UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Rok Derenčin

Trend razvoja informacijsko-komunikacijske tehnologije in varnostna tveganja

Diplomsko delo

Ljubljana, 2009

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Rok Derenčin

Mentor: doc. dr. Vladimir Prebilič
Somentor: asist. dr. Uroš Svete

Trend razvoja informacijsko-komunikacijske tehnologije in varnostna tveganja

Diplomsko delo

Ljubljana, 2009

Trend razvoja informacijsko-komunikacijske tehnologije in varnostna tveganja

V diplomskem delu proučujemo vprašanje varnosti in zasebnosti na informacijsko-komunikacijskem področju. Informacijsko-komunikacijska tehnologija se hitro razvija in glavni trend, ki temu sledi, je omogočiti posameznikom neoviran dostop do interneta ter uporabo raznih spletnih aplikacij. V gospodarstvu se vedno bolj uveljavlja razpršen sistem računalništva, ki temelji na odročnih podatkovnih centrih in organizacijam zagotavlja storitve, za katere so prej potrebovali lastne podatkovne centre. Organizacijam tako ni več treba imeti lastnih podatkovnih centrov, temveč lahko dostopajo do tako imenovane storitve oblaka, s katero lahko bolj učinkovito opravljajo svoje dejavnosti. Ta trend se vedno bolj uveljavlja tudi v komercialni rabi. Primer tega sta spletni storitvi Gmail in Google apps. V prihodnje bodo imeli posamezniki vedno manj podatkov in programov shranjenih na osebnem računalniku. Vedno več storitev se bo opravljalo v oblaku na internetu. S tem, ko posameznik podatkov ne bo več shranjeval pri sebi, ne bo mogel poskrbeti za ustrezno zaščito le-teh. Ker se bodo vsi podatki nahajali v oblaku, bo posameznik izpostavljen nenehni nevarnosti vdora v zasebnost ter drugim manipulacijam z lastnimi podatki. Cilj diplomskega dela je predvsem izpostaviti nekatere nevarnosti, ki se bodo pojavile kot posledica razvoja informacijsko-komunikacijske tehnologije.

Ključne besede: Informacijsko-komunikacijska tehnologija, zasebnost, informacijska varnost, razpršeno računalništvo, grožnje.

Future trend of information-communication technology and security risks

The thesis deals with the question of security and privacy in the field of information-communication technology. Information-communication technology is fast developing and the main trend it follows is, enabling an individual unimpeded access to the internet and the use of different on-line applications. In economy the use of cloud computing system is growing. It is based on remote data centers which assure different organizations the services that have previously demanded their own data centers. Now organizations no longer need their own data centers for they can access the so called cloud service which allows them to do their activities more effectively. The trend is also increasing in commercial use, examples of which are Gmail and Google apps. In the future fewer data and programs will be stored on personal computers as more and more services will be done in the cloud on the internet. With data not being stored on personal computers an individual will not be able to take appropriate measures of securing it in order to prevent unauthorized access. With all the data being stored in the cloud an individual will be constantly exposed to the danger of invasion of privacy and other manipulation of his data. The aim of this paper is above all to expose some of the dangers that will emerge as a consequence of information-communication technology development.

Key words: information-communication technology, privacy, information security, cloud computing, threats.

KAZALO

SEZNAM KRATIC

DoS	Denial of Service
EU	Evropska unija
HTML	Hypertext markup language
IKT	Informacijsko komunikacijska tehnologija (angl. Information communication technology)
IT	Informacijska tehnologija (angl. Information technology)
KMDC	Kompleks podatkovnih centrov
MDC	Modularni podatkovni center (angl. Modular data center)
TCP/IP	Transmission control protocol/Internet protocol
WAN	Wide area network
ZDA	Združene države Amerike

1 UVOD

V zadnjih dvajsetih letih je bil narejen velik napredek na področju informacijsko-komunikacijske tehnologije (IKT). Z razvojem interneta, HTML-ja (»Hypertext markup language«), ki je omogočil komercializacijo, in grafičnega uporabniškega vmesnika, se je internet razširil bistveno bolj, kot bi si lahko kateri od snovalcev predstavljal.

Z globalno povezanostjo računalnikov čas in lokacija nista več ovira za izmenjavo informacij, saj je posameznikom omogočeno, da lahko kadarkoli dostopajo do raznih informacij in storitev. IKT je danes tako vpleten v družbeno sfero, da je prešel iz koristnosti v odvisnost. Moderna družba skoraj ne more več delovati brez podpore IKT-ja. Ta odvisnost se kaže tako v informacijski infrastrukturi kot tudi v odvisnosti posameznikov od nadzora nad informacijami. Govorimo lahko o kritični informacijski infrastrukturi.

Z novimi dimenzijami, ki jih je prinesel razvoj informacijsko-komunikacijske tehnologije, so se pojavili tudi novi pogledi na varnost, ki so v zadnjih dveh desetletjih začeli vključevati tudi področje informacijske tehnologije. Vedno večji pomen imata tudi zasebnost uporabnikov in varovanje podatkov. Zaradi decentraliziranosti interneta, so tudi uporabniki in podatki, shranjeni na internetu, bolj varni. Z razvojem IKT-ja v smeri razpršenega računalništva pa se vračamo nazaj v centralizacijo internetnih storitev in s tem k manjši varnosti.

Pri razpršenem računalništvu uporabniki ne bodo več uporabljali računalnikov za shranjevanje in obdelavo podatkov, temveč bodo z njimi le dostopali do podatkov in storitev, ki se bodo nahajali v oblaku[1]. Posameznik bo na ta način izgubil določeno mero nadzora nad lastnimi podatki[2]. Pojavila se bodo nova tveganja in nove nevarnosti za posameznike, ki bodo izhajale iz sistema delovanja razpršenega računalništva.

V diplomskem delu bom najprej razdelal nekatere ključne pojme, ki so povezani z razpršenim računalništvom ter vprašanjem varnosti. Nato bom na kratko povzel dosedanji razvoj IKT-ja ter poskušal nakazati smer razvoja IKT-ja v prihodnje. V petem poglavju bom izpostavil nekatere pomanjkljivosti sistema razpršenega računalništva tako z vidika strojne opreme kot tudi z vidika uporabnika. Poseben poudarek bom namenil tudi vprašanju zasebnosti v primeru uporabe oblakov.

[1] Omrežni zbor strojne in programske opreme.
[2] Skozi celotno delo bom razlikoval med zasebnimi podatki, kamor spadajo vsi podatki, ki jih uporabnik shranjuje, ne glede na vrsto, ter osebnimi podatki, kot so na primer davčna številka, domači naslov in podobno.

2 METODOLOŠKI OKVIR

Delo bo v izhodišču temeljilo na deskriptivni in analitični metodi. Kot tako bo osredotočeno na določitev in opredelitev nekaterih pojmov in procesov v razvoju IKT-ja, napoved prihodnjih procesov ter umestitev teh teoretičnih procesov v prakso. Ob tem bo pomembna izpostavitev nekaterih problemov in tveganj, ki bi se ob tem (lahko) pojavili.

Diplomsko delo je osnovano na ideji, da se nakazuje razvoj IKT-ja, ki bo v prihodnje temeljil na rabi interneta oziroma konceptu razpršenega računalništva. Vse več komunikacijskih naprav bo temeljilo na internetni tehnologiji in standardih. Internet bo dobil spremenjeno vlogo v družbi, vse bolj se bo pojavljal kot storitev. Vedno manj bodo v rabi razni podatkovni nosilci, ki bi jih posamezniki imeli fizično pri sebi[3]. Vedno bolj se bo podatke in tudi programje shranjevalo na spletu, posameznik pa bo do njih dostopal preko različnih komunikacijskih naprav in aplikacij. Prenos in shranjevanje podatkov ne bosta več toliko povezana z nosilcem. Vedno bolj se vračamo nazaj v dobo terminalov. V središču bo posameznik, ki bo zaradi prihajajočega načina računalništva vse bolj izpostavljen možnostim kršitve zasebnosti.

Pri izdelava diplomskega dela bom uporabil naslednje metode družboslovnega raziskovanja:

- Zbiranje in analiza vsebine primarnih in sekundarnih virov. Tako kot pri vsakem raziskovalnem delu, je pomembna natančna opredelitev raziskovalnega področja. To bom dosegel s proučevanjem dejstev v relevantni literaturi. S tem bom postavil teoretično osnovo, iz katere bom nato izhajal pri nadaljnjem raziskovanju.
- Deskriptivna metoda. Z njo bom definiral in opisal ključne pojme in procese na teoretični ravni. Ob tem se bom z definicijami že poskušal približati področju proučevanja ter v ta namen izpostavil vidike, ki so za razumevanje dela bolj relevantni.
- Analitična metoda bo služila poskusu umestitve teoretičnih procesov v prakso ter predvidevanju nekaterih groženj varnosti, ki jih ti procesi predstavljajo posamezniku.

[3] Fizični podatkovni nosilci (USB ključi in podobno) se bodo še vedno prosto uporabljali, vendar pa je vseeno pričakovati zmanjšanje rabe le-teh.

2.1 Hipoteza in cilj

Diplomsko delo temelji na predpostavki, da se bo razpršeno računalništvo prej ali slej iz gospodarstva preneslo tudi v splošno rabo. Nekaterim prednostim, ki jih ponuja razpršeno računalništvo, se industrija ne bo mogla upreti. Težnja proizvajalcev strojne in programske opreme računalništva je bila, preko marketinga ter zaščite intelektualne lastnine, v končni fazi vedno zaslužek[4]. Razpršeno računalništvo omogoča nove načine za proizvajalce, da se izognejo težavam, ki jih prinaša piratstvo (slaba varnost zaradi vprašljivih kopij programov in podobno), saj omogoča večji nadzor uporabe strojne opreme, rabe programov ter pretoka informacij.

Ob uveljavljanju razpršenega računalništva bo računalništvo, kot ga poznamo danes, postopoma izginilo, kar bo imelo posledice tudi na varnostnem področju. V smislu zasebnosti bo največ izgubil posameznik (uporabnik), ki ne bo imel več tolikšnega nadzora nad lastnimi podatki, kot mu to do neke mere omogoča računalništvo danes.

Hipotezo sem zastavil na podlagi vsebine proučenih virov ter določitvijo nekaterih trendov v razvoju IKT-ja. Moja hipoteza je, da, *v kolikor se bo trend razvoja IKT-ja nadaljeval v isti smeri, bo razpršeno računalništvo nadomestilo današnji način računalništva, kar bo posamezniku onemogočalo ustrezno varovanje zasebnih podatkov ter nadzor nad osebnimi podatki. Posledično bo tretjim osebam omogočen lažji dostop do podatkov uporabnika, kar ga izpostavlja nekaterim tveganjem in nevarnostim.*

Cilj diplomskega dela je ugotoviti nadaljnji razvoj IKT-ja ter določiti nekatere možne posledice tega razvoja na področju varnosti oziroma izpostaviti nekatera varnostna vprašanja.

[4] Izjema so proizvajalci in ponudniki prostega in odprtokodnega programja.

3 TEMELJNI POJMI

3.1 Varnost

Obstaja paleta definicij varnosti, ki so jih podajali razni pisci. Nekatere od teh definicij podajajo popolnoma različne poglede na varnost, druge so komplementi že obstoječim definicijam ali pa v sebi združujejo različne vidike varnosti. Medtem ko se večina definicij varnosti nanaša na odsotnost oboroženega konflikta oziroma oborožene sile, so za področje diplomskega dela pomembnejše definicije, ki presegajo realistično[5] videnje mednarodnih odnosov in varnosti ter v definicije varnosti vključujejo tudi netradicionalne vidike ogrožanja ter subjekte.

Večjo pozornost namenimo razširjenemu varnostnemu konceptu, torej konceptu varnosti, ki je obravnavan s širšega družbenega konteksta. Premik je v prenosu z državocentričnega dojemanja varnosti na dojemanje, ki vključuje poleg države tudi nedržavne institucionalizirane in neistitucionalizirane družbene entitete po koncu hladne vojne. Pomembnejši referenčni subjekt je postal posameznik. V kontekstu varnosti so se vse bolj začeli pojavljati poleg materialnih vidikov tudi vrednotni (Svete 2005).

Razširitev pojma varnosti, kot je veljal v obdobju hladne vojne, na nove razsežnosti, je bila nujno potrebna. Za zagotavljanje varnosti je potreben celovit pristop, kar v praksi pomeni, da mora pojmovanje varnosti oziroma groženj varnosti odražati tudi spremenjene družbene razmere in odnose. Bolj natančno bi lahko rekli, da se mora pojmovanje varnosti razvijati hkrati z družbenim razvojem. V obdobju po hladni vojni, ko lahko vse več držav uvrščamo med informacijske države, ni presenetljivo, da se je pojmovanje varnosti razširilo tudi na področje informacijske tehnologije (Svete 2005, 32).

Pomembno je kompleksno obravnavanje varnosti, ob razumevanju, da posameznik, ki naj bi bil sposoben sam razvijati lastne potrebe ter interese te potrebe zadovoljiti, živi v skupnosti, ter da je njegova varnost odvisna od dejavnosti drugih posameznikov kot tudi države same (Buzan 1991, 37). Posameznik ima lastne interese glede zagotavljanja varnosti, vendar posameznik v razpršenem računalništvu teh interesov ne more uresničevati v polni meri.

[5] Realistična varnostna paradigma jemlje kot referenčni subjekt državo. Tako predvideva tudi grožnje s strani druge države. Vidike varnosti bom v diplomskem delu obravnaval bolj z vidika konstruktivizma, ki predvsem poudarja pomen norm, vrednot. Več o varnostnih paradigmah glej Svete 2005.

Grožnje, ki so povezane s konceptom razpršenega računalništva, so, kot jih poimenujeta Buzan in koebenhavenska šola[6], predvsem societalne. Med te grožnje spadajo ***grožnje pravicam,*** pravica do zasebnosti, varstvo osebnih podatkov ter druge svoboščine; ***ekonomske grožnje***, zavrnitev dostopa do dela in sredstev, zaseg lastnine in podobno; ***grožnje položaju***, ponižanje, onečaščenje; ***fizične grožnje***[7], bolečine, poškodbe, smrt (Buzan 1991, 37). Sama kompleksnost ogrožanja je izražena z medsebojno povezljivostjo posameznih groženj. Kršitve na enem področju vsebujejo tudi posledice na drugem. Zagotovo je potrebno societalnemu področju zagotavljanja varnosti v informacijski družbi nameniti več pozornosti.

Poleg samega pojava novih groženj varnosti je pomembna tudi zaznava groženj. Arnold Wolfers komentira, da »varnost v objektivnem smislu meri odsotnost groženj temeljnim vrednotam, v subjektivnem smislu pa pomeni odsotnost strahu, da bodo te vrednote ogrožene« (Wolfers v Buzan 1991, 17). Razkorak se pojavi pri odnosu med dejansko grožnjo ter zaznavo grožnje. Posamezniki so lahko ogroženi, torej obstaja objektivna grožnja varnosti. Vprašanje pa je, ali sami to grožnjo zaznajo in ali v primeru razpršenega računalništva sploh vedo, da nevarnost obstaja. Uporabnikom je pomembno, da lahko podatke nemoteno shranjujejo na spletu, kot na primer pri uporabi storitev Gmail, Google docs, Facebook, Myspace in drugih, da lahko do njih nemoteno dostopajo ter da uporabljajo razne spletne aplikacije. Uporabnikov pogosto ne zanima, kje se podatki dejansko nahajajo ter ali so zaščiteni pred dostopom tretjih oseb.

3.1.1 Človekova varnost

Najmanjša enota, na katero lahko apliciramo koncept varnosti, je človek. Koncept človekove varnosti izziva pojmovanje varnosti, kot jo razlagajo realisti, saj se osredotoča na posameznika. Kot tak je močno povezan z vrednotami in normami, kot obstajajo v mednarodnem sistemu (Svete 2005, 93).

---

[6] Buzan in koebenhavenska šola razširita tradicionalno pojmovanje varnosti, ki je osredotočena predvsem na vojaške razsežnosti ogrožanja varnosti, še na politično, gospodarsko, societalno (ali družbeno) in okoljsko. Predstavljata konstruktivistično videnje mednarodnih odnosov, predvsem v smislu razvoja koncepta societalne varnosti.

[7] Morda bi si težko predstavljali, da se grožnje, katerim je posameznik izpostavljen v informacijskem okolju, izrazijo tudi v fizičnem okolju. Treba pa je izpostaviti, da eskalacija konkretizacije groženj pravicam, ekonomskemu položaju ter družbenemu položaju, lahko privede do posledic, ki se na posameznika nanašajo neposredno v fizičnem okolju. Primer je samomor, za katerega se odloči posameznik po tem, ko je bil izpostavljen različnim pritiskom v digitalnem okolju: lažna identiteta sogovornika, prikrivanje ter izkrivljanje dejstev in podobno.

Proti koncu hladne vojne, je vedno bolj prevladovalo prepričanje, da je mir osnova družbenega razvoja. Prav tako se je vedno bolj pojavljalo tudi prepričanje, da so grožnje, ki pretijo posamezniku, bolj pomembne od tradicionalnih groženj miru (Ball in Nef v Vogrin in drugi 2008, 11).

»Človekova varnost je razumljena kot zagotavljanje svobode in varnosti posameznika ter skupnosti z oblikovanjem okolja, v katerem bodo zagotovljeni preživetje, temeljne človekove pravice in svoboščine ter zaščita vsakega posameznika, vključujoč tudi zaščito civilnega prebivalstva med oboroženimi konflikti (Svete 2005, 93).« Predstavlja pogoj bivanja posameznika, v katerem morajo biti posameznikove temeljne materialne potrebe zadovoljene. Prav tako mora biti posamezniku zagotovljeno dostojanstvo ter sodelovanje v življenjski skupnosti Thomas v Vogrin in drugi 2008, 13).

Izhajajoč iz vedenja, da ima izguba človekove varnosti učinke tudi na stabilnost države, kot tudi na odnose med državami, ostaja v interesu države, da sama zagotavlja človekovo varnost (Svete 2005, 94). Za zaščito posameznika je potrebno (so)delovanje držav, mednarodnih organizacij, nevladnih organizacij ter drugih nevladnih skupin (Bajpai v Vogrin in drugi 2008, 12). Vendar je država sama velik vir tako zagotavljanja varnosti, kot tudi groženj varnosti posameznika (Buzan 1991, 35).

Koncept človekove varnosti izvira v Poročilu o človekovem razvoju, ki ga je leta 1994 s sodelavci zastavil Mahbub ul Haq (Vogrin in drugi 2008, 11). Usmerjen je na ***ekonomsko področje***, dohodek, socialna pomoč; ***prehransko področje***, dostop do osnovne hrane; ***zdravstvena zaščita***, minimum zdravstvenega varstva; ***okoljska zaščita***, zaščita pred divjanjem narave in propadanjem okolja; ***osebna zaščita*** pred fizičnim nasiljem; ***zaščita skupnosti***, varovanje pred izgubo tradicije in vrednot, varovanje pred etničnim in sektaškim nasiljem; ***politična zaščita***, spoštovanje temeljnih človekovih pravic, zavarovanje pred nadzorom oblasti nad idejami in informacijami (Program združenih narodov za razvoj 1994, 24–33).

Človekova varnost ima dva vidika. Prvi vidik je preživetje in je povezan z varnostjo pred različnimi grožnjami[8]. Drugi vidik pa je trajnost, pomeni pa zaščito pred spremembami v vzorcih delovanja posameznika (Kaul in Kirdar v Vogrin in drugi 2008, 15).

[8] Lakota, bolezen, zatiranje in podobno.

Koncept človekove varnosti je usmerjen k ljudem. Pomeni pa tako osvobojenost od strahu, kot tudi osvobojenost od potreb. Glavne vrednote, ki jih izpostavlja pa so varnost (angl. Safety), dobrobit (angl. Well-being) ter dostojanstvo posameznika (Bajbai v Vogrin in drugi 2008, 14–5).

Na področju IKT-ja koncept človekove varnosti vključuje vse od nepooblaščenih vdorov do izobraževanja uporabnikov za izogibanje varnostnim kršitvam (Strebe in drugi 1998, 8). Za razpravo o varnostnih implikacijah je potrebna usmeritev na netradicionalno dojemanje varnosti ter ne-civilno družbo. »Politične, ekonomske in tehnološke spremembe, ki so omogočile globalizacijo, so omogočile delovanje tudi zlem silam, ki predstavljajo resen izziv demokraciji, razvoju in varnosti (Svete 2005, 96).« Glavna uporabna vrednost koncepta človekove varnosti je v njegovi sposobnosti emancipacije ter opozarjanje na grožnje, ki se pojavljajo v svetu. Poleg aktivnosti same države za zagotavljanje varnosti, je potrebna tudi lastna zaščita delovanja in pa širitev znanja ter zavedanja o tveganjih na področju IKT-ja (Svete 2005, 103–4).

3.2 Zasebnost

Ko govorimo o varnosti in IKT-ju, velja omeniti tudi vprašanje zasebnosti, ki je z varnostjo povezano. Pogosto se oba termina uporabljata skupaj, vendar ju je treba razlikovati. Varnost je nujen pogoj za zasebnost, vendar ne pomeni nujno tudi njene zagotovitve.

Landoll (2006, 33) pravi, da vsebujejo informacijski sistemi številne podatke, ki so občutljive narave tako za organizacije, kot tudi za posameznike. Zasebnost definira kot skrb, da bi bili podatki o posamezniku razkriti nepooblaščenim osebam. Skrb, da bi bili razkriti podatki o organizacijah, pa je označil kot »zaupnost«. Landoll kot glavno prvino kršenja zasebnosti označi nepooblaščeno osebo, ki so ji bili podatki razkriti. Kovačič pa izpostavi, da zlorabe opravljajo tako nepooblaščene kot tudi pooblaščene osebe (Kovačič 2006, 31). Medtem ko Landoll ne daje teže samim podatkom, Kovačič poudari tudi pravico posameznika, da sam odloča, kaj se z njegovimi podatki dogaja ter kdo lahko do njih dostopa. Nadaljuje, da je glavna lastnost zasebnosti možnost, da posameznik ravna na tak način, kot želi. Pravo podeljuje pravico do zasebnosti z namenom zadovoljevanja tega interesa (Pavčnik v Kovačič 2006, 37). Zasebnost izpostavi kot interes in ne kot pravico. Pojavi se vprašanje, kako ta interes zaščititi, oziroma ali se lahko določi nek minimalen standard zaščite zasebnosti. V

povezavi s t.i. informacijsko zasebnostjo, kjer je v ospredju izmenjava informacij (trgovanje z osebnimi podatki), lahko posplošimo, da pri pravici do zasebnosti ne gre za postavljanje absolutne meje, ki se je ne sme prestopiti, temveč (zgolj) za regulacijo poseganja v zasebnost (Kovačič 2006, 37, 75). V splošnem lahko zasebnost razumemo kot način določanja meje, do katere lahko družba posega v zadeve drugega (Trček 2006, 3). V ospredju je iskanje ravnotežja, tehtanje različnih interesov posameznika ter družbe kot celote (Kovačič 2006, 40). Družbeni interes lahko prevlada nad interesom posameznika in takrat je poseg v zasebnost legitimen. Vprašanje, ki ga je vredno postaviti je, do katere mere javni interes opravičuje poseganje v zasebnost. Kot argumentirata Agre in Rotenberg (2001, 149), je v mnogih državah prevladujoče prepričanje, da so sodišča in policija del problema kriminala. V takem primeru je vdor v zasebnost razumljen kot cena, ki jo je potrebno plačati zavoljo varnosti, posamezniki pa so jo tudi pripravljeni plačati. Zasebnost tako postane vprašanje ravnotežja namesto temeljne pravice.

Če govorimo o demokratičnem političnem sistemu, je v konceptu svobode varstvo podatkov pomemben in nepogrešljiv element (Etzioni v Kovačič. 2006, 40). Nekateri celo trdijo, da sodobna družba brez zasebnosti ne bi mogla obstajati (Trček 2006, 141). Bellottijeva ugotavlja, da je pravico do zasebnosti mogoče definirati normativno in operacionalno. Normativno pomeni, da so določeni vidiki posameznikovega delovanja in narave zasebni, se jih ne sme razkriti drugim. Ta definicija je zelo kontekstualno in družbeno pogojena[9]. Med različnimi kulturami prihaja do razlikovanja v razumevanju kaj velja za zasebno. Vlogo igra torej tudi subjektivna presoja vsakega posameznika, zaradi česar je težko postaviti univerzalne kriterije, kaj zasebnost je (Kovačič 2006, 41). Operacionalno se zasebnost nanaša na nadzor nad dostopom, torej zmožnost posameznika, da ima nadzor nad informacijami o sebi. Bistvenega pomena je, da posameznik lahko sam odloča, katere informacije se bodo izmenjevale z okolico in katere ne (Bellotti v Kovačič 2006, 40).

Judith Wagner DeCew pravi, da je zasebnost pomembna za samospoštovanje in občutek identitete, ter da zagotavlja zmožnost nadzora nad odločanjem (Wagner DeCew v Kovačič 2006, 41). »Naše vzdrževanje samospoštovanja zahteva zasebnost in nadzor nad določeno sfero naših življenj, informacije o nas so bistvenega pomena, če želimo biti neodvisna človeška bitja, sposobna rasti, izpolnjevanja, neodvisno od pritiskov, čustvenega stresa, predsodkov ali izgube samospoštovanja in drugih vplivov, ki spremljajo izgubo zasebnosti

[9] Tako je po terorističnem napadu 11. septembra 2001 poostren nadzor na letališčih postal sprejemljiv. V nekaterih državah smatrajo biometrične osebne izkaznice za vdor v zasebnost, spet drugje so lahko že v rabi.

(Ibid.).« Zasebnost omogoča posamezniku, da drugi ne dostopajo do njega, ter da tudi on sam ne posega v domeno drugega. Zaradi zasebnosti posameznik ni izoliran, temveč lahko stopa v stike z drugimi posamezniki avtonomno, kar ima tako družbeni kot tudi politični pomen. Posameznikom je s tem posredno omogočeno združevanje in politično delovanje (Wagner DeCew v Kovačič 2006, 42).

David Flaherty, svetovalec na področju zasebnosti, je pravico do zasebnosti povezal z: »pravico do samostojnega in neodvisnega delovanja, pravico biti puščen pri miru, pravico do zasebnega življenja, pravico nadzorovanja informacije o sebi, pravico omejiti dostopnost do sebe, pravico ekskluzivnega nadzora dostopa do zasebnega področja, pravico zmanjšati nadlegovanje na najmanjšo možno mero, pravico pričakovati zaupnost, pravico uživati osamljenost, pravico uživati intimnost, pravico uživati zadržanost ter pravico do tajnosti« (Cate v Kovačič 2006, 39).

Do razlikovanja v pojmovanju zasebnosti ne prihaja samo med različnimi avtorji. Pojmovanje zasebnosti se razlikuje tudi med Evropsko unijo (EU) in Združenimi državami Amerike (ZDA). EU zasebnosti, za razliko od ZDA, ne dojema kot nek interes temveč kot temeljno pravico. Natančno je bila navedena tudi v Temeljni listini človekovih pravic in svoboščin. Razumevanje zasebnosti ni samo z vidika obveznosti, temveč tudi z vidika pravic. V praksi to pomeni, da morajo biti zagotovljeni ustrezni pogoji, da posameznik koristi pravico do zasebnosti (Trček 2006, 141).

Širše lahko posplošimo, da pravica do zasebnosti omogoča posamezniku delovanje brez vmešavanja tretjih oseb ter mu predstavlja interes, katerega doseg mu mora biti omogočen.

4 RAZVOJ INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE

4.1 Informacijsko-komunikacijska tehnologija

Pri iskanju odgovora na vprašanje, kaj je IKT, pri pregledu literature naletimo na različne razlage. Pojavljata se dva sorodna pojma, in sicer informacijska tehnologija (IT) in IKT. Termina se v nemalo primerih uporabljata kot sinonima, kljub temu pa obstajajo določena razlikovanja.

Po slovarski definiciji je IT »znanost in tehnologija uporabe računalnikov in druge elektronske opreme za shranjevanje in pošiljanje informacij« (Cambridge advanced learner's dictionary v Trček 2006, 3). Druga definicija pravi, da je »informacijska tehnologija veja tehnologije, ki je usmerjena v študijo in aplikacijo podatkov ter njihovo obdelavo. Sem spada avtomatsko zajemanje podatkov, hramba, manipulacija (tudi transformacija), management, prenos, nadzor, prikaz, zamenjava, menjava, oddajanje in sprejemanje podatkov« (ATIS Committee v Trček 2006, 3). Na splošno se IT nanaša na rabo računalniške opreme, tako strojne kot programske, za upravljanje z informacijami. V večjih organizacijah so IT službe odgovorne za shranjevanje, zaščito, obdelavo, oddajanje in pridobivanje informacij (About.com 2009).

IKT je po mnenju Pinteriča (Pinterič in Grivec 2007, 17) »tista tehnologija, ki temelji na združevanju predhodnih tehnologij za prenos informacij ter omogočanje komunikacijskih procesov«. Svete (2005, 16) opredeli IKT kot »sposobnost, znanje, spretnost oz. tehniko, da predvsem z uporabo strojev in naprav, ki omogočajo informacijske dejavnosti, dosežemo želene rezultate«. Med informacijske dejavnosti lahko štejemo zbiranje, obdelavo in prikaz podatkov. Svete ob definiciji izpostavi tudi pomembnost komunikacijskega elementa, ki (še posebej) v zadnjem času dobiva na pomenu, saj se v IKT-ju čedalje večji poudarek daje na prenos podatkov (Eriksson v Svete 2005, 16).

V obeh primerih, tako pri IT-ju kot tudi IKT-ju, so gradniki isti. Gre za rabo računalniške strojne in programske opreme ter za manipulacijo podatkov. Izpostavljen je tudi element komuniciranja, vendar je pri opredeljevanju IKT-ja večji poudarek prav na prenosu podatkov, medtem ko je pri IT-ju večji poudarek na njihovi hrambi in obdelavi. Za potrebe diplomskega dela, bom IKT v odnosu do IT-ja obravnaval kot krovni pojem.

4.2 Zgodovina informacijsko-komunikacijske tehnologije

Jeremy G. Butler[10] (1998) je razvoj IKT-ja zgodovinsko razdelil na štiri obdobja. Kot glavni kriterij razvrščanja je označil tehnologijo za reševanje vprašanj »inputa« informacij, procesiranja, »outputa« ter komunikacijskih ovir. Štiri obdobja, ki jih je označil, so predmehanska doba, mehanska doba, elektromehanska doba in elektronska doba.

V ***predmehanski dobi***, ki je trajala od približno leta 3000 pred našim štetjem in do 1450 našega štetja, so nastale prve pisave in abecede. V tem obdobju je bil izumljen tudi papir in različna pisala. Pojavili so se prvi hranitelji informacij, knjige. Razvit je bil tudi številski sistem in prvi kalkulator, Abak.

V ***mehanski dobi***, ki je trajalo med leti 1450 in 1840, se je zgodila prva informacijska eksplozija. Obdobje se je začelo z iznajdbo tiska s premičnimi kovinskimi črkami[11] (Butler 1998). Pomembna iznajdba je bilo odkritje logaritmov in izdelava prvih računskih tablic, kar je naredil John Napier (Božić 2003). V tem času so bili izumljeni nonij[12], pascaline[13], Leibnizov stroj[14], Shichardov stroj[15]. Sledili so izumi Charlesa Babbagea, ki je naredil model diferenčnega stroja[16], analitični stroj[17], koncept programiranja z luknjanimi karticami[18] (Butler 1998). Kot prvega programerja lahko iz tega obdobja omenimo Avgusto Ado Byron. Njena ideja, da bi z uporabo Bernulijevega zaporedja lahko določila funkcije, ki bi jih stroj prepoznal in izvršil brez posredovanja človeka, je bila široko sprejeta kot prvi program (Redshaw 1996).

Sledila je ***elektromehanska doba*****,** in sicer od 1840 do 1940. Glavno odkritje tega obdobja je bilo odkritje načinov koriščenja električne energije. Obdobje predstavlja začetke

[10] Profesor za film, radio ter nove medijske smeri na Univerzi v Alabami in Univerzi v Arizoni.
[11] Iznašel ga je Johann Gutenberg.
[12] Raztegljivo merilo, kjer je ob glavnem merilu drseče pritrjeno stransko merilo. Izumil ga je William Oughtred okoli leta 1600. Predstavlja prvi primer analognega računalnika.
[13] Priprava za seštevanje odštevanje, deljenje in množenje. Izumil ga je Blaise Pascal leta 1642.
[14] Stroj, ki je omogočal seštevanje in množenje 5-12 mestnih števil. Izumil ga je Gottfried Wilhelm von Leibniz 1671 (Redshaw 1996).
[15] Prvi znani mehanični kalkulator za operacije seštevanja, odštevanja, množenja in deljenja. Izumil ga je Wilhelm Schickard leta 1623 (Nill 1999).
[16] Namen stroja je bil pregledno izpisati polinome. Stroja nikoli ni izdelal (Redshaw 1996).
[17] Namenjen je bil računanju poljubnih matematičnih operacij (Ibid.).
[18] Preko kartic, ki so bile luknjane, je bilo predvideno, da bi se lahko izvrševale določene računske operacije popolnoma avtomatsko. Kartice so določale, katere operacije naj se izvršijo, nad katerim številom, kaj se naj zgodi potem in kam naj gredo rezultati. Te kartice bi lahko danes opisali kot program. Koncept, ki ga je pobral Babbage, po tem ko ga je izpopolnil Joseph Marie Jacquard (Božić 2003).

telekomunikacije z iznajdbo voltne baterije[19], telegrafa[20], Morsejeve abecede, telefona[21] in radia[22](Butler 1998). Radio je bil prvi medij, v smislu prenosa informacij, ki je posameznikom omogočal, da je med poslušanjem lahko počel tudi kaj drugega, česar tiskani mediji niso omogočali (Pinterič in Grivec 2007, 17). Na področju elektromehanskega računalništva omenimo Hermana Holleritha, nemško-ameriškega statistika, ki je razvil mehanski tabulator[23], kasneje pa ustanovil podjetje IBM (»International Business Machines Corporation«) (Aul 1972). Leta 1942 je s pomočjo IBM-a Howard Aiken dokončal računalnik Mark I[24] (»Automatic Sequence Controlled Calculator«) (Butler 1998).

Elektronska doba se je začela 1940 in traja še danes. Elektromehanski računalniki so relativno hitro zatonili, predvsem zaradi počasnosti računanja ter nezanesljivosti delovanja zaradi velikega števila mehanskih elementov. Leta 1943 so v Angliji izdelali prvi popolnoma elektronski računalnik, pri katerem so uporabili vakuumske elektronke za izvajanje operacij in ne več mehanskih delov (Božić 2003). Eckert in Mauchly sta leta 1945 dokončala ENIAC[25] (»Electronic Numerical Integrator and Calculator«). Ta še ni imel možnosti shranjevanja podatkov, kar je dosegel Mark I iz Manchestra leta 1948. Leto kasneje je bil izdelan EDSAC (»Electronic Delay Storage Automatic Calculator«) in postal prvi računalnik z možnostjo shranjevanje programov v splošni rabi (Butler 1998).

Po končani drugi svetovni vojni sta hiter razvoj in napredek zajela tehnično in tehnološko področje, kar je imelo implikacije na področju IKT-ja. Kljub pojavu radia že pred drugo svetovno vojno, se je razmah dogodil po drugi svetovni vojni, in sicer z množično uporabo televizije. Prelomno je bilo leto 1956, ko so lahko Američani prvič gledali preko televizijskih zaslonov soočenje predsedniških kandidatov (Pinterič in Grivec 2007, 17).

[19] Baterija, poimenovana po njenem izumitelju, Alessandru Giuseppeju Antoniju Anastasiju Volti.
[20] Izumil Joseph Henry 1830, izpopolnil ga je Samuel Morse, tudi izumitelj Morsejeve abecede, leta 1858 (Bellis 2009).
[21] Graham Bell leta 1876.
[22] Guglielmo Marconi leta 1894.
[23] Električne povezave so sprožile števec, ki je beležil informacije. Kartice z luknjami so bile lahko preštete in razvrščene mehansko, podatki pa so bili posebej zabeleženi. Končno potrdilo o patentu je bilo izdano leta 1889.
[24] Deloval je na enak princip kot Babbagovi stroji in za pomnilnik uporabljal števna kolesa, le da je deloval elektromehansko. Ukazi so bili vneseni z luknjanim trakom, rezultate pa je izpisoval na tiskalnik ali na luknjane kartice (Jones 2005).
[25] Pojavila se je potreba po računalniku, ki bi računal bistveno hitreje od predhodnih elektromehanskih. Uporabljen je bil za računanje in tiskanje balističnih tabel (Božić 2003).

4.3 Internet

O osebnih računalnikih se v petdesetih letih prejšnjega tisočletja še ni govorilo. Takrat je bilo obdobje velikih osrednjih računalnikov, kamor so bili priključeni posamezni terminali za izmenjevanje podatkov. Pojavljati so se začeli tudi »mini« računalniki. Ti so bili velikosti povprečne garderobne omare. Na začetku računalništva je obdelava podatkov potekala v osrednjih računalnikih, shranjeni pa so bili na magnetnih trakovih pomnilniških naprav, ki so bile zunaj računalnikov. Prenos podatkov je potekal tako, da so magnetni trak (ali naluknjane kartice ali velikanske diskete) vzeli iz pomnilniške naprave ter fizično prenesli iz enega računalnika na drugega (Pahor 1996, 2).

Revolucijo v svetu IKT-ja je povzročil pojav interneta, ki so ga na začetku razvijali za potrebe obrambe. Nastajal je pod okriljem Agencije ameriškega obrambnega ministrstva za napredne raziskovalne projekte (DARPA - Defence Advanced Research Projects Agency) in pa Nase. Med leti 1963 in 1967 je DARPA raziskovala možnost računalniške povezave, prvo povezavo pa so naredili leta 1969[26] (Whittaker 2002, 16). Omrežna komunikacija (ARPANET) je na začetku potekala med štirimi računalniki (Pinterič in Grivec 2007, 18). Naslednje generacije povezav, naj bi že omogočale komunikacijo v primeru jedrskega napada, kar je bila glavna želja ameriške vlade od samega začetka, torej ustvariti komunikacijsko sredstvo, ki bi preživelo jedrski napad ter omogočalo komunikacijo tudi v primeru izpada enega ali več komunikacijskih kanalov (Honeycutt 1997, 13).

ARPANET je bilo omrežje enakovrednih računalnikov in kot tako ni imelo glavnega središča, ki bi usmerjal pretok podatkov. Usmerjanje podatkovnih paketov[27] je prevzel računalnik, skozi katerega so podatki potovali v tistem trenutku. Omrežje je delovalo bolje kot je bilo pričakovano. Oglasili so se tudi akademski krogi, ki so želeli namesto razvijanja svojega novega zaprtega omrežja uporabljati že obstoječi standard ARPANET. To jim je vojska tudi omogočila, ko je objavila vse potrebne tehnične podatke (Pahor 1996, 3).

Želja univerz je bila vzpostaviti omrežje, ki bi omogočalo uporabnikom z ene univerze komunikacijo z uporabniki druge univerze. Na začetku so ga uporabljali znanstveniki,

[26] Za začetno točko razvoja interneta lahko smatramo tudi izstrelitev Sputnika v vesolje leta 1957. Gre za prvi umetni satelit in začetek tekme za vesolje. Prav tako je poudaril pomen telekomunikacijskega sistema, v katerega bi se nato lahko internet priključil.

[27] Paket podatkov je osnovna enota za komunikacijo preko omrežja. Podatki se, preden se jih pošlje, razgradijo na manjše enote (pakete) ter se jih na končni lokaciji ponovno sestavi.

računalniški izvedenci, inženirji in knjižničarji. ARPANET se je izkazal kot idealna metoda izmenjave podatkov. Med leti 1970 in1980 so bile povezane že vse glavne univerze v ZDA. Prva medcelinska povezava se je zgodila 1973, in sicer z Londonskim univerzitetnim kolidžom (angl. University College of London). Izraz »internet« je prišel v veljavo in zamenjal izraz ARPANET leta 1974 (Vurušič in Vurušič 2006, 7–8). Postopoma je presegal meje in postajal vedno bolj globalno omrežje ter nepogrešljivo orodje za akademske raziskave na vseh področjih. Leta 1983 je prišlo do razcepa na vojaški (DARPANET) in civilni del (internet) (Pagon in drugi 1997, 18).

Kot posledica nesoglasij na obrambnem ministrstvu ZDA, predvsem kot posledica nesoglasij glede samega namena in uporabe interneta, so se začela pojavljati tudi druga omrežja, na primer BITNET (»Because It's Time«) in CSNET (»Computer Science Network«). Na začetku so delovala samostojno, kasneje pa so se začela medsebojno povezovati. Pomemben napredek je bil leta 1986, ko so v National Science Foundation z namenom izboljšave obstoječega omrežja naredili NSFnet, ki je medsebojno povezoval 5 superračunalnikov z različnih univerz, uporabnikom pa omogočal, da preko mreže dostopajo do podatkov. NSFnet je postal hrbtenica interneta, kar deloma ostaja tudi danes (Honeycutt 1997, 13).

Zaradi interesov ameriške zvezne vlade glede razvoja interneta, je ta dolgo ostal nekomercialen. Internet je hitro postajal vedno boj priljubljen. Dostop so postopoma začele ponujati tudi nekatere komercialne organizacije[28]. Do interneta so začeli dostopati tudi ljudje zunaj raziskovalnih dejavnosti (Jerman-Blažič 1996, 10).

V komercialno rabo je internet vstopil z razvojem grafičnega uporabniškega vmesnika ter nastankom HTML-ja. Ta internetni jezik[29] je omogočil globalno širjenje informacij (komercialnih vsebin). Oblikovan je bil internet, kot ga poznamo danes, to je svetovni splet (WWW[30] – World Wide Web) (Pinterič in Grivec 2007, 18). HTML je omogočal standardno povezan informacijski sistem, do katerega je bilo moč dostopati preko različnih operacijskih sistemov. K porasti uporabe interneta je pripomogel prvi internetni brskalnik, Mosaic, ki je bil razvit leta 1992. Razvili so ga pri NCSA (»National Center for Supercomputer Applications«) (Vurušič in Vurušič 2006, 8). Z razvojem Netscape Navigatorja, se je internet oblikoval v nov

[28] Na primer AT&T in British Telecom.
[29] Oblikoval ga je Tim Berns-Lee na CERN-u v Ženevi in ga predstavil leta 1991.
[30] Svetovni splet ni enako internet. Internet je omrežje omrežij, ki medsebojno povezuje različne računalnike. Informacije potujejo preko interneta z različnimi protokoli, na primer FTP (»File transfer protocol«). Splet predstavlja enega od načinov dostopanja do informacij preko interneta. Za to uporablja HTTP protokol (»Hypertext transfer protocol«) ter različne brskalnike. Splet predstavlja vsebino, medtem ko internet predstavlja transport (Webopedia 2008a).

množični medij. Leto kasneje, leta 1995, je Microsoft izdelal prvo verzijo Internet Explorerja. Tistega leta je bilo na svetu približno 26 milijonov uporabnikov, leto poprej pa le 3 milijone. V letu 2000 je bilo internetnih uporabnikov v svetu okoli 407 milijonov, število teh pa se vztrajno povečuje (Pinterič in Grivec 2007, 18). Od začetnih 4 medsebojno povezanih računalnikov pred štiridesetimi leti se je število medsebojno povezanih računalnikov povečalo na približno 1.596 milijonov[31]. Med leti 2000 in 2008 se je število uporabnikov interneta povečalo za 340%. Kljub velikemu številu uporabnikov je teh v primerjavi s svetovno populacijo 24% (Internet World Stats 2009). Razkorak med svetovno populacijo in uporabniki interneta nekateri pojmujejo kot digitalni razkorak[32].

Osnovo digitalne družbe predstavlja digitalizacija, ki »pomeni razčlenitev informacij v najenostavnejše dele (bite), pri čemer ni pomembno, ali gre za govor, pisavo, tonske zapise, slike, grafike ali video« (Svete 2005, 18). Način enake obravnave vseh informacij omogoča lažje in cenejše shranjevanje le-teh. Prav tako tudi prenose in razmnoževanje informacij. Za vse to zadostuje en medij in ne več različnih nosilcev, kot je bilo to potrebno v preteklosti[33]. »Na digitalni tehniki temelječa računalniška omrežja predstavljajo tako »super« medij, ki je sposoben združiti vse dosedanje informacijske in komunikacijske medije ter jih hkrati dopolniti s funkcionalnimi zmogljivostmi, ki še niso bile na razpolago (Ibid.).«

[31] Na dan 31. marec 2009.

[32] Pinterič povzame različne oblike digitalnega razkoraka. Prvi digitalni razkorak je med tistimi, ki imajo dostop do IKT-ja in med tistimi, ki tega dostopa nimajo. Dvojni digitalni razkorak izhaja iz predpostavke, da je prvo razlikovanje oblikovano na uporabnike in neuporabnike interneta. Dvojnost razlikovanja med neuporabniki interneta izpostavlja dva dejavnika, subjektivnega in objektivnega. Subjektivni dejavnik je neuporabljanje zaradi nezanimanja, objektivni dejavniki pa predstavljajo druge ovire za uporabo interneta. Drugi digitalni razkorak (nanašajoč se na IKT v celoti in ne nujno samo na internet) je med samimi uporabniki. Razkorak je med tistimi, ki tehnologijo uporabljajo že dalj časa, so je tudi bolj vešči, in tistimi, ki so »novi« uporabniki. Tretji digitalni razkorak je med uporabniki interneta, ki imajo dostop do širokopasovnega interneta in tistimi, ki take povezave nimajo. Ti so v primerjavi s tistimi, ki imajo širokopasovno povezavo, v določenih možnostih uporabe interneta hendikepirani (Dolničar in drugi v Pinterič in Grivec 2007, 28–9).

[33] Spomnimo se lahko različnih nosilcev, ki so bili v splošni uporabi. Če je posameznik želel prenesti neke podatke z enega računalnika na drugega, jih je spravil na disketo, če je želel poslušati glasbo, je imel kasetni predvajalnik ali predvajalnik zgoščenk. Danes pa so v splošni uporabi multifunkcionalne naprave, ki niso več omejene na en sam tip podatkov, kar je omogočila ravno digitalizacija informacij. Na primer MP3/MP4 predvajalniki, ki so v široki uporabi danes, se tako uporabljajo za poslušanje glasbe, gledanje video vsebin (MP4) ter prenos dokumentov ali drugih podatkov. Prav tako so v obtoku različni telefoni, ki so tudi multifunkcionalne. Primer je Applov iPhone mobilni telefon, ki bi ga morda lahko bolj ustrezno označili za žepni računalnik z možnostjo opravljanja telefonskih klicev in pošiljanja sporočil.

4.3.1 Internet in varnost

Z vse večjo splošno uporabo interneta je postajalo vedno bolj pomembno tudi vprašanje varnosti. Preden je internet postal prevladujoča tehnologija[34], se je odvijalo tekmovanje med različnimi tehnologijami in omrežji širokega dosega (angl. Wide area network – WAN). IBM je pripravil Sistemsko omrežno arhitekturo (angl. Systems network architecture – SNA), ki je predstavljala osnovo za BITNET WAN. Digital si je prizadeval za lastno »DIGITAL network architecture« (DNA), ki bi se lahko razvila v »DECNET networks«. Nowell je predstavil svoje protokole, Microsoft svoje in tako naprej. Vsi napori različnih podjetij so ustvarili nepovezane mreže. V končni fazi je 1. januarja 1983 prevladal protokol TCP/IP (»Transmission Control Protocol/Internet Protocol«) (Trček 2006, 7–8). Ta protokol predstavlja povezovalni člen med vsemi lokalnimi mrežami, kar je bil tudi eden izmed razlogov za veliko začetno širitev interneta (Tanenbaum 1996, 52).

Potek razvoja oziroma uveljavitev protokola TCP/IP[35] je imel učinke tudi na področju varnosti. Prvi začetki na področju varnosti pri internetu segajo v šestdeseta in sedemdeseta leta prejšnjega tisočletja. Prve aktivnosti so bile na področju kriptografskih algoritmov in vzpostavitve varnega operativnega sistema. V začetku devetdesetih let pa se je začelo poudarjati tudi druge metode zaščite in sisteme izgradnje varnosti. Z razvojem varnostne tehnologije se je predvidevalo, da bodo težave, povezane z informacijsko varnostjo odpravljene, kar se ni zgodilo (Trček 2006, 8).

Protokol TCP/IP je bil narejen kot poskus za mrežno izmenjavo paketov podatkov. V svoji osnovi ni predvideval identifikacije uporabnikov, varne izmenjave podatkov, uporabe spletnih računov ali nadzorovanja dostopa uporabnikov. Ker so bili mehanizmi varnosti za kodiranje, identifikacijo in nadzor dostopa izpuščeni iz same zasnove protokola, morajo zato biti vključeni v storitve, ki ta protokol uporabljajo (Strebe in drugi 1998, 414–5). Nekatere storitve uporabijo razne mehanizme, kot na primer NFS (»network file sharring«) in nekatere ne, kot je primer SMTP (»Simple mail transfer protocol«). Večina storitev sodi nekje vmes in zagotavljajo določeno mero zaščite, vendar ne dovolj, da bi odvrnila tudi bolj vztrajne napadalce (glej Strebe in drugi 1998, 415–21).

[34] Tehnologija je na tem mestu razumljena kot protokol na osnovi katerega deluje internet. Internet v današnjem pomenu temelji na TCP/IP protokolu.

[35] Trenutno je v rabi IP verzija 4 (IPv4), ki uporablja 32-bitne IP naslove. Ti naslovi so večinoma zapisani kot štiri decimalna števila med 0-255, na primer 175.21.3.14. Postopoma se že prestopa na IP verzijo 6 (IPv6), ki uporablja 128-bitne IP naslove in bo nudila večje število edinstvenih IP naslovov (Anderson 2008, 635).

4.4 Prihodnja smer razvoja

Da bi lahko pravilno predvideli, kakšen bo IKT v prihodnje, je potrebno poznati posamezne korake dosedanjega razvoja ter, podobno kot pri kompasu, ugotovit smer gibanja. Trende razvoja lahko razdelimo v dve skupini. Prvo skupino predstavljajo splošni trendi, ki veljajo v svetu. Med te trende spadajo Moorov zakon[36], globalizacija, digitalizacija, mobilnost, rast vrednotenja znanja ter splošno povečevanje koristnosti IKT-ja. Za drugo skupino trendov lahko rečemo, da predstavljajo specifične trende. Ti so povezani s specifičnimi zahtevami in vprašanji, ki se pojavljajo skupaj z razvojem. Sem spadajo vprašanja varnosti računalnikov na internetu, medsebojna komunikacija računalnikov, zagotavljanje spletnih storitev in podobno (Fraber Consulting 2002).

Richard MacManus, ustanovitelj ReadWriteWeb-a, je leta 2007 zajel 10 trendov, ki bodo po njegovem mnenju v ospredju razvoja IKT-ja v naslednjih desetih letih. Na prvem mestu je semantično omrežje. Govori pravzaprav o verziji interneta Web 3.0. v katerem bi računalniki lahko medsebojno komunicirali ter na tak način naredili mrežo bolj inteligentno. Računalniki bi namreč sami reševali določene težave. Drugi trend je umetna inteligenca, ki jo nekateri avtorji označujejo kot peto generacijo računalnikov[37]. Cilj je omogočiti računalnikom reševanje težav in opravljanje logičnih miselnih procesov, ki so ljudem enostavni. Ker so računalniki pri preračunavanju bistveno hitrejši od človeka, bi na ta način lahko reševali težave, ki so bile predhodno nerešljive. Tretji trend so navidezni svetovi, kjer ne gre samo za dvojno oziroma alternativno življenje posameznikov, temveč tudi za razlago realnega sveta z digitalnimi informacijami. Četrti trend se naj bi odvijal na področju mobilne telefonije in »mobilnega mreženja«, torej dostopa do internetnih vsebin. Peto področje je na področju ekonomije, kjer bo vse več kontekstualnega spletnega oglaševanja, kar pomeni, da bo iz

[36] Gordon Moore je trdil, da se moč procesorjev vsake 18 mesecev pri njihovih konstantnih cenah podvoji oziroma, da se cena procesorjev iste moči procesiranja vsake 18 mesecev razpolovi (Svete 2005, 18).

[37] Prva generacija računalnikov je bila med leti 1940 in 1956. Temeljila je na strojnem jeziku, najnižji ravni programskega jezika. Računalnik je za vezje uporabljal vakuumske elektronke ter magnetni boben kot pomnilnik. Ukazi so bili vneseni s pomočjo naluknjanih kartic. Druga generacija računalnika je bila med leti 1956 in 1963, ko so elektronke zamenjali tranzistorji. Ti računalniki so bili že manjši, hitrejši, cenejši, učinkovitejši in zmogljivejši. Prav tako so si lahko določene ukaze že zapomnili. Tretjo generacijo, med leti 1963 in 1971, zaznamuje integrirano vezje. Pojavi se uporaba tipkovnice in monitorja preko operacijskega sistema. Ti računalniki so že lahko izvajali različne aplikacije. Prvič so tudi postali dovolj majhni in cenovno dostopni za javnost. Četrto generacijo računalnikov, po letu 1971, predstavlja mikroprocesor, kjer je tisoče integriranih vezij vgrajenih na silikonski čip. Povezovanje teh čipov medsebojno proizvede še večje zmogljivosti procesiranja, kar je imelo tudi velik vpliv na razvoj interneta. Peto generacijo bo zaznamovala umetna inteligenca, ki je še v razvoju, kljub temu, da so nekatere aplikacije, kot je na primer prepoznavanje glasu, v rabi že danes. Peta generacija računalnikov bo lahko sprejemala ukaze v naravnem jeziku ter se bo sposobna učiti (Webopedia.com 2008b).

obiskanih spletnih strani sistem lahko razbral, katere vsebine uporabnika zanimajo ter vanj usmeril temu primerne reklamne vsebine. Šesti trend so spletne strani kot storitve. Sedmi trend bo spletna televizija. Osmi trend so obogatene spletne aplikacije, ki bodo uporabnikom bolj prijazne ter bolj učinkovite. Deveti trend je mednarodna mreža, kjer bodo ZDA izgubile večino internetnega tržnega deleža na račun Kitajske in Indije. Deseti trend je poosebljane spleta, kjer si uporabnik/obiskovalec neke spletne strani le-to uredi po meri (MacManus 2007).

Nekateri od trendov, ki jih je napovedal MacManus, so danes že razviti. Navidezni svetovi, mobilno mreženje, kontekstualno spletno oglaševanje s pomočjo piškotkov[38] (angl. Cookies), spletne strani kot storitve, spletna televizija in poosebljanje spleta so vse že v splošni rabi. Semantična mreža in umetna inteligenca sta sicer še daleč, vendar obstajajo podjetja, ki raziskujejo tudi na tem področju[39].

Glavne tehnologije, ki so se razvijale, omogočajo hitrejše, boljše in cenejše komuniciranje ter informiranje. V prihodnje lahko pričakujemo vse več multifunkcionalnih naprav, ki bodo uporabnikom omogočale hiter način pridobivanja informacij in komuniciranja. Primer je razvoj aparatov mobilne telefonije, ki se je v roku 10 let razširil iz zagotavljanja storitve klicanja in pošiljanja sporočil na snemanje in pošiljanje videov in slik, izvajanja videokonferenčnih klicev, dostopa do internetnih vsebin, urejanja in pisanja dokumentov, poslušanja glasbe in podobno (Pinterič in Grivec 2007, 17). Tudi Evropska unija je oznanila, da bo leta 2010 namenila 18 milijonov evrov za podporo generaciji mobilnih omrežij 4G[40], v katerih bo zagotovljen hitrejši širokopasovni dostop do interneta po nižjih cenah ter druge storitve kot sta visokokakovostna televizija ali video na zahtevo. V obdobju med leti 2007 in 2013 bo Evropska unija za razvoj omrežij namenila več kot 700 milijonov evrov, polovica tega zneska naj bi šlo za raziskave brezžičnih omrežij (STA 2009).

[38] Piškotki so deli informacij, ki jih ustvari strežnik in shrani na računalniku uporabnika. Omogočajo pridobivanje informacij o uporabniku glede obiskanih spletnih strani ter tudi nekatere osebne podatke (Whalen 2002).
[39] Na primer Numenta in Hakia.
[40] 1G generacijo mobilnih telefonov predstavljajo prvi mobilni telefoni z brezžično povezavo, ki je uporabljala analogno tehnologijo (»Nordic Mobile Telephony« - NMT). 2G generacija mobilnih telefonov je deloma že temeljila na digitalni tehnologiji (»Global System for Mobile Communications« - GSM). 2G generacija je bila nato nadgrajena na pred-3G tehnologijo (»General Packet Radio Service« - GPRS). Trenutno je v rabi 3G tehnologija (»Universal Mobile Telecommunications System« - UMTS) (Trček 2006, 134).

Kot argumentira Hiner (2009), so nekateri trendi, ki bodo prevladovali, na spletu temelječe aplikacije, virtualizacija spletnih storitev, tanki klienti[41] ter pametni telefoni. Greengard dodaja še mobilnost delovnega kadra, učinkovitejši podatkovni centri, povečanje varnosti in števila socialnih mrež (Greengard 2008).

4.5 Razpršeno računalništvo ali »Cloud computing«

Najpogostejša definicija razpršenega računalniškega sistema (razpršenega računalništva[42], angl. Cloud computing), ki se pojavlja na spletu, je, da je »razpršeni računalniški sistem računalniška paradigma, v kateri so naloge prenesene na različne povezave, programe in storitve, do katerih posameznik dostopa preko omrežja« (Pant in Sharma 2009). Razpršeno računalništvo je storitev, ki izhaja iz oblakov[43]. Ta predstavljajo navidezno mesto, ki omogoča uporabo raznih aplikacij za doseganje želenih rezultatov. Ob enem pa so v oblaku shranjeni tudi razni podatki, kamor jih shranjujejo uporabniki spleta. Uporabnikom je z dostopom do oblaka zagotovljen dostop do zmogljivosti superračunalnika. Preko vstopnih točk[44] in aplikacij lahko posameznik dostopa do virov, torej informacij in storitev, ki jih potrebuje[45].

Razpršeno računalništvo lahko postavimo kot nasprotje tradicionalnim osebnim računalnikom, kjer uporabnik za doseganje želenih rezultatov uporabi zmogljivosti svojega računalnika. Pri razpršenem računalništvu mreža postane superračunalnik. Posameznik zažene aplikacijo, želi nekaj opraviti in sistem sam izbere dejanski, optimalni način izvedbe. Sposobnost procesiranja podatkov je omogočena preko distribuiranega računalništva. To zagotovi uporabniku večjo računalniško moč procesiranja ter večji vir informacij (Ibid.).

Razpršeno računalništvo predstavlja infrastrukturo IKT-ja, v kateri dostop do virov predstavlja storitev. Najprej se je začelo pojavljati v gospodarstvu, vendar se prebija tudi v komercialno sfero. Potreba po razpršenih računalniških sistemih se je pojavila zaradi dveh glavnih razlogov. Prvi razlog so stroški, ki so jih imela razna podjetja z vzpostavljanjem in

[41] Programska ali strojna oprema, ki temelji na principu dela odjemalec strežnik (angl. client/server). Program ali strojna oprema je odvisna od strežnika, ki opravi večino dela. Tanki klient vsebuje le toliko informacij, da se zažene ter poveže s strežnikom.
[42] Nekateri avtorji ga prevajajo kot »računalništvo v oblakih«
[43] Izraz se zmotno uporablja tudi za internet. Gre za omrežni zbor strojne in programske opreme.
[44] Na primer iPhone, Blackberry, prenosnik in drugo.
[45] Ker posamezniki uporabljajo kar potrebujejo, lahko o tem načinu računalništva govorimo kot o računalništvu na zahtevo.

vzdrževanjem lokalnih, lastnih podatkovnih centrov[46] (angl. Data center). Podjetjem z uporabo storitve razpršenega računalništva ni več potrebno imeti v lasti strojne in programske opreme ter zanjo skrbeti. Drugi razlog, ki je prispeval k vzpostavitvi razpršenih računalniških sistemov, pa so povečanje sodelovanja v gospodarstvu, nove naprave, ki se povezujejo z internetom, pretakanje[47] (angl. Streaming), nove telefonske storitve, razne Web 2.0[48] aplikacije (IBM 2008). Ključnega pomena je večja hitrost prenosa podatkov.

Na področju razpršenega računalništva ima prednost Google. To je predvsem zaradi vse večjega povpraševanja in zahtev po hitrem dostopu do natančnih in točnih informacij. Google je, za potrebe zagotavljanja rezultatov dnevnega iskanja velikega števila uporabnikov, izdelal veliko število lastnih strežnikov, ki so medsebojno povezani ter da zagotavljajo močan in stabilen sistem. Na oblaku bazirajo vse spletne aplikacije, kot so na primer Google apps, maps, Gmail (Pant in Sharma 2009).

Razpršeno računalništvo bo omogočalo uporabnikom plačevanje storitev in hrambo podatkov glede na to, koliko bodo neko programsko opremo uporabljali ter koliko podatkov bodo prenašali, koliko časa bo potrebnega za prenos in podobno. Eden izmed učinkov, ki jih bo razpršeno računalništvo imelo, bo povečanje vpliva industrije programske opreme. Posamezniki ne bodo več uporabljali fiksno naložene opreme programske opreme na domačem računalniku. Uporabljali bodo programe neposredno iz oblaka. Plačevanje bo glede na uporabo, torej kolikor minut bo uporabnik nek program uporabljal, toliko bo zanj plačal (Ibid.). Na ta način bo industrija lahko otežila uporabo piratskih kopij ter povečala svoj prihodek. Uporabnikom licenčnih programov[49] se v tem primeru lahko zgodi, da programov ter strojne opreme ne bodo preplačali glede na dejansko rabo in potrebe[50]. Razpršeno računalništvo se razvija in se uveljavlja, vendar popolnega prestopa iz klasičnega računalništva na razpršeno računalništvo v naslednjih nekaj letih ne gre pričakovati.

[46] Izraz podatkovni center se uporablja za mesto, kjer se shranjuje računalniške sisteme (strežnike) ter komponente. Kot podatkovni center razumemo tako celotno omrežno infrastrukturo.
[47] Večinoma se nanaša na multimedijske vsebine, ki jih zagotavlja ponudnik pretakanja. Uporabniku se vsebina predvaja brez potrebnega predhodnega nalaganja.
[48] Termin Web 2.0 se nanaša na tako imenovano drugo generacijo spleta, ki je nastopila po letu 2001. Pri Web 2.0 se je spremenil način uporabe spleta s strani programerjev in končnih uporabnikov. Pri Web 1.0 je bil uporabnik odjemalec informacij, Web 2.0 pa pomeni večjo aktivnost uporabnika, ki ima vlogo kreatorja informacij (Sharma 2008).
[49] Mišljeno je ob upoštevanju ekonomije obsega, uporabnik je v tem kontekstu organizacija, drugače predstavlja uporabnik posameznika, ki uporablja IKT.
[50] Mišljena je uporaba strojne opreme, postavitev kapacitet, ki je potrebna za neko organizacijo, da lahko vzdržuje svoj oblak. Postavitev lastnih podatkovnih centrov in vzdrževanje sta lahko za podjetje velik strošek, še posebej, če se izkaže, da zmogljivosti niso v celoti izkoriščene ter konstantno v rabi.

O'Reilly trdi, da so vse spletne aplikacije aplikacije, ki obstajajo v oblaku. Ugotavlja tudi, da prihaja do razlikovanja v pojmovanju samih uporabnikov spletnih aplikacij. Termin oblak večina uporablja za spletne aplikacije, ki so se predhodno nahajale na osebnem računalniku, na primer razne preglednice, programi za obdelavo besedil, elektronska pošta in podobno. Kljub temu, da delujejo v oblaku, uporabniki ne dojemajo aplikacij kot sta Google search in maps za aplikacijo v oblaku. Do tega razlikovanja prihaja zaradi drugačnega odnosa do aplikacije, ki hrani osebne podatke. Z vidika človekove varnosti ni težko razumeti, da je izguba osebnih podatkov ali pa samo trenutna nedostopnost le-teh veliko bolj skrb vzbujajoča, kot je izpad storitve, za katero se brez težav najde zamenjava[51]. Uporabnik vrednoti različne aplikacije glede na koristnost, ki mu jo le-ta predstavlja, zato ni presenetljivo, da prihaja do subjektivnega razlikovanja v dojemanju razpršenega računalništva (O'Reilly 2008).

Predvsem govorimo o dveh tipih oblakov. Zasebni oblaki temeljijo na internih podatkovnih centrih in niso dostopni javnosti. Uporabljajo jih razne organizacije za svoje dejavnosti. Javni oblak v nasprotju z zasebnim ponuja storitve prav javnosti (Armbrust in drugi 2009, 4).

Razpršeno računalništvo bi lahko primerjali z omrežnim računalništvom ter storitvenim računalništvom (angl. Utility computing). Primerjava z omrežnim računalništvom je v obliki distribuiranega računalništva, vendar pri razpršenem računalništvu ne gre samo za navidezni superračunalnik, ki je sestavljen iz več mrež ter medsebojno povezanih računalnikov. Prav tako kot omrežja, potrebuje tudi razpršeno računalništvo določeno programsko ter strojno opremo, da lahko zagotavlja storitve iz oblaka, torej razdeljevanje in distribucija komponent programov in informacij (Pant in Sharma 2009). Razlika je v tem, da pri distribuiranih sistemih posamezniku drugi avtonomni računalniki[52] niso vidni. Pri omrežju se posameznik prijavi na točno določen računalnik, sam sproži določene dejavnosti ter sam prestavlja določene podatke. Pri distribuiranih sistemih je drugače, saj oblak deluje navidezno kot en računalnik[53] (Tanenbaum 1996, 2). Distribuiran sistem je postavljen na omrežju in temelji bolj na programski opremi. Druga primerjava, s katero lahko opišemo razpršeno računalništvo, je storitveno računalništvo. To pomeni, da oblak vsebuje računalniške vire, ki so dostopni kot javna storitev[54] (O'Reilly 2008). Za razpršen računalniški sistem ne moremo v

[51] V primeru izpada Google maps-a posameznik lahko poseže po Microsoft live maps.
[52] Računalnik, na katerega uporabnik preko svojega računalnika ne more vplivati, ga ne more vklopiti, izklopiti ali drugače nadzorovati.
[53] Razpršeno računalništvo temelji na virtualizaciji (navideznosti). Pomeni pa navidezno ustvarjanje verzije nečesa namesto dejanskega, gre za neke vrste simuliranje nekega stanja.
[54] Za to se uporablja izraz »Software as a Service« (SaaS).

celoti trditi, da gre za omrežje, prav tako tudi ne storitveno računalništvo. Je naslednji korak obeh skupaj.

Poleg spletnih aplikacij sta vključena v razpršeno računalništvo tudi strojna in programska oprema v modularnih podatkovnih centrih[55] (angl. Modular data center - MDC), ki zagotavljajo obstoj oblaka (Armbrust in drugi 2009, 4).

[55] Modularni podatkovni center je podatkovni center, ki je sestavljen iz večjega števila strežnikov (med 1000 in 2000) in nudi veliko moč procesiranja. Strežniki so sestavljeni v podatkovni center znotraj ohišja, ki ga predstavlja standardizirani tovorni kontejner (Lai 2008a).

5 INFORMACIJSKA VARNOST IN RAZPRŠENO RAČUNALNIŠTVO

V sodobni družbi je čedalje več uporabnikov interneta ter spletnih storitev. Vedno večji del današnje družbe je odvisen od IKT-ja in iz te odvisnosti izhaja, kot pravi Svete (2005, 105) »oblika varnostne predstave, ki je usmerjena v zavarovanje omrežja samega pred razpadom sistema, izgubo, krajo ali uničenjem podatkov ter prekinitvijo informacijskih tokov«.

Kot nadaljuje, ima informacijska varnost dve dimenziji. Prva se nanaša na zaščito neokrnjenosti podatkov ter na interni pretok informacij do posameznih delov sistema. Druga dimenzija pa se nanaša na same informacijske tokove med ponudniki in potrošniki. Koncept informacijske varnosti kot cilj ogrožanja izpostavi v ospredje celotno IKT (Svete 2005, 106).

Trček razlikuje med varnostjo informacijskih sistemov in varnostjo informacijske tehnologije. Slednja se nanaša na varnost sistema, ki temelji na računalnikih ter jo obravnava s tehnološkega vidika. Varnost informacijskih sistemov prav tako temelji na računalniških sistemih, vendar poudarja človeški faktor kot pomemben element ogrožanja ter zagotavljanja varnosti (Trček 2006, 3–4).

Da bi lahko govorili o varnosti informacijske tehnologije, je treba najprej natančno določiti na katera premoženja se ta nanaša, oziroma kaj pomeni »celotna IKT«. Trček (2006, 21) trdi, da se informacijska varnost nanaša na:

- informacijsko premoženje: operacijski podatki znotraj podatkovnih baz ter druge vrste dokumentov, podatki shranjeni na različnih medijih ter v vseh oblikah;
- strojno opremo: računalniki, komunikacijska oprema, dodatna računalniška oprema, oprema, ki zagotavlja nemoteno delovanje strojne opreme;
- programsko opremo: sistemska in uporabniška;
- materialno premoženje: nepremičnine, premičnine, gotovina, storitve;
- ljudi;
- neotipljivo premoženje, kot sta na primer ugled ali delež trga.

S pojavom novih tehnologij ter njeno uporabo, lahko nastanejo tudi nove oblike ogrožanja, ter novi akterji zagotavljanja varnosti. Te grožnje lahko spremenijo temelje, na katerih sta bila zasebnost ter varnost osnovana (Agre in Rotenberg 2001, 7; Svete 2005, 32). V primeru razpršenega računalništva se nanašata varnost in zasebnost na nekaj, nad čemer posameznik nima dejanskega nadzora, saj podatki, ki morajo biti predmet zaščite, niso shranjeni na način, ki bi to posamezniku omogočal.

Razpršeno računalništvo omogoča uporabnikom dostop do večjih računalniških zmogljivosti ter različnih storitev. Da sistem lahko vzdržuje oblak, je potrebna velika zmogljivost procesiranja podatkov. Tukaj nastopijo podatkovni centri v kontejnerjih ali MDC-ji.

Hamilton trdi, da ima vsaka storitev, ki jo ponujajo različne organizacije ali podjetja na internetu, svoj lasten podatkovni center. Ena od težav, ki se pojavljajo je dostava posameznega strežnika iz tovarne v podjetje na drugem koncu sveta ter njegova namestitev. Stroški storitve so, zaradi stroškov naročanja in pošiljanja individualnih enot ter dodatnih potreb po usposobljenem kadru, ki to opremo potem namesti, zelo visoki. Poleg tega se zaradi velikega števila posameznikov, ki so vključeni v sam proces, poveča možnost napake (Hamilton 2007, 2).

Način, kako se izogniti velikim stroškom pošiljanja ter namestitve je, da se strežnikov in omrežnih komponent ne pošilja individualno, temveč se jih namesti v kontejnerje po tisoč ali več strežnikov. S tem lahko podjetja uživajo ugodnosti, ki izhajajo iz ekonomije obsega, poleg tega pa se zmanjša možnost napak ob namestitvi, saj je vsak modul pripravljen za takojšnjo uporabo. Podjetja bodo tako sčasoma lahko naročala le še celotne podatkovne centre. Naročnik mora zagotoviti le elektriko, omrežno povezavo ter vodo za hlajenje (Ibid.). Večja mobilnost je zagotovo ena izmed prednosti, ki jih ponuja MDC. Tovorni kontejnerji, v katerih so nameščeni strežniki, so standardizirani za potrebe transporta. Kontejnerski terminali so skoraj v vseh tovornih pristaniščih, od tam pa se lahko brez težav tovorijo po cesti ali železnici. MDC se lahko postavi kamorkoli. Podjetjem za njegovo postavite ni potrebno nameniti posebnih prostorov v zgradbi. Prav tako MDC-jev ni potrebno vzdrževati, saj delujoče enote prevzamejo naloge tiste v okvari[56]. Po določenem času se modul vrne proizvajalcu na reciklažo, kjer se popravi, kar se da, ter nadomesti ostalo (Hamilton 2009, 3–7). MDC-ji so v primerjavi s klasičnim načinom postavljanja omrežja skorajda »plug and play« (priključi in igraj) oprema. Poleg priključka ni potrebno narediti ničesar. Oprema je

[56] Hamilton trdi, da lahko MDC s 50% okvarjenih strežnikov še vedno deluje s 95% zmogljivosti.

takoj pripravljena za uporabo (Lai 2008b). Zaradi standardiziranih kontejnerjev, je le-te lažje tudi medsebojno povezati v visoko zmogljive komplekse MDC-jev[57] (KMDC), ki bi lahko vzdrževali oblak.

MDC-je so med prvimi predstavili Sun Microsystems in Microsoft. Microsoft prav tako načrtuje postavitev KMDC-jev na različnih lokacijah. Gradnja se je že pričela v Chicagu, San Antoniu, Washingtonu in Dublinu. Ti kompleksi so sestavljeni iz približno 200 MDC-jev na območju velikem 51.000 m^2, kar pomeni 440.000 strežnikov. Kapacitete teh kompleksov so tako velike, da bi več teh lahko vzdrževalo oblak (Lai 2008a).

Analizo varnosti razpršenega računalništva bomo proučili predvsem z vidika informacijske varnosti, ki se nanaša na zasebnost posameznika. Za potrebe diplomskega dela bom vpeljal definicijo informacijske varnosti uporabnika v oblaku, ki jo razumemo kot *stanje, v katerem ima uporabnik popoln nadzor nad lastnimi podatki, ki jih shranjuje v oblaku. Nedovoljen dostop do teh podatkov je tretjim osebam onemogočen in s svojim delovanjem ne morejo zmotiti vsakodnevnih ritualov uporabnika ter/ali ga fizično ogrožati, ekonomsko ogrožati, ogroziti njegovih temeljnih pravic ali njegovega družbenega statusa. Prav tako so zaščiteni tudi osebni podatki pred nedovoljeno obdelavo in/ali uporabo s strani pooblaščenih kot tudi nepooblaščenih oseb za upravljanje s podatki.*

Grožnje informacijski varnosti lahko v razpršenem računalništvu razdelimo na dve skupini. Prva skupina groženj preti strojni opremi in jo lahko označimo kot fizične grožnje informacijskim sistemom. Druga skupina groženj poudarja uporabniški vidik ter jo lahko označimo kot uporabniške grožnje (Svete 2005, 107).

Tako strojna kot programska oprema imata določene ranljivosti. ***Strojno ranljivost*** predstavlja ranljivost strojne opreme na okoljske razmere, nepravilno vzdrževanje, odvisnost od napajanja ter nepravilno odstranitev opreme. ***Programsko ranljivost*** predstavljajo slabe specifikacije za razvijalce opreme, nezadostno ter neprimerno testiranje, kompliciranа uporaba programov, pomanjkanje overovljanja, nadzor dostopanja, avtorizacijski mehanizmi, nenadzorovana nameščanja, pomanjkanje dokumentacije, neprimernost rezervnih kopij in neprimerna odstranitev programov. ***Komunikacijska ranljivost*** so nezaščiteni mediji, nepravilno upravljanje z povezavami (kabli ali omrežja) ter pomanjkanje varnostnih storitev. ***Infrastrukturno ranljivost*** predstavlja neprimeren nadzor, zaščito ali stabilnost kakršnega koli oskrbovanja. ***Ranljivost dokumentov*** predstavlja nezaščiteno shranjevanje,

[57] Nekateri avtorji to poimenujejo strežniška farma.

nenadzorovano razmnoževanje le-teh ter nepremišljen izbris. ***Ranljivost osebja*** predstavlja pomanjkanje ali neprimerne postopke novačenja, pomanjkanje ali neprimerno usposabljanje za zaposlene, pomanjkanje nadzora nad osebjem ter pomanjkanje zavedanja o varnostnih tveganjih. ***Okoljsko ranljivost*** predstavlja neprimerna ali neobstoječa fizična zaščita, pomanjkljiva ali neprimerna elektromagnetna zaščita ter sama neprimerna lokacija. ***Splošno ranljivost*** predstavlja pomanjkanje ustreznih politik, obstoj točke ranljivosti (angl. Single point of failure) ter slabo vzdrževanje in servisiranje (Trček 2006, 23–4).

5.1 Fizične grožnje

Ranljivosti, ki jih ima strojna oprema so predvsem strojne, infrastrukturne, okoljske, splošne ter ranljivosti zaradi osebja (Ibid.).

Fizične grožnje, ki pretijo MDC-jem, so predvsem tiste, ki povzročijo začasno ali stalno izgubo podatkov. Trček kot fizične grožnje označi okoljske grožnje. Med te uvrsti ekstremno vreme, vlago, temperaturo, prah, vibracije, elektromagnetno sevanje, statiko ter potres (Ibid.) Poleg teh lahko dodamo še poplave, ki niso nujno posledica vremena, požar ter nestabilnost napajanja (Svete 2005, 108).

KMDC bo moral biti postavljen na območju, kjer ni večje nevarnosti naravnih nesreč. Najbolje bi ga bilo postaviti na območje, kjer se lahko koristi naravne pogoje sebi v prid, na primer hladna klima kot dodatno hlajenje (Lai 2008b). Fizična zaščita se nanaša tudi na zaščito samih stavb, sob in območij. To se doseže s postavitvijo ograj, zidov, fizičnim varovanjem, videonadzornim sistemom ter drugimi varnostnimi mehanizmi. Kompleksi bodo morali imeti tudi razne alarmne sisteme, ki bi opozarjali na nepooblaščen dostop oseb, sisteme za dostop, ki bi preprečeval nepooblaščen dostop, na primer biometrične ključavnice, detektorje dime, gasilne naprave ter podobno (Trček 2006, 30).

Sam vstop v MDC je omejen. Ker ne potrebujejo vzdrževanja, se praktično izniči možnost napak kot posledice nepravilnega vzdrževanja. Dejansko na območju KMDC-ja razen varnostnikov ter vzdrževalcev napeljav ne bo smelo biti nikogar drugega (Hamilton 2007, 3).

Vsak MDC bi moral imeti tudi neke vrste brezprekinitvenega napajalnika (angl. Uninterruptible power supply – UPS), ki bi zagotavljal ustrezno napetost, preprečeval

prebijanje električne napeljave ter poškodbe opreme. Prav tako bi zagotavljal rezervno napajanje (Lai 2008b).

Občutljivost na vremenske razmere pri MDC-ju ne bo imelo večjih učinkov. Zabojniki so že v osnovi narejeni tako, da so odporni na različne vremenske pojave. Večje težave lahko povzroči izpad elektrike, omrežne povezave ali hlajenja. V zasnovi imajo MDC-ji napako. Imajo namreč eno točko priključka. Kar je zamišljeno kot prednost, ker ni veliko ukvarjanja s priključevanjem, je lahko slabost. V kolikor se ta povezava prekine, se onesposobi več tisoč strežnikov. Ker ni zamišljenega sistema glavnega A in rezervnega B priključka, tako ni možnosti rezervnega dostopa. Ob prekinitvi povezave se podatki sicer ne bi izgubili, le dostop do njih ter nekaterih storitev bi bil za nekaj časa onemogočen (Lai 2008b).

Vsak MDC bo imel poleg zunanjega nadzorovanja tudi notranje senzorje. Ti bodo merili temperaturo in vlago zraka ter po potrebi aktivirali klimatske naprave, ki bodo zagotovile ustrezno mikroklimo (Ibid.).

Za podatke uporabnikov največje nevarnosti predstavljajo ekstremno vreme, izpad elektrike, fizično uničenje MDC-ja v požaru, poplavah in podobno ter potres. Rezervnih kopij, kot se jih dela v podjetjih, se v primeru razpršenega računalništva, zaradi same količine podatkov, ne bo moglo narediti. V oddaljenih MDC-jih bodo tako shranjene kopije le za tiste podatke, ki so nujni za ponovno vzpostavitev in delovanje sistema.

5.2 Uporabniške grožnje

Uporabniške grožnje se nanašajo na ranljivost programske opreme, komunikacijsko ranljivost, infrastrukturno ranljivost, ranljivost dokumentov, ranljivost osebja, okoljsko ranljivost ter splošno ranljivost. V središču uporabniških groženj je človek, grožnje pa lahko razdelimo na namerne in na nenamerne grožnje (Trček 2006, 23–4).

Med namerne grožnje sodijo kraja, prevare, poneverbe, falsificiranje, izsiljevanje, grožnje, kršitve zasebnosti, sabotaže, sporočanje zaupnih podatkov, vohunjenje, pornografija, propaganda, vandalizem, terorizem, umori, heking[58], izdelava ter distribucija virusov,

[58] Heker je izraz za kiberkriminalca. Thomas in Loader ločita med hekerji in phreakerji, trgovci z informacijami in teroristi, deviantneži ter ekstremisti. Phreakerji se ukvarjajo predvsem z zlorabo telefonskih sistemov, trgovci z informacijami stremijo za dobičkom, teroristi, deviantneži in ekstremisti pa uporabljajo informacijske sisteme za nezakonite politične ali družbene dejavnosti. Heker se prav tako loči od krekerja (angl. Cracker), ki znanje

piratstvo na področju programske opreme ter napadi DoS[59] (»Denial of Service«) (Svete 2005, 108).

Trček (2006, 23) namerne grožnje opiše kot krajo, fizično uničenje z uporabo orožja, ognja ali vode, neposreden fizični napad[60], prikriti napad[61] ter operacijske napake in nepravilna raba opreme. Nenamerne grožnje so posledica slabe organiziranosti, nediscipline, nemarnosti, monotonosti, nestrokovnosti ter utrujenosti (Svete 2008, 108). Zajemajo pa fizično uničenje, neposreden napad, operacijske napake ter napačno rabo opreme (Trček 2006, 23).

Pri razpršenem računalništvu je velika ovira pri varovanju podatkov dejstvo, da uporabnik podatkov ne bo imel shranjenih pri sebi, temveč v oblaku. Podatki bodo ostali v oblaku tudi potem, ko uporabnik splet zapusti, kar poveča možnost dostopa do njih.

Podatki so najprej ogroženi, ko se vnašajo preko računalnika. Ker na samem računalniku posameznik ne bo več shranjeval podatkov, se v njih ne bo vdiralo z namenom neposredne kraje podatkov. Računalnik bo imel shranjenih le toliko podatkov, da se bo lahko zagnal ter priključil na omrežje. Računalnik bo najverjetneje vseboval unikaten elektronski podpis, ki ga bo omrežje prepoznalo ter omogočilo dostop do storitev oblaka. Enak princip[62] bi se uporabljal tudi za plačevanje storitev, saj bi oblak prepoznal računalnik ter beležil (u)porabo storitev v oblaku. Kljub temu, da uporabnik na svojem računalniku ne bo shranjeval podatkov, bo napadalec posredno podatke lahko pridobival z opazovanjem dela uporabnika[63].

Naslednja grožnja je komunikacijski kanal, torej prenos podatkov iz računalnika na strežnik ali obratno, ter komunikacija med strežniki. Nekatere nevarnosti, ki pretijo uporabniku so

---

uporabljajo za vlamljanje v tuje računalnike s pridobitnimi nameni, medtem ko heker vlamlja zaradi intelektualnega izziva v premagovanju omejitev. Hekerji so prav tako zaslužni za razvoj številnih orodij za zaščito zasebnosti (Kovačič 2006, 141–3). Vseeno je hekanje vdor v zasebnost nekega uporabnika in kot tako varnostno tveganje.

[59] Napad DoS je napad z namenom povzročiti nedostopnost sistema oziroma ovirati njegovo delovanje. Napadalec da sistemu veliko količino zahtevkov, zaradi česar se sistem upočasni ali preneha, ker mu ne uspe obdelati vseh zahtevkov (Kovačič 2006, 164).

[60] Na primer okvara klimatske naprave ali elektromagnetno sevanje.

[61] Prisluškovanje in maskiranje.

[62] Princip, na katerega se sklicujemo je zaupanja vredno računalništvo (angl. Trusted computing). Razvijati so ga začeli Microsoft, Intel, IBM, HP in Compaq za potrebe bolj varnega osebnega računalnika. Temelji na čipu (»Trusted Platform Module«, TPM), ki je integriran v matično ploščo računalnika in ob zagonu preveri stanje računalnika, poskrbi za avtenifikacijo ter vzpostavi povezavo z omrežjem (Anderson 2008, 111–2).

[63] Podoben princip kot je storitev »remote desktop«. Napadalec bo lahko vdrl v osebni računalnik uporabnika ter videl preko lastnega zaslona isto, kar vidi uporabnik.

prisluškovanje, prestrezanje komunikacije z namenom pridobitve podatkov[64] ter krekanje (Leitold 2001, 78).

Električni signali povzročajo elektromagnetno sevanje ali radijski signal. Za klasične povezave lahko trdimo, da so pravzaprav antene, ki oddajajo podatke, ki jih prenašajo[65]. Pri napeljevanju kablov je zato pomembno, da se upošteva tudi nevarnost prisluškovanja. Sprememba na področju povezav je optični kabel, kateremu se zelo težko prisluškuje. Optični kabel prevaja svetlobo namesto električnega signala. Svetloba (signal), ki se izgubi na poti, ni dovolj močna za prisluškovanje. Edini način bi bil s prestreznikom (Strebe in drugi 1998, 675–83).

Še najmanj varne so brezžične povezave[66]. Podatki, ki se prenašajo preko brezžične povezave, so lahko prestreženi v veliko širšem območju kot pri navadnih povezavah (Trček 2006, 133–5). Tudi pri mobilni telefoniji in raznih digitalnih beležnicah je uporabnik vedno bolj zainteresiran za pošiljanje elektronske pošte, brskanje po spletu ter opravljanje drugih spletnih dejavnosti (Jerman-Blažič in drugi 2001, 17). Pri vseh teh napravah je tveganje veliko večje. Osnovna logika ostaja, da v kolikor lahko do posameznih podatkov dostopi uporabnik, lahko do taistih podatkov dostopi tudi nekdo, ki mu ti podatki niso namenjeni[67].

Tretjo ranljivost podatkov predstavlja oblak oziroma ponudnik oblaka. S tem, ko uporabnik podatke shranjuje na drugem strežniku, izgubi določeno mero nadzora nad zasebnimi podatki. Uporabnik ne more z gotovostjo vedeti, kaj se z njegovimi podatki dogaja ter ali so varni. Ponudniki oblaka bodo imeli glavno vlogo pri zaščiti podatkov in ti bodo vedno lahko dostopali do zasebnih podatkov. V primeru, da bi do nekih podatkov želele priti preiskovalne agencije, bodo to lahko storile preko ponudnika oblaka, ne da bi uporabnik za to vedel. Prav tako bo ponudnik nekatere podatke lahko delil z raznimi oglaševalnimi podjetji (Privacy rights clearinghouse 2008).

Glede na to, da bodo vsi zasebni podatki shranjeni v oblaku, torej v »eni bazi podatkov«, lahko logično sklepamo, da bodo nekateri mehanizmi identifikacije vzpostavljeni, ne moremo pa z gotovostjo trditi, da bo dostop do zasebnih podatkov tretjim osebam onemogočen. Veliko

[64] Primer strojne opreme, ki se jo lahko namesti na kabel med tipkovnico in računalnikom in zazna tipkanje, je »KeyGhost« (Kovačič 2006, 124).
[65] Tem signalom se lahko prisluškuje z vmesnikom, ki se namesti med uporabnikom in strežnikom ali z napravo, ki lahko lovi te radijske valove. Ti radijski valovi so dovolj močni za lovljenje le do 15 cm oddaljenosti od kabla.
[66] Na primer povezava z internetom preko tankega klienta ali raba usmerjevalnikov (angl. Router).
[67] V primeru brezžične povezave podatkov med dvema ali več tankimi klienti.

avtorjev poudarja pomen kriptografije kot sredstva za zaščito podatkov. Vendar je kriptografija učinkovita le v določenem obsegu.

Ponudniki storitev oblaka bodo prav tako imeli tudi vpogled v osebne podatke uporabnikov. Le-ti bodo morali te posredovati, v kolikor bodo želeli dostopati do storitev oblaka. Osebni podatki se bodo lahko obdelovali v različne namene, kot je na primer kontekstualno oglaševanje, tudi zunaj podjetja, ki ponuja dostop do oblaka. V teh podjetjih ni nujno, da veljajo enaki pogoji zaščite podatkov, kot to velja v matičnem podjetju. Dejstvo ostaja, da je uporabnik v nekem obsegu sam odgovoren za varnost in celovitost lastnih podatkov, tudi ko jih hrani tretja oseba. V ta namen mora sprejeti določene varnostne ukrepe za zaščito zasebnih podatkov še preden jih shrani v oblak (Brodkin 2008). V spletnih aplikacijah je danes shranjenih toliko osebnih podatkov[68], da lahko uspešen napadalec pridobi velike količine podatkov, ki jih lahko nato s pridom izkorišča (Anderson 2008, 735).

5.3 Razpršeno računalništvo in zasebnost

Z razvojem tehnologije se povečuje tudi možnost izvajanja nadzora. Več storitev ko posameznik opravlja na spletu, lažje je zbiranje osebnih podatkov za različne akterje. Z razvojem razpršenega računalništva se bo nadaljevalo v isti smeri. Razvoj gre v smeri nadzora in stran od zasebnosti. Bolj kot zaščita zasebnosti je v ospredju zaščita intelektualne lastnine in marketing (Kovačič 2006, 167, 208).

Možnost dostopanja do komunikacijskih storitev preko interneta je vedno večja. Prav tako se posamezniki vedno bolj zanašajo na internet kot sredstvo za zadovoljevanje lastnih potreb po računalništvu. Uporabnikom se odpirajo nove priložnosti, saj bodo z razpršenim računalništvom vse storitve, vse programje ter vsi podatki v oblaku. Ob tem se bodo pojavile tudi nove nevarnosti za njihove osebne podatke ter zasebnost (Kovačič 2006, 143).

Uporabniki danes pravzaprav sami brišejo mejo med javnim in zasebnim, ki je bila nekoč relativno jasna. Uporabnik z lastnim sodelovanjem na raznih forumih ter uporabo spletnih aplikacij omogoča drugim, da posegajo v njegovo domeno. Prav tako tudi sam s svojo dejavnostjo posega v zasebnost drugih (Pinterič in Grivec 2007, 23).

[68] V nekem primeru je napadalec vdrl v podatkovno bazo Monster.com-a ter dostopil do osebnih podatkov približno 1,3 milijona iskalcev zaposlitve.

Z razvojem razpršenega računalništva si bodo uporabniki prizadevali za čim večjo varnost in zasebnost ob največji možni razpoložljivosti storitev oblaka. Pri razpršenem računalništvu gre pričakovati, da bodo osebni in zasebni podatki v oblaku medsebojno ločeni. Osebni podatki o uporabnikih bodo shranjeni v zasebnem oblaku, zasebni podatki pa v javnem (Ibid.).

Nasproti prednosti, ki jih bo ponujalo razpršeno računalništvo, se bodo z razvojem pojavile tudi nove možnosti nadzora. Z nekaterimi novejšimi statističnimi tehnikami obdelave podatkov, kot je na primer rudarjenje po podatkih (angl. Data mining), se bo lahko uporabnike razvrščalo v različne skupine ali kategorije tveganja, kar Kovačič označi kot statistično diskriminacijo. Večji poudarek bo na predvidevanju ter preventivi dejanj, ki predstavljajo grožnjo varnosti. Nadzor bo postal vseobsežen, inštrumentaliziran, neselektiven ter neopazen (Kovačič 2006, 30).

Ker bodo vsi podatki dostopni v oblaku, se pojavi vprašanje poseganja v podatke uporabnikov. Na primer države lahko pod pretvezo zagotavljanja varnosti posegajo v zasebnost posameznika[69]. Popolna ignoranca podatkov, ki »so na razpolago« pa bi lahko dopuščala preveč svobode, kar bi razne teroristične skupine lahko s pridom izkoristile za koordiniranje svojih dejavnosti. Po terorističnem napadu 11.9.2001 se je številne baze podatkov po svetu začelo medsebojno povezovati. V luči vojne proti terorizmu so se po svetu pojavile težnje po zmanjševanju potrebne birokracije glede zahtevkov po prisluškovanju ter drugih oblik nadzorovanja. Z vsem programjem in podatki, ki bodo v oblaku, bodo oblasti ali ponudniki lahko omejili dostop do nekaterih (potencialno nevarnih) informacij, kar v skrajnem primeru lahko privede so splošnega nadzora informacij, podobno kot se še vedno dogaja na Kitajskem (Pinterič in Grivec 2007, 25).

Razni zakoni o varovanju osebnih podatkov določajo nekatere omejitve glede zbiranja in obdelave podatkov. V nekaterih državah je tako prepovedan prenos podatkov preko državne meje. Posameznik ima tudi pravico, da ve, kateri podatki se o njem zbirajo ter s kakšnim namenom se obdelujejo. Prav tako mu dovoljujejo, da zbiranja določenih podatkov ter določene obdelave ne dovoli (Kovačič 2006). Ker je razpršeno računalništvo tehnologija, ki se ji ne bo moč izogniti, uporabniki ne bodo več imeli toliko nadzora nad lastnimi podatki.

[69] Eden izmed takih primerov je sistem ECHELON, ki predstavlja globalno mrežo računalnikov, ki pregledujejo sporočila, fakse, elektronsko pošto in podobno, v njih pa iščejo določene besede, ki so zajete v ECHELON-ovem slovarju. Namen ECHELON-a je najti grožnjo preden se uresniči (Pike 2008).

Težava je v tem, da je IKT bistveno bolj napredovala, kot je napredovalo na tem področju pravo. Nekatera vprašanja je zagotovo potrebno rešiti, še preden se razpršeno računalništvo uveljavi v celoti. Na primer kdo je lastnik podatkov, uporabnik ali ponudnik? Ali lahko ponudnik uporabniku onemogoči dostop do podatkov? Kaj se zgodi s podatki, če ponudnik (podjetje) slučajno propade? Najpomembnejše vprašanje pa bo najverjetneje ostalo, kako bo ponudnik ščitil uporabnika (Privacy rights clearinghouse 2008).

6 SKLEP

S povezavo več računalnikov medsebojno v omrežje, lokacija ter čas nista več tako pomembna faktorja pri pridobivanju nekaterih podatkov, kot sta bila nekoč. Računalnik na enem koncu lahko brez težav komunicira z računalnikom na drugem koncu sveta. Ideja, da lahko uporabnik kadarkoli dostopa do različnih podatkov, storitev ter aplikacij, je gonilo razvoja IKT-ja.

Vedno bolj se v splošni uporabi pojavljajo elektronske komunikacijske naprave, ki omogočajo posamezniku dostop do interneta ter raznih spletnih storitev. Dandanes si ne predstavljamo več, da je nekdo brez mobilnega telefona ali nedosegljiv, ko ga potrebujemo. Ni več sprejemljivo, da do nekih podatkov uporabnik v kratkem času ne more dostopati. Razpršeno računalništvo naj bi zagotavljalo, da bi vsakdo lahko dostopal do česarkoli, kjerkoli uporabljal katerekoli računalniške storitve ter lahko bil v vsakem trenutku povezan z oblakom, dokler ima pri sebi komunikacijsko napravo. Trend, ki ga jasno nakazujeta tudi razvoj računalnikov in mobilne telefonije.

Uporabniki zelo radi posežemo po novostih, po novih »igračkah«, ki nam jih prinese nova tehnologija. Ob tem pa se ne zavedamo v polni meri nevarnosti, ki nam potencialno pretijo. Večina ljudi se nikoli ni resno ukvarjala z vprašanjem, koliko se s priključitvijo na internet dejansko izpostavljajo. Razpršeno računalništvo bo tveganje poneslo na novo raven. Prepričan sem, da velika večina uporabnikov interneta danes ne ve, kje se nahaja njihova elektronska pošta, kje se podatki, ki jih shranjujejo na internetu, dejansko nahajajo ter kaj se z njimi dogaja, kdo lahko do njih dostopa in podobno.

Razpršeno računalništvo prinaša nove možnosti in nove prednosti, vendar prinaša tudi nove nevarnosti. S tem, ko uporabnik nima podatkov pri sebi, so ti bistveno manj varni, kot so bili prej. Uporabnik mora imeti veliko mero zaupanja v ponudnika oblaka, da izvaja vse potrebne preventivne ukrepe, ki ščitijo uporabnike. Če podatki niso zaščiteni, potem tudi posameznik ni varen. Že danes ponudniki storitev razpršenega računalništva ne morejo z gotovostjo trditi, kje se posamezni podatki nahajajo. Z uvedbo razpršenega računalništva se to ne bo bistveno spremenilo.

Uporabnik mora imeti podatke na voljo, ko jih potrebuje. Tudi dosegljivost podatkov je vprašljiva. MDC-ji niso stoodstotno odporni na razne izpade, ki bi onemogočili njegovo

delovanje. Zasnova MDC-jev je taka, da imajo ranljivost v eni točki dostopa. Ena povezava s strežniki, eno napajanje, en dovod vode. V načrtih kompleksov MDC-jev ni predvideno rezervno napajanjo, več komunikacijski povezav s strežniki, alternativa vodnemu hlajenju, če ta odpove, kar lahko privede do izpada MDC-ja. Prav tako bo količina podatkov v oblaku enormna, kar praktično onemogoči rezervne kopije vseh podatkov. In četudi bi obstajale kopije, kje bi bile in kdo bi izvajal nadzor nad njimi?

Žal hitrosti razvoja tehnologije ne sledi niti pravo. Nekateri avtorji poudarjajo potrebo po pravni ureditvi področja razpršenega računalništva tudi z promoviranjem Listine pravic (angl. Bill of rights), ki poudarja temeljne pravice uporabnikov in dolžnosti ponudnikov, vendar je Listina še daleč od sprejetja. Z novimi tehnologijami se pojavljajo tudi nove dimenzije ogrožanja, novi akterji ogrožanja ter tudi novi akterji zagotavljanja varnosti (Svete 2005, 32). Pravo bistveno zaostaja za razvojem računalništva na tem področju. Prav tako tudi razmišljanje uporabnikov.

Glede na ugotovljeno, lahko zaključim, da zaradi pomanjkanja ustreznih sistemov zaščite podatkov, programske in pravne, ter ranljivosti samih fizičnih kapacitet za zagotovitev razpršenega računalništva, le-to predstavlja določena varnostna tveganja in grožnjo varnosti posameznika. Hipotezo tako lahko v celoti potrdim.

7 LITERATURA

1. About.com. 2009. *Information Technology – Definition and History.* Dostopno prek: http://jobsearchtech.about.com/od/careersintechnology/p/ITDefinition.htm (2. avgust 2009).
2. Agre, Philip E. in Marc Rotenberg, ur. 2001. *Technology and Privacy: The New Landscape.* London: MIT.
3. Anderson, Ross. 2008. *Security Engineering: A guide to building dependable distributed systems.* Indianapolis: Wiley Publishing, Inc.
4. Armbrust, Michael, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica in Matei Zaharia. 2009. *Above the Clouds: A Berkeley View of Cloud Computing.* Dostopno prek: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf (14. avgust 2009).
5. Aul, William R. 1972. Herman Hollerith: Data Processing Pioneer. *Think.* Dostopno prek: http://www-03.ibm.com/ibm/history/exhibits/builders/builders_hollerith.html (12. avgust 2009).
6. Bellis, Mary. 2009. *The History of the Electric Telegraph and Telegraphy: The Beginning of Electronic Communication.* Dostopno prek: http://inventors.about.com/od/tstartinventions/a/telegraph.htm (12. avgust 2009).
7. Božić, Mile. 2003. *Zgodovina računalništva.* Dostopno prek: http://www.educa.fmf.uni-lj.si/izodel/sola/2002/di/bozic/PC_history/index1.html (12. avgust 2009).
8. Brodkin, Jon. 2008. *Gartner: Seven cloud-computing security risks.* Dostopno prek: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,1 (19. avgust 2009).
9. Butler, Jeremy G. 1998. *A History of Information Technology and Systems.* Dostopno prek: http://www.tcf.ua.edu/AZ/ITHistoryOutline.htm (11. avgust 2009).
10. Buzan, Barry. 1991. *People, states and fear.* New York: Harvester Wheatsheaf.
11. Fraber Consulting. 2002. *IT-Trends 2005-2010.* Dostopno prek: www.fraber.de/university/web_services/IT-Trends.2005-2010.ppt (16. avgust 2009).
12. Greengard, Samuel. 2008. *Top 10 Trends in IT for 2009.* Dostopno prek: http://www.baselinemag.com/c/a/IT-Management/Top-10-Trends-in-IT-for-2009/ (16. avgust 2009).

13. Hamilton, James. 2007. *An Architecture for Modular Data Centers.* Dostopno prek: http://arxiv.org/ftp/cs/papers/0612/0612110.pdf (18. avgust 2009).
14. Hiner, Jason. 2009. *Predicting the IT trends of 2009: What's in and what's out.* Dostopno prek: http://blogs.techrepublic.com.com/hiner/?p=903 (16. avgust 2009).
15. Hoffman, Paul. 1996. *Vse o internetu in World Wide Webu*. Prevod Oštir-Sedej Krištof. Ljubljana: Pasadena.
16. Honeycutt, Jerry. 1997. *Internet v uporabi.* Izola: DESK.
17. IBM. 2008. *Made in IBM Labs: IBM Announces European Cloud Computing Hub in Dublin.* Dostopno prek: http://www-03.ibm.com/press/us/en/pressrelease/23710.wss (14. avgust 2009).
18. *Internet World Stats*. 2009. Dostopno prek: http://www.internetworldstats.com/stats.htm (11. avgust 2009).
19. Jerman-Blažič, Borka. 1996. *Internet.* Ljubljana: Novi Forum.
20. Jones, Hallie. 2005. *Howard Hathaway Aiken.* Dostopno prek: http://www.thocp.net/biographies/aiken_howard.html (12. avgust 2009).
21. Kovačič, Matej. 2006. *Nadzor in zasebnost v informacijski družbi.* Ljubljana: Fakulteta za družbene vede.
22. Lai, Eric. 2008a. *Walking the talk: Microsoft builds first major container-based data center.* Dostopno prek: http://www.computerworld.com/s/article/9075519 (18. avgust 2009).
23. --- 2008b. *6 reasons why Microsoft's container-based approach to data centers won't work*. Dostopno prek: http://www.computerworld.com/s/article/9080738/ (18. avgust 2009).
24. Landoll, Douglas J. 2006. *The Security Risk Assessment Handbook.* New York: Auerbach Publications.
25. Laudon, Kenneth C in Jane Price Laudon. 1995. *Information Systems: A Problem-Solving Approach.* Philadelphia: The Dryden Press.
26. Leitold, Herbert. 2001. Integration of Security Services into Networks: Comparing TCP/IP-security and ATM-security. V *Advanced Security Technologies in Networking*, ur. Borka Jerman-Blažič, Wolfgang S. Schneider in Tomaž Klobučar, 77–93. Amsterdam: IOS Press.
27. MacManus, Richard. 2007. *10 Future Web Trends.* Dostopno prek: http://www.readwriteweb.com/archives/10_future_web_trends.php (16. avgust 2009).

28. O'Reilly, Tim. 2008. *Web 2.0 and Cloud Computing.* Dostopno prek: http://radar.oreilly.com/2008/10/web-20-and-cloud-computing.html (14. avgust 2009).
29. Pagon, Milan, Ivica Janjac in Igor Belič. 1997. *Modri internet: uporaba interneta na policijsko-varnostnem področju.* Ljubljana: Quatro-Gnosis.
30. Pahor, David. 1996. *Z miško po Internetu.* Ljubljana: Atlantis.
31. Pant, Durgesh in M K Sharma. 2009. *Cloud Computing.* Dostopno prek: http://www.csi-india.org/cloud-computing (14. avgust 2009).
32. Pike, John. 2008. *Echelon.* Dostopno prek: http://www.fas.org/irp/program/process/echelon.htm (22. avgust 2009).
33. Pinterič, Uroš in Malči Grivec, ur. 2007. *Informacijsko komunikacijske tehnologije v sodobni družbi: multidisciplinarni pogledi.* Nova Gorica: Fakulteta za uporabne družbene študije.
34. Privacy house clearinghouse. 2008. *Alert: The Privacy Implications of Cloud Computing.* Dostopno prek: http://www.privacyrights.org/ar/cloud-computing.htm (23. avgust 2009).
35. Program Združenih narodov za razvoj. 1994. *Human Development Report 1994: New dimensions of human security*. New York: Oxford University Press. Dostopno prek: http://hdr.undp.org/en/media/hdr_1994_en_chap2.pdf (10. avgust 2009).
36. Redshaw, Kerry. 1996. *Pioneers.* Dostopno prek: http://www.kerryr.net/pioneers/index.htm (12. avgust 2009).
37. Sharma, Prashant. 2008. *Core Characteristics of Web 2.0 Services.* Dostopno prek: http://www.techpluto.com/web-20-services/ (21. avgust 2009).
38. STA. 2009. EU v razvoj nove generacije mobilnih omrežij G4 za hitrejši prenos internetnih podatkov. *Dnevnik.si,* 18. avgust. Dostopno prek: http://dnevnik.si/novice/znanost/1042291918 (18. avgust 2009).
39. Strebe, Matthew, Charles Perkins in Michael G. Moncur. 1998. *NT Network Security*. San Francisco: Network Press.
40. Svete, Uroš. 2005. *Varnost v informacijski družbi.* Ljubljana: Fakulteta za družbene vede.
41. Tanenbaum, Andrew S. 1996. *Computer Networks.* New Jersey: Prentice-Hall, Inc.
42. Vogrin, Andreja, Iztok Prezelj in Bojko Bučar. 2008. *Človekova varnost v mednarodnih odnosih.* Ljubljana: Fakulteta za družbene vede.

43. Trček, Denis. 2006. *Managing Information Systems Security and Privacy.* Berlin, Heidelberg, New York: Springer.

44. Vurušič, Petra in Robert Vurušič. 2006. *Internetni kažipot.* Ljubljana: Tehniška založba Slovenije.

45. Webopedia. 2008a. *The Difference Between the Internet and the World Wide Web.* Dostopno prek: http://www.webopedia.com/DidYouKnow/Internet/2002/Web_vs_Internet.asp (22. avgust 2009).

46. --- 2008b. *The Five Generations of Computers.* Dostopno prek: http://webopedia.com/DidYouKnow/Hardware_Software/2002/FiveGenerations.asp (21. avgust 2009).

47. Whalen, David. 2002. *The Unofficial Cookie FAQ.* Dostopno prek: http://www.cookiecentral.com/faq/ (2. september 2009).

48. Whittaker, Jason. 2002. *The Internet: The basics.* London: Routledge.