od drugih podjetij v ZDA, pa nadzorniki vseeno zahtevajo, da bo podjetje aktivno sodelovalo v preiskavi z evropskimi nadzorniki in drugimi pristojnimi organi v državah, v katerih Google zagotavlja svoje storitve.

Preiskava je pokazala, da Google daje nepopolne ali približne informacije o namenu, za katerega se zbirajo. Te informacije niso podrobno in eksiplicitno definirane, ne povedo niti kaj bodo počeli z zbranimi in združenimi podatki. Ugotavljajo, da so v nasprotju z Direktivo, ki v Oddelku I in v 6. členu druge alineje navaja: »Osebni podatki morajo biti zbrani za določene, izrecne ter zakonite namene in se ne smejo naprej obdelovati na način, ki je nezdružljiv s temi nameni. Nadaljna obdelava podatkov v zgodovinske, statistične ali znanstvene namene se ne šteje za nezdružljivo, če države članice zagotovijo ustrezne zaščitne ukrepe«. Poleg tega je Googlov pravilnik v neskladju z 10. in 11. členom te Direktive, saj ni izpolnil obveznosti »informacij v primerih zbiranja podatkov od posameznika, na katerega se osebni podatki nanašajo« in »informacij, kadar podatki niso bili pridobljeni od posameznika, na katerega se osebni podatki nanašajo«.

Pravilnik je mešanica izjav in primerov, ki ni natančno določena v samo enem pravilniku, saj so dodatne informacije na voljo v številnih obvestilih v centru za pomoč ali na blogih podjetja. Informacije v teh dokumentih so v neskladju v nekaterih virih in jezikih. S tem pravilnikom uporabnike zavaja, saj jim ne da natančnih informacij o dejanskih namenih. Hkrati nadzorniki, ne samo Google, tudi ostala podjetja pozivajo, naj pravilniki o zasebnosti ne bodo predolgi, preveč kompleksni in prepredeni s pravniško terminologijo.

Google rad poudarja, da so z novim pravilnikom nadomestili več kot 60 različnih pravilnikov, ki so veljali za vsako storitev posebej. Delovna skupina opozarja, da Google vseh teh 60 starih pravilnikov ni omogočil na vpogled v svojem arhivu in niso na voljo na spletu. Podatki,

ki se obdelujejo, so v pravilniku zapisani preveč splošno in ne zagotavljajo ustreznih informacij uporabniku, ko uporablja določene storitve. Google prav tako ni zagotovil spoštovanja načela zmanjšanja količine zbranih podatkov. Pri tem ni navedel, kateri podatki se povezujejo s katero storitvijo. Pasivni uporabniki niso obveščeni o tem, da Google obdeluje osebne podatke na podlagi IP naslovov in piškotkov.

Nadalje so se uresničile skrbi evropskih nadzornikov o povezovanju podatkov in združevanju iz vseh storitev. Nova politika Googlu to omogoča za kateri koli namen. Nadzorniki menijo, da podatki ne bi smeli biti združljivi z namenom, za katerega so bili ti podatki zbrani, poleg tega pa od uporabnika Google ne dobi nedvoumnega soglasja za zbiranje tako obsežne zbirke podatkov. Google ni dokazal, za kakšen namen se obdelujejo zbrani podatki, niti ni zagotovil svojim uporabnikom orodja, ki bi omogočalo obvladovanje osebnih podatkov.

Delovna skupina je identificirala nekatere namene povezovanja podatkov. Med te sodijo zahteve uporabnikov po povezovanju (npr. uporabnik želi dostopati do kontaktov v Gmailu), povezovanje brez vednosti uporabnika, povezovanje zaradi varnostnih razlogov, oglaševanja, analitičnih razlogov, raziskovalnih razlogov in tako dalje.

CNIL (Commission Nationale de l'Infromatiave et des Libertes) v svojem sporočilu za javnost (Article 29 Data Protection Working Party, CNIL Press Release 2012) opozarja, da ni mogoče ugotoviti, da Google spoštuje ključna načela varstva podatkov, kakovosti podatkov, zmanjšanje količine podatkov, sorazmernosti podatkov in pravice do ugovora. Google tudi ne zagotavlja oziroma zavrača obdobje hranjenja obdelanih osebnih podatkov.

Nadzorniki od Googla pričakujejo, da bo sprejel vse potrebne ukrepe, da bodo informacije o povezovanju podatkov jasnejši in v skladu z zakonodajo in Evropsko Direktivo. V ta namen so izdali še nekaj priporočil:

- Google naj dopolni informacije o postopkih obdelave podatkov, zbranih za točno določen namen;
- Google naj ne obdeluje zbranih osebnih podatkov za vsako storitev enako;
- Google naj razvije interaktivno predstavitev, ki bi uporabnikom omogočila enostavno pregledovanje vsebine politik zasebnosti;
- Google naj zagotovi dodatne in točne občutljive podatke uporabnika (biometrični, kreditne kartice, lokacija), ki lahko vplivajo na zasebnost;
- Google naj obvešča tudi pasivne uporabnike;

- Google naj razvije orodje, s katerimi bo imel uporabnik jasen pregled nad tem, kateri osebni podatki se o njem zbirajo in mu hkrati daje možnost nadzora nad osebnimi podatki.

Evropski nadzorniki se zavedajo, kakšno vlogo igra Google v spletnem prostoru. S priporočili ne želijo vplivati na poslovanje podjetja, temveč zgolj nuditi varnost uporabnikom in jim zagotoviti, da so njihovi osebni podatki v skladu z zakonodajo.

# 6 VARNOST NA INTERNETU

Varnost je sredstvo za doseganje cilja ali pa sam cilj, ki se nanaša na posameznikovo zavest. Varnost predstavlja stanje ravnotežja mednarodnih, meddržavnih, medskupinskih, družbenih, interpersonalnih in intrapersonalnih procesov, zaradi česar se v zavesti posameznika oblikuje občutek stabilnosti, homeostatičnosti, torej tudi zagotovljenih pogojev za življenje in preživetje (Edmonds in Jelušič v Svete 2005, str. 33).

V sodobni informacijski družbi sta kvaliteta in varnost našega življenja odvisni tudi od informacijskih tehnologij, v katera so vpleteni sistemi, kot so: socialna in geosocialna omrežja, elektronska pošta, sistemi trenutnega sporočanja, elektronsko bančništvo, telefonija, GPS lokacijske storitve in ostale tehnologije brez katerih si sodoben človek ne zna več predstavljati življenja. Hkrati je sodobna tehnologija pred uporabnika informacijskih tehnologij postavila vrsto varnostnih vprašanj. Posameznik je izpostavljen nevarnostim kot so: vdori, goljufije, tatvine identitete, izsiljevanja ipd. (Caf in drugi, 2010).

Uporabniki se nevarnosti zavedajo, ne vedo pa, kako se pred njimi zavarovati (Caf in drugi, 2010). Po mnenju dr. Dušana Cafa je področje varovanja podatkov še vedno v obdobju »divjega zahoda«, kjer je kraja informacij zelo donosen posel in so tatovi zelo inovativni ter iznajdljivi.

Razvoj informacijsko-komunikacijske tehnologije (IKT) in njena uporaba v sodobnih družbah sta doživela revolucionaren razmah. Telekomunikacije, satelitske povezave in računalniška omrežja so velik del sveta povezala v prepleteno celoto, in sicer informacijsko družbo (Svete, 2005).

Razvoj IKT tehnologij omogoča lažje zbiranje, shranjevanje, dostopnost in nadzor nad ogromno količino podatkov (Praprotnik, 2006). Hkrati ima ta tehnologija pri zbiranju, obdelavi in prenosu podatkov izrazite varnostne implikacije (Malešič v Svete, 2005).

Problem varnosti in zasebnosti na internetu po mnenju Kovačiča (2003) ni samo tehnični, pač pa je tudi družbeni problem. To 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.

Organizacija Privacy Rights Clearinghouse je že kmalu po množični razširitvi uporabe interneta ugotovila, da »pravzaprav ni internetne (on-line) dejavnosti, ki bi omogočila popolno zasebnost« (Privacy Rights Clearinghouse v Kovačič 2006, str. 139). Problem interneta je tako predvsem v tem, da tehnologija že sama po sebi, zaradi svojih lastnosti, omogoča nekatere zlorabe zasebnosti bolj, kot bi bile te mogoče v fizičnem prostoru (Mlinar v Kovačič 2006, str. 139–140).

## 6.1 Zasebnost na internetu

Uporabnik interneta ima na internetu na voljo številne storitve, ki jih uporablja. Primožič (2005) jih našteje le nekaj najpogostejših. To so elektronska pošta, iskanje, klepetalnice, elektronsko poslovanje in oglaševanje. Vsaka od teh storitev pa predstavlja določeno tveganje s stališča varnosti osebnih podatkov in zasebnosti.

Osebne podatke se na internetu zbira na več načinov. Prvi način je, da uporabnik sam vnaša osebne podatke, opravi kakšno registracijo na spletni strani, si postavi svoj blog in drugo. Drugi način, ki se ga strani pogosto poslužujejo, pa je ta, da v zameno za kakršno koli stvar – naj si bo za različne nagradne igre, ankete ipd. – te strani zahtevajo osebne podatke. Dandanes na skoraj vseh straneh piše, za katere namene se bodo zbrani podatki uporabljali.

Zasebnost posameznika na internetu je ogrožena. Za to skrbijo številne grožnje zasebnosti, ki so predstavljene v naslednjem poglavju.

## 6.2 Grožnje zasebnosti

Z vsakodnevno uporabo interneta uporabnik pušča digitalne sledi. Vse te sledi se nekje zbirajo in shranjujejo. S sestavljanjem vseh teh podatkov pa je mogoče zgraditi profil uporabnika interneta ter ga tudi identificirati v realnem svetu (Praprotnik, 2006).

Isti avtor nadalje navaja, da v dobi informacijske družbe največjo grožnjo zasebnosti predstavlja razvoj novih tehnologij, kot so video nadzor, biometrija, radio frekvenčna identifikacija, osebne kartice in ostali. Grožnjo predstavljajo tudi ekonomski interesi in pa nadzor države nad njenimi državljani.

Video nadzor se v informacijski družbi uporablja zelo pogosto. Kamere imajo dvojno vlogo, po eni strani nadzorujejo obnašanje posameznika, po drugi strani pa lahko odkrijejo in razkrijejo nepridiprave. Video nadzor se izvaja v številnih nakupovalnih središčih, gospodarskih poslopjih, uradnih službenih prostorih in drugih. V Sloveniji je video nadzor urejen z Zakonom o varstvu osebnih podatkov, kjer določbe navajajo, da mora oseba, ki izvaja video nadzor objaviti obvestilo na vidnem mestu in posameznika seznaniti, zakaj se nad njim video nadzor izvaja.

Biometrija je naslednji vidik grožnje zasebnosti, ki pa se v današnjem času vse bolj uveljavlja. Gre za proces zbiranja, proučevanja in shranjevanja podatkov o posameznikovih fizičnih lastnostih z namenom identifikacije in avtentikacije.

Huš (2012) je v svojem članku navedel, da se v ZDA pripravlja sistem za množični nadzor nad posamezniki, ki pa ga predlagatelji, financerji in podporniki utemeljujejo z bojem proti terorizmu in kriminalu. Biometrični sistem *Next Generation Identification* bo vzpostavil centraliziran sistem za sledenje posameznikom na podlagi biometričnih podatkov.

Menim, da je vidik zasebnosti tu vsekakor izključen, bo pa tehnologija med ljudi vnesla določeno stopnjo varnosti.

Radiofrekvenčna identifikacija je v svetu prisotna že dolgo, vendar se, kot navaja Primožič (2005), še ni uveljavila, ker še niso v celoti izpolnjeni pogoji za množično uporabo. S pomočjo te tehnologije, tako navaja Vindiš (v Primožič 2005), se uporabnikom sledi s pomočjo čipov, ki oddajajo radijski signal. Kavita (v Primožič, 2005) tako opozarja, da se s tem v vsakem trenutku pozna natančno pozicijo bodisi iskanega predmeta, če je čip pritrjen na predmet, bodisi človeka.

V nadaljevanju bom predstavil še druge vidike zasebnosti, ki se pojavljajo na internetu.

## 6.3 Vidiki zasebnosti na internetu

### *6.3.1 Anonimizacija*

Anonimizacija je ena izmed zaščit zasebnosti na internetu. Popolna anonimizacija uporabnika na internetu sicer ni mogoča, saj mora uporabnik, kadar želi dobiti dostop do interneta, z nekim ponudnikom skleniti pogodbeno razmerje in že zaradi tega ne more ostati anonimen. Popolna anonimnost bi bila mogoča le v primeru nezakonite vključitve v internet (npr. lažni podatki v pogodbi). Anonimizacija pride v poštev za obiskovanje spletnih strani in drugih

storitev, kakor pa za anonimno uporabo interneta v odnosu do ponudnika dostopa do interneta. Za anonimno uporabo interneta lahko uporabimo anonimni zastopniški program (angl. Anonymous Proxy), posamezniki se v internetu predstavljajo s svojim IP naslovom, zato lahko skrijejo identiteto pravega uporabnika interneta. Poleg tovrstne anonimizacije obstajajo tudi programi, ki blokirajo sledenje obiskovalcev spletnih strani s piškotki in uporabe Jave ter JavaScripta. Izklop tovrstnih metod običajno zmanjša funkcionalnost spleta, zato v praksi ta možnost ni vedno priporočljiva (Kovačič, 2003).

### *6.3.2 Zaščita pred prestrezanjem*

Drugi vidik zasebnosti na internetu Kovačič (2003) vidi v zaščiti pred prestrezanjem. Podatke lahko uporabnik spremeni v tako obliko, da si oseba, ki prestreže te podatke, z njimi ne more pomagati. To je metoda kriptografije, kjer s šifriranjem podatkov uporabnik poskrbi, da napadalcu prepreči dostop do vsebine teh podatkov. Temeljno sporočilo se v kriptografiji imenuje čistopis, zašifrirano pa tajnopis. Čistopis se po nekem postopku, algoritmu, spremeni v tajnopis, pri tem pa se uporabi vrednosti (ključ ali geslo) za parametre v šifrirnem algoritmu. Sogovornika se dogovorita o algoritmu in ključu, da si lahko pošiljata šifrirana sporočila.

Eden izmed precej učinkovitih algoritmov je RSA, kjer so podatki, zaščiteni s to kriptografsko metodo, izjemno varni (Vidmar v Kovačič, 2003). Ta sistem predvideva, da imata pošiljatelj in prejemnik vsak svoj par ključev (javnega in zasebnega). Za pošiljanje šifriranega sporočila pošiljatelj potrebuje naslovnikov javni ključ in zasebnega, prejemnik pa potrebuje pošiljateljev javni ključ in svojega zasebnega.

Kovačič (2003) tudi navaja, da imajo dobre kriptografske metode lahko nekatere omejitve. Varnost metode RSA je tako na primer odvisna od dolžine uporabljenega ključa in tudi izbire gesla. Gesla morajo biti sestavljena tako, da jih ni mogoče hitro uganiti. Najboljša je kombinacija številk in črk. V svojem drugem delu isti avtor (2012) priporoča uporabo kompleksnih gesel, to so običajno gesla, sestavljena iz številk, velikih črk, malih črk in posebnih znakov v dolžini vsaj 20 znakov.

### *6.3.3 Zaščita pred vdori in zasegom podatkov*

Včasih se da podatke zaseči še pred šifriranjem ali neposredno po dešifriranju. Najbolj značilen primer je uporaba instruktivnega virusa, s katerim lahko napadalec prestreže geslo v času, ko se vnašajo v računalnik. Ena najpomembnejših stvari, na katero opozarjajo strokovnjaki za računalniško varnost, je dobra zaščita pred virusi (Kovačič, 2003), ki je v tem delu opisan kot tretji vidik varnosti na internetu.

Prva temeljna zaščita je redno posodabljanje programske opreme in operacijskega sistema. Microsoft vsak drugi torek v mesecu redno izdaja popravke in posodobitve operacijskega sistema. Verjetnost možnosti vdora v računalnik je možno zmanjšati še na dva načina. Prvi je uporaba protivirusnega programa.

Dobri programi so plačljivi, vendar zanesljivi, saj uporabnik nima tveganja, da bi prišlo do okužbe z virusom ali izgube podatkov. Dobri programi tudi prepoznajo, katere spletne strani na internetu so škodljive in katerih ni priporočljivo uporabiti. Poleg tega avtomatično prepoznajo nevarnosti, nanje opozarjajo in redno ter sproti brišejo potencialne viruse, ki se pojavljajo na internetu. Še posebej koristni so pri uporabi elektronske pošte, saj vsebujejo filtre za nezaželeno pošto, neprimerno vsebino in podobne. Pri tem je pomembno, da uporabnik uporablja licenčno protivirusno zaščito pri zaupljivem ponudniku teh storitev.

Drugi način, s katerim uporabnik zmanjša verjetnost možnosti vdora v računalnik, je uporaba požarnega zida (angl. Firewall). Ta preprečuje nepooblaščene dostope iz omrežja v omrežje. Pečjak (2004) ga definira kot program, ki prestreza komunikacijo med uporabnikovim računalnikom in internetom.

Nekateri programi za nemoteno uporabo računalnika in interneta zahtevajo, da za uporabo programa uporabnik izklopi požarni zid in tako dovoli pošiljanje podatkov v internet. Pri tem mora uporabnik paziti, da ne dovoli dostop mimo požarnega zidu programom, za katere sumi, da bi lahko prišlo do vdora v uporabnikov računalnik. Zato je za varnost priporočljivo uporabiti prednastavljene nastavitve. Za osebno, domačo rabo računalnika so požarni zidovi brezplačni in prednameščeni v operacijskem sistemu računalnika, medtem ko so za strojno opremo plačljivi.

### *6.3.4 Brisanje elektronskih sledi*

Kovačič (2003) vidik brisanja elektronskih sledi deli na sledi v lokalnem sistemu in zunaj njega. Pri slednjem uporabnik nanj nima vpliva in vse, kar lahko stori je, da pušča čim manj sledi. V lokalnem sistemu pa lahko sledi briše tako, da briše piškotke (angl. Cookies), čiščenje zastarelih zapisov v registru računalnika (za uporabnike operacijskega sistema Windows), brisanje morebitnih lokalnih datotek aktivnosti in praznega prostora na disku ter brisanje začasnega pomnilnika oziroma tako imenovanih začasnih datotek (angl. Temporary Files).

Pri elektronskih sledeh gre za transakcijske oziroma prometne podatke, ki jih nadzorni sistemi samodejno zbirajo in shranjujejo. Na internetu se elektronske sledi zapisujejo samodejno,

predvsem pa nezaznavno (Kovačič, 2006). Med te sledi Knez (2009) uvršča, katere spletne strani je uporabnik obiskal, katere datoteke prenesel, s katerim brskalnikom je dostopal operacijskim sistemom in tako dalje. Te informacije lahko ponudniki internetnih storitev zbirajo in na podlagi tega izdela profiliranje uporabnikov.

### *6.3.5 Ribarjenje*

Izraz ribarjenja (angl. Phishing) kot peti vidik zasebnosti na internetu izhaja iz angleških besed password (geslo) in fishing (ribarjenje). Spletni goljufi želijo s pomočjo lažnih spletnih strani in elektronskih sporočil od uporabnika dobiti osebne podatke. Pri tem so iznajdljivi in uporabijo številne tehnike. Nevednost ali naivnost lahko uporabniku povzročita relativno majhne težave (npr. odtujenost računa brezplačne elektronske pošte) ali precej večje (npr. kraja denarja na bančnem računu). Za varnost pred ribarjenjem mora uporabnik biti pazljiv in preverjati identiteto lastnikov spletnih strani in posredovanih vsebin (Informacijski pooblaščenec Republike Slovenije).

### *6.3.6 Pharming*

Pharming izhaja iz angleške besede farming (kmetijstvo) in pharmacy (farmacija), za uporabnika pa so po mnenju Informacijskega pooblaščenca Republike Slovenije bistveno bolj nevarni, saj jih je težje prepoznati. Pri teh napadih gre za bodisi neposreden napad na domenske strežnike bodisi za napad na določeno datoteko, ki se nahaja na računalniku uporabnika (gre za tako imenovano datoteko, kjer se nahajajo podatki o URL-jih in domenah, angl. Hosts File). Uporabnik je v teh primerih prepričan, da se nahaja na pravi strani, saj je vtipkal pravil URL naslov v oknu brskalnika, v resnici pa ga je eden izmed omenjenih načinov preusmeril na lažne strani, ne da bi se URL naslov v oknu brskalnika pri tem spremenil. Uporabnik v prepričanju, da se nahaja na pravi strani, vnaša svoje osebne podatke. Uporabnik se pred pharming napadom najlažje zavaruje z ustreznim protivirusnim programom in požarnim zidom, ki lahko napadalcem prepreči vstop v računalnik preko nezaščitenih komunikacijskih vrat.

### *6.3.7 Datoteke aktivnosti*

Datoteke aktivnosti (angl. LOG Files) so naslednja nevarnost, s katero običajni uporabnik ni seznanjen. Odlazek (v Primožič, 2005) navaja, da gre za datoteke, kamor računalnik avtomatsko vpisuje aktivnosti uporabnikov. To pomeni, da se vse aktivnosti uporabnika (npr. kdaj je prebral elektronsko pošto, katere spletne strani je obiskal in kdaj) avtomatsko zapisujejo na strežnik podjetja, ki zagotavlja uporabniku internetne storitve.

Kovačič (2006) tako pravi, da so te datoteke v informacijskih sistemih namenjene zapisovanju aktivnosti uporabnikov oziroma prometnih podatkov. Uporabne so za odkrivanje zlorab, pa tudi za ugotavljanje in odpravljanje napak, zato so nepogrešljiv del vsakega informacijskega sistema.

### *6.3.8 Rudarjenje*

Rudarjenje (angl. Data Mining) pomeni pridobivanje podatkov preko podatkovnih zbirk podjetij z namenom odkriti vzorce potrošniškega obnašanja. Rudarjenje pomeni tudi nit avtomatiziranih postopkov, ki se uporabljajo za izluščitev še nepoznanih delov informacij iz velikih podatkovnih baz (Cavoukian v Praprotnik, 2006). Isti avtor navaja tri korake poteka rudarjenja:

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

Po mnenju Cavoukianove (v Praprotnik, 2006) predstavlja rudarjenje z vidika zasebnosti tudi nevarnost, predvsem zaradi naslednjih dejavnikov:

- **Kvaliteta podatkov**: z rastjo interneta se je povečala količina podatkov iz različnih virov. Nekateri podatki so lahko zastareli, nenatančni ali netočni.
- **Možnost dostopa**: potrošnik do teh podatkov ne more dostopati.
- **Namen uporabe**: na začetku procesa se namen uporabe ne more identificirati.
- **Odprtost in transparentnost**: rudarjenje ni odprta in transparentna aktivnost.

### *6.3.9 Piškotki*

Piškotki (angl. Cookies) so tekstovne datoteke, ki na internetu prepoznajo uporabnikov računalnik. Tu ne gre za prepoznavo uporabnika, temveč računalnika, ki je bil uporabljen pri dostopu. Ker piškotki na nek način posegajo v zasebnost posameznika, jih je priporočljivo izklopiti ali redno brisati (SAFE-SI, 2012).

Ko se uporabnik ob vsakem naslednjem obisku vrne na stran, se mu ohranijo nastavitve, ki jih je uporabil že prej (SAFE-SI, 2012). Na ta način spletna stran lahko ugotovi, ali je uporabnik spletno stran v preteklosti že obiskal in zabeleži vso zgodovino obiskov (Kovačič, 2009).

Sodobna omrežja omogočajo zbiranje številnih osebnih podatkov. Problema zbiranja osebnih podatkov s pomočjo piškotkov se je zgodaj zavedla tudi Evropska unija, ki je leta 2002 sprejeti *Direktivi o zasebnosti in elektronskih komunikacijah 2002/58/EC*, v 24. točki posebej izpostavila problem spletnih piškotkov. Določila je, da jih mora imeti uporabnik možnost zavrniti, hkrati pa mora biti seznanjen s tem, kakšne informacije se s pomočjo piškotka o njem shranjujejo.

Za varnost uporabnik lahko poskrbi tako, da po vsaki uporabi interneta pobriše vse piškotke, ali pa jih trajno onemogoči. V tem primeru nekatere storitve, še posebej podjetja Google, ne bodo delovale pravilno.

### *6.3.10 Iskalniki*

Vsa sporočila, ki se jih pošilja na javno dostopna mesta, bodisi gre za forume, bloge ipd., so dostopna vsakomur in lahko ostanejo shranjena še dolgo časa. Te informacije je možno pridobiti z raznimi iskalniki, ki poleg sporočil vsebujejo še druge informacije o internetnih straneh (Knez, 2009). Gindin (v Knez 2009) tako v iskalnikih vidi veliko skrb za zasebnost, »zaradi svoje kapacitete pridobivanja podatkov ter ohranitve vsakega sporočila poslanega v omrežje.«

### *6.3.11 Vdori in napadi*

Vdor v računalniške sisteme je eden izmed najbolj neposrednih napadov na zasebnost. Do njega lahko pride zaradi malomarnosti pri postavitvi in vzdrževanju sistemov. Pri vdiranju v sisteme gre za načine iskanja varnostnih pomanjkljivosti in za izkoriščanje le-teh (Knez, 2009).

Verdonik in Bratuša (2005) vdor definirata kot posledico napak v programski opremi, operacijskemu sistemu, na strežniku ali pa kot napačno ravnanje uporabnikov. Najpogostejši načini vdora v računalnik so preko elektronske pošte, kjer napadalci pošiljajo datoteke in skušajo zavesti uporabnike.

Z vidika zasebnosti so vdori in napadi nedopustni. Ker je znano dejstvo, da veliko vdorov pride ravno zaradi nevednosti uporabnikov, Evropski parlament in Svet (2009) v svoji *Direktivi 2002/58/EC o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij* pišeta, da morajo ponudniki internetnih storitev sprejeti ustrezne ukrepe za zagotovitev varnosti svojih storitev, hkrati obvestiti naročnike o tveganjih in jim

zagotoviti zaščito pred vdiranjem v zasebnost z nepovabljenimi elektronskimi sporočili, SMS sporočili in podobnimi.

### *6.3.12 Profiliranje*

Seničar in drugi (v Praprotnik, 2006) navajajo, da je profiliranje uporabnikov na internetu zapisovanje in klasificiranje obnašanja uporabnikov interneta. S pomočjo zbiranja informacij, sledenjem in uporabo piškotkov se naredi podatkovna baza, v katero se shranjuje profil uporabnika. Ti podatki so v večini neosebni, lahko pa se povežejo s podatki, ki jih pusti uporabnik na internetnih straneh (ime, spol, starost, izobrazba, elektronska pošta, IP naslov, demografija).

S profiliranjem veliko pridobi komericalni sektor, saj je po mnenju Kovačiča (2003) potrebno potrošnika dobro spoznati, ti podatki pa imajo veliko tržno vrednost. Z natančnim profiliranjem lahko podjetja svoje stranke spoznajo, kakšne nakupovalne navade imajo. Vendar pa Gandy v Baruh (v Kovačič, 2006) vidi nevarnost predvsem v tem, da bodo podjetja manipulirala s posameznikom in mu ponujala storitve, ki jih bo glede na ocenjene preference potrošnik lažje sprejel, kot pa v resnici potreboval.

### *6.3.13 Neželena elektronska pošta*

Vsak dan po svetu na milijone ljudi dobiva elektronsko pošto. Med običajno pošto pa se veliko pošilja tudi neželene pošte (angl. Spam, Junk Mail). Po mnenju avtorja Whithworth (v Praprotnik, 2006) je taka oblika pošte neligitimna in nepoštena komunikacija, ki poteka v eno smer. Težava pa je, da je zelo težko odkriti pošiljatelja sporočila.

Mramor (v Žbogar, 2009) tako navaja, da med glavne značilnosti neželene elektronske pošte sodijo »neprijetna vsebina, zavajanje uporabnikov, varljive ponudbe, kršenje zasebnosti in nelegalnost.«

Primožič (2005) ugotavlja, da preko elektronske pošte prihaja 95 % vseh virusov in drugih škodljivih programov, ki jih napadalci najraje in zelo pogosto uporabljajo za širjenje le-teh.

### *6.3.14 Spyware in prikrita omrežja*

Izraz spyware povezujemo s pojmom vohunski program, njegov namen pa je prikrito pridobivanje informacij o uporabnikih programske opreme. Sam izraz sicer ne pomeni, da so vsi vohunski programi namenjeni zgolj prikritemu zbiranju podatkov, niti ne delujejo povsem prikrito, saj uporabnika, sicer v drobnem tisku, obvestijo o tem, kaj bodo počeli. Spyware se

zato delno prekriva s pojmoma adware (prikazovanje oglasov) in malware (zlonamerna oprema za nezakonite dejavnosti) (Kovačič, 2006).

Isti avtor še navaja, da je primarni namen teh programov zbiranje podatkov, na podlagi katerih se potem prikazujejo oglasi. Gre za neposredno trženje, katerih vsebina je izbrana glede na trenutne internetne dejavnosti uporabnika.

### 6.4 Tehnologije za boljše varovanje zasebnosti

Tehnologija za boljše varovanje zasebnosti pomeni celovit sistem ukrepov IKT, ki varuje zasebnost z odstranitvijo ali zmanjšanjem količine osebnih podatkov ali s preprečevanjem nepotrebne in/ali neželene obdelave osebnih podatkov, ne da bi se funkcionalnost informacijskega sistema zmanjšala (Komisija evropskih skupnosti, 2007).

Komisija evropske skupnosti (2007) navaja več primerov tehnologij za boljše varovanje zasebnosti:

- avtomatsko anonimiziranje podatkov po določenem času podpira načelo, da se obdelanih podatkov v obliki, ki omogoča identifikacijo oseb, na katere se podatki nanašajo, ne sme hraniti dlje, kot je potrebno za namene, za katere so bili podatki prvotno zbrani;
- orodja za šifriranje, ki preprečujejo krajo podatkov, ko se podatki posredujejo po internetu, podpirajo obveznosti upravljalca podatkov, da sprejme ustrezne ukrepe za varstvo osebnih podatkov proti nezakoniti obdelavi;
- filtri za piškotke, ki zablokirajo piškotke, ki se brez vednosti uporabnika shranijo na njegovem osebnem računalniku, krepijo načela, da morajo biti podatki obdelani pošteno in zakonito in da mora biti oseba, na katero se podatki nanašajo, o tem obveščena.

Komisija meni, da je treba PET tehnologije razvijati in širše uporabiti zlasti, kadar so osebni podatki obdelani preko omrežij IKT. Hkrati menijo, da bi uporaba PET tehnologij izboljšala varovanje zasebnosti in pomagala pri spoštovanju pravil o varstvu podatkov (Komisija evropskih skupnosti, 2007).

Cranoer (v Praprotnik 2006, str. 38) navaja 7 osnovnih funkcij, ki jih morajo pokrivati PET tehnologije:

- zaščita pred neavtoriziranim dostopom do komunikacij in shranjenih datotek;

- avtomatska vzpostavitev informacij o zbiratelju podatkov, politiki o zasebnosti in avtomatskem kreiranju odločitve uporabnika na osnovi teh primerov;
- avtomatska objava politike o zasebnosti zbiratelja podatkov;
- filtriranje neželenih sporočil;
- preprečevanje avtomatskega zbiranja podatkov s pomočjo piškotkov, spyware programov;
- zaščita komunikacije pred povezavo s točno določeno osebo;
- podpora transakcijam, da razkrijejo minimalen obseg osebnih podatkov.

Eden najpomembnejših principov varovanja zasebnosti je, da se ne zbira in obdeluje nič več osebnih podatkov, kot pa je res nujno potrebno za natančno določen namen (Blarkom in drugi v Praprotnik 2006, str. 38).

### 6.5 Nadzor nad posamezniki

Kot sem spoznal do sedaj, je posameznikova zasebnost na internetu ogrožena, vendar neglede na številne negativne strani, ima tudi nekatere pozitivne stvari. S tem se ureja življenje v družbi. Potrebno se je zavedati, da se nadzora v današnji družbi ne da preprečiti. Svet je izrazito kapitalistično naravnan, saj ima elita številne ekonomske interese po še povečanju kapitala in nadzora nad uporabniki interneta.

Kovačič (2003, str. 11) nadzor posameznikov opredeli kot sredstvo družbenega nadzora in sredstvo za zagotavljanje pravic družbene participacije. Nadzor je tesno povezan s tehnologijo. Informacijske tehnologije so namenjene tudi zbiranju in obdelavi vseh vrst podatkov in informacij. Zato je informacijska družba pravzaprav družba nadzora.

Zasebnost podatkov pa na internetu ogrožajo napadalci z vdiranjem v sisteme, številni virusi, ki se pošiljajo po elektronski pošti in zlonamerna programska oprema. Pomembno pri tem je, da bi se moralo posamezniku omogočiti izobraževanje, saj se nekateri še vedno ne zavedajo nevarnosti, ki pretijo na internetu.

Med glavne razloge, zakaj prihaja do takšnega nadzora nad posamezniki, štejem teroristične organizacije, saj z napadi ogrožajo številna življenja, tudi nedolžnih. Nadzor v informacijski družbi se je drastično spremenil po 11. septembru 2001, ko so se številne države pričele še bolj zavedati terorizma, še posebej v ZDA, kjer uvajajo številne varnostne ukrepe, poostrujejo nadzor nad posamezniki, poslužujejo se sistemov za identifikacijo posameznika, prisluškovanje ljudem in tako dalje.

Zasebnost se na internetu varuje z izjavo o varovanju zasebnosti (angl. Privacy Policy), kjer upravljalci strani izjavljajo, kakšno stopnjo zasebnosti ima posameznik na internetu in kaj se dogaja z osebnimi podatki uporabnikov.

### 6.6 Varstvo osebnih podatkov

Po navedbah Horvata (2012) na internetu ni 100 % varnosti, za varno in prijetno uporabo interneta in uporabo socialnih omrežij pa lahko največ poskrbi kar uporabnik sam. Pri uporabi interneta in socialnih omrežij je pomembno, da omeji količino objavljenih osebnih podatkov. Četudi od njega zahtevajo vse mogoče, je pomembno, da občutljivih podatkov, kot so EMŠO, davčna številka, številke bančnih kartic ne objavlja, saj te podatke lahko zahtevajo le nekatere pristojne institucije.

Isti avtor pravi, da je potrebno biti na internetu pazljiv, da ni potrebno verjeti vsemu, kar se lahko prebere, ni potrebno nasedati različnim sporočilom, da je uporabnik zadel nagrade in da sedaj te institucije potrebujejo le še njegov osebni naslov ali številko bančnega računa, saj gre za klasične internetne prevare..

Po mojem mnenju je zanimivo podjetje Google, ki, kot sem že spoznal tekom diplomske naloge, o uporabniku zbira ogromno podatkov. Prvi korak je zagotovo, da se vsak seznani s pogoji uporabe in pravilnikom o zasebnosti. V primeru, da se z njimi strinja, kar stori večina populacije, čeprav ne prebere teh pravilnikov, lahko nemoteno uporablja njihove storitve. V nasprotnem primeru pa je potrebno poiskati alternativne možnosti. Najbolj učinkovita metoda, ki bi Googlu preprečila zbiranje podatkov je, da med brskanjem po spletu uporabnik ni prijavljen v Googlov račun. Po vsaki uporabi je priporočljivo, da pobriše piškotke in zgodovino iskanja (nekateri brskalniki imajo možnost nastavitve teh možnosti), s tem bo hkrati onemogočil Googlu, da si bo na podlagi piškotov zapomnil prejšnje seje uporabnika. Tudi gesel ni varno imeti shranjenih, zato je priporočljivo, da pred vsako prijavo v katerokoli internetno storitev uporabnik vsakič znova vnese geslo. Ravno gesla so ena izmed ključnih izhodišč varnosti na internetu, saj uporabnik za mnoge storitve (od uporabe elektronske pošte, do nakupovanja) za prijavo v sistem potrebuje geslo.

## 7 UGOTOVITVE ANALIZ

V uvodu diplomske naloge sem zapisal 5 hipotez, ki sem jih med izdelavo diplomske naloge želel preveriti in jih ovreči oziroma potrditi.

**H1:** *Delež populacije, ki se zaveda nevarnosti in tveganj pri uporabi interneta, je majhen.*

Hipoteza je potrjena. Številni avtorji in spletne strani opozarjajo na nevarnosti, ki se pojavljajo na internetu. Uporabnik lahko najde ogromno vodičev in nasvetov za varno rabo interneta. V Sloveniji za to področje skrbi Informacijski pooblaščenec. Opažam namreč, da kljub vdorom, tatvinam in goljufijam uporabniki še vedno nasedajo spletnim prevaram. Dnevno nastaja več sto novih lažnih strani, kjer skušajo napadalci izkoristiti nepazljivost uporabnikov. Največ prevar je opaziti na spletnih socialnih omrežij, kjer napadalci s pomočjo oglasov uporabniku izpisujejo sporočilo, da so zadeli denarno nagrado ali katero koli drugo nagrado. Opaziti je tudi trend, da povprečni uporabnik računalnika ne uporablja licenčne programske protivirusne opreme, s katero bi zaščitil svoj računalnik pred nepooblaščenim dostopom, pa tudi piratske verzije operacijskih sistemov so izjemno priljubljene.

**H2:** *Zakonodaja na področju varstva osebnih podatkov je v posameznih državah zelo različna.*

Hipoteza je potrjena. Evropski pristop k urejanju področja varovanja osebnih podatkov, za razliko od ameriškega, je precej strog. Če je v Evropi na prvem mestu zasebnost posameznika, je v ZDA na prvem mestu dostop do informacij. V ZDA se zavzemajo za svoboden pretok podatkov v ekonomiji, ki je bistvenega pomena za poslovanje ameriških podjetij. V Evropi je zasebnost ustavna pravica, ki velja tako za javni kot tudi za zasebni sektor, medtem ko v ZDA zasebnost ni ustavna pravica, velja pa le za javni sektor, saj se zasebni sektor sprejemu te zakonodaje upira, kajti interes ameriških podjetij je pridobiti osebne podatke posameznikov v tržne namene. Nadalje, v Evropi je zakonodaja enotno usklajena in omogoča večji nadzor držav članic nad njihovimi državljani, na drugi strani pa v ZDA ni enotnega zakona, ki bi urejal področje varovanja osebnih podatkov, temveč je več zakonov, ki jih je potrebno upoštevati tako na področju ZDA kot v posameznih zveznih držav. Poleg tega si v ZDA državljani ne želijo, pa tudi sama vlada ne, da bi vlada imela nadzor nad državljani. Nadzor nad posamezniki ima trg.

Zasebnost na internetu in posledično varnost posameznika je v Evropi in ZDA različno obravnavana. Vendar pa bi taka ureditev prinesla veliko težav pri poslovanju med državami, še posebej v ZDA, saj tamkajšnja podjetja ne bi mogla prejemati osebnih podatkov državljanov iz članic držav Evropske unije. Potreben je bil sporazum, imenovan Safe Harbor, s katerim so se ZDA zavezale, da bodo lahko prejemala osebne podatke iz Evropske unije, v

kolikor bodo spoštovale osnovna načela zasebnosti, ki jih navaja Evropska Direktiva o varstvu osebnih podatkov.

**H3:** *Google močno posega v zasebnost posameznika.*

Hipoteza je potrjena. Podjetje ima v svojih strežnikih ogromno količino podatkov o uporabnikih interneta, s katerimi imajo praktično nadzor nad njimi. Storitve, ki jih ponuja Google, pred začetkom leta 2012 niso bile tako sporne, situacija pa se je spremenila po 1. marcu 2012, ko so uvedli novo politiko zasebnosti, ki je tudi glavna obravnava te diplomske naloge.

Nova politika zasebnosti je bila sprejeta 1. marca 2012. Uporabnike internetnih storitev je najbolj razveselilo dejstvo, da nova politika nadomešča več kot 60 različnih starih. Sedaj obstaja le ena politika, kjer ni toliko pravniške terminologije, s čimer je politika nekoliko jasnejša, krajša in bolj razumljiva. Dejstvo, da uporabniku nova politika omogoča na podlagi iskalnih poizvedb oglase, ki ga zanimajo in so v skladu z njegovimi preferencami, s čimer uporabnik dobi boljše zadetke pri iskanju, se mi ne zdi sporno. Uporabnikom gotovo ustreza, da dobijo tisto, kar jih zanima, kar največkrat iščejo, si ogledujejo, saj se s tem lahko poveča obiskanost oglasov, s tem pa se večajo tudi njihovi prihodki.

Dobrodošla novost je vsekakor tudi dejstvo, da uporabnik ne potrebuje več poljubno mnogo računov za vsako storitev posebej, temveč lahko z enim računom dostopa do vseh storitev. Sporna se mi zdijo dejstva, da Google povezuje podatke o uporabi vseh svojih storitev. Tako lahko vse storitve, ki se jih uporabnik poslužuje, povezujejo podatke, ki se stekajo v en račun. To pomeni, da če želi uporabnik uporabljati Gmail, bo z istim računom lahko dostopal tudi do drugih storitev, npr. YouTube, v njegovem profilu pa bo Google videl vse aktivnosti, ki jih uporablja na teh storitvah. Mnogi uporabniki se ne zavedajo, da Google pridobiva neverjetno bazo podatkov o uporabniku. Ti podatki lahko povedo o uporabniku več kot o sebi ve uporabnik sam.

Poseg v zasebnost posameznika se dotika tudi na točki, kjer si Google dovoli posredovati podatke uporabnikov tretjim osebam, in sicer z dovoljenjem posameznika, problem pa nastane, ker osebne podatke brez dovoljenja posameznika lahko obdelujejo tretje osebe ali ustanove, ki jih za to pooblasti Google. To ustreza oglaševalskim podjetjem, ki na podlagi tega pridobivajo dobiček.

Ena izmed redkih pozitivnih stvari v novi politiki je tudi ta, da ima uporabnik možnost nadzora nad tem, katere izdelke uporablja in tako vidi, katere osebne podatke Google o njem zbira. Žal pa uporabnik vidi le del svojih podatkov, saj tistih bistvenih podatkov, kot so dnevniški podatki (datum in čas poizvedb, kaj išče uporabnik, kako dostopa do interneta, katere piškotke Google zbira, kje se nahaja uporabnik, s kakšno opremo dostopa do interneta, zgodovina iskanja, piškotki, IP naslovi in ostali) ne vidi. V kolikor želi uporabnik izklopiti npr. piškotke, s katerimi Google vohuni za uporabnikom, potem mu storitve Googla ne bodo delovale pravilno.

Še bolj so na udaru uporabniki mobilnih telefonov, ki uporabljajo platformo Android, ki je v lasti Googla. Tu zasebnosti za uporabnika ni, saj je pri uporabi telefona 24 ur na dan prijavljen v sistem, kjer Google beleži vse klice, sporočila, aktivnosti, dostope do omrežja in podobne.

Z mojega vidika je zelo moteč element pri Googlu njegovo nadležno vsiljevanje storitev vse povsod. V primeru, da uporabnik uporablja brskalnik Mozilla Firefox, Internet Explorer, Safari ali drug, se na osnovni domači strani nenehno pojavlja okence, s katerimi Google opozarja, da naj uporabnik prevzame brskalnik Google Chrome za hitrejše in »varnejše« brskanje po internetu. Pri uporabi brskalnika Chrome Google sinhronizira vse podatke in aktivnosti uporabnika.

Še en primer vsiljevanja je pri namestitvi programske opreme. Google je sklenil številna partnerstva s ponudniki programske opreme, ki ob namestitvi ponudi možnost, da poleg namenske opreme uporabnik zraven namesti še Google Chrome. V nekaterih primerih zraven vsiljuje tudi svojo orodno vrstico.

Dodaten poseg v zasebnost Googla vidim v uporabniških računih. V kolikor želi uporabnik izbrisati račun pri Googlu, ga ne more več obnoviti. Zame je to zadosten dokaz, da uporabniški podatki tudi po izbrisu še vedno ostanejo na strežnikih podjetja. Google se očitkom brani, da reaktivacije ne omogočajo zato, ker v nobenem primeru ne morejo zagotoviti, da gre za istega uporabnika. S tem je jasno, da se podatki prejšnjega uporabnika hranijo še nekaj časa, pa čeprav bi se morali izbrisati.

**H4:** *Nova Googlova politika zasebnosti je v nasprotju z zakonodajo v EU.*

Hipoteza je potrjena. Francoski informacijski pooblaščenec (CNIL) trdi, da je v nasprotju z Evropsko Direktivo 95/46/EC, saj ni jasno definirano, za kakšen namen se zbirajo osebni

podatki, hkrati pa s povezovanjem storitev onemogočajo jasno vedeti, kateri podatki so s kakšnim namenom združeni s posamezno storitvijo. Tudi Viviane Reding (Evropska komisarka za pravosodje) pravi, da krši zakonodajo, saj se pri njeni implementaciji niso posvetovali z javnostjo, ne deluje v skladu z načelom preglednosti in omogoča deljenje podatkov s tretjimi osebami, ne da bi uporabniki imeli možnost odjave (opt-out).

V zadnjih mesecih je sledilo več tožb s strani evropskih podjetij, v času pisanja te diplomske naloge pa se je odvijala tudi obsežna preiskava nadzornih organov za varstvo podatkov v EU (v okviru Delovne skupine iz člena 29), še posebej CNIL-a, saj so želeli natančno preučiti novo politiko zasebnosti Googla. Ugotovili so, da ta z Evropsko Direktivo ni v nasprotju le v eni točki, temveč jo krši na več točkah.

**H5:** *Za varnost na internetu lahko uporabnik največ stori sam.*

Hipoteza je potrjena. Dejstvo je, da 100 % varnosti na internetu ni. Za varnost lahko uporabniki največ storijo sami. Ko so enkrat podatki na internetu, tam tudi ostanejo. Tudi če jih uporabnik izbriše, se še vedno hranijo v strežnikih, do katerih imajo dostop zaposleni v podjetju. Na internetu je potrebno biti previden, čeprav opažam, da se uporabniki ne zavedajo dovolj, da je njihova zasebnost na internetu ogrožena, dejansko si niti ne vzamejo časa, da bi prebrali pogoje uporabe, vendar na hitro obkljukajo, da se z vsem strinjajo. Očitno je, da povsem tolerirajo početje Googla, saj v nasprotnem primeru delež uporabnikov ne bi naraščal. Opaziti je tudi, da se nova politika še nekaj časa ne bo korenito spreminjala, saj so z novo praktično storili vse, kar je mogoče. Konec koncev je pa na posamezniku, da presodi, ali mu je mar ali ne za njegovo zasebnost. Informacijska družba definitivno ogroža posameznikovo zasebnost.

# 8 SKLEPNE MISLI

Internet je globalen medij, ki ne pozna državnih meja in kjer je meja med javnim in zasebnim slabo definirana oziroma je sploh ni. Je sredstvo, ki je dostopno kadar koli in kjer koli, v zadnjih letih pa se je s pojavom pametnih telefonov dostop razširil tudi na mobilne naprave. Pri tem se mi zdi pomembno, da četudi danes v svetu prevladuje denar, da je dostop do interneta omogočen vsakomur, ne glede na to, ali si bogat ali reven ali glede na kateri koli drug dejavnik. Poleg tega brez interneta življenja skorajda ne bi bilo, vsaj ne komunikacije z uporabniki iz celega sveta, poslovanje med podjetji bi bilo oteženo. Internet je naredil pravo revolucijo v globalnem merilu, saj danes skorajda ne mine stvar, ne da bi o njej izvedeli na inernetu.

Ko govorim o internetu, je z njim tesno povezan pojem zasebnosti in varovanja zasebnosti. Uporabnik ima pravico do zasebnosti, vendar je pravica tako zelo kompleksna, da si jo številne institucije, ki zagotavljajo storitve in skrbijo za zasebnost uporabnika, razlagajo na drugačen način. V začetku dobe interneta je uporabnik imel neko anonimnost in svobodo, danes pa temu ni tako, saj globalizacija in razvoj informacijsko-komunikacijskih tehnologij prinašata sicer mnogo ugodnosti, hkrati pa tudi številna tveganja za zasebnost posameznika in njegove osebne podatke, ki jih objavi na internetu. Glede na to, da se na internetu nahaja neverjetna količina podatkov uporabnika, lahko sodobne tehnologije te podatke povezujejo, zbirajo in obdelujejo za drugoten namen.

Na uporabnika interneta pretijo številne nevarnosti, ki ogrožajo njegovo zasebnost, to so vdori, goljufije, tatvine identitete, izsiljevanja in podobni. Z različnimi tehnologijami se uporabniku lahko sledi in za njim vohuni tako, da se v vsakem trenutku uporabnika lahko identificira, kje se ta nahaja, kaj počne na internetu, kako dostopa do njega in še mnogo drugih podatkov. Ugotavljam, da je cilj ogrožanja zasebnosti posameznika na internetu izključno premoženjski, saj z vdori in goljufijami od uporabnika pridobijo podatke, ki jih lahko naprej prodajo.

Na drugi strani pa so tu velike korporacije, ki uporabniku ponujajo številne storitve računalništva v oblaku, kjer uporabnik lahko naloži vsebino slik, dokumentov, videov in drugih oblik datotek, potem storitve komuniciranja, socialnih omrežij, elektronske pošte in ostalih. S ponujanjem storitev od uporabnika pridobvajo veliko količino vseh, tudi osebnih podatkov. S temi podatki upravljajo in na podlagi zbranih podatkov, npr. kaj uporabnik preferira, mu prikazujejo oglase, saj je oglaševalski trg izjemno dobičkonosen.

Informacijska družba je naredila velik napredek na področju tehnologije zbiranja, shranjevanja in obdelave osebnih podatkov, hkrat pa prinesla veliko tveganje posamezniku. Številne države, vlade, državne agencije in ostali so v prehodu na elektronsko poslovanje, uporabo informacijske tehnologije v zdravstvu, bančništvu, davčnem sektorju in drugod o posamezniku dobivale še več podatkov. Ti podatki se centralizirajo in do njih imajo dostop številne institucije.

Zato je bilo potrebno na tem področju urediti zakonodajo, ki ščiti posameznika in njegove osebne podatke. Pri tem mora država s svojo zakonodajo uskladiti dve pomembni lastnosti, in sicer zasebnost posameznika ter prost pretok podatkov. Različne države so se urejanja tega področja lotile na različne načine. V Sloveniji to področje ureja *Zakon o varstvu osebnih podatkov*, nad varovanjem zasebnosti pa bdi Informacijski pooblaščenec, ki ima pristojnosti za varstvo osebnih podatkov in za informacije javnega značaja. Slovenska zakonodaja je usklajena z *Evropsko Direktivo 95/46/EC*, kjer države članice Evropske unije, med katerimi je tudi Slovenija, varujejo temeljne pravice in svoboščine posameznika ter varujejo njihovo pravico do zasebnosti pri obdelavi osebnih podatkov.

Omenjena Direktiva zahteva, da se implementira takšno tehnologijo, ki ščiti osebne podatke pred uničenjen, izgubo, zlorabo in nepooblaščenim dostopom, hkrati pa omogoča nadzor nad državljani in tehnologije, s katerimi se varuje zasebnost in zaupnost podatkov.

V prihodnje bosta varnost podatkov na internetu in razvoj tehnologij za zaščito varnosti na internetu še naprej eni od glavnih tem v sodobni informacijski družbi. Dejstvo je, da je varnost na internetu zelo kompleksen pojem. Google je s svojo politiko naredil korak naprej na področju varnosti (pa tudi kršenja) zasebnosti. Pričakovati je, da bodo po podobni poti stopila tudi druga podjetja, začenši z Microsoftom.

# 9 LITERATURA IN VIRI

## 9.1 Literatura


1. AULETTA, KEN (2009) *Googled: The End of the World as We Know It.* New York: The Penguin Press.
2. BOGATAJ, JOŽE (2002) *Varstvo osebnih podatkov.* Ljubljana: Ministrstvo za pravosodje.
3. CARR, NICHOLAS (2011) *Plitvine: Kako internet spreminja naš način razmišljanja, branja in pomnjenja.* Ljubljana: Cankarjeva založba Založništvo.
4. CVETKO, ALEKSEJ (1999) *Varovanje zasebnosti v delovnih razmerjih.* Ljubljana: Gospodarski vestnik.
5. ČEBULJ, JANEZ (1992) *Varstvo informacijske zasebnosti v Evropi in v Sloveniji.* Ljubljana: Inštitut za javno upravo pri Pravni fakulteti v Ljubljani.
6. GRAHAM, IAN (1999) *Putting privacy in Context: An overview of the Concept of Privacy and of Current Technologies.* Toronto: Centre for Academic Technology. Dostopno prek: http://www.iangraham.org/talks/privacy/privacy.html (26. 7. 2012).
7. HORNIAK, VIRGINIA (2004) *Privacy od Communication – Ethics and Technology.* Vasteras: Malardalen University, Department of Computer Science and Engineering. Dostopno prek: http://www.idt.mdh.se/utbildning/exjobb/files/TR0390.pdf (26. 7. 2012).
8. JANČIČ BOGATAJ, MAJA, KLEMENČIČ, GORAN, MAKAROVIČ, BOŠTJAN, TIČAR, KLEMEN in TOPLIŠEK, JANEZ (2007) *Pravni vodnik po internetu.* Ljubljana: GV Založba.
9. KNEZ, MARKO (2009) *Varovanje zasebnosti in zaščita podatkov na internetu.* Ljubljana: Fakulteta za upravo Univerze v Ljubljani.
10. KOMAN PERENIČ, LIDIJA (2009) *Varstvo osebnih podatkov in mediji: smernice za medije, ki skušajo odgovoriti, kako ravnati v primerih, ko trčita med seboj pravica do obveščenosti in pravica do varstva osebnih podatkov.* Ljubljana: Informacijski pooblaščenec Republike Slovenije.
11. KOVAČIČ, MATEJ (2003) *Zasebnost na internetu.* Ljubljana: Mirovni inštitut.
12. KOVAČIČ, MATEJ (2006) *Nadzor in zasebnost v informacijski družbi: informacijski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu.* Ljubljana: Znanstvena knjižnica Fakultete za družbene vede.

13. KOVAČIČ, MATEJ, ŽAVBI, ALENKA, DOLENC, TOMI, BOŽIČ, GORAZD, ZUPANČIČ, TINA, ŠTERK, TANJA in KUŽELIČKI JERMAN, AJDA (2008) *Deskanje po varnih vodah: gradiva za učitelje.* Ljubljana: Projekt Safe-si.
14. LAMPE, ROK (2004) *Sistem pravice do zasebnosti.* Ljubljana: Bonex Založba.
15. LEVIN, AVNER in NICHOLSON JO, MARY (2005) *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground.* University of Ottawa Law & Technology Journal. Dostopno prek: http://www.uoltj.ca/articles/vol2.2/2005.2.2.uoltj.Levin.357-395.pdf (30. 7. 2012).
16. LOADER, BRIAN (ur.) (1997) *The governance of cyberspace: politics, technology and global restructuring.* London: Routledge.
17. MAKAROVIČ, BOŠTJAN, MOŽINA, DAMJAN, MEŽNAR, ŠPELA, BIZJAK, DOMEN, BOGATAJ, MAJA in KLEMENČIČ, GORAN (2003) *Internet in pravo.* Ljubljana: Pravna fakulteta Univerze v Ljubljani.
18. MUSAR PIRC, NATAŠA, PRELESNIK, MOJCA in BIEN, SONJA (2006) *Varstvo osebnih podatkov: vstop v zasebnost prepovedan.* Ljubljana: Informacijski pooblaščenec.
19. NIJHAWAN RAJ, DAVID (2003) *The Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States.* Nashville: Vanderbilt University Law School. Dostopno prek: http://law.vanderbilt.edu/publications/vanderbilt-law-review/archive/volume-56-number-4-april-2003/index.aspx (27. 7. 2012).
20. O'REILLY & ASSOCITAES INC. (1997) *The Harvard Conference on The Internet and Society.* Cambridge: O'Reilly & Associates Inc.
21. PRAPROTNIK, DARJA (2006) *Varovanje podatkov in zasebnost na internetu.* Ljubljana: Ekonomska fakulteta Univerze v Ljubljani.
22. PRAPROTNIK, TADEJ (2003) *Skupnost, identiteta in komunikacija v virtualnih skupnostih.* Ljubljana: Institutum Studiorum Humanitatis.
23. PRIMOŽIČ, ROK (2005) *Specialistično delo: Internet in pravica do zasebnosti.* Ljubljana: Ekonomska fakulteta Univerze v Ljubljani.
24. RAAB, CHARLES (2004) *The future of privacy protection.* Cyber Trust & Crime Prevention Project: Edinburgh University. Dostopno prek: http://www.bis.gov.uk/assets/foresight/docs/cyber/the_future_of_privacy_protection.pdf (27. 7. 2012).

25. ROVŠEK, JERNEJ (2005) *Zasebno in javno v medijih: Pravna ureditev in praksa v Sloveniji.* Ljubljana: Mirovni inštitut.
26. SCOTT, VIRGINIA (2008) *Google: Corporations That Changed The World.* London: Greenwood Publishing Group.
27. SVETE, UROŠ (2005) *Varnost v informacijski družbi.* Ljubljana: Knjižna zbirka Varnostne študije Fakultete za družbene vede Univerze v Ljubljani. Dostopno prek: http://www.fdv.uni-lj.si/zalozba/pdf-ji/171.pdf (22. 8. 2012).
28. VERDONIK, IVAN in BRATUŠA, TOMAŽ (2005) *Hekerski vdori in zaščita.* Ljubljana: Založba Pasadena.
29. VISE, DAVID in MALSEED, MARK (2005) *The Google Story*. New York: Delta Trade Paperbacks.
30. ŽBOGAR, MAJA (2009) *Zasebnost in internet.* Maribor: Fakulteta za varnostne vede Univerze v Mariboru.

## 9.2 Viri


1. ARTICLE 29 DATA PROTECTION WORKING PARTY (2012) *Letter about Google Privacy Policy.* Dostopno prek: https://www.ip-rs.si/fileadmin/user_upload/Pdf/Article_29_WP/Google_Privacy_Policy_-_letter_WP29.pdf (16. 10. 2012).
2. ARTICLE 29 DATA PROTECTION WORKING PARTY (2012) *Recommendation about Google Privacy Policy.* Dostopno prek: https://www.ip-rs.si/fileadmin/user_upload/Pdf/Article_29_WP/Google_Privacy_Policy_-_recommendations.pdf (16. 10. 2012).
3. ARTICLE 29 DATA PROTECTION WORKING PARTY (2012) *CNIL Press Release to Google Privacy Policy.* Dostopno prek: https://www.ip-rs.si/fileadmin/user_upload/Pdf/Article_29_WP/Google_Privacy_Policy_-_CNIL_press_release.pdf (16. 10. 2012).
4. BANISAR, DAVID in DAVIES, SIMON (1999) *Privacy and Human Rights: An International Survey of Privacy Laws and Practice.* Dostopno prek: http://gilc.org/privacy/survey/intro.html (13. 6. 2012).
5. BATEMAN, JAMES (2012) *Why is Google so successful?* Dostopno prek: http://www.ftadviser.com/2012/10/10/opinion/james-bateman/why-is-google-so-successful-AUY1FdWCsZLkruI6h7QqGM/article.html?ftar=true (6. 10. 2012).
6. CAF, DUŠAN, JERMAN, ROK in BRATUŠA, TOMAŽ (2010) *Projektna organizacija dela in informacijska tehnologija in varnost informacijskih sistemov.* Zbornik prispevkov 3. posveta dolenjskih in belokranjskih informatikov. Dostopno prek: http://www.fis.unm.si/media/pdf/ZBORNIK_3PDBI_2010.pdf (20. 8. 2012).
7. COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES (2012) *Courrier Google.* Dostopno prek: http://www.cnil.fr/fileadmin/documents/en/Courrier_Google_CE121115_27-02-2012-EN.pdf (23. 9. 2012).
8. ENAA MAGAZIN – DNE TEHNO (2012) *Google: Od naivnega fantiča do preračunljivega gospodiča.* Dostopno prek: http://dne.enaa.com/E-svet/E-druzba/Google-Od-naivnega-fantica-do-preracunljivega-gospodica.html (6. 10. 2012).
9. EVROPSKI PARLAMENT – PARLAMENTARNA VPRAŠANJA (2012) *Odgovor komisarke Viviane Reding v imenu Komisije.* Dostopno prek: http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2012-004040&language=SL (23. 9. 2012).

10. EVROPSKI PARLAMENT IN SVET (2009) *Direktiva 2002/57/EC Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij.* Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:SL:PDF (10. 10. 2012).
11. EXPORT GOVERMENT (2009). *Safe Harbor Privacy Principles.* Dostopno prek: http://export.gov/safeharbor/eu/eg_main_018475.asp (4. 8. 2012).
12. GENERALNI DIREKTORAT ZA PRAVOSODJE, SVOBODO IN VARNOST (2010) *Varstvo osebnih podatkov v Evropski uniji.*. Dostopno prek: http://ec.europa.eu/justice/data-protection/files/eujls08b-1002_-_protection_of_personnal_data_a4_sl.pdf (1. 8. 2012).
13. GOOGLE. Dostopno prek: http://www.google.si/intl/sl/about/corporate/company/ (23. 6. 2012).
14. GOOGLE POLICY EUROPE (2011) *Our commitment to the Safe Harbor privacy framework.* Dostopno prek: http://googlepolicyeurope.blogspot.com/2011/09/our-commitment-to-safe-harbor-privacy.html (5. 8. 2012).
15. GOOGLE PRIVACY PRINCIPLES. Sprejel in uvedlo jih je podjetje Google. Dostopno prek: http://www.google.com/intl/en/policies/privacy/principles/ (15. 8. 2012).
16. GOOGLE TERMS OF SERVICE. Sprejel in uvedlo jih je podjetje Google. Dostopno prek: http://www.google.com/intl/en/policies/terms/ (15. 8. 2012).
17. GOOGLE TRANSPARENCY REPORT: USER DATA REQUEST. Prikaz zahtevkov za posredovanje osebnih podatkov za polletno obdobje julij – december 2011. Dostopno prek: http://www.google.com/transparencyreport/userdatarequests/ (20. 8. 2012).
18. HOPKINSON, CARL (2009) *Why is Google the most successful search engine?* Dostopno prek: http://www.engageweb.co.uk/why-is-google-the-most-successful-search-engine-1504.html (6. 10. 2012).
19. HORVAT, SIMON (2012) *Varnost na spletu – socialna omrežja in osebni podatki.* Pravni nasveti. Dostopno prek: http://pravninasvet.com/VincitOmniaVeritas/varnost-na-spletu-socialna-omrezja-osebni-podatki/ (23. 8. 2012).
20. HUŠ, MATEJ (2011) *Google praznuje 13. rojstni dan.* Slo Tech. Dostopno prek: http://slo-tech.com/novice/t485767 (23. 6. 2012).

21. HUŠ, MATEJ (2012a) *Hekerji dobili pol milijon gesel uporabnikov Yahoo! Voices.* Slo Tech. Dostopno prek: http://slo-tech.com/novice/t526384 (17 .7. 2012).
22. HUŠ, MATEJ (2012b) *Hekerji napadli Android Forums in Nvidio.* Slo Tech. Dostopno prek: http://slo-tech.com/novice/t526471 (17. 7. 2012).
23. HUŠ, MATEJ (2012c) *Francija in Komisija: Googlova nova politika zasebnosti krši Evropsko zakonodajo.* Slo Tech. Dostopno prek: https://slo-tech.com/novice/t509128 (23. 9. 2012).
24. HUŠ, MATEJ (2012d) *V ZDA se pripravlja največji biometrični sistem za sledenje.* Slo Tech. Dostopno prek: https://slo-tech.com/novice/t534497 (10. 10. 2012).
25. INFORMACIJSKI POOBLAŠČENEC. Dostopno prek: https://www.ip-rs.si (4. 8. 2012).
26. KOMISIJA EVROPSKIH SKUPNOSTI (2007) *Sporočilo komisije Evropskemu parlamentu in svetu o spodbujanju varstva podatkov s tehnologijami za boljše varovanje zasebnosti (PET).* Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0228:SL:HTML (23. 9. 2012).
27. KOVAČIČ, MATEJ (2000) *Zasebnost v informacijski družbi.* 37 (6), str. 1019- 1034. Dostopno prek: http://dk.fdv.uni-lj.si/tip/tip20006kovacic.PDF (26. 7. 2012).
28. KOVAČIČ, MATEJ (2009) *Evropska unija bo morda omejila uporabo spletnih piškotkov.* Pravokator. Dostopno prek: http://hr-cjpc.si/pravokator/index.php/2009/11/30/evropska-unija-bo-morda-omejila-uporabo-spletnih-piskotkov/ (24. 8. 2012).
29. KOVAČIČ, MATEJ (2012) *Gesla in varna hramba gesel: mala šola informacijske varnosti, 1. del.* Pravokator. Dostopno prek: http://hr-cjpc.si/pravokator/index.php/2012/07/30/gesla-in-varna-hramba-gesel-mala-sola-informacijske-varnosti-1-del/ (24. 8. 2012).
30. LENZIE, MATT (2010) *Why is Google So Successful?* Dostopno prek: http://ezinearticles.com/?Why-is-Google-So-Successful?&id=3963846 (6. 10. 2012).
31. MOVIUS, LAUREN in KRUP, NATHALIE (2009) *U.S. and EU Privacy Policy: Comparison of Regulatory Approaches.* International Journal of Communication, 3 (2009), str. 169-187. Dostopno prek: http://ijoc.org/ojs/index.php/ijoc/article/view/405/305 (30. 7. 2012).
32. PEČJAK, JERNEJ (2004) *Požarni zidovi.* Monitor. Dostopno prek: http://www.monitor.si/clanek/pozarni-zidovi/ (24. 8. 2012).

33. REGAN, PRISCILLA (2003) *Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows.* George Mason University: Journal of Social Issues, 59 (2), str. 263-282. Dostopno prek: http://cip.gmu.edu/archive/archive/1540-4560.00064.pdf (5. 8. 2012).
34. RUTER, ALEŠ (2007) *Google želi vse.* Finance. Dostopno prek http://www.finance.si/195832/Google_%BEeli_vse (21. 6. 2012).
35. SAFE-SI (2012) *Kaj so piškotki (cookies)?* Dostopno prek: http://www.safe.si/c/1003/Piskotki_cookies (24. 8. 2012).
36. SCHRIVER, ROBERT (2002) *You Cheated, You Lied: The Safe Harbor Agreement and its Enforcement by the Federal Trade Commission.* The Fordham Law School Institutional Repository, 70 (29), str. 2777-2818. Dostopno prek: http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=3848&context=flr (4. 8. 2012).
37. SKRT, RADOŠ (2004) *Google – zgodba o uspehu.* Nasvet. Dostopno prek http://www.nasvet.com/google/ (21. 6. 2012).
38. SPLOŠNA DEKLARACIJA O ČLOVEKOVIH PRAVICAH. Sprejela in razglasila jo je Generalna skupščina Združenih narodov 10. decembra 1948 z resolucijo št. 217 A (III). Dostopno prek: http://www.scnr.si/test/wp-content/uploads/splosna_deklaracija_clovekovih_pravic.pdf (9. 6. 2012).
39. SULLIVAN, BOB (2006) *»La difference« is stark in EU, U.S. privacy laws.* Dostopno prek: http://www.msnbc.msn.com/id/15221111/#.UBJxnKAXLK4 (27. 7. 2012).
40. THE UNITED STATES DEPARTMENT OF JUSTICE (2003) *The Privacy Act of 1974.* Dostopno prek: http://www.justice.gov/opcl/privstat.htm (26. 7. 2012).
41. THE UNITED STATES DEPARTMENT OF JUSTICE (2010) *Overview of the Privacy Act of 1974, 2010 Edition.* Dostopno prek: http://www.justice.gov/opcl/1974privacyact-overview.htm (25. 7. 2012).
42. URADNI LIST REPUBLIKE SLOVENIJE (2004) *Zakon o varstvu osebnih podatkov (ZVOP-1).* Dostopno prek: http://www.uradni-list.si/1/objava.jsp?urlid=200486&stevilka=3836 (17. 7. 2012).
43. USTAVA REPUBLIKE SLOVENIJE (1991) *Uradni list Republike Slovenije 33l/1991.* Dostopno prek: http://www.uradni-list.si/1/objava.jsp?urlid=199133&stevilka=1409 (9. 6. 2012).
44. WAFA, TIM (2009) *Global Internet Privacy Rights: A Pragmatic Approach.* Intellectuall Property Law Bulletin, 13 (2), str. 131-158. Dostopno prek:

http://www.scribd.com/doc/87478957/Global-Internet-Privacy-Rights-A-Pragmatic-Approach (6. 8. 2012).

45. WESEARCH.ORG *Why is Google so Successfull?* Dostopno prek: http://www.wesearchsg.org/why-is-google-so-successful.php (6. 10. 2012).