poročilo

# MEDNARODNA POLETNA ŠOLA *IFIP 2009*

Peto mednarodno poletno šolo (IFIP Summer School)[1] so organizirali v Nici od 6. do 11. septembra 2009 v sklopu evropskega projekta PrimeLife[2] v sodelovanju z organizacijo IFIP (International Federation for Information Processing). Osnovna tema konference je bila zasebnost in upravljanje identitete v prihajajočih spletnih aplikacijah v celotnem življenju posameznika.

V teh dneh se je zvrstilo večje število predavanj, dve panelni razpravi in več vzporednih delavnic, na katerih so svoje prispevke predstavljali študenti. Za razliko od preostalih dni je prvi dan konference potekal v raziskovalnem centru Eurecom[3] v mestu Sophia Antipolis.

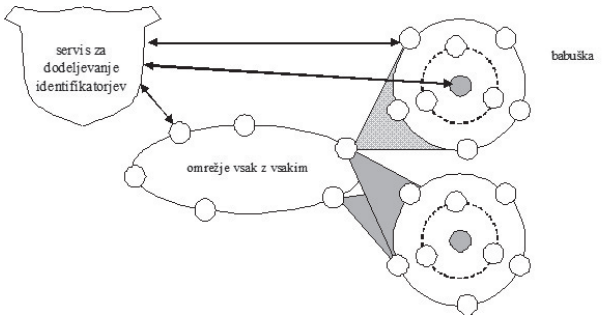
Konferenco je vodil Michele Bezzi (SAP Research) iz Francije.

**Refik Molva** (Eurecom) je predstavil zelo aktualno temo, in sicer nov model socialne mreže z imenom Safebook (*Safebook: a privacy-preserving peer-to-peer social network application*).

Hitra rast in priljubljenost spletnih socialnih mrež, kot so Facebook, MySpace in številne druge, vzbuja resne pomisleke glede varnosti in zasebnosti njihovih uporabnikov. Poleg običajnih ranljivosti spletnih podatkov se pri spletnih socialnih mrežah pojavljajo specifične težave v zvezi z zasebnostjo. Velika težava je ta, da je na enem mestu zbranih ogromno osebnih podatkov, ki jih je mogoče med seboj enostavno povezati. Vsi podatki so v večini primerov tudi trajno shranjeni in zanje skrbi kakšen komercialni ponudnik spletnih storitev. Ponudniki spletnih storitev lahko kadar koli dostopajo do njih in jih uporabljajo ali posredujejo po lastni volji, saj se vsi podatki shranjujejo in zbirajo centralizirano na enem mestu.

Predstavil je spletno socialno mrežo, ki preprečuje centraliziran nadzor in zbiranje podatkov. Struktura te mreže temelji na omrežju vsak z vsakim (angl. *peer to peer – P2P*). Omrežja vsak z vsakim izključujejo potrebo po centralnih strežnikih in omogočajo medsebojno komunikacijo posameznim računalnikom, ki so obravnavani kot enakopravni viri podatkov po principu "kdor sodeluje, tudi prispeva". Že struktura omrežja vsak z vsakim sama po sebi zaradi popolnoma porazdeljene narave preprečuje kakršen koli centralni nadzor ponudnika storitev. Pri običajnih mrežah je problem, da smo vidni le, kadar je naš računalnik priklopljen na splet. To bi odpravili tako, da bi posameznikove podatke hranili na več mestih, pri njihovih resničnih prijateljih, sosedih, znancih. Ti bi hranili kodirane podatke, vendar sami ne bi imeli dostopa do njih in z njimi ne bi mogli manipulirati. Okoli posameznika bi se tvorile tako imenovane babuške (rus. *matrjoška*, angl. *matryoshka*). Vsak bi bil del drugih babušk in bi tudi sam hranil podatke svojih prijateljev. Pri trenutnih socialnih mrežah se poleg osebnih podatkov hrani ogromna količina dodatnih podatkov o uporabnikih, njihovih navadah, ki so dostopne in trajno hranjene pri ponudnikih storitev, zato ti ponudniki postajajo veliki brat (angl. *big brother*). Kako pomembni so ti podatki, kaže cena, ki jo dosegajo ponudniki socialnih mrež. Tako je družba News corporation leta 2005 kupila Intermix Media, ki je lastnik MySpaca za 580 milijonov dolarjev,[4] vrednost Facebooka pa naj bi bila glede na posel z Microsoftom leta 2007 ocenjena na 15 milijard dolarjev.[5] Tudi težave s sledenjem, nepovezljivostjo podatkov, anonimnostjo in shranjevanjem vseh aktivnosti uporabnikov naj bi odpravili z enolično določenimi psevdonimi in identificiranimi vozlišči. Tudi ta rešitev ima svojo slabo stran, ker potrebujemo neki zaupanja vreden servis, ki bo dodeljeval enolično določene identifikatorje. Zasebnost bodo zagotovili s komunikacijo med posameznimi vozlišči, ki predstavljajo medsebojne prijatelje, njihove prijatelje itd. Pri skokih preko prijateljev so vezi skrite s pomočjo babuške. V osnovi je ta model spletne socialne mreže sestavljen iz treh komponent (gl. sliko 1):

- večje število babušk,
- omrežje vsak z vsakim (P2P),
- servis za dodeljevanje identifikatorjev.




Slika 1: Glavne komponente spletne socialne mreže

Več o Safebooku in podobnih temah si lahko preberete v člankih, ki so objavljeni na spletnih straneh Eurecoma.[6]

**Jan Camenisch** (IBM Zurich Research Laboratory) je predstavil temo o varovanju osebnih podatkov in zasebnosti v okviru razvojnega projekta PrimeLife, ki ga financira Evropska komisija *(Privacy Enhancing Cryptography: Theory and Practice)*.

V prvem delu predavanja je predstavil težave, ki se pojavljajo na področju anonimnosti, osebnih podatkov in zasebnosti. Težava je, da uporabniki želimo biti anonimni in identificirani, velikokrat oboje hkrati. Podobne težave se pojavijo na področju socialnih mrež, pri uporabi telefonov, raznih nakupovalnih in plačilnih kartic, osebnih izkaznic in drugih vsakodnevnih storitvah, ki nam jih ponuja okolje. Njihova vizija na področju zasebnosti, zaupanja in upravljanja z osebnimi podatki je, da lahko posamezniki v informacijski družbi delujejo in se medsebojno združujejo na varen in zanesljiv način, pri čemer ohranjajo nadzor nad svojo "zasebno sfero" (zasebnostjo). Problemi nastanejo, ker računalniki ne pozabljajo, shranjevanje podatkov je vedno cenejše in "rudarjenje podatkov" vedno bolj učinkovito. Težava je tudi v ljudeh samih, saj jih večina rada širi informacije, kar je danes enostavno in hitro. Zaradi tega postaja nadzorovanje informacij vse težje, vzpostavljanje zaupanja in varnosti pa še težje. Torej morajo biti zasebnost, identiteta in zaupanja vredno upravljanje z osebnimi podatki vodilo na vseh področjih.

V drugem delu je predstavil PrimeLifovo vizijo in pristop k težavam. Cilj je vzpostaviti trajno zasebnost in upravljanje z osebnimi podatki na področju prihodnjih omrežij in storitev. Za doseganje teh ciljev izvajajo pri PrimeLifu dejavnosti v šest glavnih sklopih:

1. *Zasebnost v življenju*. Glavna področja so zaupne vsebine, selektiven nadzorovan dostop v socialne mreže in upravljanje z osebno določljivimi podatki v resničnem življenju.
2. *Politika*. Raziskave ter razvoj novodobne politike in zahteve, ki jih je treba vključiti.
3. *Mehanizmi*. Glavna področja so kriptografija, preventivni ukrepi, zaščita podatkov in tudi zaščita uporabniško ustvarjenih podatkov.
4. *Uporabnost*. Naloga je ustvariti uporabnikom prijazne, zanesljive in zaupanja vredne vmesnike, ki bodo hkrati tudi enostavni za uporabo s strani upravljavcev.
5. *Infrastrukture*. Zgradba in sestava ponujenih storitev.
6. *"Zasebnost v živo"*. Stvari je treba predstaviti širši javnosti in z njo sodelovati, pomembno je tudi izobraževanje, uporaba odprtokodnih rešitev, standardizacija.

V tretjem sklopu je predstavil, kako si lahko s kriptografijo izboljšamo raven zasebnosti. Kriptografija se uporablja na različnih področjih, kot so anonimni elektronski certifikati, prikriti podpisi (angl. *blind signatures*), pozabljivi prenosi (angl. *oblivious transfer*), elektronska glasovanja itd. Na področju varovanja zasebnosti in osebnih podatkov si prizadevajo doseči stanje, da bo ob identifikaciji treba razkriti ali posredovati le minimalno zahtevane podatke. To želijo doseči s pomočjo zasebnih digitalnih certifikatov, ki bi jih vsakemu posamezniku dodeljevale ustrezne ustanove, ki bi lahko izdane certifikate v primeru potrebe tudi odvzele. Tako bi dobili certifikat za osebno izkaznico, ob opravljenem vozniškem izpitu, pri zavarovanju avtomobila in podobno. Podatke na certifikatih bi lahko sestavljali v nove enote, s katerimi bi posredovali le nujno potrebne podatke za določeno identifikacijo. V teoriji lahko za vse poskrbi kriptografija tudi s pomočjo pametnih kartic. V praksi je malo drugače in kljub temu da se zavest ljudi dviga, se podobni izdelki še ne uporabljajo razširjeno. Veliko tehnologij je pripravljenih za uporabo v praksi, vendar jih je treba pred tem narediti uporabne in prijazne do uporabnikov. Raziskave je treba usmeriti v razvoj uporabniških vmesnikov, infrastrukturo, kriptografijo in tudi politiko.

Tudi ta možnost zaščite osebnih podatkov in zasebnosti ni popolna, saj neke ustanove dodeljujejo certifikate, pri katerih lahko pride do zlorab, in tudi kar velja danes za dobro kodirano zaščito s pomočjo kriptografije, je lahko čez 10, 20 ali več let nezadovoljivo.

**Andreas Pfitzmann** (Tehniška univerza v Dresdenu) je predstavil problem vseživljenjske zasebnosti (*Lifelong Privacy*).

Zaradi globalnih digitalnih omrežij javne uprave, zasebna podjetja in posamezniki v vedno večji meri razkrivajo, shranjujejo, obdelujejo in uporabljajo osebne podatke. Družba nima izkušenj, kakšen vpliv bo to imelo na posameznikovo zasebnost skozi njegovo življenje, ker je obdobje, v katerem sta se razširili informacijska in komunikacijska tehnologija, veliko krajše od življenjske dobe ljudi. Vzdrževati zasebnost je že v kratkem časovnem obdobju težavno, družba pa se sooča s problemom dolgoročnega ohranjanja zasebnosti v nenehno

spreminjajočem se svetu. Zato preučujejo tveganje in opozarjajo na možne pravne ali tehnološke ukrepe, da bi se ustrezno spopadli z izzivom vseživljenjske zasebnosti.

Pri vseživljenjski zasebnosti imamo v mislih obdobje 100 let, kot je približno dolgo življenje posameznika. V tem obdobju se mi sami, svet in razne tehnologije hitro spremenijo in razvijejo. Podatki, ki so enkrat objavljeni na spletu, se skorajda ne morejo več izbrisati oziroma jih je skoraj nemogoče uničiti, zato se poraja vprašanje, kaj storiti. Za doseganje vseživljenjske zasebnosti posameznika potrebujemo:

- minimiziranje objavljenih osebnih podatkov,
- dolgoročne varnostne ukrepe.

Identiteta je veliko več, kot samo ime (ki si ga enostavno zapomnimo), identifikatorji (edinstveni) in načini preverjanja pristnosti (zaščita). Identiteta je predvsem nabor vrednosti oznak in lastnosti. Nekatere od njih se lahko skozi čas spreminjajo, nekatere nam dodelijo. Glede na to, da je zelo težko, če ne celo nemogoče izbrisati razširjene podatke, se digitalna identiteta kot nabor vrednosti veljavnih oznak poglablja. Da bi dosegli varnost in zasebnost morajo uporabniki razdeliti svojo identiteto v tako imenovane delne identitete, od katerih bi vsaka imela svoje lastno ime, lastne identifikatorje in lastna sredstva za preverjanje pristnosti. Uporaba delnih identitet pa zahteva osnovno razumevanje delovanja uporabnikov, vladnih organizacij in podjetij. Vsakdo bi potreboval vsaj en osebni računalnik, ki bi bil popolnoma pod njegovim nadzorom in preko katerega bi upravljal s svojimi osebnimi podatki in izvrševal kriptografske protokole. Potrebovali bi še digitalne psevdonime za varno preverjanje pristnosti in anonimne poverilnice za prenos certifikatov med posameznimi delnimi identitetami. Vsaka delna identiteta ima svoje identifikatorje in svoj namen izkazovanja. Vse osebne podatke je nemogoče zavarovati, zato je smiselno, da zavarujemo vsaj jedro identitete – podatke, ki jih ni mogoče preprosto spreminjati, ki se ne spreminjajo skozi čas (ali pa lahko njihovo spreminjanje napovemo), ki so nam dodeljeni, vsebujejo stranske informacije in so občutljivi.

**Sabrina De Capitani di Vimercati** (Univerza v Milanu) je predstavila deljenje in kodiranje podatkov o posamezniku *(Privacy of Data)*.

Osnovni problem zasebnih podatkov nastane zaradi povezovanja različnih podatkov, ki se navezujejo na eno osebo. Rešitev je v deljenju podatkov na več množic, npr. $R_1$ in $R_2$, ki skupaj sestavljajo celoto ali osnovno množico podatkov R ($R = R_1 \cup R_2$). Pri deljenju podatkov na več množic se te shranjujejo ločeno na različne strežnike. Pri tem morajo biti tudi podatki, ki se lahko medsebojno povezujejo, ločeni. Kadar podatkov ne moremo dovolj dobro ločiti, jih kodiramo s pomočjo kriptografije. Za povezovanje teh množic potrebujemo še neko identifikacijsko številko, ki nastopa v vsaki taki množici.

$$R_1 = \{ID, Ime, Spol, Poštna številka, Osebni dohodek^e\}$$
$$R_2 = \{ID, delovno\ mesto, e-naslov^e, telefon^e\}$$

***Primer:***
*Množico podatkov $R_1$ shranimo na strežnik $S_1$ in množico $R_2$ na strežnik $S_2$. Uporabnik dostopa do podatkov na dveh strežnikih, ki jih ob dostopu tudi dekodira.*

Pri takšnem shranjevanju podatkov se pojavita dve težavi. Prva je združevanje in drobljenje podatkov, druga pa kodiranje. Rešitev je ta, da se podatki razdrobijo na več posameznih množic in da so tudi kodirani. Torej je $F_i \subseteq R, \quad i = 1..., m$ in $F_i \to C_i \cup E_i$. V vsakem delčku so vsi kodirani podatki. Poizvedba oziroma iskanje podatkov pa se lahko izvede le na enem takšnem delčku, kjer dobimo vse podatke. Vsi delci so shranjeni na enem strežniku, in sicer tako, da jih med seboj ni možno povezati. Cilj je najti takšno delitev, ki bo omogočala poizvedovanje in ščitila posameznike, in ena možnost je deljenje podatkov na dva dela, pri čemer bi uporabnik imel del nekodiranih podatkov shranjenih pri sebi, drugi pa bi bili kodirani in shranjeni na oddaljenem strežniku.

**Ronald Leenes** (Univerza v Tilburgu) je predstavil zasebnost in družabnost na področju socialnih internetnih mrež (*Where the rubber meets the road*).

Socialne internetne mreže (angl. *social network sites – SNS*) v veliki meri opravljajo neko socializacijsko funkcijo povezovanja med ljudmi. Posamezniki na njih digitalno predstavljajo svojo identiteto in vezi med tako imenovanimi prijatelji. V zadnjem času uporablja te mreže vedno več delodajalcev, šol in univerz, ki preko njih črpajo podatke o svojih kandidatih.

Izpostavil je štiri bistvene smeri razprave: neobstoj povezave med uporabniki in fizičnim okoljem, permanentno hranjenje in prisotnost informacij, prepletanje več fizičnih in virtualnih okolij in sklepanje o soljudeh na osnovi njihovega profila. Podal je tudi tri domnevne razlage, zakaj je uporaba SNS tako razširjena. Uporabniki naj ne bi bili dovolj osveščeni, da je uporaba SNS tvegana. Osveščenost uporabnikov naj bi se dvigala, kljub temu pa moramo začeti izobraževati predvsem mladostnike, saj med njimi prevladuje prepričanje, da ne komunicirajo s komer koli, ampak s prijatelji, in v tem javnem okolju zahtevajo neko zasebnost. Kot tretje je navedel, da uporabniki (predvsem mladostniki) nimajo izbire, saj če niso prisotni v teh mrežah, niso "in" (v smislu: ker nisi na MySpace, ne obstajaš) in zaradi tega trpi njihov osnovni "socialni kapital". Zavedati se moramo, da mladostnikom dom ne predstavlja privatne sfere in da nadomestilo zanjo

ponujajo socialne mreže, ki jim dajejo občutek zasebnosti. Napredek je po Leenesovem mnenju v povečanju varnosti in nadzoru oziroma preprečitvi dostopa do podatkov ponudnikom internetnih mrež ali platform. To bi dosegli z dodatkom Firefoxa, ki bi skrbel za pregledno šifriranje podatkov. Posamezne podatke bi lahko dešifrirali le pripadniki posameznih skupin oziroma le določeni uporabniki. Kriptografiranje besedila naj bi bilo na voljo v začetku leta 2010 in naj bi se uporabljalo na vseh SNS-jih. Izpostavil je dejstvo, da se ljudje v resničnem življenju razlikujemo glede na različno področje. Tako na delu, med prijatelji, v trgovini itd. ne nastopamo z enako identiteto (podobo), ampak jo vsaj do neke mere spreminjamo. Na spletnih mrežah pa nastopamo vedno kot celota in tu se naše različne identitete združijo v eno. Potrebovali bi možnost, da v eni spletni mreži nastopamo z različnimi podobami. Imeli bi lahko ločene profile za službo, prijatelje, hobije ... in bi lahko stvari tudi ločeno objavljali za posamezne skupine, s tem pa ohranjali svoje različne javne podobe. Člane bi ločevali na podlagi Elgg (odprtokodne platforme za socialne mreže), dostop bi bil urejen na podlagi pravilnika, ki vključuje skupine in posamezne priključke.

**Eleni Kosta** (Katolišča univerza Leuven) je predstavila pravni pristop k socialnim mrežam *(Freddi Staurs of Social Networking – A legal approach)*.

Omenila je zanimivo raziskavo družbe Sophos, v kateri so prikazali nepazljivost posameznikov pri posredovanju svojih osebnih podatkov. Na Facebooku so ustvarili namišljeni profil *Freddi Staurs*[7] in preko njega vzpostavili kontakt z 200 naključnimi uporabniki. Okoli 40 % teh uporabnikov je bilo pripravljenih posredovati svoje osebne podatke (e-poštni naslov, popoln datum rojstva, naslov, izobrazbo, delovno mesto ...) neznani osebi, ki bi jih lahko zlorabila za kloniranje njihovega profila. Predavateljica je poudarila, da profili in objavljeni podatki na internetnih mrežah niso realne slike posameznikov, saj lahko tudi drugi objavljajo stvari o nas samih.

V nadaljevanju je podala neke vrste definicijo osebnih, občutljivih podatkov. Osebni podatki so informacije, ki se nanašajo na določeno ali določljivo fizično osebo. Občutljivi podatki so podatki, ki kažejo na rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje, sindikalno članstvo in predelavo podatkov v zvezi z zdravjem ali spolnim življenjem. V socialne internetne mreže bo treba vpeljati tudi nadzor, ki ga bodo lahko opravljale fizične ali pravne osebe, javni organi, agencije ali kateri koli drug organ, ki sam ali skupaj z drugimi določa namen in način obdelave osebnih podatkov. Trenutno nadzorujejo in upravljajo podatke v socialni mreži kar ponudniki storitev. Oni zagotavljajo vse potrebno za obdelavo uporabniških podatkov, ponujajo osnovne storitve za upravljanje in odločajo o uporabi zbranih podatkov. Z našimi podatki pa lahko upravljajo tudi ponudniki raznih zunanjih aplikacij, ki niso del teh mrež, če mi te aplikacije zaganjamo oziroma jim dovolimo dostop do nekaterih naših podatkov. Poraja se vprašanje, ali lahko vsak posameznik nadzoruje svoje podatke.

Obdelavo osebnih podatkov ureja direktiva o varstvu podatkov, iz katere je izvzeta obdelava osebnih podatkov, ki jih pridobijo fizične osebe z njihovo popolnoma zasebno ali vsakdanjo aktivnostjo. V tem primeru mora biti opredeljen namen zbiranja in obdelave podatkov in pridobljeno mora biti soglasje.

Po 29. členu direktive EU je bila ustanovljena Delovna skupina za varstvo posameznikov pri obdelavi osebnih podatkov, splošno znana kot Article 29 Working Party.[8] Delovna skupina želi uskladiti uporabo pravil o varstvu podatkov po vsej EU in objavlja mnenja in priporočila za varstvo podatkov o različnih temah. Ta delovna skupina navaja, da obstaja izjema, kadar je profil SNS javen in kadar lahko podatke indeksirajo iskalni programi. Izjema so podatki, zbrani za novinarske namene ter umetniško ali literarno izražanje.

Da se kot uporabniki strinjamo z obdelavo naših osebnih podatkov, je dovolj naša privolitev in strinjanje s pogoji. V praksi en klik pomeni, da soglašamo, da se naši podatki lahko uporabljajo za neposredno trženje, morebitno posredovanje drugim strankam, pregledovanje naših profilov in uporabo občutljivih podatkov. Tako npr. Facebookov pravilnik o zasebnosti[9] navaja, da lahko Facebook zbira informacije o vas tudi iz drugih virov, kot so časopisi, dnevniki, spletni dnevniki, in od drugih uporabnikov Facebookovih storitev z namenom, da bi vam ponudili več koristnih informacij, ki bi temeljile na bolj osebnih izkušnjah. Vprašanje je, koliko uporabnikov raznih spletnih aplikacij si je prebralo pristopne izjave in koliko od njih bi se odločilo za uporabo storitve, če bi vse prebrali. Predlaga, da bi pri nastavitvah zasebnosti morala biti privzeta najvišja možna varnost oziroma bi bila uporabljena zasebnosti prijazna nastavitev. Druge možnosti so vpeljava roka veljavnosti podatkov in profilov, vpeljava kodeksov ravnanja itd. Pri roku veljavnosti bi se po njegovem poteku, če ga ne bi obnovili, izbrisal uporabniški račun skupaj z vsemi nanj vezanimi podatki.

**Caspar Bowden** (Microsoft EMEA) je predstavil problematiko dostopa posameznika do osebnih podatkov, ki jih ima nekdo zbrane o njih *(Improving the implementation of the right of data subject access)*.

Po zakonu ima vsak posameznik pravico do vpogleda v svoje osebne podatke, ki jih ima zbrane neka družba. Pri tem se velikokrat pojavijo različne težave, od zavlačevanja do posredovanja nepopolnih podatkov itd. Močni lobiji velikih družb preprečujejo, da bi se sprejeli in zapisali zakoni o varstvu osebnih podatkov, ki bi začeli veljati tudi na področju svetovnega spleta. To je v

veliki meri zato, ker ponudniki zbirajo naše podatke in podatke o zgodovini našega brskanja po spletu tudi po več let in s tem pridobijo zelo dragocene podatke (vedo, kako mi funkcioniramo in kaj nas zanima). Poudaril je, da bi nam moral biti omogočen vpogled v naše podatke, kjer bi moralo biti vidno, kdaj in kdo jih je zahteval ali pregledoval. Morali bi imeti pravico do vpogleda v kriterije in postopke, po katerih nas ocenjujejo in tudi pravico vedeti, kakšna je njihova ocena o nas. Kot primer preprečevanja konkurenčnosti je omenil, da bi posamezniki morali imeti možnost prenosa vseh svojih podatkov pri zamenjavi ponudnika internetne storitve, kot je e-pošta ali kaj podobnega. Trenutno ljudje zelo redko menjajo različne ponudnike storitev, ker je treba pri menjavi vse stike, podatke itd. prenesti ročno.

**Wainer Lusoli** (JRC Sevilja) je predstavil pravne, tehnične in ekonomske vidike osebnih podatkov *(Write privacy read identity: legal, technical and economic aspects of a new regulatory framework).*

Pravna osnova za varovanje podatkov in zasebnosti v telekomunikacijah je v EU enotna, vendar pa področje identitete ureja državna zakonodaja. Med uporabo raznih spletnih storitev in našo varnostjo je treba najti neki kompromis. Naša e-identiteta ali digitalna identiteta je aktivna oziroma se nenehno spreminja in dopolnjuje. Ljudje se v splošnem ne zavedamo svojih digitalnih pravic, zaradi česar se tudi stanje na tem področju ne spreminja kaj dosti. V prihodnosti bodo družbe pripravljene plačevati za uporabo naših osebnih podatkov, s katerimi danes dobro služijo ponudniki spletnih storitev, in prej ko se bomo začeli zavedati tega, prej se bo trg digitalnih identitet sprostil in uredil.

Trenutno obstajajo tri vrste trgov digitalnih identitet:

1. Svetel trg (angl. *bright market*) je legalen in pod kontrolo države, ki nam izdaja potne liste, osebne izkaznice itd.
2. Senčni trg (angl. *shadow market*) je treba dobiti pod nadzor, saj se tam zakoni kršijo in zaobidejo.
3. Črni trg (angl. *black market*) je področje, kjer organizacije in tudi državni organi nadzirajo posameznike, jih zalezujejo in zbirajo razne podatke na nelegalen način.

Konkretne vrednosti zbranih podatkov za posamezne družbe, države ali celo posameznike še ne poznamo in tudi o trgih digitalnih identitet nimamo prave predstave. Treba je vložiti še dosti truda, da se bodo te stvari normalizirale in bodo vsaj do neke mere pod nadzorom. Treba je povečati pritisk na industrijo, ki bo povečala samokontrolo (ponudila varne strani za otroke ...). Treba je postaviti določene standarde, ki se jih bodo industrija in ponudniki spletnih storitev morali držati. Treba je dvigniti zavest ljudi, da se bodo zavedali nevarnosti, ki se pojavljajo na spletu. Potreben je tudi razvoj različnih tehnologij, ki bodo omogočale diskretnost posameznikom itd.

Za varovanje in urejanje osebnih digitalnih identitet obstajajo tri možne poti razvoja:

- urejanje z zakoni,
- urejanje s strani uporabnikov samih,
- urejanje s strani sistemov samih.

Velik poudarek v njegovi predstavitvi je bil namenjen trgovanju z osebnimi podatki. S podatki trgujejo velike družbe, kar predstavlja kar velik finančen zalogaj in je trenutno zelo neurejeno področje, uporabniki oziroma "lastniki" podatkov pa od tega nimajo nič.

**Charles Raab** (Univerza v Edinburghu) je predstavil načela o zasebnosti za upravljanje z identitetami *(Privacy Principles for Identity Management)*.[10]

Načela ali temelji za področje zasebnosti so potrebni, da nam dajo neke smernice za javne servise, da se izboljša varnost na področju upravljanja s podatki in da se dvigne zavest ljudi na področju zbiranja in hranjenja podatkov (kdo hrani podatke, kateri podatki so to in za kaj so uporabljeni). Ta načela naj bi povečala zaupanje v upravljanje osebnih podatkov in se navezujejo na:

1. *Dokazovanje identitete in upravičenost identifikacije*. To pomeni, da se identificiramo oziroma izkažemo svojo identiteto le, kadar je nujno potrebno in so takrat zahtevani in podani minimalni možni potrebni podatki. Treba je zagotoviti varno in uporabno identifikacijo, pri čemer se je potrebno izogniti izločanju in diskriminaciji.
2. *Upravljanje in odgovornost*. Vse, ki opravljajo javne storitve, tudi v zasebnem in prostovoljnem sektorju, je treba s pogodbami zavezati k spoštovanju teh načel in zagotoviti varno uporabo. Na zasebnost je treba gledati kakor na osnovno pravico.
3. *Obvladovanje in soočanje s tveganji*. Danes sta zaradi novih tehnologij dostop in pridobivanje informacij postala zelo enostavna. Zaradi tveganja je treba presoditi o vplivih na zasebnost, da zagotovimo nove pobude za določanje in izpostavljanje spornih vprašanj glede zasebnosti.
4. *Upravljanje in izmenjava podatkov*. Družbe bi se morale izogibati centralnemu zbiranju osebnih podatkov. Hranjenje osebnih podatkov in prenosljivih podatkov (naše delovanje, zgodovina spletnega brskanja) mora biti ločeno. Postaviti bo treba strožje kriterije in zahteve za dostop do podatkov in njihovo uporabo.
5. *Izobraževanje in vključevanje*. Javne institucije morajo pojasniti, zakaj določene informacije

potrebujejo in za kaj jih bodo uporabili ali posredovali. Treba je dvigniti javno zavest glede identitete in nevarnosti, s katerimi se na tem področju soočamo. Javnost je treba bolje informirati, da bodo ljudje z boljšim razumevanjem lahko sprejemali varnejše odločitve glede svoje identitete.

Ob vsem naštetem se postavi vprašanje, ali je to sploh uresničljivo ali pa so to samo utopične želje.

**Angela Sasse** (University College London) je predstavila upravljanje podatkov kakor posel *(Why Less Data Means Better Business )*.

V preteklosti se je na zasebnost gledalo v glavnem z legalne in etične plati. V poznih devetdesetih letih je postal z raziskavami Anne Adams pogled na zasebnost uporabniško osredotočen. Zavedati se moramo, da sami podatki niso kritični, kritična je dejavnost, ki se izvaja na podlagi pridobljenih informacij preko zbranih podatkov, zato je treba zaščititi poleg podatkov tudi uporabnike. Ključno tveganje, s katerim se srečujemo, so nepravilne interpretacije podatkov, netočnosti, motnje, sekundarna raba podatkov, ki se je v večini primerov ne zavedamo, razne zlorabe, nenamerno odtekanje podatkov itd. Urejanje s predpisi na področju varstva podatkov ni dovolj, vedno več uporabnikov ne verjame, da se bodo njihovi podatki hranili varno, zato želijo, da v primeru kršitve ali zlorabe odgovorni tudi odškodninsko odgovarjajo. Zaradi težav, ki se lahko pojavijo, so uporabniki začeli dajati lažne podatke, ne želijo uporabljati raznih storitev (izberejo možnost, da npr. v telefonskem imeniku ne objavijo svoje številke) in poskušajo sami nadzirati svoje podatke. Na področju ovrednotenja z vidika vseh zainteresiranih strani podatkov poteka v Veliki Britaniji projekt Privacy Value Networks Project.[11] Cilj projekta je izraziti vrednost podatkov z vidika vseh vpletenih strani in izdelati model, s katerim bi izboljšali pregled nad stroški in koristmi za različne zainteresirane strani. Vrednotenje informacij poteka od zbiranja preko hranjenja, vrednotenja, obdelave in na koncu prezentacije podatkov. Dejansko ljudje posredujejo vedno manj podatkov, in še to nekakovostnih podatkov in sprejemajo različne ukrepe, da se zaščitijo. Prihaja do razhajanj med zbranimi podatki in realnostjo, zato je tudi vrednost teh podatkov vedno manjša. Pojavijo se poslovne koristi in tudi stroški za uporabo, hranjenje in obdelavo podatkov. Treba bo ponovno razmisliti o pristopu k zbiranju, obdelavi in shranjevanju podatkov in kako vse skupaj vpliva na uporabnike. Zakorakati bo treba v smeri pravičnega in gospodarsko koristnega načina obdelave podatkov.

## ZAKLJUČEK

Hiter razvoj in nove smeri razvoja interneta predstavljajo vedno večjo dilemo na področju osebnih podatkov in zagotavljanja zasebnosti. Tako so v sodobni informacijski družbi potrebe posameznika po ohranitvi nadzora nad lastnimi osebnimi podatki in zaščiti svoje samostojnosti vedno večje. Posameznik vedno težje nadzira podatke, ki se navezujejo nanj, še posebej težavna pa je odstranitev zastarelih ali neželenih podatkov, da le-ti ne bi ostali trajno shranjeni in izpostavljeni. Teh potreb posameznika informacijske in komunikacijske tehnologije oziroma ljudje, ki o njih odločajo, jih razvijajo in so odgovorni za njihovo implementacijo, skorajda ne upoštevajo in s tem v veliki meri izpostavljajo in ogrožajo posameznikovo zasebnost. Na tem mestu naj dodamo, da se je v času nastajanja poročila na straneh spletne socialne mreže Facebook le zgodil premik na bolje. Izboljšali so varnost na področju izmenjave informacij, tako da posameznikom omogočajo nadzor nad tem, kako delijo svoje podatke na Facebooku. Poleg tega splet omogoča posamezniku, da sestavi svojo aplikacijo ali ponudi neko storitev in s tem tudi prispeva k distribuciji podatkov oziroma informacij. Vse to je znatno povečalo zahteve po zasebnosti s tehničnega, socialnega, pravnega in etičnega vidika. V to smer iskanja rešitev je bila naravnana tudi ta poletna šola. Poudarek je bil na izpostavljanju težav in problemov, podane so bile različne smeri razvoja in možne izboljšave. Predstavljenih je bilo tudi nekaj konkretnih rešitev, ki pa imajo po našem mnenju skupno slabo stran, da vedno potrebujejo neko organizacijo ali neko tretjo stranko, ki ji je treba zaupati in ki lahko zlorabi naše podatke. Postavlja se vprašanje, kdo naj bo ta stranka zaupanja? Morda kakšna državna organizacija, neki komercialni ponudnik ali morda kdo drug?

Nekateri od omenjenih prispevkov in večina predstavitev z delavnic bo objavljenih v zborniku referatov.

## Opombe

1 http://www.it.kau.se/IFIP-summerschool/
2 http://www.primelife.eu/
3 http://www.eurecom.fr/
4 http://news.bbc.co.uk/2/hi/business/4695495.stm
5 http://www.microsoft.com/Presspass/press/2007/oct07/10-24FacebookPR.mspx
6 http://www.eurecom.fr/people/molva.en.htm
7 http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html
8 http://www.dataprotection.ie/ViewDoc.asp?fn=/documents/european/article29.htm&CatID=31&m=u
9 http://www.facebook.com/policy.php#INFO_USE
10 http://www.scotland.gov.uk/Publications/2009/08/PrinciplesConsultation
11 http://www.pvnets.org/

Stanislav Pavlič