UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Mitja Pritržnik

Google: Največja grožnja človekovi varnosti?

Diplomsko delo

Ljubljana, 2014

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Mitja Pritržnik

Mentorica: doc. dr. Janja Vuga

Somentor: doc. dr. Uroš Svete

Google: Največja grožnja človekovi varnosti?

Diplomsko delo

Ljubljana, 2014

Največja grožnja človekovi varnosti

V diplomskem delu je, preko prehoda iz tradicionalnega koncepta pojmovanja varnosti, ki ima za referenčni objekt, na katerega se varnost nanaša, državo, do sodobnega, kjer je v ospredje postavljen posameznik, problematizirana koncentracija in potencialna nevarnost monopolnega položaja največjega obdelovalca osebnih in drugih uporabniških podatkov na svetu, podjetja Google Inc. Sodobna varnostna paradigma se je v času globalizacije, po hladni vojni, premaknila od države (nacije) do posameznika. Globalizacija pa je prinesla tudi tehnološko revolucijo in zaradi trendov rasti uporabe novih spletnih tehnologij, je postala prav tehnologija potencialen vir ogrožanja človekove varnosti, saj sta človekova in informacijska varnost močno povezani. V delu orišem magnitudo sodobnih e-komunikacijskih poti in hrambe občutljivih podatkov v splošnem, katere podatke Google zbira o svojih uporabnikih in komu ter koliko jih posreduje, kako vplivajo izpadi Google storitev na človekovo varnost ter kako varna je pravzaprav Gmail komunikacija in Google uporabniški račun v splošnem? V delu torej raziščem ali je Google Inc. danes potencialna grožnja človekovi varnosti.

Ključne besede: *Google, človekova varnost, informacijska varnost, Google račun.*

Google: Greatest threat to human security

Thesis demonstrates, through the transition from traditional understanding of the concept of security, which focuses on the state, to contemporary, which has it`s reference point built around an individual, the concentration and potential danger of a monopoly position of the largest processor of personal and other user information in the world, Google Inc. The modern security paradigm has shifted from the state (nation) to an individual in the age of globalisation and post-Cold War. With globalisation also came the technological revolution and the trend of growing use of new technologies has positioned technology itself as a potential threat to human security, as human and information security are these days actually one. Here I outline the magnitude of modern e-channels of communication and storage of sensitive data in general, what data Google collects about its users and to whom and how many to, how Google service downtime impacts human security and how safe is actually Gmail communication and the Google account in general.

Keywords: *Google, human security, informational security, Google account.*

KAZALO

KAZALO TABEL IN GRAFOV

Uvod

Kaj je v ospredju, človek ali država, posameznik ali nacija? Nekaj podobnega so se spraševali tudi snovalci novega koncepta varnosti oziroma ogrožanja le-te, t. j. človekove varnosti. Protislovno lahko rečemo, da se je koncept človekove varnosti razvil kot posledica globalizacije, ki jo hkrati omejuje in krči. Svetovni mir je vse bolj posledica sledenju napotkov in zagotavljanja človekove varnosti (Prezelj 2008, 18). Objekt varnosti torej postaja posameznik ali kot bom poskušal pokazati v nadaljevanju dela, uporabnik. V ospredje so torej prišle nekatere doslej spregledane kulturno-civilizacijske razsežnosti varnosti, zato današnje razprave posvečajo večjo pozornost drugačnim prvinam sodobne varnostne problematike, kot so degradacija okolja, podnebne spremembe, odvisnost od tehnologij (npr. spletnih storitev podjetja Google Inc.), lakoti, neenakomernemu ekonomskemu razvoju, nalezljivim boleznim torej ne le zgolj vprašanje fizičnega obstoja posameznikov, temveč njegovi blaginji. In prav odvisnost od tehnologije je tisto področje, na katero se bom opiral v nadaljevanju. Monopol na področju človekovih informacijskih podatkov, kot ga izvaja Google pri svojem poslovanju, je namreč človekovi varnosti nevaren pojav in splošno sprejeto prepričanje danes je, da je posledica zmanjšanja ali izgube človekove varnosti, zmanjšanje stabilnosti znotraj in zunaj državnih meja, kar pa ima neposreden učinek na mir.

Moja teza gre v smeri, da ima Google prevelik monopol na trgu podatkov; človekovih podatkov, tistih o njegovem obnašanju in drugih, kar da potencialno ogroža človekovo varnost.

Glavna valuta informacijsko-komunikacijske dobe so informacije, saj na njih temeljijo pravzaprav vsa področja človekovega življenja in dela (Pirc-Musar 2013). Znanje in informacije se s komuniciranjem dograjujejo, izpopolnjujejo in poglabljajo, s čimer se večata moč in pomembnost informacij, ki so v vsakdanjem življenju bistvenega pomena. Značilnosti informacijske dobe se izražajo v spremenjenem načinu dela, ki je podprto s tehnološko opremo, ki omogoča hitrejše in učinkovitejše sprejemanje informacij, v spreminjajočem se načinu učenja, praktično bi lahko rekli, da se spreminja način življenja nasploh. Vsi vse iščemo, hranimo in delamo na spletu, vsa naša interakcija s tehnologijami pa potuje in se hrani po bolj ali manj varnih kanalih. Izpad ali manipulacija s takim podatkovnim tokom lahko predstavlja resno grožnjo človekovi varnosti. Nekdo lahko v danem trenutku denimo določi

točno lokacijo večine prebivalstva določenega geografskega ozemlja ali izve za poslovne izide konkurence, kar je potencialen vir grožnje človekovi varnosti. Svetovna nedostopnost Google storitev bi denimo po svetu lahko sprožila nemire. Zelo pomembna za zagotavljanje človekove varnosti je torej informacijska varnost. Bistvo informacijske varnosti je namreč dejstvo, da se ščitijo podatki oziroma informacije pred nepooblaščenim dostopom.

Za podjetje Google Inc. (v nadaljevanju Google) lahko brez večjih zadržkov rečemo, vse vidi, vse sliši in vse ve, saj pokriva vsa področja sodobnega človekovega delovanja na spletu; email in IM komunikacijo, spletno brskanje, mobilni operacijski sistem, spletna hramba podatkov ter ostali nabor praktično vseh aplikacij, ki jih vsakodnevno uporablja večina Zemljanov. V trenutku, ko tipkam tole diplomsko delo, naj bi bilo na spletu 2,925,249,355 spletnih uporabnikov (7,9 % rast), 7,243,784,121 Zemljanov (1,14 % rast), kar pomeni, da je cca. 40,4 % uporabnikov povezano na svetovni splet. Vsako sekundo spletni uporabniki preko Googlovega iskalnika pošljejo preko 44 tisoč iskalnih poizvedb in si izmenjajo preko 2,3 milijona e-poštnih sporočil. Število uporabnikov interneta na pametnih mobilnih telefonih je po podatkih raziskovalne agencije IDC letos celo prvič v zgodovini preseglo število tistih, ki za ta namen uporabljajo osebne in prenosne računalnike, saj na Kitajskem do svetovnega spleta preko pametnih mobilnih telefonov in tabličnih računalnikov skupaj dostopa dobrih 524 milijonov uporabnikov, preko osebnih računalnikov pa le 512 milijonov (Računalniške novice 2014).

V tem diplomskem delu se ne bom osredotočal na iskanje možnih scenarijev, kaj bi se lahko zgodilo, če bi vsi Google uporabniki ostali brez storitev ali če bi njihovi podatki prešli v nepooblaščene roke. S tem diplomskim delom želim le opozoriti na magnitudo potencialne nevarnosti koncentracije tako velikih podatkovnih zbirk pri enem ponudniku na način, kot to počne Google in njegov potencialno negativen vpliv na človekovo varnost.

Google Inc. je v svoji 16-letni zgodovini do danes prevzel 160 podjetij, ki jih je spretno inkorporiral v svoje storitve in izdelke. Poslanstvo podjetja se glasi »Google's mission is to organise the world's information and make it universally accessible and useful.«, torej organizirati svetovne informacije in jih narediti univerzalno dostopne (Google 2014). Srhljiv stavek, ko pomislimo, da želi eno podjetje urediti vse informacije na svetu in kot kaže, je na dobri poti, da uspe.

Google za vse svoje storitve uporablja poenoten Google uporabniški račun (Google account), na katerega so vezani vsi podatki o uporabniku in njegovem obnašanju, ki jih Google zbira o svojih uporabnikih in je za uporabnike brezplačen. Taki podatki vključujejo uporabnikove osebne podatke, podatke o plačilnih sredstvih, zgodovino uporabe Google storitev, njihove fizične lokacije z zgodovino premikov, vsebino e-poštne druge e-komunikacije in druge občutljive podatke, ki jih Google hrani na svojih strežnikih. Aktivnih Google uporabniških računov je bilo konec leta 2013, 540 milijonov, neaktivnih pa dosti več. Družabno omrežje Google+ v juniju 2014 beleži 343 milijonov aktivnih uporabnikov, skupaj pa je Google+ računov že preko 1,15 milijarde. Google beleži milijardo aktivnih uporabnikov operacijskega sistema Android, preko česar uporabniki dnevno razpošljejo 20 milijard tekstovnih sporočil, zajamejo 93 milijonov »selfijev«, telefoni uporabnikov pa se v uporabi 100 milijardokrat dnevno. Operacijski sistem Android je nameščen na 62 % vseh odposlanih tabličnih računalnikih. Spletni brskalnik Google Chrome uporablja več kot polovica oziroma 54,8 % vseh spletnih uporabnikov, medtem ko njegova mobilna različica, mobilni brskalnik Chrome for Mobile, beleži 300 milijonov aktivnih uporabnikov. Google.com je po Alexi, spletni storitvi, ki ocenjuje promet na spletnih straneh, najbolj obiskana spletna stran na svetu.

Če vzamemo največja števila, t. j. skupno število Google računov, podatke o trenutnem številu Zemljanov in uporabnikov interneta izračunamo, da je potencialno ogrožena človekova varnost 15,9 % svetovnih prebivalcev (1.150.000.000/7.251.737.604) in kar 39,3 % vseh spletnih uporabnikov na svetu (1.150.000.000/2925249355). Ne morem trditi, da je to največja podatkovna zbirka uporabnikov na svetu, saj je aktivnih uporabnikov samo Facebooka 1.1280.000.000, zato tudi težko trdim, da je Google največja grožnja človekovi varnosti v smislu števila potencialno ogroženih uporabniških računov, lahko pa trdim, da so ti uporabniški računi opremljeni z največ podatki o njih, narava podatkov pa je resnejša (osebna in poslovna komunikacija, hranjeni podatki, lokacijski podatki, in tako naprej).

Kako lahko Google ogroža človekovo varnost? Podatke o uporabnikih lahko (in jih) predaja tretjim osebam, kot so organi pregona, za čimer stoji tudi kontroverzen zakon FISA, ki denimo dovoljuje zbiranje obveščevalnih podatkov o tujih osebah za namene državne varnosti. Število zahtev vlad in sodišč z vsega sveta za razkritje uporabniških podatkov od leta 2009 do 2013 se je več kot podvojilo, kjer niti EU na zaostaja tako, kot bi si morda mislili.

Varnost Googlovih računov se sprva kaže, da je na zadovoljivem nivoju, zaskrbljujoče pa je dejstvo, da je na koncu za varnost lastnih podatkov hitro lahko kriv posameznik sam in to, da daje Googleprednost pred varnostjo, hitrosti svojih storitev. Vseeno poznamo številne primere odtujitve Google uporabniških podatkov. V 2011 je Matthijs R. za potrebe eksperimenta denimo zbral osebne podatke kar 35 milijonov Google+uporabnikov, preko njihovih javnih profilov, podatki pa so vključevali imena, gesla in biografske podatke uporabnikov. Vsi podatki in vse informacije, ki jih upravlja Google, so hranjeni v eni sami ogromni podatkovni tabeli (BigTable), kar je varnostno zelo tvegana odločitev, kot denimo, kadar imamo preveč kartic v eni denarnici – ko jo izgubiš, izgubiš vse. Našteti primeri kažejo na to, da Google račun ni varen in da je človekova varnost posledično lahko potencialno ogrožena.

Vsebina in ostali podatki ob e-poštni komunikaciji je lahko šifrirana, kar pa ni vedno tako. V povprečju je danes šifriranih 74 % odhodnih in 56 % dohodnih e-poštnih sporočil. Odstotek šifrirane e-pošte preko storitve Gmail se sicer povečuje.

Raziskava IDC-ja nakazuje, da kar 65 % vseh srednje velikih in malih podjetij z manj kot 1000 zaposlenimi svoje podatke hrani v oblačnih storitvah, kot je denimo Google Drive. Če so take storitve v danem trenutku nedostopne, je potencialno ogroženih 65 % srednje velikih in malih podjetij. Kar 80 % podjetij ocenjuje, da jih čas izpada ali čas v katerem dogovorjena storitev ni na razpolago, stane vsaj 20 tisoč USD na uro ali več, preko 20 % pa jih ocenjuje, da vsaj 100 tisoč USD na uro. Če bi torej hkrati brez dostopa do svojih oblačnih storitev ostalo 65 % podjetij na svetu, bi bila to gospodarska katastrofa globalnih razsežnosti, kar bi nedvoumno negativno vplivalo na človekovo varnost. Za nastalo Google seveda ne odgovarja (Tsoriev 2014).

V času tipkanja te diplomske naloge je brez dostopa do pomembnih storitev le Kitajska, in sicer 59 zaporednih dni, do 31. 7. 2014. V preteklosti torej ni bilo večjih razlogov za skrb in nedostopnost Google storitev ni v pretirani meri vplivala na človekovo varnost pa tudi trend gre v smer manjšanja tako števila prizadetih območij, kot tudi absolutnega števila motenj delovanja.

V kakšni meri lahko torej trdimo, da je Google največja grožnja človekovi varnosti, če sploh?

Metodološki načrt

Namen in cilj raziskovanja

Namen in cilj diplomskega dela je orisati sodobno pojmovanje varnosti, ki se je od naroda, kot referenčnega objekta, premaknila do posameznika oziroma uporabnika spletnih storitev, kot so denimo spletne storitve podjetja Google Inc. Preko analize primarnih in sekundarnih virov, izpeljanega intervjuja s PR službo podjetja Google in analize Googlovih splošnih pogojev poslovanja želim pokazati, kako sta povezani informacijska in človekova varnost, po drugi strani pa konkretno opozoriti na veliko potencialno grožnjo človekovi varnosti s strani tega spletnega giganta, podjetja Google Inc. Kot glavni dejavnik grožnje vidim unificiran Google račun, ki poseduje preveliko varnostnih tveganj, kot načine ogrožanja človekove varnosti pa posredovanje občutljivih uporabniških podatkov s strani Googla tretjim osebam, njihova odtujitev s strani tretjih oseb, nedostopnost Google storitev ter prestrezanje in manipulacijo e-pošte preko storitve Gmail.

Sklepi

Glavna hipoteza:

- Google je velika grožnja človekovi varnosti 21. stoletja

Delovne hipoteze:

- Google je ena večjih entitet na svetu, v smislu števila aktivnih uporabnikov, ki uporablja in so odvisni od storitve nekega ponudnika.
- Informacijsko-varnostne ranljivosti Googla predstavljajo informacijsko-varnostni izziv celotnemu Svetu.
- Google aktivno sodeluje z varnostno-obveščevalnimi agencijami po svetu.
- Googleov argument zbiranja ogromne količine podatkov o Svetu je učinkovitejše ciljano oglaševanje.
- Stopnja zasebnosti je med uporabniki Google storitev v veliki meri odvisna od njih samih.
- Poslovni model Googla temelji na predpostavki, da se bodo uporabniki strinjali s podatkovnim rudarjenjem (datamining).

Uporabljena metodologija

Pri izdelavi diplomskega dela sem uporabil naslednjo metodologijo:

- Pregled relevantne literature na področju človekove in informacijske varnosti
- Sintetično-analitična analiza literature, kjer preko povezave med globalno informacijsko in človekovo varnostjo pokažem na grožnjo, ki jima jo predstavlja podjetje Google Inc.
- Intervju z Google PR službo in informacijsko pooblaščenko RS

Zgradba diplomskega dela

Diplomsko delo je grajeno iz petih delov. V uvodu opredelim problem v luči sodobnega mednarodnega okolja v času globalizacije in informacijske revolucije. V drugem delu metodološko opredelim strukturo dela, uporabljene metodologije ter predstavim hipoteze. V tretjem delu opišem raziskovalni problem skozi relevantno teorijo, preko globalnega premika od nacionalne k človekovi varnosti in poiščem povezavo med informacijsko in človekovo varnostjo (teoretični del), v četrtem delu pa teoretske ugotovitve apliciram na svojo glavno hipotezo (praktični del). Zadnji, peti del predstavlja sklep, v katerem preverim hipoteze in predstavim ugotovitve diplomskega dela.

1 Teorija in praksa človekove varnosti

1.1 Od države do posameznika

Kaj je v ospredju, človek ali država, posameznik ali nacija? Nekaj podobnega so se spraševali tudi snovalci novega koncepta varnosti oziroma ogrožanja le-te. Ko se spremeni varnostno okolje, se namreč spremeni tudi pojmiovanje varnosti. Vse do konca hladne vojne je namreč veljala premisa nacionalne varnosti k njej pa so se nagibale večina teorij, ki so varnost postavljala ob bok domene narodov – tj. edina varnost je bila pravzaprav nacionalna varnost (Bayils 2008, 27).

Od Vestfalske mirovne pogodbe (1648) je namreč obveljalo, da so države najpomembnejši akter v mednarodnih odnosih in imajo legitimno pravico, da si v anarhičnem mednarodnem sistemu zagotavljajo lastno varnost na račun svojih sosedov oziroma drugih držav (Grizold in Bučar 2011).

Varnost je bila po koncu 2. Svetovne vojne nov vodilni koncept. Njeno proučevanje se je v času hladne vojne (dvopolni odnos med idejno-političnima, ekonomsko-znanstveno-tehnološko in vojaško-obrambnima blokoma) zožilo na vojaško-politične razsežnosti v okviru konceptov nacionalne in mednarodne varnosti. Glavni akter zagotavljanja nacionalne in mednarodne varnosti je bila torej država, preko vojaških in političnih prijemov, pri čemer so bile najpomembnejše sredstvo zagotavljanja le-te oborožene sile in posledično politična moč države. Diplomacija je bila postranskega pomena oziroma pomoč za uravnoteženje različnih interesov držav (Grizold in Bučar 2011, 829–830). Zato ne čudi, da je v celotnem obdobju hladne vojne v mednarodnih varnostnih študijah prevladovalo raziskovanje vprašanj v zvezi z vojaško ogroženostjo, jedrskim orožjem in Sovjetsko zvezo kot poglavitno vojaško in ideološko grožnjo zahodnim državam (Buzan in Hansen 2009).

Za konec hladne vojne, ko je tradicionalno jedrska blokovska tenzija popustila, vseeno pa so se nadaljevali in pojavljali številni lokalni oboroženi spopadi, so značilne strateške, ekonomske, politične in kulturne spremembe v mednarodnem okolju, ki s pojavom globalizacije dobivajo nove razsežnosti. Globalno gledano, se je vojaška grožnja zmanjšala, pred oči javnosti pa so prišle nekatere nove grožnje, ki jih tradicionalni pristopi k zagotavljanju nacionalne, regionalne in globalne varnosti, niso več mogli učinkoviti analizirati, interpretirati in obvladovati. Spremembe povrožajo nova kompleksna ogrožanja,

ki se ne omejujejo na meje posamezne države. Sem štejemo denimo širjenje orožja za množično uničevanje, okoljsko ogrožanje, lakoto, bolezni, mednarodni terorizem, nespoštovanje človekovih pravic in svoboščin, naravne nesreče in še bi lahko naštevali. Posledica globalizacije je tudi bolj povezan svet, kar pravzaprav narekuje sodelovanje namesto tekmovanja med glavnimi akterji zagotavljanja mednarodnih odnosov pri zagotavljanju varnosti.

Glavna debata je potekala med realisti in idealisti. Realisti so, kot je to njim v navadi, poudarjali pomen moči kot sredstvu za dosego varnosti, medtem ko so idealisti vztrajali, da je edina varnost mogoča le v stanju trajnega miru (Buzan 2007, 26). Ključna letnica spremembe je 1994, saj je bilo takrat prvič objavljeno poročilo o človekovem razvoju (Human Development Report), ki je za vedno spremenilo ustaljen pogled na sodobno varnost. Več varnostnih teoretikov je po hladni vojni neorealističnemu pojmovanju varnosti, kot varovanja temeljnih vrednost oziroma nacionalnega interesa, očitalo, da se ne ve več, čigave interese se pravzaprav brani pred katerimi zunanjimi vojaškimi grožnjami ter s kakšnimi sredstvi (Prezelj 2008, 17).

Poleg poročila o človekovem razvoju se je pomemben premik zgodil tudi v Kanadi s strani vlade in nekaj akademikov, ko so dali pobudo za ustanovitev Mreže za človekovo varnost, ki ji je sicer predsedovala tudi Republika Slovenija. Ta mreža je spodbujala raziskovanje človekove varnosti kot take preko seminarjev, okroglih miz ter javnih debat skupaj s Komisijo za človekovo varnost. Poleg teh so vprašanja človekove varnosti odpirale tudi druge, večje mednarodne organizacije, kot je denimo Organizacija združenih narodov (OZN), G'/G8, Afriška unija, ASEAN in seveda Evropska unija. Vse je začel zanimati bolj posameznik, kot nacija, vsaj v smislu varnosti, oziroma pri opredeljevanju njenega koncepta, torej teorije.

Začelo se je dogajati, da so vlade po svetu pričele z vključevanjem takšnih konceptov v svoje politične programe in plane, čemur so seveda sledili še mediji, ki so sprožili javne razprave o konceptih zagotavljanja individualne varnostiu, v katere so se vključile različne stroke in vede.

Protislovno lahko rečemo lahko, da se je koncept človekove varnosti razvil kot posledica globalizacije, ki jo hkrati omejuje in krči. Svetovni mir je vse bolj posledica sledenju napotkov

in zagotavljanja človekove varnosti. Objekt varnosti torej postaja posameznik ali kot bom poskušal pokazati v nadaljevanju dela, uporabnik.

Na grožnjo človekovi varnosti lahko gledamo lokalno (posamezne države, etnične skupnosti, itd.) ali globalno (denimo globalno »segrevanje« ali tudi globalni igralec, ki upravlja občutljive podatke, kot je denimo podjetje Google Inc.). Pa je lahko grožnja globalni človekovi varnosti tudi ena sama korporacija? V tem diplomskem delu bom poskušal argumentirati, da je lahko. Okrnjena informacijska varnost velikega podatkovnega modela (oziroma podjetja, ki take podatke upravlja preko svojih storitev), ki upravlja osebne in druge človekovi varnosti potencialno nevarne podatke večine Zemljanov, je lahko velik razlog za skrb. Informacijska (ne)varnost je lahko v takšnem primeru vzvod človekovi (ne)varnosti. In takšno podjetje je nedvomno Google Inc.

Poleg zmanjšane medblokovske nevarnosti so h krepitvi človeške dimenzije varnosti prispevali še:

- krepitev pomena človekovih pravic in svoboščin,
- naraščanje števila konfliktnih območij, v katerih je bilo prizadetih veliko število ljudi (humanitarne krize),
- vedno večje zavedanje pomena človekovega življenja in blagostanja,
- globalizacija, in tako naprej (Prezelj 2008, 18).

Slednja je pripeljala do okoliščin, ki so drastično vplivale na dinamiko ogrožanja varnosti:

- krčenje prostora (pomen geografske in fizične razdalje se zmanjšujejo),
- krčenje časa (tehnologija povečuje hitrost prenosa informacij ipd.),
- izginjanje meja (kar se predvsem nanaša na zmanjševanje vloge nacionalnih meja za pretok ljudi, kapitala, dobrin, idej in tako naprej) (Prezelj 2008, 18).

Zelo očitna posledica je možnost hitrega prenosa groženj varnosti na večja geografska območja, kjer nacionalne meje ne igrajo več tako pomembne vloge. Takšno okolje je bilo plodno za horizontalno (vključitev okoljske, gospodarske, demografske, kriminalitetne, teroristične, zdravstvene, informacijske, migracijske in drugih dimenzij nevojaškega ogrožanja varnosti) in vertikalno (poudarjanje pomena varnosti posameznikov, skupin ljudi,

in tako naprej) širjenja koncepta varnosti. Prvi pogoj vertikalne širitve je bila horizontalna širitev (Prezelj 2008, 18). V tem delu se bom naslonil predvsem na vertikalno dimenzijo.

V ospredje je torej prišla t. i. človeška dimenzija, varnost je začela zanimati bolj človekovo preživetje in njegovo zaščito kot preživetje nacije, kot take. Kot bom argumentiral v nadaljevanju, je lahko monopol na področju »človekovih informacijskih podatkov« velika potencialna nevarnost človekovi varnosti.

Po hladni vojni, ko se je globalizacija torej še okrepila, se je še dodatno spremenilo geopolitično, geoekonomsko in geostrateško okolje, kar je imelo za posledico večjo angažiranost nedržavnih akterjev (posamezniki, družbene skupine in organizacije v okviru civilne družbe, nastajajoča globalna družba oziroma nadnacionalni akterji – multinacionalna podjetja in organizacije) v razpravo o varnosti. Varnostna paradigma je v novih razmerah dobila nove (globalne) razsežnosti, ki so se izražale predvsem v dveh smereh:

1) ozemeljski, ki vključuje posameznike, skupine in organizacije na lokalni, državni, regionalni in svetovni ravni, ter

2) konceptualni, ki vključuje vse vidike človekovega obstoja in delovanja (kulturnega, ekonomskega, političnega, izobraževalnega, zdravstvenega, obrambnega idr.), torej tiste pojavne oblike družbenega življenja, ki jih prištevamo med družbene vrednote (Bilgin 2003, 207).

V mojem delu se bom opiral na obe smeri, saj Google upravlja praktično z vsemi sferami posameznikov, ki so njegovi uporabniki.

V ospredje so torej prišle nekatere doslej spregledane kulturno-civilacijske razsežnosti varnosti, zato današnje razprave posvečajo večjo pozornost drugačnim prvinam sodobne varnostne problematike, kot so degradacija okolja, podnebne spremembe, odvisnost od tehnologij (Google storitev), lakoti, neenakomernemu ekonomskemu razvoju, nalezljivim boleznim torej ne le zgolj vprašanje fizičnega obstoja posameznikov temveč njegovi blaginji. V ospredje je prišlo drugačno pojmovanje varnosti: globalne in človekove varnosti (Bilgin 2003, 207). In prav odvisnost od tehnologij je tisto področje, na katero se bom opiral v nadaljevanju.

Poleg globalizacije se sočasno danes razvija še individualizacija, kjer se poudarja pomen posameznika tako v nacionalnem, kakor tudi v mednarodnem okviru. Splošno sprejeto prepričanje je, da je posledica zmanjšanja ali izgube človekove varnosti, kot je denimo resna epidemija, ekonomsko pomanjkanje, kršitve človekovih pravic in tako naprej, zmanjšanje stabilnosti znotraj in zunaj državnih meja, kar pa ima neposreden učinek na mir. Tako je v interesu držav, zavoljo lastne varnsoti, tudi varnost človeka, ne le kot zagotavljanje njegovega fizičnega obstoja, temveč tudi kot zagotavljanje njegove blaginje.

Čeprav so nekateri elementi človekove varnosti prisotni že od kar se filozofija in politika ukvarja z družbenimi problemi, je koncept človekove varnosti (Human Security Concept) razmeroma nov. Novo je pravzaprav to, da se na varnost gleda celostno. Razmerje med posameznikom in državo se je nenehno spreminjalo tako, da je postopoma bogocentričnost od zgoraj navzdol (bog je suveren nad vesoljem), zamenjal suveren ljudstva nad državo (od spodaj navzgor). Vplivni dejavnik so bili tudi ekonomija, predvsem multinacionalke, ki so pravzaprav gonilna sila globalizacije ter kontra družbena gibanja za predrugačenje globalizacije. Na ravnanje vlad so začeli vplivati gospodarski subjekti in civilna družba, vsak s svojo agendo, s svoje strain in lastnimi prijemi. Spremenjen svet je zahteval drugačno razumevanje držav, njenih mej ter avtonomnosti nacionalne jurisdikcije, tako na nacionalni, kot tudi na mednarodni ravni. Na nacionalni in mednarodni ravni se je pogled na stanje stvari preusmerilo od državocentričnega v antropocentričnega. In le normalno je, da nas torej zanima, kako lahko tako visoka odvisnost tako veliko uporabnikov po svetu od Google tehnologij, ogroža posameznika.

Zgodovinsko gledano, je levji delež prispeval tudi razvoj človekovih pravic, ki jih po vzoru gesla francoske revolucije (1789) klasificiramo v:

1) svobodo (državljanske in politične pravice),
2) enakost (ekonomske, socialne in kulturne pravice) ter
3) bratstvo (solidarnostne pravice).

Delimo jih še na individualne in kolektivne (narodne, manjšinske ipd.), če pa k temu prištejemo še okoljsko problematiko, bi po Grizoldu in Bučarju človekove pravice lahko sistematizirali kot:

1) politični, ekonomski in demokratični razvoj;
2) pravice političnih in kultur- nih skupnosti (narodov in manjšin), ter
3) preprečitev zlorabe – pretirane uporabe naravnih virov in trajnostni razvoj okolja (Grizold in Bučar 2011, 837).

Po padcu komunističnih režimov se je na vzhodu povečala pozornost na svobodo posamezika, deset let zatem pa se je na zahodu po padcu Svetovnega trgovinskega centra (9/11) preusmerila nazaj na (pretirano) varnost, velikokrat tudi na račun človekovih pravic. Sredstva, ki opravičujejo cilj in podobno.

V sedemdesetih letih prejšnjega stoletja, ko je zasedal helsinški proces in je bila podpisana Helsinška sklepna listina leta 1975, sta pričela veljati oba pakta o človekovih pravicah, ki sta odslej temelj vsem kasnejšim konvencijam o človekovih pravicah, pri čemer je pomembno dejstvo tudi, da je pravica do samoodločbe narodov v Ustanovni listini ZN in Splošni deklaraciji človekovih pravic (1948) prinesla še pravico do ekonomske samoodločbe.

Po tem, ko je generalna skupščina (GS) ZN leta 1974 sprejela Deklaracijo o ustanovitvi nove mednarodne gospodarske ureditve (res. GS 3201 S-VI), čigar cilj je bil na novo določiti odnose med državami (enakopravnost, medsebojno odvisnost, skupni interes in sodelovanje, ravnotežje, suverenost nad naravnimi viri ter odpravljanje neenakosti kot nevarnosti za mir), so se seveda s problem razvoja človeštva začeli ukvarjati še politiki, pa tudi gospodarstveniki, in znanstveniki. Eden takšnih je bil zbiralnik razmišljanja (think tank*),* ki je zaslovel kot t. i. Rimski klub. Ta je kasneje (1972) izdal precej odmevno poročilo Meje rasti*,* ki je obravnavalo probleme industrializacije, rasti prebivalstva, črpanje neobnovljivih virov, degradacijo okolja itn. (Meadows 1972).

1977 je bila ustanovljena t. i. Brandtova komisija, ki v svojem poročilu Sever-Jug: program preživetja (Brandtovo poročilo) kot največje probleme obravnava: lakoto in prehrano; prebivalstvo – rast, mobilnost in okolje; razoroževanje; trgovino s surovinami; energijo; industrializacijo in svetovno trgovino; transnacionalna podjetja, investicije in transfer tehnologije; svetovno monetarno ureditev in financiranje razvoja. Gospodarska varnost (svetovna prerazporeditev prihodkov med revnimi in bogatimi) postane nujen prvi pogoj in sredstvo za dosego politične varnosti.

Kasneje (1982) je Palmejeva komisija v svojem poročilu Obča varnost – program razoroževanja ugotovila, kako vojaška varnost ogroža ekonomske odnose in razvoj človeštva nasploh. Poročilo, ki izhaja iz premise o nemogočnosti zmagovalca jedrskega spopada, zavrača varnostno tekmovanje in poudari pomen sodelovanja, kot sredstva za dosego varnsoti. To je bil verjetno prvi primer celostnega pristopa in hkratne oddaljitve od tradicionalnega pojmovanja varnosti.

Bruntlandina komisija je leta 1987 v svojem poročilu Naša skupna prihodnost govori o trajnostnem razvoju (okolje in gospodarstvo), torej o tem, kako blaginja obstoječe generacije ne bo ogrožala prihodnjih (World Commission on Environment and Development 1987). To poročilo je postalo gradnik za Svetovni vrh (1992) in sprejetje Agende 21, Deklaracije iz Ria, ustanovitev Komisije za trajnostni razvoj, Svetovnega vrha v Kopenhagnu in še bi lahko naštevali. Čez leta so ekonomiji in okolju dodali še tretji pol trajnostnega razvoja, tj. socialna pravičnost.

Čeprav je zaradi dolžniške krize v 80-ih zamrla ideja neuvrščenih oziroma t. i. Novi mednarodni gospodarski ureditvi (NMGU), je svoje mesto na političnem parketu obdržala ideja o pravici do razvoja iz tretje generacije človekovih pravic, saj je razvoj potreben tako posameznikom kot tudi človeštvu v celoti. Grizold meni, da nerazvoj ne pomeni le stagnacije, temveč tudi počasen propad družb in posameznika. Človekov razvoj merimo z indeksom človekovega razvoja, ki sestoji iz:

1) Odsotnosti nasilja, torej obstoja miru;
2) pravica do obstoja (zadovoljitev temeljnih potreb, kot so nedotakljivost življenja, telesa in lastnine, zagotovljena prehrana in zdravje);
3) pravica do razvoja (dostop do dela, zaslužka in izobraževanja);
4) kakovost bivanja (primerna nastani- tev in zdravo okolje) in
5) kakovost življenja (nediskriminacija in politična participacija) (Grizold in Bučar 2011).

Tudi padec berlinskega zidu (1989) je, poleg razbremenitvi strahu pred jedrskim udarom, med ljudi vsadil pričakovanje po povečani svobodi za posameznika. Vprašanja okolja, zagotavljanje varnosti in miru družbeno-ekonomskega razvoja so postala vprašanja mednarodnega okolja in svetovne politike, ki jih suverene države niso mogle več naslavljati same v okviru klasičnih meddržavnih odnosov.

Ključno za razvoj človekove varnosti pa je bilo, kot že rečeno, Poročilo o človekovem razvoju (Human Development Report), ki ga je izdal Program Združenih narodov za razvoj (UNDP). Od tod izhaja Indeks človekovih svoboščin (Human Freedom Index), ki poveže izobrazbo, zdravje in politične svoboščine. Človekove pravice so postale predpogoj razvoja družbe in človeštva, kot celote. V drugem poročilu (1991) je UNDP opredelil človekovo varnost kot osvobojenost od strahu in potreb (freedom from fear & want). Koncept se je sicer najbolj nanašal Na varnost posameznika pred lasnimi, domačimi oblastmi. Poročilo se je strinjalo s premiso, da države resda varujejo posameznika, spraševalo pa se je – pred kom? Po tem konceptu je za sodobne varnostne grožnje značilno, da neposredno prizadenejo navadnega državljana (Prezelj 2008, 18–19).

Drugačen pogled na sodobno varnost je omogočilo šele poročilo iz leta 1994, ki našteje sedem kategorij človekove varnosti, ki se kasneje konsolidirajo v spodnja področja:

1) ekonomska (revščina, brezdomstvo);
2) finančna (zaposlitev, preživljanje);
3) prehrambena (lakota);
4) zdravstvena (bolezni, slaba zdravstvena oskrba);
5) okoljska (degradacija, onesnaževanje, naravne katastrofe);
6) osebna (fizično nasilje, kriminal, prometne nesreče);
7) spolna (enakopravnost žensk, pedofilija);
8) skupnostna (diskriminacija, zatiranje, dezintegracija) in
9) politična (represija, mučenje, izginotja, kršitve človekovih pravic) (UNDP 1994).

Človekova varnost je tako postal krožno soodvisen diskurz, ki med sabo prekriva področja človekovih pravic, varnosti in razvoja (npr. zdravstvena varnost ni mogoča brez odprave revščine, revščina povzroča nasilje, nasilje onemogoča razvoj itd.) (Grizold in Bučar 2011).

Čeprav se je blokovska delitev konsolidirala, po koncu hladne vojne ni bilo miru. Nasprotno, število znortajdržavnih oboroženih spopadov in z njimi civilnih žrtev je skokovito naraslo. Poročilo iz leta 1999 odkriva nova varnostna vprašanja, ko ugotavlja, da je kar 90 % takšnih žrtev civilistov, pa tudi, da nedržavni akterji niso zavezani k spoštovanju (in ne spoštujejo) mednarodnega prava oboroženih spopadov.

Ruanda (1990–1994) in Bosna in Hercegovina (1992–1995) sta krivi za razvoj misli, da lahko takšne žrtve zaščiti mednarodna skupnost. Leta 2004 je bilo v poročilu Varnejši svet: naša skupna odgovornost zapisano, da lahko varnostni svet Združenih narodov odobri vojaško akcijo za zaščito ljudi, če in ko meni, da situacija ogroža mednarodni mir in varnost, kjer morajo biti izpolnjeni štirje pogoji:

1. pravi namen (zaustavitev grožnje);
2. zadnja možnost (izčrpana sredstva mirnega reševanja sporov);
3. sorazmernost (pri uporabi sile) in
4. uravnoteženost posledic (ali bo vojaška akcija odpra- vila grožnjo) (Združeni narodi 2004).

Koncept človekove varnosti najdemo prikrit tudi v širšem pomenu mednarodne varnosti (International Security Concept). Ko gledamo na mednarodno varnost celostno, ta namreč poleg kolektivne varnosti in orginiziranega kriminala (ozko pojmovanje), vojaške varnosti (nacionalna raven) in pravne državo (raven posameznika), vključuje še ekonomska in okoljska vprašanja, vprašanji energetskih in človeških virov (nacionalna raven) ter seveda vprašanja človekove varnostji (raven posameznika) (Grizold in Bučar 2011, 841).

Človekovo varnost torej opredeljujejo dostop do osnovnih življenjskih potrebščin, osebno varnost pred nasiljem ali škodo (denimo nedostopnost ključne informacijske storitve), kamer štejemo še zaščito posameznika pred terorizmom in kriminalom (predvsem organiziranim – belo blago, orožje in droge), nalezljivimi boleznimi, politično in drugo korupcijo, množičnimi migracijami, in tako naprej.

Lincoln Chen, ki je tvorec besedne zveze človekova varnost je menil, da je za razliko od ostalih varnosti, ki so lahko le sredstvo za dosego človekove, denimo vojaške, ta končni cilj in smisel vseh varnostnih prizadevanj, usmerja pa da se k preživetju, dobrobiti in svobodi ljudi (Vogrin 2006, 12).

Vse kaže, da je človekova varnost tudi danes nič več, kot le koncept in še ta je tarča mnogih kritik. Problem je namreč vpeljava v prakso. Če bi želeli, da koncept človekove varnosti zaživi v realnosti, bi bile potrebne mnoge strukturne spremembe v mednarodnem sistemu, sodelovanje celega spectra vladnih in nevladnih (humanitarnih, okolijskih in drugih)

organizacij pri preventivni diplomaciji, učinkovitejše napore sodelovanja držav na mednarodni ravni, pa tudi s civilno družbo, regionalnimi in lokalnimi oblastmi. Takšna implementacija bi zahtevala predrugačenje mednarodnega sistema (finančnega, trgovinskega in tako naprej), vloge držav oziroma funkcije suverenosti in nenazadnje tudi spremenjeno vlogo posameznika pri odločanju na nacionalni (oblast) in vključevanju na mednarodni ravni (Grizold in Bučar 2011, 841).

Koncept človekove varnosti je pronical celo v pojmovanje tradicionalne nacionalne varnosti, kjer pomika v ospredje posameznika, kot osnovni refenčni object varnosti, namesto države, pravtako pa se je preko njega varnost tesneje povezala s konceptom trajnostnega človekovega razvoja.

Po Newmanu obstajajo štirje vidiki človekove varnosti:

1. temeljne človekove dobrine (ekonomska, fiziološko, zdravstvena, osebna, okoljska, kulturna in politična varnost) – občutki (ne)varnosti izvirajo zgolj iz vsakdana, človekova blaginja pa je najboljši kazalnik le-te;
2. dogmatična / intervencionistična smer (humanitarne intervencije) - varnost države ne zagotavlja nujno varnost posameznika, lahko jo celo ogroža, največji problem pa je vprašanje motiva izvajalcev in medijev, ki konflikte problematizirajo ali pa ne (Wheeler 2000);
3. družbena blaginja/razvojna smer (družbeni razvoj, kot sredstvo, je glavna prvina za razvoj drugih dobrin in svoboščin, pomembnih za zagotavljanje posameznikove varnosti in nepriznavanje minimalnih standardov varnosti) – Koncept človekove varnosti in strategija za njegovo dosego morata biti integralna;
4. koncept nove varnosti (epidemiologija, mamila, terorizem, nehumana orožja, kiber-netsko bojevanje in destruktivna narava človeka). Varnost posameznika je odvisna tudi od suverenosti in varnosti države.

Spremembe (predvsem tehnološke), ki so dale zeleno luč globalizaciji, hkrati povročajo resen izziv demokraciji, varnosti in razvoju. Pri konceptu nove varnosti sta glavna naslovnika tako država, kot posameznik, saj je ogrožanje posameznika vedno povezano s šibkimi državnimi institucijami, ki naj se krepijo za rešitev problema (Newman 2001).

Danes niti v stroki niti v politiki (še) ni neke končne definicije ali vsaj konsenza o definiciji človekove varnosti. Nekateri koncepti izhajajo iz države, ki zavoljo lastne legitimnosti skrbi še za varnost posameznikov (zahodne liberalne demokracije), druge pa kot izhodišče postavljajo posameznika. Ne glede na zorni kot problematike je očitno dejstvo, da varnost posameznika izključuje državno suverenost, ki ostaja ključni gradnik mednarodne varnosti in obratno. Odprto vprašanje seveda ostaja, kako v praksi zagotoviti človekovo varnost ter na kaj se naj bi človekova varnost v končni fazi nanašala?

Thomas in Tow menita, da merilo varnosti države ne more biti več zgolj varnost njenih meja, temveč tudi njeni državljani, humanitarno intervencijo pa vidita kot najpomembnejši mehanizem zagotavljanja človekove varnosti v razmerju do državne suverenosti. Dejstvo je, da svetovne varnostne organizacije, kot so NATO in OZN, širijo koncept človekove varnosti, hkrati pa sejejo dvom v njegove akterje oziroma zahtevajo premislek o odnosu med njimi.

Termin človekova varnost bi tako morali natančneje opredeliti s ciljem po večji aplikativnosti (od teorije k dejanjem), zato predlagata pristop, ki temelji na treh temeljnih premisah:

1. državne strukture se niso prilagodile globalizaciji, od koder izvirajo transnacionalne grožnje mednarodnim vrednostam, kar za posameznike znotraj držav ne more pomeniti nič dobrega,
2. niti država niti posamezniki se s takimi ranljivostmi ne morejo spopasti sami, kar vodi do tretje premise, kjer
3. tako države kot tudi posamezniki zahtevajo intervencijo tretje strani, s čimer da bodo zagotovljene njihove osnovne potrebe, ki so temeljni cilji človekove varnosti.

Bistvenega pomena po njuno je, da se mobilizira mednarodna civilna družba ki naj zavaruje mednarodne norme in ponovno razdeli moč med državo in nedržavnimi akterji (Thomas in Tow 2002, 178–179).

Caroline Thomas po drugi strani namesto zaščito pred ogrožanjem zagovarja udeležbo v družbenem življenju, človekova varnost pa da so postale razmere, v katerih »so zadovoljene tako temeljne človekove potrebe kot tudi človekovo dostojanstvo, ki vključuje udeležbo v življenju družbene skupnosti« (Thomas 1999, 3).

Zagovorniki koncepta človekove varnosti izpostavljajo zlasti naslednje prednosti:

- človekova varnost predstavlja nov pogled na varnosti, ki se osredotoča na grožnje v vsakdanjem življenju ljudi (zdravje, kriminal in tako naprej);
- se usmerja od države k posameznikom;
- izpostavlja povezanost varnosti in nevarnosti v sodobnem svetu;
- teži k temu, da bo manjšina (bogati) razvila bolj odgovoren odnos do večine (revni);
- potencialno spodbudi pozitivno globalno zavedanje ljudi;
- spodbuja interdisciplinarno raziskovanje.

Kritiki po drugi strani poudarjajo spodnje pomanjkljivosti:

- termin človekove varnosti je preširok in je konceptualno nejasen ter tako neprimeren za znanstveno proučevanje;
- je zgolj drugo ime za človekove pravice;
- zagovarja napačen pristop pri določanju prioritetnih groženj sodobnim družbam (Booth 2007, 322–323).

1.2 Človekova varnost danes

Po pregledu vseh vidikov in kritik pojma človekove varnosti je jasno, da pravzaprav vsi pristopi poudarjajo nekonvencionalne vire ogrožanja varnosti, kljub temu pa ne zanemarjajo tistih tradicionalnih.

Med grožnje, ki značilno ogrožajo človekovo varnost, tako štejemo:

- gospodarske,
- politične,
- okoljske,
- prehrambne,
- zdravstvene,
- demografske,
- naravne nesreče,
- kriminalitetne grožnje v vseh oblikah, vključno s terorizmom,
- nasilne oborožene konflikte in vojne,
- genocid, etnocid,
- mine,

- lahko pehotno orožje in njegovo širjenje in tako naprej (Prezelj 2008, 19).

Pristopi se nekoliko razlikujejo, glede na prioritetiziranje nevojaškega ogrožanja, sicer pa splošnega konsenza o najnevarnejši nevojaški netradicionalni grožnji pravzaprav ni, kar je do neke mere logično, saj se grožnje med samo prekrivajo in dopolnjujejo.

Kot že omenjeno, se nekateri pristopi naslanjajo na pomen posameznikove svobode pred strahom (UN), kar se v zahodnjih liberalnih demokracijah najlažje empirično meri z javnomnenjskimi raziskavami, v Sloveniji SJM (CJM 2014). Drugi (kanadski pristop) kot grožnjo posameznikom v ospredje postavijo kvaliteto življenja. Dejstvo pa je, da pravzaprav vsi na državo gledajo kot na subjekt, ki bo varnost zagotovil. Spomnimo, prav država je tista, ki ima edina legitimno pravizo do uporabe fizične sile za zagotavljanje človekove in državne varnosti. Seveda ne gre spregledati spektra pristopov, ki se opirajo predvsem na nedržavne akterje, ki imajo lahko veliko vlogo pri preprečevanju ali zmanjševanju humanitarnih kriz, preko preventivnih (zmanjšanje ranljivosti posameznikov) in reaktivnih ukrepov (sekundarno sredstvo zagotavljanje človekove varnosti). Uporaba sile je zadnji korak.

Med pogosto uporabljena sredstva za dosego človekove varnosti tako štejemo:

- humanitarna intervencija ali humanitarna pomoč,
- mirovne operacije (peace operations),
- graditev miru (peacebuilding),
- nadzor nad oboroževanjem,
- zagotavljanje spoštovanja človekovih pravic in svoboščin,
- zagotavljanje trajnostnega gospodarskega razvoja,
- zgodnje opozarjanje,
- diplomatske misije,
- fokusirane (pametne) sankcije,
- preventivna namestitev oboroženih sil,
- preventivna diplomacija,
- krepitev civilne družbe,
- zagotavljanje minimalnih življenjskih standardov,

- krepitev zmogljivosti posameznikov za soočanje s humanitarnimi in varnostnimi problemi (npr. skozi izobraževalne procese)
- in tako naprej (Prezelj 2008, 20).

Podobno kot velja za vire ogrožanja, se tudi tukaj priostopi razlikujejo glede na prioritetiziranje zgornjih sredstev, splošnega konsenza o vrstnem redu pa tudi tukaj ni. Veliko teorije govori v prid preventivnim ukrepom, čeprav praksa kaže, da je učinkovitejša reakcija.

Razlike med tradicionalnim in človekovim konceptom varnosti najbolje ponazarja Bajpai v tabeli 1.1, spodaj. Iz tabele je razvidno, da gre glavne razlike iskati v razumevanju referenčnega objekta, katere vrednote se ščitijo, pred katerimi grožnjami se zagotavlja varnost in kot že omenjeno, s kakšnimi sredstvi se varnost dosega.

Tabela 1.1: Primerjava koncepta tradicionalne in človekove varnosti

	NACIONALNA VARNOST	ČLOVEKOVA VARNOST
Na koga se varnost nanaša?	Primarno na državo	Primarno na posameznika
Katere vrednote se ščitijo?	Ozemeljska celovitost in nacionalna neodvisnost	Osebna varnost in svoboda
Varnost pred katerimi grožnjami?	Tradicionalne grožnje (vojaške grožnje, nasilje drugih držav)	Tradicionalne in netradicionalne grožnje, prevladujejo netradicionalne, nevojaške grožnje
Sredstva za dosego varnosti	- sila je primarno sredstvo za zagotavljanje varnosti, uporablja se enostransko, za varnost države; ravnotežje sil je pomembno; - moč se enači z vojaškimi zmogljivostmi, ki so pomembne za zaščito; - redko sodelovanje med državami, le zavezništva; - norme in institucije le omejeno koristne, predvsem na varnostnem/vojaškem območju	- preprečevalni ukrepi, predvsem trajnostni človekov razvoj, primarno sredstvo zagotavljanja varnosti; - popravni oziroma kurativni ukrepi, tudi kolektivna uporaba sile, sekundarno sredstvo zagotavljanja varnosti; - ne le zaščita, tudi usposabljanje ljudi; - sodelovanje med državami in nedržavnimi akterji učinkovito in trajno; - norme in institucije so pomembne

Vir: Bajpai (2000).

Namen koncepta človekove varnosti ni nadomestitev klasičnega pojmovanja varnosti, temveč njegova dopolnitev v smislu človeških dejavnikov varnosti. Axworthy tako meni, da oba koncepta pravzaprav le predstavljata različne predstave, kako odgovarjati na določene obstoječe grožnje, razlika pa je v suverenu, ki je pri tradiciopnalnem pojmovanju država, pri pojmovanju človekove varnosti pa posameznik. Ti dve suverenosti v realnosti ne samo sobivajo, ampak tudi vzajemno souplivajo druga na drugo. Potrebe posameznika, da so postale »pomembna vhodna determinanta pri oblikovanju nacionalne in mednarodne varnostne politike« (Axworthy 1999).

Človekova varnost naj bi torej postala sestavni del nacionalnih varnostnih politik. Pa je res tako? Koncept človekove varnosti je povezan s konceptom mednarodnega zagotavljanja miru in varnosti. Poročilo Visokega odbora OZN o ogrožanju tako enači ogrožanje človekove varnosti z ogrožanjem nacionalne, med vire pa šteje tako nedržavne subjekte, kot tudi državo samo. Taisti odbor je tudi predlagal celovit sistem kolektivne varnosti, ki bi ščitil tako stare, kot tudi nove aspekte varnosti ter upravljal varnostne težave vseh držav, močnih in šibkih. Zelo jasno je torej, da je OZN razširil lasten koncept razumevanja varnosti, ki se je tradicionalno osredotočal na mir med državami, na humanitaren spokoj znotraj države. Od tod naprej lahko med grožnje mednarodnega miru štejemo tudi notranje vojne, genocide in ostale grobe krđitve človekovih pravic. Tudi pregled OZN-ovih resulucij kaže tako, denimo resolucija 668 (1991) o Iraku, ki poudarja grožnjo zatiranja civilnega prebivalstva, ki predstavlja pravo grožnjo mednarodnemu miru in varnosti. Tudi bližje, etnično čiščenje v BiH je bilo označeno za kršitev mednarodnega humanitarnega prava in kot grožnja miru ter varnosti, podobno velja za genocid v Ruandi leta 1995.

Zrcalo teoriji kaže tudi povezanost človekove varnosti s človekovim razvojem, saj kot že rečeno, trajnosti razvoj nudi neugodne pogoje grožnjam človekove varnosti. V prevodu to pomeni, da so okolja z dobrim šolskim sistemom, dolgo življenjsko dobo in spodobnim standardom življenja tradicionalna bolj varna (Prezelj 2008, 21–22). V ta namen se izračuna tudi indeks človekovega razvoja (Human Development Index ali HDI). V tabeli 1.2 si lahko ogledamo indeks za nekaj izbranih držav ter njihov vrstni red (UNDP 2014).

Tabela 1.2: Indeks človekovega razvoja izbranih držav

Država	Rang med državami	Indeks čovekovega razvoja
Norveška	2	0,968
Švedska	6	0,956
Avstrija	15	0,948
Italija	20	0,941
Nemčija	22	0,935
Grčija	24	0,926
Slovenija	27	0,917
Hrvaška	47	0,850
BiH	66	0,803
Albanija	68	0,810
Makedonija	69	0,801
Kitajska	81	0,777
Turčija	84	0,775
Iran	94	0,759
Egipt	112	0,708
Sudan	147	0,526

Vir: UNDP (2014).

Zgornja tabela 1.2 prikazuje le majhen vzorec držav, a vendar se lepo vidi korelacija med človekovim razvojem in človekovo varnostjo. Varno okolje je torej civilizacijski prvi pogoj za uspešnost kakršnegakoli razvojnega projekta. Dokaj logično, prebivalstvo z zagotovljenimi osnovnimi življenjskimi potrebami se manj zateka k nasilju.

Spregledati ne gre niti korelacije med spoštovanjem človekovih pravic in svoboščin in stopnjo človekove varnosti. Ugotovili smo že, da je bistvo človekove varnosti tako spoštovanje človekovih pravic in svoboščin kot tudi zagotavljanje varnosti posameznika. Kot je to ponavljal nekdanji generalni sekretar OZN, Kofi Anan, je zelo pomembno vzajemno dopolnjevanje konceptov varnosti, razvoja in človekovih pravic. Sodobnost ne pozna razvoja brez varnosti, varnosti brez razvoja ter obeh brez spoštovanja človekovih pravic in svoboščin,

kar potrjuje tudi praksa. Ne pozabimo, da je tudi varnost človekova pravica (Prezelj 2008, 24).

Na primeru boja proti terorizmu lahko opazujemo kompleksno razmerje med človekovimi pravicami in človekovo varnostjo. Terorizem kot tak je ena ključnih groženj znotraj EU, kar potrjuje tudi zadnje poročilo Europola, ki pravi, da je bilo v 2012 znotraj EU 537 aretiranih osumljencev, 400 sodno obtoženih posameznikov sicer pa kar 219 terorističnih napadov in 17 smrtnih žrtev le-teh. Za večino napadov in njih poskusov, je bila značilna uporaba nasilja za dosego političnih, predvsem secesijskih ali verskih ciljev (Europol 2013).

Boj proti terorizmu povzroča dokaj velik poseg v človekove pravice, ki so zagotovljene z ustavami in mednarodnim pravom. Vse kaže, da je prioritetna človekova pravica tista, po varnosti. Nekatere vrste legalnega poseganja v človekove pravice niso tako sporne, kot tiste ilegalne, v imenu boja proti terorizmu. Bolj odmevni, sporni primeri so zloglasni tereoristični zapor na Kubi Guantanamo, Abu Graib, tajni zapori CIE, predolga zadrževanja osumljencev, nelegalno prisluškovanje, predaja terorističnih osumljencev v tretje države, kjer je mučenje dovoljeno in tako naprej. Sem lahko štejemo tudi primorano predajo osebnih podatkov Googla državnim organom ZDA, o čemer pišem v poglavju o Googlu.

1.3 Skrbniki človekove varnosti

Na drugi strani so tukaj mednarodne organizacije, projekti in združbe, katerih cilj je dvig človekove varnosti. Denimo Organizacije za varnost in sodelovanje v Evropi (OVSE), kjer je človekova varnost trdno vsidrana ob bok vojaško-politični ter ekološki dimenziji. Cilj OVSE-ja je zagotoviti spoštovanje človekovih pravic in temeljnih svoboščin, spoštovati zakone, promovirati demokratična načela in institucije in tako naprej. Opertivno to pomeni veliko instucionalnih mehanizmov ter terenskih misij. Ključni je Urad za demokratične institucije in človekove pravice (ODIHR), ki ima spodnje naloge:

- spodbujanje demokratičnih volitev preko nadziranja volilnega procesa,
- podpora pri utrjevanju demokratičnih institucij in človekovih pravic ter krepitvi civilne družbe in vladavine prava,
- obveščanje in preprečevanje konfliktov prek nadzora uresničevanja obvez v človekovi dimenziji.

Drugi, slovenskemu medijskemu prostoru bližji, je OVSE-jev predstavnik za svobodo medijev, čigar naloga je nadzor delovanja medijev predvsem v luči njihovega svobodnega in nemotenega delovanja. Čeprav imata oba mehanizma na voljo veliko političnih ukrepov v primeru nespoštovanja zavez v človekovi dimenziji, se v praksi kaže, da mehanizma delujeta opozorilno in dejansko lahko prispevata k izvajanju mednarodnega pritiska na kršilce temeljnih zavez (OSCE: Organization for Security and Co-operation in Europe 2014).

Tudi EU vedno bolj zagotavlja koncept človekove varnosti, ne samo navznoter (do svojih članic) temveč tudi navzven (mednarodno krizno odzivanje). V evropski varnostni strategiji se prvič povežejo grožnje s konkretnimi ukrepi. Gre torej za strategijo, ki prepleta varnost držav in posameznikov (človeško varnost), kot ključne grožnje pa izpostavi:

- terorizem,
- širjenje orožja za množično uničevanje,
- regionalne konflikte,
- razpad držav in
- organiziran kriminal.

Pri ukrepih poudari številna sredstva, kot so:

- obveščevalna,
- policijska,
- pravosodna,
- vojaška in druga.

V nadaljevanju se naveže tudi na pomen varne okolice (Balkan) in pomena večstranskega sodelovanja. V madridskem poročilu (2007) celo predlaga, naj postane koncept človekove varnosti ključni koncept varnostnega delovanja EU v prihodnosti. Čeprav pristop vojne za zagotovitev miru preverjeno ne deluje najbolj, je EU te dni globalni varnostni akter za posredovanje v številnih krizah po svetu. Zato je skupina znanstvenikov predlagala šest načel zunanje varnostne dejavnosti EU:

1. primat človekovih pravic,
2. nujnost zagotovitve legitimne politične oblasti,
3. pristop od spodaj navzgor, kar vključuje angažiranje civilne družbe,

4. učinkovit multilateralem,
5. integralen regionalen pristop ter
6. jasno ter transparentno strateško usmerjanje (Prezelj 2008, 24).

Od leta 2004, po sprejetju haaškega sporazuma, smo v EU priča prizadevanju za vzpostavitev evropskega prostora svobode, varnosti in pravice, katerega cilj je maksimizirati varnost z minimalnim poseganjem v človekove pravice.

Tudi NATO se vse bolj ukvarja z zagotavljanjem človekove varnosti, kar se kaže tudi s širjenjem članstva, saj to poudarja kriterij demokratičnega političnega sistema in spoštovanja temeljnih človekovih pravic in svoboščin. NATO-vi vojaki morajo biti vešči civilizacijskih veščin (poleg vojaških, seveda) saj je vedno več misij tistih, za zagotavljanje varnosti ogroženim skupinam (humanitarne naloge, naloge izgradnje lokalne infrastrukture, pomoč pri razdeljevanju pomoči, ščitenje t. i. varnih območij in tako naprej).

Na koncu lahko še enkrat poudarimo že omenjeno mrežo za človekovo varnost (Human Security Network), kjer gre za skupino podobno mislečih držav (Avstrija, Grčija, Irska, Čile, Kanada, Slovenija, Jordanija, Nizozemska, Mali, Norveška, Švica in Tajska, Južnoafriška republika pa je opazovalka), ki se prek ministrstev za zunanje zadeve posvetujejo o aktualnih vprašanjih človekove varnosti.

2 Vpliv varnosti na človekovo varnost

Za lažje razumevanje povezave med človekovo in informacijsko varnostjo, spodaj podajam nekaj definicij informacijske varnosti, kjer zapise slovarjev in enciklopedij navajam zgolj za lažje razumevanje pojma, ne pa striktne definiranosti pojava.

Bistvo informacijske varnsoti je dejstvo, da se ščijijo podatki oziroma informacije pred nepooblaščenim dostopom. Informacijska varnost pa je tudi širši pojem in se ne nanaša zgolj na zaščitito e-podatkov pred nepooblaščeno uporabo, saj kot predmet ogroženosti vključuje poleg same informacije še celotno infrastrukturo, ki omogoča uporabo informacij, to je informacijsko in teklekomunikacijsko tehnologijo (IKT), vključno z zbiranjem in obdelavo podatkov in delovanje strojne opreme v splošnem (Svete 2005, 107). Vendar se tukaj s širšim pojmovanjem ne bomo ukvarjali, saj nas zanima predvsem odnos med človekovo in informacijsko varnostjo.

Državni slovar informacijsko varnost opredeljuje kot zaščito informacijskih sistemov pred nepooblaščenim dostopom do informacij, njenimi modifikacijami, ne glede na to ali govorimo o hranjeni informaciji ali manipulaciji pretoka informacij ter pred zatajitvijo samega sistema, vključno z vsemi podsistemi za odkrivanje in dokumentiranje in zavračanja tovrstnih groženj (Hayden 2003, 33).

IBM-ov slovar računalništva pravi, da so informacijska varnost koncepti, tehnike, tehnični in administrativni ukrepi za zaščito informacij pred namernimi ali nenamernimi nepooblaščenimi pridobitvami, povzročanjem škode, razkritjem informacij, spremembo informacij, manipuliranje z njimi ali izgubo in uporabo informacij (McDaniel 1994).

Ogrožanje delovanja IKT ali ogrožanja informacijske varnosti po Petroviću (2004) razdelimo v štiri skupine, pri čemer Svete (2005) te dodatno razdelili v dve, kjer se prva nanaša na fizične oblike ogrožanja informacijske varnosti, druga pa zajema uporabniški vidik ogrožanja informacijske varnosti. Omenjena delitev je prikazana v tabeli 2.1.

Tabela 2.1: Oblike ogrožanja informacijske varnosti

Višja sila	Pomanjkljivosti strojne in programske opreme	Človeški dejavniki (nenamernost)	Človeški dejavniki (namernost)
Fizične oblike ogrožanja informacijske varnosti		**Uporaba kot ogrožanje informacijske varnosti** (družbeno in kulturno ogrožanje)	
• Potres • Nevihte • Poplave • Strele • Požar • Visoka temperatura • Visoka vlažnost • Onesnaženost • Radarsko sevanje • Akustično sevanje • Elektromagnetsko sevanje v obe smeri • Nestabilnost napajanja z električno energijo • Izredne razmere • Vojno stanje	• Izpad sistema • Tehnične napake na osrednji enoti –strežniku • Tehnične napake na odjemalcih • Logične napake v strežnih programih • Logične napake v aplikativnih programih	• Slaba organizacija • Nedisciplina • Nemarnost • Nestrokovnost • Monotonost • Utrujenost	• Kraje • Prevare • Poneverbe • Falsificiranje • Izsiljevanje • Grožnje • Kršenje zasebnosti • Sabotaže • Sporočanje zaupnih podatkov • Vohunjenje • Pornografija • Propaganda • Vandalizem (crackerji) • Terorizem • Umori • Heking • Izdelava ter distribucija virusov • Piratstvo na področju programske opreme • Napadi DoS

Vir: Petrovič (2004, 20).

Ugotovili smo, da se je, globalno gledano, pojmovanje varnosti premaknilo od države, kot referenčnega objekta, do posameznika in vse kaže, da je varnost posameznika te dni najvišja vrednota. Po drugi strani smo ugotovili, da se informacijska varnost ukvarja z varnostjo informacij in informacijskega sistema. V nadaljevanju želim pokazati, da se ti dve področji medsebojno povezujeta in druga na drugo vzajemno vplivata. Pokazati želim, da se informacijska varnost pravzaprav ukvarja s človekovo varnostjo in obratno.

2.1 Informacije kot orožje

Po letu 1972 se je industrijska doba prevesila v informacijsko, ki zahteva usklajevanje in povezovanje informacij z različnih področij, s tem pa tudi komuniciranje na različnih ravneh, zato ji pravimo tudi informacijsko-komunikacijska doba. »Glavni viri informacijsko-komunikacijske dobe je informacija oziroma informacije in z njimi odnosi, na katerih temeljijo vsa področja človekovega življenja in dela. Znanje in informacije se s komuniciranjem dograjujejo, izpopolnjujejo in poglabljajo, s čimer se večata moč in pomembnost informacij, ki so v vsakdanjem življenju bistvenega pomena« (Wikipedia 2014).

Značilnosti informacijske dobe se izražajo v spremenjenem načinu dela, ki je podprto s tehnološko opremo, ki omogoča hitrejše in učinkovitejše sprejemanje informacij, v spreminjajočem se načinu učenja, praktično bi lahko rekli, da se spreminja način življenja nasploh. »Z zornega kota odvijajoče se informacijske in komunikacijske revolucije živimo v času mega trenda, ki ga imenujemo nastajanje globalne informacijske družbe« (Haywood 1997). Sping in Zimmer sta že leta 2008 pravila, da se gospodarski razvoj industrije skozi daljše časovno obdobje začne najprej s »spletnimi iskalniki« in konča z veliko prevlado le teh na trgu, kot sta Google in Yahoo. Tem spletnim iskalnikom, so se in se še vedno pridružujejo novi, vendar bi lahko rekli, da niso še tako dobro uveljavljeni in nimajo pri uporabnikih take moči (Sping in Zimmer 2008).

Nič kaj nov ni stavek, da je valuta v informacijski dobi prav informacija. Karkoli torej želi kdorkoli naresti, potrebuje informacije, ki so lahko pridobljene na legalen, nesporen način ali na ilegalen, uporabnikom sporen način, ki torej ogroža njegovo, človekovo varnost.

> *V današnjem svetu smo priča zanimivemu pojavu - vzbujanju občutka ogroženosti (najbolj skrajno zaradi terorizma, pa tudi čisto običajnega zaradi varovanja premoženja ...) in vtisa, da se ta lahko zmanjša z različnimi ukrepi, ki (grobo) posegajo v našo zasebnost. Tako postaja npr. videonadzor stalni spremeljevalec naših poti, pa čeprav nihče ne dela analiz, ali in za koliko so se zaradi videonadzora zmanjšala nezaželena ravnanja. Podobno je npr. z uporabo tehnologije GPS - tudi v delovnih razmerjih; zbirajo se velike količine osebnih podatkov, pogoste so zahteve po kopijah osebnih dokumentov - vse za (navidezno) povečanje varnosti. Znan je izrek Benjamina Franklina, ameriškega izumitelja, novinarja, diplomata, o tem, da družba, ki se*

odpove svobodi zaradi večje varnosti ne zasluži ne enega, ne drugega in oboje izgubi. Bojim se, da je imel prav (Lemut-Strle 2014).

2.2 Maksimiziranje varnosti v zameno za minimalno zasebnost?

Po 9/11 je to postala globalna debata: Koliko zasebnosti smo se pripravljeni odreči v zameno za zagotavljanje mednarodne in domače varnosti? V ZDA očitno več, kot drugje po svetu, saj so le šest tednov po terorističnem napadu na t. i. dvojčka (WTC) sprejeli protiustavni Patriotski zakon (USA PATRIOCT act), ki je z vidika zasebnosti posameznikov sporen vsaj v spodnjih štirih točkah:

1. Povečanje pristojnosti državnim službam pri pridobivanju preiskovalnih nalogov, ki jih izdajajo sodišča (potencialno ogrožanje zasebnosti posameznikov in nepooblaščen vdor v njihove domove),
2. Dovoljenje državnih organov, da preiskovanca o preiskavi obvestijo šele po zaključku le-te,
3. Širša pooblastila za telefonsko in e-poštno prisluškovanje ter
4. Večja moč državi pri kontroli in nadzoru interneta in pretoka informacij preko njega.

Ta zadnja nas bo najbolj zanimala, saj se zadnja leta po večjih svetovnih medijih veliko piše in govori o kršitvah zasebnosti in predaji podatkov obveščevalnim službam. Nekateri kritiki menijo, da je PATRIOT act kot tak neustaven, saj zakon posega v osnovne svoboščine, ki so v ZDA zagotovljene z ustavo, kot denimo pravica do zasebnosti, varstva pred neutemeljenimi zasegi in preiskavami, svobode govora in združevanja, in tako naprej. Zakon je seveda bil sprejet brez večjih težav, saj so bili Američani takrat pod vtisom, da jim preti teroristična gonja (Electronic privacy information center 2014).

ZDA navajam le kot najodmevnejši primer, kako zakonsko urediti teren za neomejeno poseganje v zasebnost posameznikov in s tem potencialno ogrožanje njihove, torej človekove varnosti. Več o zloglasni ameriški zakonodaji PATRIOT Act in FISA (Foreign Intelligence Surveillance Amendments) je zapisano v poglavju o Googlu, tukaj pa še omenimo, da lahko na podlagi teh zakonov ZDA dostopajo tudi do podatkov evropskih subjektov, ki so shranjeni v podatkovnih centrih pod evropsko jurisdikcijo. Vsaj tako ugotavlja Alex Arnbak s sodelavci v svoji raziskavi. Čeprav je EU zakonodaja na področju varovanja podatkov precej stroga, tukaj nima pravega učinka, saj večina ponudnikov storitev

v oblaku, tudi Google, zapadejo pod ameriško jurisdikcijo. V primeru Googla zato, ker je Google ameriško podjetje, ne glede na to, da se podatki fizično nahajajo na ozemlju EU. Ameriški organi pregona in obveščevalne službe lahko torej zahtevajo dostop do osebnih in drugih podatkov Evropejcev ali državljanov katerekoli druge države, ne glede na to, da so takšni podatki shranjeni na strežnikih, ki se nahajajo v Evropi ali kateri tretji državi. Tako lahko ameriške oblasti zaobidejo strožjo lokalno zakonodajo, pri čemer jim ni treba niti poročati o številu takšnih zahtevkov ali o tem, kakšni podatki, če sploh, so bili posredovani (Axel in drugi 2012).

K sreči je sam Google letos dosegel javno poročanje takšnih zahtevkov, v luči njegovega »prizadevanja za transparentnost poslovanja in skrbi po spletni, informacijski in človekovi varnosti« (Google 2014).

Sporne niso le države, kot entitete. Sleherna informacija v nepravih rokah z nečisto agendo je lahko namreč orožje, kar še zlasti velja za informacije osebnega značaja. Vse je odvisno od iznajdljivosti nepridiprava, ki z informacijami manipulira ali jih razkriva tretjim osebam. Ni si prav težko predstavljati, da se konkurenčna podjetja ne bi branila vpogleda v podatkovne baze strank ali denimo poslovnih izidov.

Googleov poslovni model temelji na premisi brezplačnosti njegovih storitev v zameno za ogromne količine zbranih podatkov o obnašanju svojih uporabnikov. Zakaj? Zaradi učinkovitejše prodaje oglasov, seveda. Kontekstualno oglaševanje je krivec, ki vam pred oči na spletu pripelje točno tisto storitev ali izdelek, za katerega morda niti pomislili še niste, da ga kupujete, pa ga! Ciljano oglaševanje kot tako sicer ne predstavlja neposredne grožnje človekovi varnosti, posedovanje podatkov, ki to omogočajo, pa potencialno lahko.

Kaj pa naše lastne informacije, torej informacije na ravni posameznika in naši osebni podatki, ki jih razkrijemo na spletu? Na različnih lokacijah v različnih oblikah in pri različnih ponudnikih se hranijo pravzaprav vse informacije o nas; osebni podatki, življenjski stil, naše osebne preference in lastnosti in še bi lahko naštevali. Z namestnico informacijske pooblaščenke RS sem se pogovoril o nekaterih aspektih zbiranja in posredovanja osebnih podatkov.

Najprej me je zanimalo, kaj sploh so osebni podatki in kako so varovani pri nas? Rosana Lemut-Strle meni, da

> *varovanih osebnih podatkov ni mogoče našteti, saj ne poznamo t. i. zaprtega kroga varovanih osebnih podatkov. Osebni podatek je po definiciji (ki jo ZVOP-1 prevzema iz Direktive 46/95) vsak podatek, ki posameznika določa ali ga dela določljivega, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa. Načeloma je vsak osebni podatek tudi varovan, razen če zakon določa drugače (da je npr. javen - kot so to podatki v zemljiški knjigi, poslovnem registru ...), ali če za razkritje obstaja drug pravni temelj (npr. v zasebnem sektorju privolitev posameznika, na katerega se osebni podatek nanaša)* (Lemut-Strle 2014).

Vedno sta za nastalo kriva dva, pavšalno rečeno, vendar načeloma drži. Smo tudi uporabniki sami krivi za preobsežno predajo lastnih osebnih podatkov ponudnikom, kot je Google? Informacijska pooblaščenka pravi, da ja. Ko svoje osebne podatke posredujemo različnim upravljavcem, bi morali biti pozorni na pogoje, pod katerimi podatke pošiljamo (običajno objavljamo na spletu). Če smo pristali na to, da upravljavec (npr. Google) naše osebne podatke obdeluje naprej tako, da jih npr. posreduje svojim pogodbenim partnerjem za namen oglaševanja ipd., smo v tem delu prostovoljno predali nadzor nad svojimi osebnimi podatki tretjim. Poudariti je še treba, da je varstvo osebnih podatkov človekova pravica v državah članicah Sveta Evrope (47), ne pa tudi širše. Ko gre torej za upravljavca s sedežem v t. i. tretji državi, zanj praviloma veljajo pravila te tretje države (države, kjer ima sedež) (Lemut-Strle 2014). Kako kompleksna so pravna razmerja, ko gre za obdelavo osebnih podatkov na splet, je lepo prikazano v odločbi sodišča EU C-131/12: Google proti Španiji (CVRIA 2014).

Informacijska pooblaščenka še meni, da

> *se je treba zavedati, da varstvo osebnih podatkov v vseh državah sveta ni obravnavano na enak način, kar posledično pomeni, da so ravnanja upravljavcev, ki bi jih evropski informacijski pooblaščenci šteli za kršitev varstva osebnih podatkov, drugje (kjer varstvo osebnih podatkov ni človekova pravica oziroma sploh ni pravica) lahko povsem zakonita. Predvsem pri udejstvovanju na spletu (in uporabi mobilnih*

aplikacij) je dobro, da se tega uporabnik zaveda - tudi na način, da vselej prebere npr. splošne pogoje za nudenje storitev (Lemut-Strle 2014).

Iz zgornjega sklepamo, da lahko Google brez posebnih obrazložitev svojim uporabnikom, njihove podatke posreduje tretji osebi, če sam to presodi. In res, tudi Google predaja pravzaprav vse vrste podatkov tretjim osebam, predvsem organom pregona ZDA. Več o tem v poglavju o Googlu.

Ne glede na ugotovitve informacijske pooblaščenke in analize splošnih pogojev poslovanja podjetja Google Inc., je med nami kar nekaj primerov razkritij (leaks) informacij, ki so tako ali drugače potencialno nevarne, sicer bolj državnim entitetam, pa vendar. V zadnjih letih sta takšna primera afera denimo Wikileaks in afera Žvižgač.

Slednja je verjetno najboljši dokaz (ali bolje indic), da nam obveščevalne in proti-obveščevalne službe sledijo, o čemer govori pred kratkim razkrita zgodba Edwarda Snowdena. Edward Joseph Ed Snowden je ameriški računalniški specialist, bivši sistemski administrator obveščevalne službe CIA in protiobveščevalni trener organizacije (DIA). Junija 2013 je razkril številne sporne dokumente iz časov, ko je delal kot podizvajalec NSA-ja za podjetje Dell in Booz Allen Hamilton. Njegovo razkritje je danes smatrano kot največje razkritje tajnih dokumentov v zgodovini ZDA. Snowdenovo razkritje je obelodanilo obstoj številnih globalnoih nadzornih programov, ki jih v večini primerov vodi in upravlja NSA in obveščevalnemu zavezništvu Avstranilje, Kanade, Nove Zelandije, Združenega Kraljestva in ZDA (Five Eyes) v sodelovanju s telekomunikacijskimi podjetji pa tudi EU vladami.

Razkritih je bilo kar nekaj programov (Boundless Informant, PRISM, XKeyscore, Tempora, MUSCULAR, FASCIA, Joint Threat Research Intelligence Group, Dishfire, Squeaky Dolphin, Optic Nerve), ki se ukvarjajo s prestrezanjem klicev, e-pošnih sporočil, podatkovnimi bazami GPS lokacij, analizami zbranih podatkov in drugimi, lokalno in globalno protiustavnimi prijemi zagotavljanja varnosti (Wikipedia 2014).

Globalno jasno dejstvo je torej postalo, da tudi spletni ponudniki, kot je Google (poleg ostalih večjih igralcev, kot so Microsoft, Yahoo, Facebook in Apple), predajajo informacije o svojih uporabnikih tretjim osebam, v tem primeru obveščevalnim organizacijam.

3 Google Inc. kot grožnja človekovi varnosti

Za podjetje Google Inc. (v nadaljevanju Google) lahko brez večjih zadržkov rečemo, da vse ve, vse vidi in vse sliši, kar bom kasneje argumentiral skozi Googlove storitve, za zdaj pa imejmo v mislih le najbolj znane in velike storitve, ki jih uporablja večina uporabnikov e-storitev, npr. tiste za osebno in poslovno komunikacijo (Gmail), IM storitev Gtalk, kartografskega sistema Google maps in še bi lahko naštevali. »Vse ve« je morda malo pretirana izjava, ki se nanaša na dejstvo, da lahko preko iskalnika Google pridemo do skoraj vseh podatkov, ki na svetu obstajajo. Tega se ne da natančno izmeriti, saj je vsako sekundo na svetovnem spletu približno 10 novih spletnih uporabnikov, ki tudi sami generirajo novo vsebino. V trenutku, ko tipkam tole diplomsko delo, naj bi bilo na spletu 2,925,249,355 spletnih uporabnikov (7,9 % rast), 7,243,784,121 Zemljanov (1,14 % rast), kar pomeni, da je cca. 40.4 % uporabnikov povezano v svetovni splet, kjer se šteje, če ima uporabnik dostop do interneta doma (Internet live stats 2014).

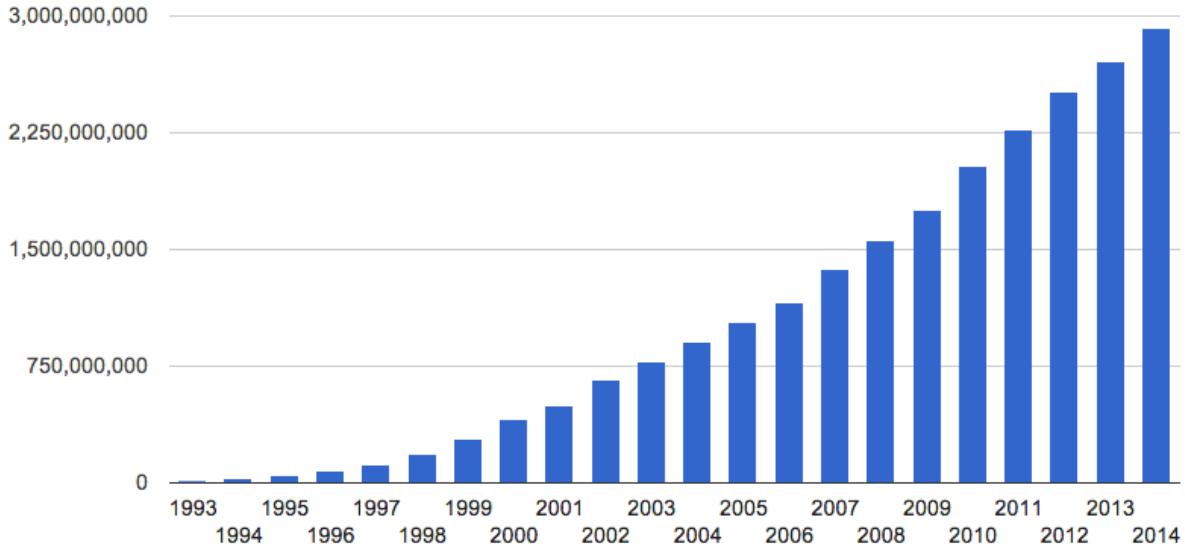
Tabela 3.1: Rast spletnih uporabnikov

Leto (1. Julij)	Spletni uporabniki	Rast uporabnikov	Svetovna populacija	Rast populacije	Penetracija (% populacije s spletnim dostopom)
2014*	**2,925,249,355**	7.9%	7,243,784,121	1.14%	**40.4%**
2013	**2,712,239,573**	8.0%	7,162,119,430	1.16%	**37.9%**
2012	**2,511,615,523**	10.5%	7,080,072,420	1.17%	**35.5%**
2011	**2,272,463,038**	11.7%	6,997,998,760	1.18%	**32.5%**
2010	**2,034,259,368**	16.1%	6,916,183,480	1.19%	**29.4%**
2009	**1,752,333,178**	12.2%	6,834,721,930	1.20%	**25.6%**
2008	**1,562,067,594**	13.8%	6,753,649,230	1.21%	**23.1%**
2007	**1,373,040,542**	18.6%	6,673,105,940	1.21%	**20.6%**
2006	**1,157,500,065**	12.4%	6,593,227,980	1.21%	**17.6%**
2005	**1,029,717,906**	13.1%	6,514,094,610	1.22%	**15.8%**
2004	**910,060,180**	16.9%	6,435,705,600	1.22%	**14.1%**
2003	**778,555,680**	17.5%	6,357,991,750	1.23%	**12.2%**
2002	**662,663,600**	32.4%	6,280,853,820	1.24%	**10.6%**
2001	**500,609,240**	21.1%	6,204,147,030	1.25%	**8.1%**
2000	**413,425,190**	47.2%	6,127,700,430	1.26%	**6.7%**
1999	**280,866,670**	49.4%	6,051,478,010	1.27%	**4.6%**
1998	**188,023,930**	55.7%	5,975,303,660	1.30%	**3.1%**
1997	**120,758,310**	56.0%	5,898,688,340	1.33%	**2.0%**
1996	**77,433,860**	72.7%	5,821,016,750	1.38%	**1.3%**
1995	**44,838,900**	76.2%	5,741,822,410	1.43%	**0.8%**
1994	**25,454,590**	79.7%	5,661,086,350	1.47%	**0.4%**
1993	**14,161,570**		5,578,865,110		**0.3%**

*** ocena za 1. Julij 2014**

Vir: Internet live stats (2014).

Graf 3.1: Rast spletnih uporabnikov



Vir: Internet live stats (2014).

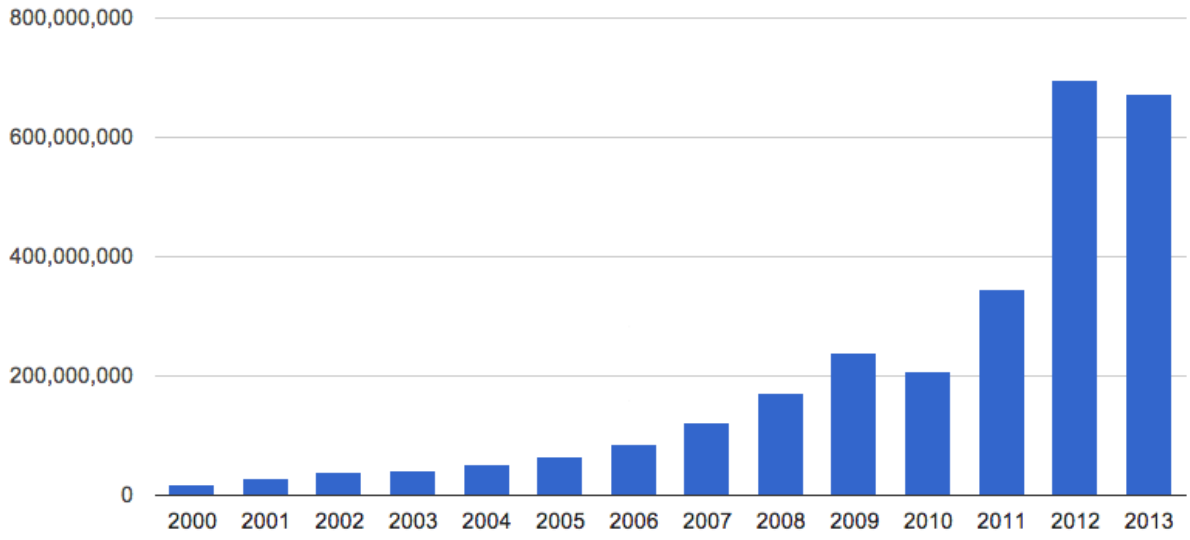
Podobno je z rastjo števila spletnih strani, saj se nova spletna stran pojavi vsako desetinko sekunde. V letu 2014 bomo priča dvema pomembnima mejnikoma, in sicer prebila se bo meja treh milijard spletnih uporabnikov in objavljena bo 1 milijarda spletnih strani. Na vsako spletno stran pride torej 3 spletni uporabniki, od česar gre 2/3 uporabnikov pripisati razvitemu svetu. Zanimivo je, da količin aspletnih strani ne raste tako hitro, kot bi si morda mislili. V letu 2013 je celo opazen negativen -3 % trend rasti (Internet live stats 2014).

Tabela 3.2: Rast spletnih strani

Leto (Junij)	Spletnih strani	Rast	Spletnih uporabnikov	Uporabnikov na spletno stran
2013	**672,985,183**	-3 %	2,756,198,420	4
2012	**697,089,489**	101 %	2,518,453,530	4
2011	**346,004,403**	67 %	2,282,955,130	7
2010	**206,956,723**	-13 %	2,045,865,660	10
2009	**238,027,855**	38 %	1,766,206,240	7
2008	**172,338,726**	41 %	1,571,601,630	9
2007	**121,892,559**	43 %	1,373,327,790	11
2006	**85,507,314**	32 %	1,160,335,280	14
2005	**64,780,617**	26 %	1,027,580,990	16
2004	**51,611,646**	26 %	910,060,180	18
2003	**40,912,332**	6 %	778,555,680	19
2002	**38,760,373**	32 %	662,663,600	17
2001	**29,254,370**	71 %	500,609,240	17
2000	**17,087,182**	438 %	413,425,190	24
1999	**3,177,453**	32 %	280,866,670	88
1998	**2,410,067**	116 %	188,023,930	78
1997	**1,117,255**	334 %	120,758,310	108
1996	**257,601**	996 %	77,433,860	301
1995	**23,500**	758 %	44,838,900	1,908
1994	**2,738**	2006 %	25,454,590	9,297
1993	**130**	1200 %	14,161,570	108,935
1992	**10**	900 %		
Aug. 1991	**1**			

Vir: Internet live stats (2014).

Graf 3.2: Rast spletnih strani



Vir: Internet live stats (2014).

Po spletu se prelije ogromno informacij, večina njih so generirani s strani domačih spletnih uporabnikov. Vsako sekundo spletni uporabniki preko Googlovega iskalnika pošljejo preko 44 tisoč isklanih poizvedb in si izmenjajo preko 2,3 milijona e-pošnih sporočil. Več podatkov, ki orišejo glomaznost spletnega komunikacijske stroja, si oglejte v tabeli 3.3.

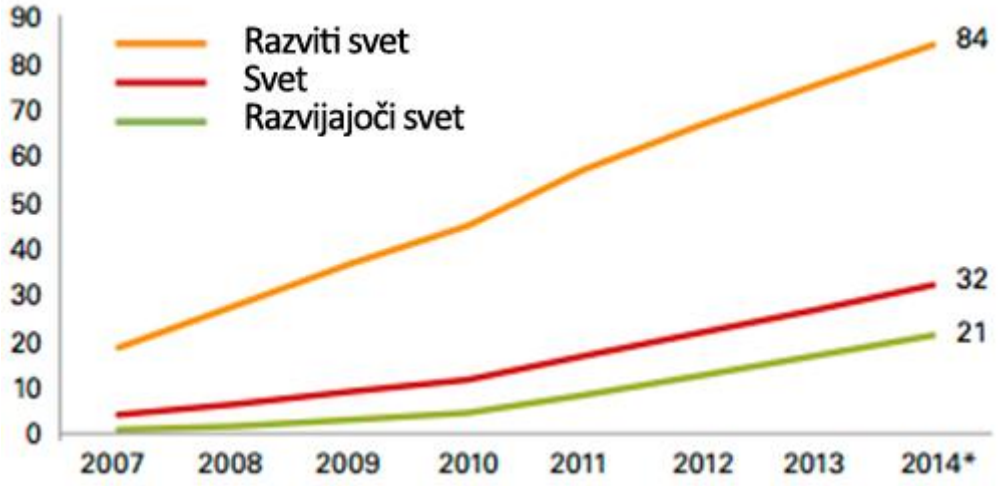
Tabela 3.3: Kaj se na spletu zgodi v eni sekundi

Tweetov	Instagram fotografij	Tumblr zapisov	Skype klicev	Spletni promet v GB	Google iskalnih poizvedb	YouTube video ogledov	Poslanih e-poštnih sporoči
7.394	1.195	1.408	1.496	22.593	44.876	86.214	2.321.483

Vir: Internet live stats (2014).

Po drugi strani beležimo v letu 2014 2,3 milijarde mobilnih uporabnikov spleta, od česar jih je 55 % iz razvitega sveta (ITU 2014). Število uporabnikov interneta na pametnih mobilnih telefonih je po podatkih raziskovalne agencije IDC letos celo prvič v zgodovini preseglo število tistih, ki za ta namen uporabljajo osebne in prenosne računalnike, saj na Kitajskem do svetovnega spleta preko pametnih mobilnih telefonov in tabličnih računalnikov skupaj dostopa dobrih 524 milijonov uporabnikov, preko osebnih računalnikov pa le 512 milijonov (Računalniške novice 2014).

Graf 3.3: Aktivni uporabniki mobilnega interneta na 100 prebivalcev



Vir: ITU (2014).

Iz zgornjih tabel, grafov in interpretacij je več kot jasna magnituda spletne penetracije v globalnem pomenu. V tem diplomskem delu se ne bom osredotočal na iskanje možnih scenarijev, kaj bi se lahko zgodilo, če bi vsi našteti uporabniki ostali brez vseh naštetih storitev ali morda, če bi podatki teh storitev prešli v neprave roke, saj bi to lahko mejilo na znanstveno fantastiko. S tem diplomskim delom želim le opozoriti na magnitudo potencialne nevarnsoti koncentracije tako velikih podatkovnih zbirk pri enem ponudniku in njegov potencialni vpliv na človekovo varnost.

Za Google bi lahko rekli, da vse vidi in vse sliši. Levji delež e-poštne komunikacije na svetu se zgodi preko Googlove storitve Gmail, zato predvidevamo, da ima Google dostop do vse komunikacije in z njo povezanih uporabniških podatkov. Poleg klasične e-mail komunikacije upravlja Google tudi z IM (instant messaging) storitvijo Gtalk, storitvijo upravljanje s fotografijami Photos, kar vse integrira v svoje na svetu peto največje družabno omrežje Google+ (eBizMBA 2014).

3.1 Koliko Google uporabnikov je ogroženih?

Google Inc. je v svoji 16 letni zgodovini, podjetje je bilo ustanovljeno 4. 9. 1998, do danes prevzel 160 podjetij, ki jih je spretno inkorporiral v svoje storitve in izdelke (Wikipedia 2014).

Google za vse svoje storitve uporablja poenoten Google uporabniški račun (Google account, v nadaljevanju Google račun), na katerega so vezani vsi podatki o uporabniku in njegovem obnašanju, ki jih Google zbira o svojih uporabnikih in je za uporabnike brezplačen. Edina omejitev je starostna, in sicer za Združene države ta znaša 13 let ali več, za Španijo 14 let, Južno Korejo 14 let, Nizozemsko 16 let in za ostale države 13 let ali več. Google Račun torej omogoča dostop do vseh Googlovih izdelkov, kot so Gmail, Google+, YouTube in drugi, z enim uporabniškim imenom in geslom. Ko se uporabnik prijavi za Google račun kjerkoli že, dobi poleg tega tudi Gmail račun in profil v Google+ omrežju. Google izdelke pa lahko uporabniki uporabijo tudi brez uporabe Google+ profila ali Gmaila. Možen je namreč naknaden izbris javnega Google+ profila in možna je tudi registracije Google računa z e-naslovom konkurenčnega ponudnika e-pošte, kot je denimo Yahoo) (Google 2014).

Aktivnih Google uporabniških računov je bilo konec leta 2013, 540 milijonov (Wikipedia 2014), neaktivnih pa dosti več. Družabno omrežje Google+ v juniju 2014 beleži 343 milijonov aktivnih uporabnikov (Statista 2014) skupaj pa je Google+ računov že preko 1,15 milijarde, od česar je torej večina neaktivnih (Marrouat 2014).

Google beleži milijardo aktivnih uporabnikov operacijekega sistema Android, preko česar uporabniki dnevno razpošljejo 20 milijard tekstovnih sporočil, zajamejo 93 milijonov »selfijev«, telefoni uporabnikov pa se v uporabi 100 milijardokrat dnevno (King 2014). Če gledamo po uporabnikih to pomeni, da vsak uporabnik dnevno 125 preveri lasten mobilni telefon (Yarow 2014). Operacijski sistem Android je nameščen na 62 % vseh odposlanih tabličnih računalnikih.

Spletni brskalnik Google Chrome uporablja več kot polovica oziroma 54,8 % vseh spletnih uporabnikov (Pennington 2014), medtem ko njegova mobilna različica, mobilni brskalnik Chrome for Mobile, beleži 300 milijonov aktivnih uporabnikov (Kahn 2014).

Google.com je po Alexi, spletni storitvi, ki ocenjuje promet na spletnih straneh, najbolj obiskana spletna stran na svetu (Wikipedia 2014).

Google račun lahko uporabljamo tudi za prijavo v druge spletne strani, kar imenujemo »Social login«. Na tem področju zaseda Facebook prvo mesto s 44 % vseh prijav preko

tretjega ponudnika, Google pa sledi s 37 %. Kar 90 % vseh spletnih uporabnikov je kdaj že uporabilo tak način prijave in več kot polovica jih to redno uporablja (Janrain 2014).

Če vzamemo največja števila, t. j. skupno število Google računov, podatke o trenutnem številu Zemljanov in uporabnikov interneta izračunamo, da je potencialno ogrožena človekova varnost 15,9 % svetovnih prebivalcev (1.150.000.000/7.251.737.604) in kar 39,3 % vseh spletnih uporabnikov na svetu (1.150.000.000/2925249355). Ne morem trditi, da je to največja podatkovna zbirka uporabnikov na svetu, saj je aktivnih uporabnikov samo Facebooka 1.1280.000.000, zato tudi težko trdim, da je Google največja grožnja človekovi varnosti v smislu števila potencialno ogroženih uporabniških računov, lahko pa trdim, da so ti uporabniški opremljeni z največ podatki o njih (Statista 2014).

3.2 Kateri podatki o Google uporabnikih so ogroženi?

Google preko svojih storitev zbira ogromne količine podatkov, s pomočjo katerih ocenjujejo enostavne stvari, kot je denimo jezik uporabnika, do bolj kompleksnih, denimo s kom se uporabnik druži in kakšne oglase si želi videvati preko svojih storitev. Podatke zbirajo na dva načina:

1) Podatki, ki jim jih zaupajo uporabniki (osebni podatki, kot so ime, priimek, e-pošta, plačilna sredstva in podrobnosti plačilnih sredstev, itd.)
2) Podatki, ki jih razberejo preko uporabe njihovih storitev
    a. Podatki o napravi uporabnika (model naprave, operacijski sistem, unikatni identifikatorji naprav, informacije o mobilnem omrežju, vključno s telefonsko številko).
    b. Podatki o uporabi Google storitev (iskalni nizi uporabnikov, uporabnikova telefonska številka in številka klicočega, posredovane in preusmerjene telefonske številke, čas, datum, trajanje in vrsta klicev, IP naslov, aktivnost sistema in njegove nastavitve, tip in jezik brskalnika, čas in datum uporabnikovega dejanja, iz katerega URL naslova je uporabnik prišel, piškoti, ki lahko uporabnika unikatno določijo)
    c. Podatki o uporabnikovi lokaciji (kadar uporabnik to funkcijo omogoči) preko GPS tehnologije in mobilnih senzorjev, ki denimo ocenijo oddaljenost wi-fi omrežij in/ali mobilnih oddajnikov (informacije o celici)

d. Unikatne številke aplikacij, ki sporočaju Googlu, kaj in kdaj se posodablja, namešča ali odstranjuje iz uporabnikove naprave
e. Lokalna hramba (na uporabnikovi lokalni napravi se lahko hranijo uporabnikovi podatki, tudi osebni, poleg cache-a)
f. Piškotki in anonimni identifikatorji (ki jih pošljejo na uporabnikovo napravo ob prvih obiskih določenih storitev ter ob interakcijah s partnerskimi storitvami, t. j. oglaševanje) (Google 2014).

V splošnih pogojih poslovanja Googla piše, da zbrane podatke uporabljajo izključno za zagotavljanje, vzdrževanje, zaščito in izboljšanje storitev, razvoj novih storitev ter varovanje Googla in uporabnikov. Poleg tega tudi za ponudbo prilagojene vsebine, na primer ustreznejše rezultate iskanja in oglase.

Ime denimo, ki ga uporabniki posredujejo za svoj Google Profil, lahko uporabijo v vseh storitvah za katere je potreben Google Račun. Če drugi uporabniki že imajo uporabnikov e-poštni naslov ali druge informacije, ki jih identificirajo, jim lahko Google pokaže javno vidne podatke iz Google Profila, kot sta ime in fotografija. Uporabnikov e-poštni naslov lahko uporabijo za obveščanje o storitvah.

Podatke, ki jih Google zbere s piškotki in drugimi tehnologijami, kot so spletni signali, uporabljajo za izboljšanje uporabniške izkušnje in splošne kakovosti storitev. Osebne podatke iz ene storitve lahko Google združi s podatki (vključno z osebnimi podatki) iz drugih Googlovih storitev, pri čemer se mora uporabnik strinjati. Preden Google uporabnikove podatke uporabi za namene, ki niso navedeni v njihovem pravilniku o zasebnosti, uporabnika zaprosili za soglasje.

Google obdeluje osebne podatke v svojih strežnikih v številnih državah po vsem svetu. Uporabnikove osebne podatke lahko obdela v strežniku, ki je zunaj države, v kateri uporabnik prebiva (Google 2014).

Uporabniki imajo nekaj moči, ko pride do obdelave njihovih podatkov:

- Preko Google Nadzorne plošče lahko uporbnik pregleda in nadzirat nekatere vrste podatkov, povezanih z Google Računom.

- V nastavitvah lahko prikaže in ureja svoje nastavitve oglasov, prikazanih v Googlu in spletu, na primer, katere kategorije vas zanimajo. V njih lahko uporabnik tudi zavrne uporabo nekaterih Googlovih oglaševalskih storitev.
- Uporabnik si lahko ogleda in nastavi, kako bodo njihov Google Profil videli določeni posamezniki.
- Uporabnik lahko nadzira, komu daje v skupno rabo svoje podatke.
- Uporabnik lahko vzeme podatke iz nekaterih storitev.

Poleg tega lahko uporabnik nastavi brskalnik tako, da bo blokiral vse piškotke, vključno s tistimi, povezanimi z Google storitvami ali si nastavi opozorila za takšne primere. Seveda tako številne storitve morda ne bodo delovale pravilno (Google 2014).

Če so uporabnikovi podatki netočni, mu Google poskuša omogočiti posodobitev ali brisanje teh podatkov, razen če jih mora shraniti zaradi zakonitih poslovnih namenov ali zakonskih zahtev. Kadar uporabnik posodablja svoje osebne podatke, lahko od njega Google zahteva, da potrdi svojo identiteto, preden obdelajo njegovo zahtevo (Google 2014). Ni nujno, da bo Google torej ugodil takšni želji, če pa že, se bo prepričal, ali so tokrat podatki res pravi. S takšnim mehanizmom Google izpopolnjuje lastne podatkovne baze uporabnikov in njih obnašanja.

Googlova tehnologija je uporabnikom na voljo brezplačno, v zameno za nekaj znanja o uporabnikovem obnašanju, preko katerega nato Google ciljano oglašuje. Google za merjenje obnašanja uporabnikov uporablja tehnologijo spletnih piškotkov, ki uporabnikom denimo omogočajo, da ne bi videli večkrat enakega oglasa ali pa prav to, če tako želi oglaševalec in predvsem za prikazovanje tistih oglasov, ki uporabnika dejansko zanimajo. Piškotek je majhna datoteka z nizom znakov, ki se pri obisku spletnega mesta pošlje v računalnik. Ko spletno mesto znova obiščete, mu piškotek omogoči, da prepozna vaš brskalnik. V piškotkih so lahko shranjene uporabniške nastavitve in drugi podatki. Brskalnik lahko nastavite tako, da zavrne vse piškotke ali vas obvesti, ko prejmete piškotek. Vendar upoštevajte, da nekatere funkcije ali storitve spletnih mest morda ne bodo pravilno delovale brez piškotkov (Google 2014).

Google v strežniških dnevnikih hrani podatke o oglasih, ki jih prikaže. Takšni dbevniki vključujejo:

- uporabnikovo spletno zahtevo,
- naslov IP,
- vrsto brskalnika,
- jezik brskalnika,
- datum in uro uporabnikove zahteve ter
- enega ali več piškotkov, ki lahko enolično določajo uporabnikov brskalnik.

Ti podatki postanejo po devetih mescih anonimni, in sicer tako, da Google odstrani del naslova IP, po 18 mescih pa podatke o piškotkih. Uporabnik se lahko izogne takšnemu sledenju na dva načina:

1) Onemogoči prikazovanje oglasov na podlagi zanimanja, vendar se tudi tako lahko prikazujejo oglasi, ki temeljijo na dejavnikih, kot so uporabnikova splošna lokacija, ugotovljena na podlagi naslova IP, vrsta brskalnika in nedavna prejšnja iskanja, povezana z uporabnikovim trenutnim iskanjem.
2) Uporabnik onemogoči piškotke

Google lahko lokacijo uporabnika ugotovi tudi na podlagi njegovega naslova IP ali ga oglaševalsko cilja, glede na podatke o uporabnikovi napravi (model, proizvajalec, vrsta brskalnika ali tipala, vgrajena v napravo, na primer merilnik pospeška, itd.).

Google dobi natančne podatke o lokaciji iz uporabnikove mobilne naprave, lokacijo pa lahko izpelje tudi na podlagi uporabnikovih iskalnih poizvedb. Googler to imenuje implicitni lokacijski podatki. Podatke o lokaciji Googlu prav tako sporočajo spletna mesta ali aplikacije, ki jih uporabnik uporablja.

Poleg naštetih tehnologij so tukaj še natančnejši prijemi, ki navadno zahtevajo uporabo mobilne naprave, ki poseduje tehnologiji Wi-Fi in GPS in ID-ji baznih postaj, ki se lahko uporabijo za določanje ali ocenjevanje točne lokacije. Nekatere naprave in/ali aplikacije nudijo tudi dodatne nastavitve za nadzor lokacije v okviru teh lokacijskih storitev v napravi. Pri nekaterih izdelkih lahko uporabnik tako izbere, ali želi te lokacije shraniti v izdelku ali zgodovini računa (Google 2014).

Iz zgoraj naštetih tehnologij sklepam, da ima uporabnik večino kontrole nad dejstvom ali Google spremlja njegovo obnašanje ali ne. Po drugi strani to niti ni tako zelo pomembno, saj je problem, ki ga orisujem širši od uporabnikove varnostne ignorance.

Pomembno vprašanje, ki si ga lahko zastavimo, je tudi, čigava je pravzaprav vsebina na Google strežnikih? Nekatere Google storitve namreč omogočajo nalaganje, hrambo, prejemanje ali pošiljanje vsebine, ki jo generira uporabnik in ki so pravtako lahko vir grožnje človekovi varnosti (denimo industrijska ali celo ekonomska špijonaža). V takih primerih uporabnik obdrži vse pravice intelektualne lastnine, kar pa ne pomeni, da Google (in drugi) do vsebine nimajo dostopa.

Ko uporabnik naloži, predloži, shrani, pošlje ali prejme vsebino v Google storitev ali prek njih, podjetju Google (in ostalim, s katerimi sodelujejo) podeli dovoljenje za uporabo, gostitev, hranjenje, razmnoževanje, spreminjanje, oblikovanje izvedenih del (kot nastanejo pri prevodu, prilagoditvah ali drugih spremembah, ki jih izvedemo, da je vaša vsebina skladnejša s storitvami), sporočanje, objavo, javno izvajanje, javno predvajanje in distribucijo takšne vsebine po vsem svetu. Uporabnik ima torej avtorske, Google pa distribucijske pravice. Takšne pravice, ki jih podelite, tako Google, so sicer le za omejen namen delovanja, promoviranja in izboljšanja storitev in za razvoj novih storitev. To dovoljenje velja, tudi ko uporabnik preneha uporabljati Google storitve (Google 2014).

3.3 Načini ogrožanja človekove varnosti

Obstaja več načinov, kako je lahko takšna koncentracija podatkov pri enem ponudniku, grožnja človekovi varnosti:

1. Google lahko podatke preda tretji osebi (na pimer državnim organom)
2. Hekerji lahko takšne podatke ilegalno odtujijo od Googla
3. Vohljači lahko prestregajo komunikacijske poti Google uporabnikov (ne primer prebiranje uporabnikove e-pošte)
4. Googlove storitve lahko v nekem trenutku prenehajo obstajati (gospodarska odvisnost od Google storitev)

3.3.1 Posredovanje uporabnikovih podatkov tretjim osebam

Ali Google predaja podatke o svojih uporabnikih tretjim osebam? Da. Temu pravijo, da dajo podatke v skupno rabo. Bi vi dali vašo davčno številko v skupno rabo s Kenijskimi »oglaševalci«? Takšni postopki milo rečeno ogrožajo človekovo varnost, če seveda ni poskrbljeno za ustrezno informacijsko varnost. Znana pa je premisa informacijske varnosti, da je edini sistem, ki je zares varen, lahko samo off-line in neaktiven (torej izklopljen iz omrežja in ugasnjen). Osebne podatke si Google torej izmenjuje z drugimi družbami, organizacijami in posamezniki zunaj Googla, pod določenimi pogoji seveda:

1) S soglasjem uporabnika

Tukaj za izmenjavo občutljivih osebnih podatkov zahtevajo izrecno soglasje. Za ponazoritev spornosti takšne politike, kolikokrat ste že kliknili »strinjam se« brez da bi prebrali, s čemer se strinjate? Spletno soglasje je torej nekaj, kar uporabniki jemljemo za bolj ali manj privzeto ravnanje. Le pomislite na spletne piškotke – kolikokrat ste se že strinjali s takimi obvestili na slovenskem spletu od implementacije novega pravilnika o spletnih piškotih iz leta 2013? Večinokrat.

2) S skrbniki domene

Če Google Račun v imenu uporabnika upravlja skrbnik domene (na primer pri uporabnikih Google Apps), bodo dostop do podatkov Google Računa (vključno z e-poštnim naslovom in drugimi podatki) imeli skrbnik domene in prodajni posredniki, ki zagotavljajo uporabniško podporo uporabnikovi organizaciji.

Skrbnik domene lahko:

- pregleduje statistiko o uporabnikovem računu, na primer statistiko o aplikacijah, ki jih namesti;
- spremeni geslo računa;
- začasno onemogoči ali ukine dostop do računa;
- dostopa do informacij, shranjenih v okviru računa, ali jih obdrži;
- prejema podatke računa, da izpolni zahteve upoštevne zakonodaje, predpisov, pravnih postopkov ali izvršljive zahteve upravnih organov;

- omeji uporabnikovo možnost brisanja ali urejanja podatkov ali nastavitve zasebnosti.

3) Za zunanjo obdelavo

Osebne podatke lahko Google da na na voljo svojim podružnicam ali drugim zaupanja vrednim podjetjem ali posameznikom, da jih v njihovem imenu obdelajo po Googlovih navodilih ter skladno z Google pravilnikom o zasebnosti in vsemi drugimi ustreznimi ukrepi za zagotavljanje zaupnosti in varnosti.

4) Zaradi zakonskih razlogov

Osebne podatke si Google izmenjuje z drugimi družbami, organizacijami ali posamezniki zunaj Googla, če v dobri veri verjame, da so dostop do takih podatkov, njihova uporaba, hranjenje ali razkritje razumno potrebni za:

- skladnost z morebitno upoštevno zakonodajo, predpisi, zakonskimi postopki ali izvršljivo zahtevo državnih organov;
- izvajanje veljavnih pogojev storitve, vključno s preiskovanjem njihovih morebitnih kršitev;
- odkrivanje, preprečevanje ali drugačno obravnavanje goljufij in varnostnih ali tehničnih težav;
- zaščito pred kršitvijo pravic ali varnosti Googla, njegovih uporabnikov ali javnosti ter pred škodo na njihovi lastnini, kot zahteva ali dovoljuje zakonodaja.

Tako imenovane združene podatke, ki ne omogočajo osebne prepoznave, lahko da Google v javno skupno rabo in jih razkrije partnerjem, kot so izdajatelji, oglaševalci ali povezana spletna mesta. Podatke lahko na primer javno objavijo, da prikažejo gibanja na področju splošne uporabe storitev.

V svojih splošnih pogojih so še zapisali, da če bo Google vključen v združitev, pripojitev ali prodajo premoženja, bo še naprej zagotavljal zaupnost vseh osebnih podatkov in prizadete uporabnike obvestil, preden se bodo osebni podatki prenesli ali bo začel zanje veljati drug pravilnik o zasebnosti. Zopet email uporabnikom, ki bo skoraj zagotovo v večini primerov spregledan (Google 2014).

Veliko je torej indicov, ki nakazujejo, da je uporabnik na spletu pravzaprav prepuščen sam sebi, podobno kot je voznik vozila sam kriv za lastno (ne)poznavanje cestno-prometne zakonodaje.

Preiskovalni urad Združenih držav (Federal Bureau of Investigation - FBI) lahko izda pismo o nacionalni varnosti, ki ga ni možno uporabiti v navadnih kazenskih, civilnih ali upravnih zadevah torej ko on ali drugi organi izvršilne veje oblasti Združenih držav izvajajo preiskave, povezane z nacionalno varnostjo. Po zakonu ECPA (18 U.S.C., razdelek 2709) lahko FBI zahteva »ime, naslov, trajanje storitve ter arhive obračunavanja lokalnih in drugih klicev« za naročnike žičnih ali elektronskih komunikacijskih storitev. Poleg omenjenih podatkov FBI ne more prdobiti nobenih drugih, kot na primer vsebina sporočila, iskalnih poizvedb, videoposnetkov v YouTubu ali uporabniških naslovov IP (Google 2014).

Za izdajo pisma o nacionalni varnosti mora direktor FBI-ja ali posebej imenovana vodilna oseba v FBI-ju pisno dokazati, da so zahtevani podatki »pomembni za dovoljeno preiskavo za zaščito pred mednarodnim terorizmom ali skrivnimi obveščevalnimi dejavnostmi«, za kar pa ni potrebna sodna odobritev. Tukaj je velika potencialna varnostna luknja oziroma tveganje človekovi varnosti, saj lahko FBI na ta način manipulira s (pre)veliko količino osebnih in drugih podatkov in sporočil Google uporabnikov.

Drug način omogoča Foreign Intelligence Surveillance Act (FISA), zakon Združenih držav iz leta 1978, ki ureja, kako državni organi Združenih držav zbirajo obveščevalne podatke o tujih osebah za namene državne varnosti. V ta namen je bilo ustanovljeno sodišče za nadzor komunikacije tujih oseb (Foreign Intelligence Surveillance Court oz. FISC), ki ga sestavlja 11 sodnikov zveznih okrožnih sodišč in lahko od podjetij in drugih zasebnih organizacij zahteva, da jim izročijo podatke v preiskavah tujih oseb.

Organe, vključene pri izvajanju dejavnosti, ki jih dovoljuje zakon FISA, sicer nadzoruje pravosodno ministrstvo Združenih držav. FISA tudi določa, da morajo ti organi redno poročati Kongresu in mu predstaviti vse povezane dokumente sodišča FISA.

Težava je v tem, da lahko državni organi na podlagi zakona FISA zaprosijo za odločbe sodišča FISA, ki med drugim od podjetij v Združenih državah zahtevajo izročitev osebnih podatkov in vsebine njihovih komunikacij. Zakon o dopolnilih zakona FISA iz leta 2008 daje državnim

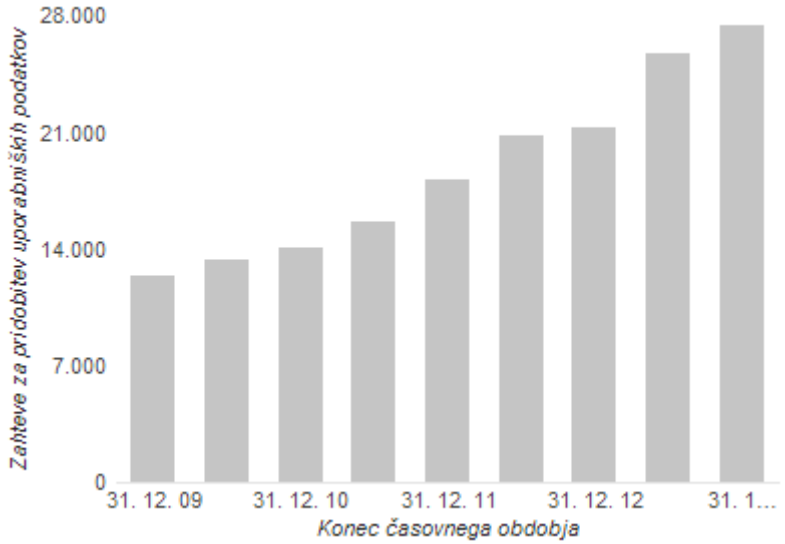
organom možnost, da od podjetij v Združenih državah zahtevajo podatke in vsebino komunikacij, povezane z računi oseb, ki niso državljani Združenih držav, ali oseb z nezakonitim stalnim bivališčem, ki so zunaj Združenih držav (FAS 2013).

Google torej redno prejema zahteve vlad in sodišč ne samo od ZDA, temveč z vsega sveta za razkritje uporabniških podatkov. Vse kaže, da je Google na strani uporabnikov in se trudi svetu obelodaniti, kako in v kakšnem obsegu nanj pritiskajo vladne in druge organizacije, po razkritju podatkov o njihovih uporabnikih. V ta namen je Google izdelal tudi t. i. Transparency report (preglednost informacij). V tem poročilu Google razkriva število zahtev, ki jih od vsake vlade prejme v šestmesečnih obdobjih. Uporaba Googlovih storitev se z vsakim letom povečuje, prav tako pa se povečuje število zahtev za uporabniške podatke.

Z obdobjem poročanja julij–december 2010 so začeli razkrivati odstotke zahtev za uporabniške podatke, ki so jim v celoti ali delno ugodili, z obdobjem poročanja januar–junij 2011 pa število uporabnikov ali računov, za katere so bili zahtevani podatki (Google 2014).

Iz grafa 3.4 je razvidno, da se je število zahtev vlad in sodišč z vsega sveta za razkritje uporabniških podatkov od leta 2009 do 2013 več kot podvojilo.

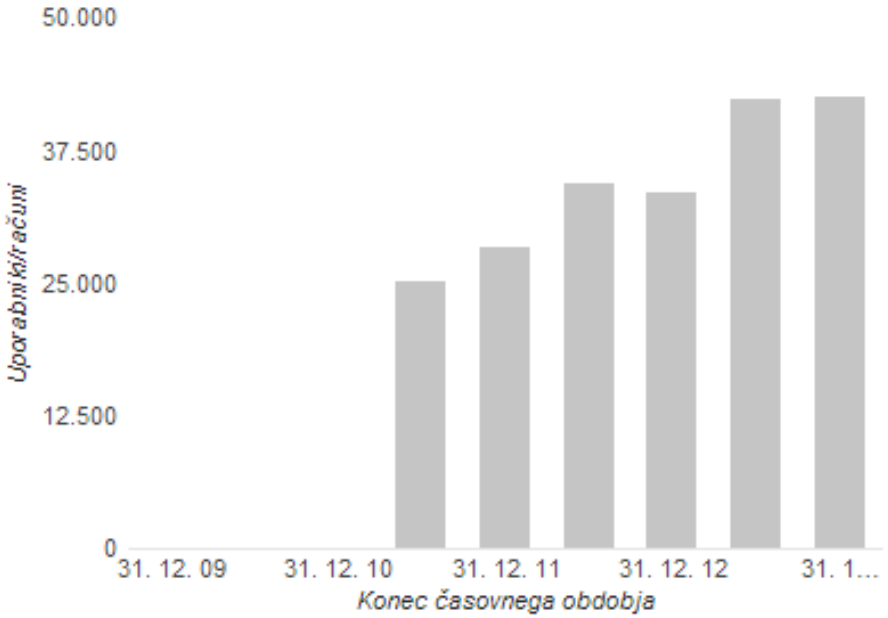
Graf 3.4: Število zahtev za pridobitev uporabniških podatkov



Vir: Google (2014).

V grafu 3.5 vidimo, da se rast števila zahtev odraža tudi v rasti števila uporabnikov, na katere se zahteve nanašajo. Podatke o uporabnikih/računih, navedenih v zahtevah za podatke, je Google začel zagotavljati šele z obdobjem januar–junij 2011, zato neposredna primerjava ni mogoča.

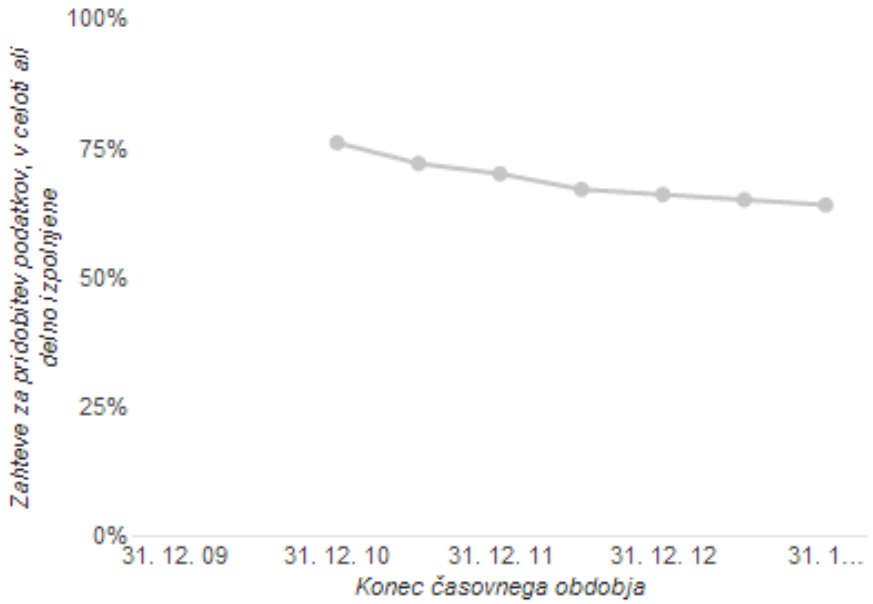
Graf 3.5: Zahteve za pridobitev uporabniških podatkov, po uporabnikih



Vir: Google (2014).

Če je Google leta 2010 ugodil kar 76 % vseh zahtev, se trend premika uporabnikom ali človekovi varnosti v prid, saj so 31.12.2013 delež ugodno rešenih zahtev spustili na 65 %, kar je razvidno iz grafa 3.6.

Graf 3.6: Odstotek zahtev, na podlagi katerih je Google poslal nekaj podatkov



Vir: Google (2014).

V tabeli 3.4 so zbrani statistični podatki, ki prikazujejo število zahtev organa kazenskega pregona za podatke, ki jih prejmeta Google in YouTube, odstotek zahtev, na podlagi katerih v celoti ali delno ukrepajo, ter število uporabnikov ali računov v zahtevah. »Vsako zahtevo pregledamo, da se prepričamo, da je skladna tako s črko kot z duhom zakona. V nekaterih primerih podatkov ne pošljemo ali zahtevamo, da se obseg zahteve omeji.« pravijo pri Googlu (Google 2014). Podatki se nanašajo na obdobje junij – december 2013.

Iz tabele 3.4 je razvidno, da je država z daleč največ zahtevki za pridobitev uporabniških podatkov ZDA (10574), sledita pa ji Francija (2750) in Nemčija (2660). Slovenija je v tem obdobju uradno zaprosila le enkrat in se s tem uvršča čisto na konec tabele 3.4. Ko gledamo odstotek ugodno rešenih zahtev, ko je Google uporabniške podatke predal, so top 3 države Finska (92 %), ZDA (83 %) in Malta (83 %). Odstotek v Sloveniji je 0 %, saj edini zahtevi ni bilo ugodeno. Če pogledamo še število navedenih uporabnikov, na katere se zahtevki nanašajo, so v vrhu zopet ZDA (18254), Indija (4401) ter Francija (3378). EU torej ne zaostaja tako zelo, kot bi si morda lahko mislili.

Skupno je Google v tem obdobju prejel 27477 zahtevkov, ki so se nanašali na 42648 uporabniških računov, od česar je bilo ugodno rešenih povprečno 64 % zhtevkov. Čeprav 64 % delež ugodno rešenih zahtevkov nakazuje na možnosti ogrožanja človekove varnosti, je

skupno število izpostavljenih uporabnikov oziroma njih računi (42624) relativno nizko, torej o neki resni aktualni ogroženmosti, ki bi imela globalne posledice, ne moremo govoriti.

Tabela 3.4: Zahteve za pridobitev uporabniških podatkov, jul-dec 2013

Država	Zahteve za pridobitev uporabniških podatkov	Odstotek ugodno rešenih zahtev	Navedeni uporabniki/računi
Argentina	123	51%	264
Avstralija	780	70%	944
Avstrija	23	26%	114
Belgija	162	73%	206
Bolgarija	1	0%	3
Brazilija	1.085	49%	1.471
Češka	74	39%	88
Čile	141	45%	199
Danska	58	62%	65
Ekvador	3	0%	4
Estonija	2	50%	4
Finska	13	92%	48
Francija	2.750	51%	3.378
Grčija	13	15%	29
Gruzija	2	0%	4
Hongkong	347	37%	356
Hrvaška	3	0%	6
Indija	2.513	66%	4.401
Irska	15	27%	51
Italija	896	42%	1.084
Izrael	43	65%	68
Japonska	111	60%	134
Južna Koreja	353	31%	619
Južnoafriška republika	2	0%	2
Kanada	52	25%	75
Kenija	8	63%	11
Kitajska	1	0%	5
Kolumbija	14	0%	17
Kostarika	1	0%	1
Libanon	3	0%	4
Lihtenštajn	1	0%	1
Litva	11	64%	18
Macao	3	0%	5
Madžarska	42	0%	42
Malezija	2	0%	2
Malta	54	83%	60
Mauritius	1	0%	1
Mehika	81	64%	120

Nemčija	2.660	40%	3.255
Nigerija	2	0%	2
Nizozemska	53	75%	63
Norveška	37	73%	51
Nova Zelandija	14	57%	17
Pakistan	3	0%	3
Peru	2	0%	4
Poljska	502	23%	740
Portugalska	283	45%	347
Romunija	16	56%	33
Rusija	90	3%	202
Singapur	755	68%	847
Slonokoščena obala	2	0%	2
Slovaška	34	15%	37
Slovenija	1	0%	1
Španija	545	53%	761
Švedska	18	28%	19
Švica	111	67%	174
Tajska	14	0%	19
Tajvan	439	61%	580
Trinidad in Tobago	1	0%	5
Turčija	133	1%	182
Ukrajina	1	0%	1
Vatikan	1	0%	1
Velika Britanija	1.397	69%	3.142
Združene države Amerike	10.574	83%	18.254
Združeni arabski emirati	2	0%	2
Skupaj	**27.477**	**64%**	**42.648**

Vir: Google (2014).

3.3.2 Kako varen je Google uporabniški računi?

Poleg predajanja informacij tretjim osebam, je večja nevarnost nasilni odvzem takšnih informacij, o čemer sem pisal v poglavju o informacijski varnosti. Za pojasnila, glede varnosti uporabniških računov sem se poleg analize pravil in pogojev poslovanja Googla obrnil tudi na njihovo PR službo. Google sicer ne odgovarja na vprašanja niti novinarjem niti kakšnim drugim organizacijam, tako da sem imel veliko sreče ob pridobitvi spodnjih odgovorov. Gabriela Chiorean je prepričana, da naredi Google vse, kar je sploh možno, da bi bili Google uporabniški računi varni.

Kot je to danes trend tudi pri drugih večjih ponudnikih, kot so Apple, Microsoft, Facebook in drugi, so uporabniški računi pri Googlu unificirani na način, da ima vsak uporabnik le en

račun, to je Google račun. Tako je mogoče, da se lahko z enakim uporabniškim imenom in geslom uporabniki prijavljajo denimo tako v YouTube in Gmail.

Med metode, s katerimi Google ohranja nivo varnosti, spdajo:

- Šifriranje SSL za celotno sejo je privzeta, kadar je uporabnik prijavljen v Gmail, Drive, Search in mnoge druge storitve. Takšna enkripcija drugim prepreči vohunjenje, kadar je uporabnik v odprtem omrežju, kot denimo, uporaba prenosnika v kavarni.
- Šifrirana je prav tako vsa podatkovna komunikacija med Googlovimi podatkovnimi strežniki.
- 2-stopenjska verifikacija nudi močnejšo varnost pri prijavi v storitve. Četudi uporabniku ukradejo geslo, to ni dovolj za dostop do uporabniškega računa. V praksi to deluje tako, da po prijavi iz neznanega računalnika Google zahteva dodatno geslo, ki ga uporabniku pošlje preko brezplačnega SMS sporočila, na vnaprej določeno mobilno številko.
- Google vsakodnevno zaščiti preko milijardo uporabnikov s svojimi »Safe Browsing« opozorili, kar tudi javno poroča koaliciji Stop Badware (www.stopbadware.org).
- Google javno objavlja podatkovne poizvedbe državnih organov v svojem Transparency reportu, o katerem sem že pisal. Vsak tak zahtevek je tudi preučen s strani Googlovih pravnikov.
- Google ne daje vladnim organom dostopa do lastnega podatkovnega sistema ali dovoljenja za nameščanje kakršnekoli opreme, ki bi takšne podatke ali dostop lahko pridobila.
- Uporabnik se lahko odjavi od prejemanja personaliziranih oglasov, torej se odjavi od »sledenja obnašanja«.
- Google uporabnike opozarja, če meni, da se z njihovim računom dogaja kaj čudnega, denimo da je uporabnik prvič prijavljen v oddaljeni državi ali takoj zatem zopet v drugi. Če Google meni, da je račun nekega uporabnika ogrožen, zahteva, da uporabnik spremeni geslo.
- Google zaposljuje preko 400 varnostnih strokovnjakov s polnim delovnim časom, ki skrbijo za zadnje varnostne tehnološke posodobitve in svetovanje.

- Google dnevno identificira preko 7500 nevarnih spletnih strani in prikaže opozorila preko 6 milijonom iskalnim zatekom in preko milijonu spletnim prenosom.
- Google je s pomočjo tehnologij, kot je kompleksna analiza tveganj za sumljive prijave v sistem od leta 2011, ko so beležili največ vdorov v račune, uspel zmanjšati grožnje odvzemu uporabniških računov za 99,7 %.
- Googlov napredni spam filter blokira, preko dnevne analize več milijard e-poštnih sporočil, več kot 99 % nezaželene pošte, da ta sploh ne pride v uporabnikovo mapo Prejeto (Chiorean 2014).

Kako se kaže Googlova varnost uporabniških računov v praksi? Ne tako zelo dobro. Da Google račun ni nedotakljiv, so namreč dokazali mnogi varnostni vdori v preteklosti. V letu 2010 so Googlu tako izmaknili sistem za gesla, ki je ključnega pomena za vse Google uporabniške račune in storitve. V tem napadu sicer niso bila odtujena gesla Google računov pa tudi Google je ranljivosti takoj odpravil, napad je le pokazal, da Googleov podatkovni sistem ni 100 % varen (Markof 2014). V 2011 je Matthijs R. za potrebe ekperimenta zbral osebne podatke kar 35 milijonov Google+uporabnikov, preko njihovih javnih profilov. Podatki so vključevali imena, gesla in biografske podatke uporabnikov (Goodin 2011). Leta 2013 so hekerji izmaknili preko 70.000 Gmail, Google+ in YouTube računov preko tehnologije beleženja tipkanja ali t. i. keyloggerja. V istem letu je bilo na enak način izmaknjenih še 54437 gesel Google računov (Pagliery 2013).

Vsi podatki in vse informacije, ki jih upravlja Google, so hranjeni v eni sami ogromni podatkovni tabeli (BigTable), kar je varnostno zelo tvegana odločitev, kot denimo, kadar imamo preveč kartic v eni denarnici – ko jo izgubiš, izgubiš vse. Ta tabela sicer ni javno dostopna nikomur, se pa lahko nanjo povezujejo uporabniki preko Google App storitev (Wikipedia 2014). Vsak podatek se celo shrani trikrat na treh ločenih lokacijah. Hekerjem je tako poenostalvjena pot do podatkov – vseh podatkov, ki na svetu obstajajo, bi lahko celo rekli. Ali drugače, ko hekerju uspe vdreti v podatkovni sistem, mu je na voljo vse, saj podatki niso razparcelirani na particije podatkov (Cleland 2010).

Našteti primeri kažejo na to, da Google račun ni varen in da je človekova varnost potencialno ogrožena.

3.3.3 Varnost e-poštne komunikacije

Mnogi ponudniki e-pošte sporočil med prenosom ne šifrirajo, kar za Google ne velja. Vsa e-pošta poslana preko Gmail, Google Apps in Google+ storitev je šifrirana, težava pa nastane, ko je Google samo eden od udeleženih ponudnikov. Ko prek katerega od teh ponudnikov uporabnik pošlje ali prejme e-poštno sporočilo, ga lahko vohljači (programska ali strojna oprema za prestrezanje prometa na omrežju, lahko tudi zlonamerna) preprosto preberejo (Slovar informatike 2014).

Šifriranje med prenosom pomaga e-pošto zaščititi pred vohunjenjem na poti med vami in tistimi, ki jim jo pošljete. Vsakodnevno se več milijard e-poštnih sporočil pošlje nešifriranih. Takšna sporočila predstavljajo odlično tarčo za prisluškovanje in množično prestrezanje, ko potujejo med desetinami optičnih vlaken in usmerjevalnikov in so potemtakom vir grožnje človekovi varnosti (Google 2014). Zavedati pa se moramo tudi dejstva, da niti šifriranje ni 100 % zagotovilo varnosti poslane in prejete e-pošte.

Vse večje število ponudnikov e-pošte si prizadeva to spremeniti s šifriranjem sporočil, poslanih iz Googlovih storitev ali prejetih vanje, z uporabo protokola TLS (Transport Layer Security). Če je e-poštno sporočilo med prenosom šifrirano s TLS-jem, drugi težje preberejo, kar uporabnik pošilja. Zavedati pa se moramo, da TLS ne šifrira e-pošte, ko ta ne potuje, torej, ko je shranjena v strežniku. Obstajajo pa drugačni prijemi, denimo tehnologija PGP, ki zagotovi stanje, ko je poslana pošta na voljo le prejemniku. V primeru PGD šifriranja Gmail ne more šifrirati vsebine sporočila za poznejše iskanje, ker je ne vidi, kar omogoča sloj varnosti, ki ga šifriranje med prenosom ne ponuja.

Kljub temu pa šifriranje med prenosom dodaja PGP-ju precejšnjo prednost z vidika zasebnosti. PGP šifrira samo vsebino e-pošte, ne pa tudi glav (npr. podatkov, kdo je pošiljatelj in kdo prejemnik e-pošte). Vohun, ki prestreže dostavo e-poštnega sporočila, šifriranega s PGP-jem, bo lahko videl naslove, na katere je bilo dostavljeno, ne pa vsebine sporočila. Če je sporočilo, šifrirano s PGP-jem, med prenosom šifrirano tudi s TLS-jem, pošiljatelj in prejemnik ne bosta vidna vohunu.

Podatki v grafih 3.7 in 3.8 kažejo, da se odstotek šifrirane e-pošte preko storitve Gmail povečuje. V povprečju je danes šifriranih 74 % odhodnih in 56 % dohodnih e-poštnih sporočil (Google 2014).

Graf 3.7: Odstotek odhodne šifrirane e-pošte storitve Gmail

Vir: Google (2014).

Graf 3.8: Odstotek dohodne šifrirane e-pošte storitve Gmail

Vir: Google (2014).

Googlovi samodejni sistemi analizirajo uporabnikovo vsebino (vključno z e-pošto), z namenom zagotavljanja ustreznih in prilagojenih funkcij storitev, kot so prilagojeni rezultati iskanja, prilagojeno oglaševanje ter odkrivanje neželene komunikacije in zlonamerne programske opreme. Takšno analiziranje se izvede, ko se vsebina pošilja, prejema in shranjuje (Google 2014).

3.3.4 Omejevanje dostopa do Google storitev

Raziskava IDC-ja nakazuje, da kar 65 % vseh srednje velikih in malih podjetij z manj kot 1000 zaposlenimi svoje podatke hrani v oblačnih storitvah, kot je denimo Google Drive, zato lahko rečemo, da je potencialno ogroženih 65 % srednje velikih in malih podjetij (industrijska špionaža). Odstotek za ZDA je višji, kar 93 % (Tsoriev 2014).

Kar 80 % podjetij ocenjuje, da jih čas izpada ali čas v katerem dogovorjena storitev ni na razpolago (Slover informatike 2014), vsaj 20 tisoč USD na uro ali več, preko 20 % pa jih

ocenjuje, da vsaj 100 tisoč USD na uro. Če bi torej hkrati brez dostopa do svojih oblačnih storitev ostalo 65 % podjetij na svetu, bi bila to gospodarska katastrofa globalnih razsežnosti, kar bi nedvoumno negativno vplivalo na človekovo varnost (Acronis 2014).

Ko govorimo o času izpada, je Google zelo natančen pri omejevanju lastne odgovornosti. Ne Google ne njegovi dobavitelji ali distributerji ne dajejo nobenih posebnih obljub glede storitev. »Ne dajemo na primer nobenega jamstva glede vsebine v storitvah in posameznih funkcij, ki so na voljo v storitvah, ter glede njihove zanesljivosti, razpoložljivosti ali primernosti za vaše potrebe. Storitve zagotavljamo take, kot so« (Google 2014).

Kadar to dovoljuje zakonodaja, Google ni odgovoren za »izgubo dobička, prihodkov ali podatkov, finančne izgube ali posredno, posebno, posledično, eksemplarično ali kaznovalno odškodnino« (Google 2014).

»Do mere, ki jo dovoljuje zakonodaja, je skupna odgovornost Googla, njegovih dobaviteljev in distributerjev za kakršne koli zahtevke na podlagi teh pogojev, vključno z implicitnimi jamstvi, omejena na znesek, ki ste ga plačali za uporabo storitev (ali, po naši izbiri, vnovično izvedbo storitev)« (Google 2014).

Google, njegovi dobavitelji in distributerji torej v nobenem primeru niso odgovorni za morebitno izgubo ali škodo, ki je »ni možno razumno predvideti« (Google 2014).

Iz zgornjih odsekov iz splošnih pogojev poslovanja Googla vidomo, da Google precej splošno definira za kaj vse ni odgovoren in v kakšnih pogojih lahko do takšne neodgovornosti pride, zelo jasno pa pove, da denarnih nadomestil (finančna odgovornost časa izpada) ne izdaja. Takšna praksa seveda velja tudi za podjetja, ki uporabljajo Google storitve, kar tudi posebej definirajo.

> *Google in njegova lastniško povezana podjetja, uradnike, posrednike in uslužbence odvezuje odgovornosti in bo poravnalo vso škodo v zvezi s kakršnim koli tožbenim zahtevkom, tožbo ali ukrepom, ki izhaja iz uporabe storitev ali je povezan z njimi ali s kršitvijo teh pogojev, vključno z vsakršno odgovornostjo ali stroški, ki bi izhajali iz kakršnih koli zahtevkov, izgub, škode, tožb, sodb, sodnih postopkov in odvetniških stroškov«* (Google 2014).

Google za vsak izdelek zabeleži število prejetih zahtev v danem časovnem obdobju, skupaj s približnim geografskim območjem zahteve. Če pride do znatnega upada prometa za izdelek ali storitev z določenega geografskega območja, to lahko pomeni, da uporabniki ne morejo dostopati do izdelka ali storitve. Googlovi algoritmi spremljajo vzorce prometa po vsem svetu skozi čas in zaznajo večje spremembe. Google prejema tudi poizvedbe novinarjev, aktivistov in ljudi na terenu s pozivi, naj preverimo grafe. Google javno objavlja nedostopnost do lastnih storitev po svetu v okviru svojega programa Preglednost informacij. Uporabnikom je bil dostop do določenih Googlovih izdelkov in storitev na neki točki omejen v več kot 30 državah po svetu, za kar gre iskati razloge pri izpadih omrežij in zaporah, ki jih zahtevajo državni organi.

Iz tabele 3.5 je razvidno, da je v času tipkanja te diplomske naloge brez dostopa do pomembnih Google storitev le Kitajska in sicer 59 zaporednih dni, do 31.7.2014. Kitajska je tudi sicer znana po zapiranju na področju spleta, torej po neodobravanju tujih ponudnikov in/ali cenzuri. Iz podatkov gre sklepati, da v preteklosti ni bilo večjih razlogov za skrb, torej nedostopnost Google storitev ni v pretirani meri vplivalo na človekovo varnost.

Tabela 3.5: Trajanja nedostopnosti Google storitev, merjeno 30. 7. 2014

Država	Trajanje nedostopnosti	Trajanje nedostopnosti v dneh	Nedostopne storitve
Irak	13. junij 2014 – danes	47	YouTube
Kitajska	31. maj 2014 – danes	59	Vsi izdelki
Kitajska	11. oktober 2009–danes	1752	Google spletna mesta
Kitajska	16. julij 2009–danes	1839	Spletni albumi Picasa
Kitajska	23. marec 2009–danes	1955	YouTube
Iran	07. april 2014–danes	114	Google spletna mesta
Iran	13. junij 2009–danes	1873	YouTube
Pakistan	17. september 2012–danes	681	YouTube
Turčija	24. junij 2009–danes	1862	Google spletna mesta

Vir: Google (2014).

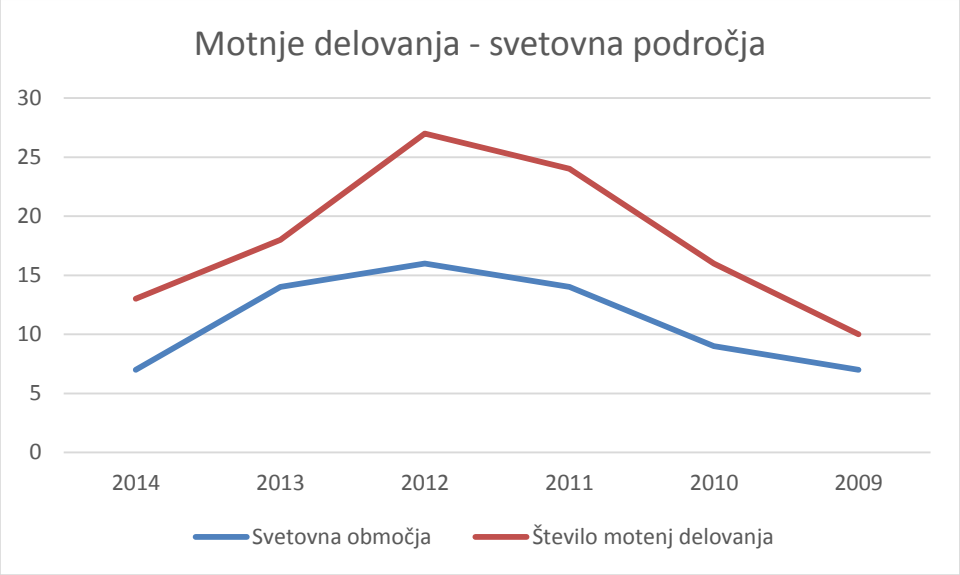
V tabeli 3.6 in grafu 3.9 vidimo trend števila motenj delovanja in svetovna območja, ki so prizadeta. Trend gre v smer manjšanja tako števila prizadetih območij, kot tudi absolutnega števila motenj delovanja. Ne gre torej opaziti indicev, da bi to lahko vlivalo na človekovo varnost v preteklosti, pa tudi trend za prihodnost temu pritrjuje.

Tabela 3.6: Trajanja nedostopnosti Google storitev po letih

	2014	2013	2012	2011	2010	2009
Svetovna območja	7	14	16	14	9	7
Število motenj delovanja	13	18	27	24	16	10

Vir: Google (2014).

Graf 3.9: Trajanja nedostopnosti Google storitev po letih



Vir: Google (2014).

Tudi, če je na nekem geografskem območju moten dostop do določene storitve, to še ne pomeni, da je dostop onemogočen vsem s tega področja.Glede na vzrok motnje lahko Google prepreči dostop do določene storitve veliki večini ljudi na nekem območju, kot je v primeru nedostopnosti sotitve YouTube na Kitajskem, ali omeji dostop samo določenim segmentom prebivalstva, kot je bilo v primeru nedostopnosti vseh Google storitev v Keniji februarja 2012.

3.4 Googlova samoregulacija

Kot je opisano v registraciji za program varnega pristana (International Trade Administration 2014), Google upošteva dogovor med EU in Združenimi državami o varnem ravnanju z osebnimi podatki ter podobni dogovor med Združenimi državami in Švico v različicah, ki ju je objavilo ameriško ministrstvo za trgovino, glede zbiranja, uporabe in hranjenja osebnih podatkov iz držav članic Evropske unije in iz Švice. Google je torej potrdil, da ravna skladno z ustreznimi načeli zasebnosti v okviru programa varnega pristana.

Google je prav tako član pobude Network Advertising Initiative (NAI), v kateri sodelujejo podjetja, ki se zavzemajo za odgovorna pravila oglaševanja v internetu. Z orodjem, razvitim v okviru pobude NAI, lahko uporabnik izve več o oglaševalskih podjetjih in izbere, da ne želi sodelovati v njihovi uporabi piškotkov na spletnem mestu NAI (Google 2014).

Google upošteva tudi načela dobre prakse Internetnega oglaševalskega urada Združenega kraljestva v zvezi s spletnim vedenjskim oglaševanjem , avstralskih smernicah najboljše prakse v zvezi s spletnim vedenjskim oglaševanjem in načela evropskega urada IAB za evropski okvir spletnega vedenjskega oglaševanja (Google 2014).

Sklep

Ali Google torej globalno gledano potencialno ogroža človekovo varnost? Da. Je Google največja grožnja človekovi varnosti na svetu? Težko bi trdil.

V diplomskem delu zaključujem, da se je varnostna paradigma premaknila od države, kot referenčnega objekta varnosti, na posameznika, čemur sledijo pravzaprav vse večje varnostne organizacije in prizadevanja po svetu (EU, NATO). V ospredje so prišle nekatere doslej spregledane kulturno-civilizacijske razsežnosti varnosti, zato današnje razprave posvečajo večjo pozornost drugačnim prvinam sodobne varnostne problematike, kot so degradacija okolja, podnebne spremembe, odvisnost od tehnologij (npr. Spletnih storitev podjetja Google Inc.), lakoti, neenakomernemu ekonomskemu razvoju, nalezljivim boleznim torej ne le zgolj vprašanje fizičnega obstoja posameznikov, temveč njegovi blaginji.

Globalizacija je prinesla tehnološko revolucijo, ki s svojim informacijskim potencialom grozi človekovi varnosti. Vsi vse iščemo, delamo, hranimo in se o tem pogovarjamo na spletu, vsa naša interakcija s tehnologijami pa potuje in se hrani po bolj ali manj varnih kanalih. Podjetja svoje podatke hranijo v oblaku. Uporabnikom ponudniki sledijo na vsakem koraku z namenom višanja dobičkov. Uporabniki razdajamo ogromne količine osebnih in drugih podatkov, poleg vsega pa ne znamo v zadostni meri poskrbeti za lastno varnost oziroma varnost svoje podatkovne zbirke.

Objekt varnosti je torej postal posameznik ali natančneje, objekt človekove varnosti je postal tudi uporabnik. Kdorkoli želi karkoli narediti, potrebuje informacije, ki so lahko pridobljene na legalen, nesporen način ali na ilegalen, uporabnikom sporen način, ki torej ogroža njegovo, človekovo varnost. Nekdo lahko v danem trenutku denimo izve točne lokacije večine prebivalstva določenega geografskega ozemlja ali poslovne izide konkurence, česar si ni prav težko predstavljati kot vir grožnje človekovi varnosti. Svetovna nedostopnost Google storitev bi denimo po svetu lahko sprožila nemire. Zelo pomembno za zagotavljanje človekove varnosti je torej informacijska varnost. Bistvo informacijske varnosti je namreč dejstvo, da se ščitijo podatki oziroma informacije pred nepooblaščenim dostopom.

Monopol na področju človekovih informacijskih podatkov, kot ga izvaja Google pri svojem poslovanju, je človekovi varnosti nevaren pojav in splošno sprejeto prepričanje danes je, da

je posledica zmanjšanja ali izgube človekove varnosti, zmanjšanje stabilnosti znotraj in zunaj državnih meja, kar pa ima neposreden učinek na mir. Google je na svetovnem spletu namreč pozicioniran kot največji upravitelj najširše podatkovne zbirke uporabniških podatkov, tudi osebnih. Ne največji v smislu absolutnega števila uporabniških računov, v čemer ga prekaša vsaj Facebook, ampak največjega v smislu količine podatkov, ki jih hrani o posameznem uporabniku. Nihče na svetu namreč ne poseduje tako raznovrstnega spektra storitev, ki bi bile povezane v en uporabniški račun (Google račun), spravljen v eni podatkovni tabeli (big table), kot je to uspelo podjetju Google Inc. v svoji 16-letni zgodovini, ko je prevzelo 160 drugih podjetij in jih inkorporiralo v svoje storitve in izdelke. Nihče tudi tako odkrito ne postavlja hitrosti višje na prioritetni lestvici od varnosti. Pomislimo le na Gmail, preko čigar si uporabniki vsako sekundo izmenjajo preko 2,3 milijona e-poštnih sporočil (osebni podatki, vsebina e-pošte in podatki o prejemniku), mobilni operacijski sistem Android, ki te dni beleži preko milijarde aktivnih uporabnikov (lokacija in zgodovina lokacij) in Google iskalnik, preko čigar uporabniki vsako sekundo pošljejo 44 tisoč iskalnih poizvedb in je tako najbolj obiskana spletna stran na svetu (vsebina in zgodovina poizvedb).

Google za vse svoje storitve uporablja poenoten Google uporabniški račun (Google account), na katerega so vezani vsi podatki o uporabniku in njegovem obnašanju. Taki podatki vključujejo uporabnikove osebne podatke, podatke o plačilnih sredstvih, zgodovino uporabe Google storitev, njegovo fizično lokacijo z zgodovino premikov, vsebino e-poštne druge e-komunikacije in druge občutljive podatke, ki jih Google hrani na svojih strežnikih. Aktivnih Google uporabniških računov je bilo konec leta 2013, 540 milijonov, neaktivnih pa dosti več. Družabno omrežje Google+ v juniju 2014 beleži 343 milijonov aktivnih uporabnikov, skupaj pa je Google+ računov že preko 1,15 milijarde. Če vzamemo največja števila, t. j. skupno število Google računov, podatke o trenutnem številu Zemljanov in uporabnikov interneta izračunamo, da je potencialno ogrožena človekova varnost 15,9 % svetovnih prebivalcev (1.150.000.000/7.251.737.604) in kar 39,3 % vseh spletnih uporabnikov na svetu (1.150.000.000/2925249355). Ne morem torej trditi, da je to največja podatkovna zbirka uporabnikov na svetu, saj je aktivnih uporabnikov samo Facebooka preko 11.280.000.000, zato tudi težko trdim, da je Google največja grožnja človekovi varnosti v smislu števila potencialno ogroženih uporabniških računov, lahko pa trdim, da so ti uporabniški računi

opremljeni z največ podatki o njih, narava podatkov pa je resnejša (osebna in poslovna komunikacija, hranjeni podatki, lokacijski podatki, in tako naprej).

Kako lahko torej Google ogroža človekovo varnost?

1) Podatke o svojih uporabnikih lahko (in jih) predaja tretjim osebam, in sicer s soglasjem uporabnika; s skrbniki domene; za zunanjo obdelavo ter zaradi zakonskih razlogov (organi pregona). V tej luči je nepomemben zakon države, v kateri biva uporabnik, saj se upošteva zakon države, kjer je registrirano podjetje Google Inc., t. j. Kalifornija, ZDA. Uporabnik je prepuščen sam sebi, podobno kot je voznik vozila sam kriv za lastno (ne)poznavanje cestno-prometne zakonodaje.

FBI lahko po zakonu ECPA v imenu varovanja nacionalne varnosti izda pismo o nacionalni varnosti, s katerim zahteva od Googla vpogled v uporabniške podatke (ime, naslov, trajanje storitve ter arhive obračunavanja lokalnih in drugih klicev). Drug način omogoča Foreign Intelligence Surveillance Act (FISA), ki ureja, kako državni organi Združenih držav zbirajo obveščevalne podatke o tujih osebah za namene državne varnosti in lahko Googla zahteva, da jim izročijo podatke v preiskavah tujih oseb.

Google torej redno prejema zahteve vlad in sodišč ne samo od ZDA, temveč z vsega sveta za razkritje uporabniških podatkov. Število zahtev vlad in sodišč z vsega sveta za razkritje uporabniških podatkov od leta 2009 do 2013 več kot podvojilo. Ker se rast števila zahtev odraža tudi v rasti števila uporabnikov, na katere se zahteve nanašajo, se je tudi to podvojilo. Če je Google leta 2010 ugodil kar 76 % vseh zahtev, pa se trend premika uporabnikom ali človekovi varnosti v prid, saj so 31.12.2013 delež ugodno rešenih zahtev spustili na 65 %. Skupno je Google v merjenem obdobju prejel 27477 zahtevkov, ki so se nanašali na 42648 uporabniških računov, od česar je bilo ugodno rešenih povprečno 64 % zahtevkov. Čeprav 64 % delež ugodno rešenih zahtevkov nakazuje na možnosti ogrožanja človekove varnosti je skupno število izpostavljenih uporabnikov oziroma njih računi (42624) relativno nizko, torej o neki resni ogroženosti, ki bi imela lahko globalne posledice, v tej luči ne moremo govoriti.

2) Podatki so lahko zlonamerno prestreženi s strani tretje osebe, brez uporabnikovega ali celo Googlovega strinjanja. Kot je to danes trend tudi pri drugih večjih ponudnikih, kot sta Apple in Microsoft, so uporabniški računi pri Googlu unificirani na način, da ima vsak

uporabnik le en račun, to je Google račun. Tako je mogoče, da se lahko z enakim uporabniškim imenom in geslom uporabniki prijavljajo denimo tako v YouTube in Gmail.

Med metode, s katerimi Google zagotavlja varnost svojih uporabniških računov in posledično uporabnikom, spadajo šifriranje SSL, 2-stopenjska verifikacija ter možnost odjave uporabnika od sledenja obnašanja. Po drugi strani Google zaposluje preko 400 varnostnih strokovnjakov s polnim delovnim časom, ki skrbijo za zadnje varnostne tehnološke posodobitve in svetovanje, opozarja uporabnike ko meni, da se z njihovim računom dogaja kaj čudnega, s pomočjo kompleksne analize tveganj za sumljive prijave v sistem, pa so od leta 2011, ko so beležili največ vdorov v račune, uspeli zmanjšati grožnje odvzemu uporabniških računov za 99,7 %.

Varnost Googlovih računov se sprva kaže, da je na zadovoljivem nivoju, zaskrbljujoče pa je dejstvo, da je na koncu za varnost lastnih podatkov hitro lahko kriv posameznik sam in to, da daje Google totalno prednost pred varnostjo, hitrosti svojih storitev. Poznamo številne primere odtujitve Google uporabniških podatkov. V letu 2010 so Googlu tako izmaknili sistem za gesla, ki je ključnega pomena za vse Google uporabniške račune in storitve. V tem napadu sicer niso bila odtujena gesla Google računov pa tudi Google je ranljivosti takoj odpravil, napad je le pokazal, da Googleov podatkovni sistem ni 100 % varen. V 2011 je Matthijs R. za potrebe eksperimenta denimo zbral osebne podatke kar 35 milijonov Google+uporabnikov, preko njihovih javnih profilov, podatki pa so vključevali imena, gesla in biografske podatke uporabnikov. Leta 2013 so hekerji izmaknili preko 70.000 Gmail, Google+ in YouTube računov preko tehnologije beleženja tipkanja ali t. i. keyloggerja. V istem letu je bilo na enak način izmaknjenih še 54437 gesel Google računov.

Po drugi strani so vsi podatki in vse informacija, katere upravlja Google, so hranjeni v eni sami ogromni podatkovni tabeli (BigTable), kar je varnostno zelo tvegana odločitev, kot denimo, kadar imamo preveč kartic v eni denarnici – ko jo izgubiš, izgubiš vse. Našteti primeri kažejo na to, da Google račun ni varen in da je človekova varnost posledično lahko potencialno ogrožena.

3) Vsebina in ostali podatki ob e-poštni komunikaciji so lahko prestreženi ali manipulirani. Šifriranje med prenosom sicer pomaga e-pošto zaščititi pred vohunjenjem na poti med vami in tistimi, ki jim jo pošljete. Vsakodnevno pa se več milijard e-poštnih sporočil pošlje

nešifriranih. Takšna sporočila predstavljajo odlično tarčo za prisluškovanje in množično prestrezanje, ko potujejo med desetinami optičnih vlaken in usmerjevalnikov in so potemtakem vir grožnje človekovi varnosti (Google 2014). Zavedati pa se moramo tudi dejstva, da niti šifriranje (TLS, PGD) ni 100 % zagotovilo varnosti poslane in prejete e-pošte. V povprečju je danes šifriranih 74 % odhodnih in 56 % dohodnih e-poštnih sporočil. Odstotek šifrirane e-pošte preko storitve Gmail se sicer povečuje, a vendar je to prevelik varnostni riziko in človekova varnost je lahko ogrožena.

4) Google storitve, vključno s hranjenimi podatki in e-poštno komunikacijo, lahko postanejo nedostopni. Raziskava IDC-ja nakazuje, da kar 65 % vseh srednje velikih in malih podjetij z manj kot 1000 zaposlenimi svoje podatke hrani v oblačnih storitvah, kot je denimo Google Drive. Če so take storitve v danem trenutku nedostopne je potencialno ogroženih 65 % srednje velikih in malih podjetij. Kar 80 % podjetij ocenjuje, da jih čas izpada ali čas v katerem dogovorjena storitev ni na razpolago, stane vsaj 20 tisoč USD na uro ali več, preko 20 % pa jih ocenjuje, da vsaj 100 tisoč USD na uro. Če bi torej hkrati brez dostopa do svojih oblačnih storitev ostalo 65 % podjetij na svetu, bi bila to gospodarska katastrofa globalnih razsežnosti, kar bi nedvoumno negativno vplivalo na človekovo varnost. Za nastalo Google seveda ne odgovarja.

V času tipkanja te diplomske naloge je brez dostopa do pomembnih storitev le Kitajska in sicer 59 zaporednih dni, do 31.7.2014. V preteklosti torej ni bilo večjih razlogov za skrb in nedostopnost Google storitev ni v pretirani meri vplivala na človekovo varnost pa tudi trend gre v smer manjšanja tako števila prizadetih območij, kot tudi absolutnega števila motenj delovanja.

Glede na zapisano ugotavljam, da je Google potencialno velika grožnja človekovi varnosti: zaradi ogromne količine podatkov, ki jih zbira o svojih uporabnikih v zgolj eni podatkovni tabeli, ki niso 100 % varni pred prestrezanjem ali manipulacijo in zaradi sprejetih zakonov, po katerih posluje Google Inc. v ZDA in njegove notranje politike poslovanja kar odpira možnost predaje podatkov o svojih uporabnikom tretjim osebam.

Literatura

1. Axel Arnbak, Joris Van Hoboken in Nico Van Eijk. 2012. *Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act*. Dostopno prek: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2181534 (27. julij 2014).
2. Axworthy, L. 1999. *Human security: Safety for People in a Changing World.* Ottawa: Canada. Department of Foreign Affairs and International Trade.
3. Bajpai, Kanti. 2000. *Human Security: Concept and Measurement.* Dostopno prek: http://www.hegoa.ehu.es/dossierra/seguridad/Human_security_concept_and_ measurement.pdf (27. julij 2014).
4. Bayils, John, Steve Smith in Patricia Owens, ur. 2008. *Globalizacija svetovne politike: mednarodni problemi*. Ljubljana: FDV.
5. Bilgin, Pinar. 2003. Individual and Societal Dimensions of Security. *International Studies Review* 5 (2): 203–222.
6. Booth, Ken. 2007. *Theory of World Security*. New York: Cambridge University Press.
7. Buzan, Barry. 2004. A reductionist, Idealistic Notion that Adds Little Analytical Value. *Security Dialougue* 35 (3): 369–70.
8. Buzan, Berry in Lene Hansen. 2009. *The Evolution Of International Security Studies*. New York: Cambridge University Press.
9. Chiorean, Gabriela. 2014. Intervju z avtorjem. Ljubljana, 22. julij.
10. *CJM - Center za reaziskavo javnega mnenja*. Dostopno prek: http://www.cjm.si/ ?q=SJM (23. maj 2014).
11. Claburn, Thomas. 2012. *Google Apps Clears Key Security Hurdle. Information week*. Dostopno prek: http://search.proquest.com.nukweb.nuk.uni-lj.si/docview/ 1021411684/fulltextPDF/876D33D759E44702PQ/1?accountid=16468 (27. julij 2014).
12. CVRIA. 2014. *InfoCuria: C-131/12 - Google Spain and Google*. Dostopno prek: http://curia.europa.eu/juris/liste.jsf?num=C-131/12 (14. julij 2014)
13. eBizMBA. 2014. *Top 15 Most Popular Social Networking Sites.* Dostopno prek: http://www.ebizmba.com/articles/social-networking-websites (27. julij 2014).
14. Electronic privacy information center. 2014. *USA Patriot Act.* Dostopno prek: http:// www.epic.org/privacy/terrorism/usapatriot/ (2. avgust 2014).

15. Europol. 2013. *EU Terrorism Situation and Trend Report*. Dostopno prek: https://www.europol.europa.eu/content/te-sat-2013-eu-terrorism-situation-and-trend-report (23. maj 2014).
16. FAS. 2013. *Reauthorization of the FISA Amendments Act*. Dostopno prek: http://fas.org/sgp/crs/intel/R42725.pdf (22. julij 2014).
17. Google. 2014a. *About Google*. Dostopno prek: http://www.google.com/about (15. julij 2014).
18. --- 2014b. *Google transparency report*. Dostopno prek: https://www.google.com/transparencyreport/ (22. julij 2014).
19. --- 2014c. *Google+*. Dostopno prek: http://en.wikipedia.org/wiki/Google%2B (5. avgust 2014).
20. --- 2014č. *Privacy Policy*. Dostopno prek: https://www.google.com/intl/en/policies/privacy/ (16. julij 2014).
21. Grizold, Anton in Bojko Bučar. 2011. Izzivi sodobne varnosti: Od nacionalne in Mednarodne do človekove varnosti. *Teorija in praksa* 48 (4): 827–851.
22. Hayden, Michael. 2003. *National information assurance glossary, Committee on national Security Systems*. Dostopno prek: https://www.ecs.csus.edu/csc/iac/cnssi_4009.pdf (27. avgust 2014).
23. Haywood, Trevor. 1997. *Info-bogataši – info-reveži: dostop in izmenjava v globalni informacijski družbi*. Maribor: Institut informacijskih znanosti.
24. IBM. 2014. *Dictionary of IBM & computing terminology.* Dostopno prek: http://www-03.ibm.com/ibm/history/documents/pdf/glossary.pdf (25. junij 2014).
25. International Trade Administration. 2014. *U.S.-EU SAFE HARBOR LIST*. Dostopno prek: http://safeharbor.export.gov/list.aspx (22. julij 2014).
26. *Internet live stats*. Dostopno prek: http://www.internetlivestats.com/ (15. julij 2014).
27. ITU. 2014. *ICT facts and figures*. Dostopno prek: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf (27. julij 2014).
28. Kahn, Jordan. 2014. *Numbers from Google I/O: Over 1 billion 30 day active users, 62% of overall tablet market*. Dostopno prek: http://9to5google.com/2014/06/25/numbers-from-google-io-over-1-billion-30-day-active-users-62-of-overall-tablet-market/ (5. avgust 2014).

29. King, Rachel. 2014. *Google I/O: Android stands at one billion active users and counting*. Dostopno prek: http://www.zdnet.com/google-io-android-stands-at-one-billion-active-users-and-counting-7000030881/ (5. avgust 2014).
30. Lemut-Strle, Rosana. 2014. Intervju z avtorjem. Ljubljana, 14. julij.
31. Marrouat, Cendrine. 2014. *Google+ now has 1.15 billion registered users!*. Dostopno prek: http://socialmediaslant.com/google-plus-traffic-stats-february-2014/ (6. avgust 2014).
32. McDaniel, George. 1994. *IBM Dictionary of computing*. New York: McGraw – Hill.
33. Meadows, Donella H.; Dennis I. Meadows; Jorgen Randers; William W. Behrens III. 1972. *The Limits to Growth: A Report for the Club of Rome's Project on the Predicament of Mankind*. New York: Universe Books.
34. *Network advertising initiative*. Dostopno prek: http://www.networkadvertising.org/ (22. julij 2014).
35. Newman, Edward. 2001. Human Security and Constructivism. *International Studies Perspectives* 2 (3): 239–251.
36. Olson, Michael. 2014. *Social Login Trends Across the Web for Q2 2014*. Dostopno prek: http://janrain.com/blog/social-login-trends-q2-2014/ (6. avgust 2014).
37. *OSCE: Organization for Security and Co-operation in Europe*. Dostopno prek: http://www.osce.org/ (23. maj 2014).
38. Pennington, Jesse. 2014. *The State of Websites in 2014: Stats & Facts You Need to Know*. Dostopno prek: http://www.kunocreative.com/blog/bid/88629/The-State-of-Websites-in-2014-Stats-Facts-You-Need-to-Know (6. avgust 2014).
39. Pirc-Musar, Nataša. 2013. *Letno poročilo Informacijskega pooblaščenca za leto 2013*. Dostopno prek: https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno_porocilo_2013_Web.pdf (6. avgust 2014).
40. Prezelj, Iztok. 2008. Človekova varnost v teoriji in praksi. *Delo in varnost* 53 (6): 17–26.
41. Računalniške novice. 2014. *Mobilni internet prvič presegel običajnega*. Dostopno prek: http://www.racunalniske-novice.com/novice/mobilna-telefonija/dogodki-in-obvestila/mobilni-internet-prvic-presegel-obicajnega.html (29. julij 2014).
42. *Slovar informatike*. Dostopno prek: http://www.islovar.org (25. junij 2014).

43. Spink, Amanda in Michael Zimmer. 2008. *Web Search: Multidisciplinary Perspectives*. London: Yale University Press.
44. Statista. 2014. *Leading social networks worldwide as of June 2014, ranked by number of active users*. Dostopno prek: http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (5. avgust 2014).
45. Svete, Uroš. 2005. *Varnost v informacijski družbi*. Ljubljana: Fakulteta za družbene vede.
46. The Commition on human security. 2014. *Commition on human security.* Dostopno prek: http://www.unocha.org/humansecurity/chs/ (13. junij 2014).
47. Thomas, Caroline, ur. 1999. *Globalization, Human Security and the African Experience*. Boulder, Colorado: Lynne Rienner.
48. Thomas, Nicholas in William T. Tow. 2002. The Utility of Human Security: Sovereignty and Humanitarian Intervention. *Security Dialogue* 33 (2): 177–192.
49. Tsoriev, Timur. 2014. *New Research Finds That 65% of Companies Are Using Cloud-Based Storage for Remote Location Disaster Recovery*. Dostopno prek: http:// www.acronis.com/en-us/pr/2014/07/09-14-35.html (30. julij 2014).
50. UNDP. 1994. *Human development report 1994*. Dostopno prek: http://hdr.undp.org/ sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf (12. junij 2014).
51. Vogrin, A. 2006. *Koncept človekove varnosti v mednarodnih odnosih*. Ljubljana: FDV.
52. We Are Social Singapore. 2014. *Social, Digital & Mobile Around The World (January 2014)*. Dostopno prek: http://www.slideshare.net/wearesocialsg/social-digital-mobile-around-the-world-january-2014 (6. avgust 2014).
53. Wheeler, Nicholas J. 2000. *Saving Strangers: Humanitarian Intervention in International Society*. Oxford: Oxford University Press.
54. Wikipedia. 2014a. *BigTable.* Dostopno prek: http://en.wikipedia.org/wiki/BigTable (15. julij 2014).
55. --- 2014b. *Edward Snowden*. Dostopno prek: http://en.wikipedia.org/wiki/Edward_ Snowden (14. julij 2014).
56. --- 2014c. *Informacijska doba*. Dostopno prek: http://sl.wikipedia.org/wiki/ Informacijska_doba (25. junij 2014).
57. --- 2014č. *Informacijska varnost*. Dostopno prek: http://sl.wikipedia.org/wiki/ Informacijska_varnost (25. junij 2014).

58. --- 2014d. *List of mergers and acquisitions by Google*. Dostopno prek: http://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Google (16. julij 2014).
59. --- 2014e. List of most popular websites. Dostopno prek: http://en.wikipedia.org/wiki/List_of_most_popular_websites (5. avgust 2014).
60. --- 2014f. *Patriot Act*. Dostopno prek: http://en.wikipedia.org/wiki/Patriot_Act (14. julij 2014).
61. World Commission on Environment and Development. 1987. *Our Common Future*. Oxford (USA): Oxford University Press.
62. Yarow, Jay. 2014. *GOOGLE: We Have 1 Billion Monthly Active Android Users*. Dostopno prek: http://www.businessinsider.com/google-we-have-1-billion-monthly-active-
android-users-2014-6 (5. avgust 2014).
63. *Your online choices*. Dostopno prek: http://www.youronlinechoices.com (22. 7. 2014).
64. Združeni narodi. Generalna skupščina. 2004. *A more Secure World: Our Shared Responsibility, Report of the High- level Panel on Threats, Challenges and Change*. Dostopno prek: http://www1.umn.edu/humanrts/instree/report.pdf (22. maj 2014).