

UNIVERZA V LJUBLJANI  
FAKULTETA ZA DRUŽBENE VEDE

Sara Jevtić

**Varovanje osebnih podatkov na internetu  
(analiza primera: Socialno omrežje Facebook)**

Diplomsko delo

Ljubljana, 2011

UNIVERZA V LJUBLJANI  
FAKULTETA ZA DRUŽBENE VEDE

Sara Jevtić

Mentorica: red. prof. dr. Danica Fink-Hafner

**Varovanje osebnih podatkov na internetu  
(analiza primera: Socialno omrežje Facebook)**

Diplomsko delo

Ljubljana, 2011

## ZAHVALA

*»Izraziti hvaležnost. Izpovedati jo. Tako, povsem iz srca. Izpovedati jo takrat, ko jo iskreno začutiš. Brez leporečja in narejenosti. Razodeti jo v vsej resnici, čisto odprto, tako kot se zjutraj razpre nebo in obsije z novo zarjo vso zemljo, brez pridržkov in senc.«*

Iskrena hvala staršema ker sta verjela vame!  
Bratec, hvala ker si to kar si...brez tebe ni mene!

Hvala prijateljem za družbo in motivacijo!

Red. prof. dr. Danica Fink-Hafner,  
brez vas, vaše podpore in motivacije...naslednji citat ne bi bil moje vodilo:  
*»Ne pudeat quae nescieris te velle doceri; scire aliquid laus est, pudor est nil discere velle.«*  
*"Naj te ne bo sram, ker želiš biti poučen o tem, kar nisi vedel; nekaj vedeti je ponos, sramota je, če se nočeš ničesar naučiti."*

Iskrena hvala!

## **Varovanje osebnih podatkov na internetu (analiza primera: Socialno omrežje Facebook)**

Zaradi vprašanja zasebnosti je Facebook težava in trn v peti mnogim analitikom in političnim strukturam. Predvsem gre tukaj za vprašanja varovanja zasebnosti in osebnih podatkov, saj je le-ta področje zaradi velikega števila uporabnikov in še večjega števila objavljenih vsebin pod velikim vprašajem. V diplomski nalogi sem obravnavala tematiko varovanja osebnih podatkov na internetu; delala sem analizo primera spletnega omrežja Facebook. Osredotočala sem se predvsem na javnopolitičen vidik, kjer sem raziskovala obstoj javnopolitičnega omrežja oziroma dejavnost le tega, če le-to sploh obstaja. Glede na to, da Facebooka ne moremo označiti kot javnopolitično omrežje, sem se osredotočila na področje varovanja osebnih podatkov, kjer je zakonodaja poznana in prav tako igralci, ki se s tematiko ukvarjajo. Pri analizi problematike sem uporabila že obstoječe raziskave, družboslovne intervjuje ter analizo zakonodaje ter dostopne literature. Za klasifikacijo javnopolitičnega omrežja sem ustvarila shemo odnosov in razmerij med igralci, katera je pokazala dinamiko stikov in odnosov v omenjenem omrežju.

**Ključne besede:** Varovanje osebnih podatkov na Facebooku, javnopolitično omrežje, Facebook, socialno omrežje, informacijska zasebnost.

## **Protection of personal data on the Internet (case study: Facebook social network)**

Because of the privacy issue, Facebook represents a big challenge and a problem for many analysts and political structures. Throughout the research, a question of privacy protection and personal data arose because of Facebook's large number of users and an even larger amount of content, published online. In my thesis, I have dealt with the subject of personal data protection on the internet through a case study of the Facebook social network. My main focus was on the public policy aspect of the observed issue, where I have researched the existence of the public policy network and the activity of the same. Considering the fact, that we cannot define Facebook as a public policy network, I have narrowed my research to the field of personal data protection, where the legislation as well as the players are accessible. While doing my analysis, I have applied the pre-existing researches, interviews and the analysis of the legislation and accessible literature. For a more surveyable classification of the public policy network I have created a scheme of relations among players, which has shown the dynamic of contacts and relations in the observed network.

**Key words:** protection of personal data on Facebook, public policy network, facebook, social network, information privacy.

## KAZALO

1	UVOD .....	6
1.1	RAZISKOVALNO VPRAŠANJE IN HIPOTEZA .....	8
2	ZVRST POLICY ANALIZE .....	9
2.1	RAZISKOVALNE METODE IN TEHNIKE .....	9
2.2	FAZE JAVNOPOLITIČNEGA PROBLEMA .....	10
2.3	IMPLEMENTACIJA ALI IZVAJANJE JAVNIH POLITIK .....	11
2.4	SPREMLJANJE IZVAJANJA JAVNIH POLITIK (monitoring).....	11
3	FACEBOOK IN DRUŽBENO POVEZOVANJE .....	12
4	VAROVANJE ZASEBNOSTI IN OSEBNIH PODATKOV .....	13
4.1	VAROVANJE OSEBNIH PODATKOV NA INTERNETU.....	15
5	KONCEPT JAVNOPOLITIČNEGA OMREŽJA .....	16
5.1	OPREDELITEV JAVNOPOLITIČNIH IGRALCEV IN AREN .....	17
5.1.1.	Nedržavni javnopolitični igralci.....	17
5.1.2.	Državni igralci (državne strukture) .....	18
6	FACEBOOK – Spletno socialno ali javnopolitično omrežje? .....	23
6.1	FACEBOOK KOT SOCIALNO OMREŽJE .....	25
6.2	FACEBOOK KOT JAVNOPOLITIČNO OMREŽJE VAROVANJA OSEBNIH PODATKOV .....	26
7	FACEBOOK IN VAROVANJE ZASEBNOSTI.....	28
7.1	KAKO JE MOGOČE ZBIRANJE OSEBNIH PODATKOV NA FACEBOOKU?.	29
7.2	HRANJENJE OSEBNIH PODATKOV NA FACEBOOKU .....	30
8	LEGISLATIVNA ZGODOVINA.....	31
8.1	KLJUČNI PRAVNI AKTI .....	33
9	RABA INTERNETA V SLOVENIJI – Spletne skupnosti 2010 .....	35
9.1	FACEBOOK IN SLOVENCİ – vidik varovanja zasebnosti .....	35
10	ZAKLJUČEK IN LASTNA ANALIZA .....	37
11	LITERATURA.....	42
	PRILOGE .....	46
	Priloga A .....	46
	Priloga B.....	49
	Priloga C.....	53
	Priloga Č.....	58
	Priloga D.....	59
	Priloga E.....	60

# 1 UVOD

Javni problemi kot taki ne nastanejo naenkrat in samostojno. Po mnenju nekaterih analitikov moramo najprej definirati kaj javni problemi sploh so. Temeljni kriterij za obstoj problema je razkorak med obstoječim družbenim stanjem in želenim stanjem. (Grdešić 1995, 57–58) Definirati javno politični problem pomeni poiskati razliko med tistim kar je, in tistim do česar želimo priti s svojim udejstvovanjem.

Pragmatičnost policy-analize od analitika zahteva da najprej preveri, ali je mogoče kaj storiti, ali se situacija lahko spremeni tako, da bo ustrezala interesom določevalca, javnega dobrega ali pravilom stroke. Če analitik pride do spoznanja, da alternativne rešitve ne obstajajo, takrat določevalcu predloži predlog kako naj se situaciji izogne. Če pa opredeli drugače in se odloči definirati javno politični problem, se spusti v nadaljnjo analizo. (Grdešić 2006, 96)

Zaradi vprašanja zasebnosti je Facebook težava in trn v peti mnogih analitikov in političnih struktur. Predvsem gre za vprašanja varovanja zasebnosti, saj je le-ta zaradi velikega števila uporabnikov in še večjega števila objavljenih vsebin pod velikim vprašajem.

Naj povzamem nekatere misli analitika Mitje Mavsarja, ki je v članku z naslovom »*ABC poslovne rabe FACEBOOKA*« v reviji Monitor iz oktobra 2008, zapisal takole:

*Težava, ki jo mnogi vidijo v Facebooku, je relativna javnost zelo osebnih informacij. V svojo mrežo po navadi najprej spustimo družino in osebne prijatelje. A kmalu se v njej znajdejo še znanci, poslovni partnerji, šefi. In prej ali slej nas za prijateljstvo prosi kdo, za katerega se niti ne spomnimo, da ga poznamo, pa se mu nočemo zameriti in torej prijateljstvo za vsak primer potrdimo. Še huje od vdora do naših osebnih informacij pa je, če se nam pripeti kraja identitete. Če za svojo spletno identiteto ne poskrbimo sami, bodo zelo mogoče, in morda ne ravno dobronamerno, to storili drugi. Povsem vsakdanji problem nastane, ko v splet naložimo slike in druge osebne informacije. Do nedavna tako ločevanje ni bilo mogoče, a pred kratkim je Facebook omogočil prav to. Vsak uporabnik zdaj sam nadzira dostopnost svojih osebnih informacij. Določen »osebni artefakt«, kot je fotografija, lahko torej »odpremo« po želji. (Mavsar 2008, 36)*

Pogoji uporabe storitev na Facebooku vsak dan bolj razširjajo pravice družabnega omrežja. Z uporabo storitve Facebooku dovoljujete, da vaše informacije, podatke in vsebine uporablja za

najrazličnejše namene, vključno s podlicenciranjem drugim ustanovam. Problem se kaže v tem, da si enake pravice jemljejo za vse te podatke **tudi po tem**, ko ste izbrisali svoj račun. Facebook zatrjuje, da spremenjeni pogoji uporabe odražajo dejansko uporabo njihove platforme in naj bi bili napisani bolj človeško in razumljivo, s katerimi bi Facebooku pridržali manj pravic, kot mu jih prejšnji. Ko po Facebooku nekomu pošljemo elektronsko pošto ne moremo pričakovati, da bodo naša sporočila izginila iz nabiralnikov vseh prejemnikov, tudi če smo svoj račun že izbrisali. (Walters 2009)

Raven zasebnosti je vseeno nekoliko drugačna, kar se lahko interpretira tudi kot nekaj pozitivnega. Ena od stvari, ki so jih družabna omrežja naredila je ravno to, da je distribucija informacij med posamezniki postala bolj učinkovita. Ko nekaj objavimo na Facebooku, nad tem preprosto nimamo več nadzora - če drugega ne, Facebook pridobi nad našo vsebino dokaj nerazumne pravice, ki jih lahko izkoristi, ali pa tudi ne. (Walters 2009)

V članku, objavljenem v časopisu Delo, avtorice Mojce Finc (Finc 2008), dr. Tanja Oblak Črnič pravi, da je pomembno dejstvo to, da uporabniki Facebooka delujejo v javnem prostoru, kjer so njihova dejanja javna in mnenja vidna, kljub temu, da nekateri mehanizmi varovanja zasebnosti obstajajo. Prav javnost podatkov in vidnost samih akcij uporabnikov, je po njenem mnenju bistvo socialnega omrežja.

Avtorica (Finc 2008) v članku še navaja, da snovalci Facebooka trdijo, da jim je zaščita oziroma ohranjanje zasebnosti ena od glavnih prioritiet, za katero se močno zavzemajo, a se kljub temu poraja vprašanje, koliko je uporabnikova zasebnost pravzaprav sploh zasebna. Urad za zaščito podatkov Evropske Unije opozarja, da socialna omrežja, kot je Facebook, dajejo uporabnikom le ohlapno zaščito. Do letošnjega februarja zapiranje oziroma brisanje osebnošnega profila na Facebooku denimo ni bilo mogoče. Avtorica se sprašuje ali je ta zagotovljena zasebnost zgolj navidezna? Ali je morda prerasla v javno zasebnost?

Podobna vprašanja kot avtorica si bom zastavljala tudi sama, saj me zanima, ali obstaja nadzor na osebnimi podatki na internetu ter posledično ali pomanjkanje nadzora vodi v vedno manjšo informacijsko zasebnost, oziroma vedno večjo javnost podatkov, objavljenih na spletnem omrežju Facebook.

## 1.1 RAZISKOVALNO VPRAŠANJE IN HIPOTEZA

### *Raziskovalno vprašanje se glasi:*

**R1:** *Zakaj v primeru varovanja osebnih podatkov na internetu (primer: Facebook), ni javnopolitičnega omrežja oziroma je le-to tako šibko in brez vpliva, da na omenjenem področju ne prihaja do sprememb?*

**R2:** *Zakaj ni potrebne javnopolitične pobude za regulacijo omenjenega problema, glede na to, da število afer na področju zlorabe uporabniških vsebin v omenjeni spletni skupnosti narašča?*

### *Hipotezo bom oblikovala na naslednji predpostavki:*

**H1:** *Na področju varovanja zasebnosti na internetu ne obstaja omrežje, ki bi se ukvarjalo z omenjeno tematiko, oziroma je tako šibko, da nima nikakršnega vpliva.*

**H2:** *Kljub naraščanju in vedno večjemu problemu varovanja osebnih podatkov ter zlorab le teh, javnopolitična pobuda na omenjenem področju, ki bi problem tudi zakonsko uredila, še vedno ne obstaja.*



## 2 ZVRST POLICY ANALIZE

Diplomska naloga predstavlja opisno policy analizo. Fink-Hafner (2007, 23) pravi, da opisna policy analiza opisno pojasnjevalna in proučuje znanje o policy procesu.

- *Osredotoča se na teorijo, odkriva vzročne zveze ter oblikuje tipologije*
- *Je razlagalna teorija*
- *Njen cilj je razumevanje javne politike*
- *Izbor raziskovalnih problemov je neodvisen*
- *Časovno obdobje izvajanja policy analize je relativno dolgo (navadno več let)*
- *Teži k znanstveni objektivnosti (glede na kriterij ponovljivosti)*

(Fink Hafner 2007, 23)

Svoj javnopolitični problem lahko uvrstim v **fazo izvajanja ali implementacije** javne politike. Spremljala sem izvajanje javne politike ter analizirala igralce, dinamiko med njimi ter proces izvajanja javne politike.

### 2.1 RAZISKOVALNE METODE IN TEHNIKE

Raziskava je temeljila na povzemanju ugotovitev že obstoječih raziskav, pregledu obstoječe zakonodaje, intervjujih z relativnimi igralci, na pregledu obstoječih člankov in na preučevanju dostopnih internetnih virov. Raziskava predstavlja študijo primera varovanja osebnih podatkov na spletnem omrežju Facebook, pri analizi pa sem se posluževala različnih metod. Za raziskavo je bilo v začetni fazi potrebno in pomembno, da sem s analizo zakonskih aktov in drugih dostopnih virov uspela identificirati glavne igralce in odnose moči med njimi ter tako na podlagi zbranih podatkov izrisala javnopolitično omrežje. Po tem je bilo potrebno pogledati časovni okvir, kako je omrežje funkcioniralo skozi čas in kako funkcionira sedaj, če le-to počne. Nadalje je bilo potrebno ugotoviti, kakšne so bile spremembe v omrežju in kako te spremembe vplivajo na oblikovanje stališča do same tematike, kar sem ugotovila s pomočjo družboslovnih intervjujev.

Družboslovne intervjuje sem opravila z:

- informacijsko pooblaščenko Natašo Pirc Musar,
- dr. Matejem Kovačičem, asistentom na FDV ter sodelavcem na Centru za raziskovanje javnega mnenja in množičnih komunikacij,
- Sašo Samardžičem, razvijalcem programske opreme pri podjetju SAOP poslovne rešitve.

## 2.2 FAZE JAVNOPOLITIČNEGA PROBLEMA

Izbrani javnopolitični problem *varovanja osebnih podatkov na internetu* lahko, glede na faze procesa oblikovanja in izvajanja javnih politik, uvrstim v fazo *implementacije* ali *izvajanja* javne politike.

Procesi oblikovanja in izvajanja javnih politik so empirični procesi. Prepoznamo jih predvsem po tem, da zajemajo administrativne, organizacijske in politične dejavnosti, s katerimi se oblikujejo in izvajajo javne politike. (Fink Hafner 2007, 19)

Med najbolj uporabnimi modeli za razumevanje znanosti o policy procesu je t.i. **procesualni model**.

*Procesualni model temelji na razumevanju procesa oblikovanja in izvajanja javnih politik kot zaporedja časovno ločenih in vsebinsko različnih faz, kot so identifikacija družbenih oziroma javno političnih (policy) problemov in oblikovanje političnega dnevnega reda, oblikovanje javno političnih alternativnih rešitev družbenega problema, uzakonitev (legalizacija) izbrane javno politične rešitve – navadno sprejem zakona, izvajanje (implementacija) javne politike, vrednotenje (evalvacija) učinkov javne politike. (Fink-Hafner 2007, 19)*

Zgoraj omenjene faze se v empiričnem političnem odločanju pogosto prepletajo. Odločilno vlogo igra prva faza tega procesa, to je faza javnega prepoznavanja družbenega problema in njenega uvrščanja na politični dnevni red. (Fink-Hafner 2007, 19)

## **2.3 IMPLEMENTACIJA ALI IZVAJANJE JAVNIH POLITIK**

Če govorimo o implementaciji, glede na proces političnega odločanja o javni politiki, opredeljujemo situacijo, ko izvršna oblast praviloma izvaja sprejetje javne politike, lahko pa to dejavnost prenese na zasebne igralce. Ko pa govorimo o zvrsti policy analize uporabne v določeni fazi pa govorimo o implementacijskih študijah, ki opredeljujejo spremljanje izvajanja javnih politik (monitoring) ter analizo igralcev in procesa izvajanja javnih politik. (Fink Hafner 2007, 25)

## **2.4 SPREMLJANJE IZVAJANJA JAVNIH POLITIK (monitoring)**

S tem procesom zbiramo podatke o tem, »kaj se dogaja, kako in zakaj.« (Dunn 1994, 403)

Ti podatki so nujno potrebni za poznejšo kvalitetno evalvacijo učinkov javne politike. Implementacijske študije lahko tudi opozorijo na težave v procesu izvajanja javne politike (problemi koordinacije, razdelitev pristojnosti, pomanjkanje določenih virov ipd.). (Fink Hafner 2007, 26)

Tako pridobljene informacije so uporabne za ugotavljanje, ali se politika odvija v smeri zastavljenega cilja, ali ključni igralci spoštujejo sprejete predpise in standarde, ali sredstva namenjena uporabnikom zares pridejo do tistih uporabnikom, katerim so namenjena. Pomagajo pri razlagi razlik med posledicami istih programov v različnih situacijah, zbiranjem indikatorjev in ugotavljanju možnih širših socialnih sprememb v družbi skozi daljše obdobje. (Grdešić 2006, 133–134)

Raziskovala sem implementacijo na izbranem primeru varovanja osebnih podatkov na Facebooku, kjer sem analizirala javnopolitično omrežje, ki že obstaja in tako ugotavljala zakaj se na izbrani tematiki ne stori več oziroma zakaj ne prihaja do sprememb.

### 3 FACEBOOK IN DRUŽBENO POVEZOVANJE

Novinarka Mojca Finc, avtorica članka »*Če nimaš svojega profila, ne obstajaš.*«, objavljenega v časopisu Delo, dne 22. junija 2011, je zapisala, da svoje spletno mesto uporabnik oblikuje z izbranimi osebnimi podatki, ki obsegajo izobrazbo, konjičke, zakonski stan in še mnoge druge osebne podatke, ob tem pa lahko doda še svojo fotografijo. Zbirko prijateljev dopolnjuje z iskalnikom, v katerega vpiše ime in priimek iskanega. Če je iskani dejaven na Facebooku, mu iskalec pošlje tako imenovano prošnjo za prijateljstvo. Novi prijatelj se vpiše v zbirko, ko s klikom na gumb potrdi, da želi postati del iskalčeve osebne mreže. Uporabnik postopoma širi krog prijateljev, jih obvešča, kaj neki trenutek počne, zapiše kakšen komentar na svoj javni zid, ki ga ima vsak, svoje fotografije, pod katere s prijatelji zapiše komentarje, umešča v galerije, objavlja zanimive videoposnetke, s prijatelji tekmuje v različnih igrah ter se pridružuje članom v različnih skupinah. Prijateljem lahko pošlje zasebno sporočilo, ko se prijavi v spletno mesto, se lahko s tistimi, ki so takrat dejavni, tudi takoj pogovarja. (Finc 2008)

Na spletni strani »What is social networking?« opredelijo sam pojem družbenega povezovanja kot obliko komunikacije 21. stoletja. Pravijo, da je družbeno povezovanje združevanje posameznikov v specifične skupine. Čeprav omenjeno povezovanje obstaja tudi prek osebnih stikov, posebno v šolah ter na delovnem mestu, je bolj aktualno prav povezovanje prek spleta, to pa zaradi tega, ker je za razliko od prizorišč, kjer se z drugimi posamezniki srečujemo osebno, svetovni splet poln posameznikov, ki želijo spoznati druge ljudi s približno enakimi interesi. Ko začnemo govoriti o spletnem družbenem povezovanju, so za omenjeni fenomen najbolj priročne spletne strani, ki jim pravimo družbene spletne strani, ki delujejo kot spletna skupnost uporabnikov interneta. Odvisno od spletne strani, le-te združujejo posameznike z istimi ali vsaj podobnimi interesi. Enkrat, ko postanemo del te mreže, se povezovanje lahko začne preko pregledovanja osebnih strani uporabnikov ali celo direktno komuniciranje z njimi. (What is social networking?)

Kot lahko opazamo obstajajo nevarnosti povezane z družbenim povezovanjem preko svetovnega spleta. Med grožnjami prevladujejo predvsem kraja podatkov, prenašanje virusov,

ki lahko ogrozijo sam sistem našega računalnika, ter pomembna predvsem za mlajše uporabnike, povezovanje in spoznavanje oseb, ki se izdajajo za nekoga, ki niso.

Vse grožnje, omejitve in mogoče rešitve sem prikazala in analizirala v poglavjih, ki sledijo.

Glede na to, da sam Facebook ne moremo opredeliti kot nek javno politični problem je bistvenega pomena to, da se zavemo, da preko njega izvira velika težava, ki močno posega v našo zasebnost. To je varovanje osebnih podatkov.

## 4 VAROVANJE ZASEBNOSTI IN OSEBNIH PODATKOV

Ko govorimo o zasebnosti gre tukaj pravzaprav za pravico do zasebnosti. Kot navaja Kovačič (2006, 37) je temeljni koncept same pravice možnost, da posameznik na določen način ravna, pravo pa pravice dodeljuje zato, da lahko posamezniki zadovoljujejo svoje interese. Cilj pravice je torej interes, pravo pa varuje tiste interese, ki so ovrednoteni kot pravno relevantni. (Pavčnik v Kovačič 2006, 37)

Večina literature o zasebnosti govori kot o pravici, ta pravica pa je navadno negativno definirana.

»Berlin negativno svobodo definira kot svobodo od, odsotnost vmešavanja, zato se negativno koncipirana svoboda nanaša na območje nadzora, ne na njegov vir. Gre za odsotnost prisile in vmešavanja drugih.« (Berlin v Kovačič 2006, 37)

*Brez politične svobode oziroma prisotnosti si le, če ti človeška bitja preprečujejo doseči namen. Sama nesposobnost doseči namen še ni odsotnost politične svobode. Neki del človeške eksistence mora ostati zunaj sfere družbenega nadzora. Zavzetje tega zatočišča, če je še tako majhno, bi bilo despotizem. Moramo ohraniti minimalno območje osebne svobode, če nočemo degradirati in zanikati svoje narave. (Berlin v Kovačič 2006, 37)*

V Berlinovem razumevanju negativne svobode je mogoče potegniti vzporednice s pomenom zasebne oziroma intimne sfere po Arendtovi. Avtorica poudarja pomen intimnega prostora pred vdorom družbenega v posameznika. Pravi, da gre za »prostor posameznika«, ki ga potrebujemo, da bi se zatopili v dialog s samim seboj takrat, kadar moramo misliti in razsojati, pri čemer avtorica tega prostora, v katerem naj bi pustili posameznika pri miru, ne

dojema samo kot privilegij filozofov, temveč ga hoče omogočiti vsakomur, ki želi postati politično bitje. (Jalušič v Kovačič 2006, 37)

Glede na vse povedano bi bilo smiselno, da si zastavimo vprašanje, kako obsežno naj bo to območje osebne svobode. Na to vprašanje Belin (Kovačič 2006, 37) odgovarja, da je to stvar razprave, ki se pod vplivom tehnološkega razvoja nadzorovanih tehnologij le še stopnjuje.

Razpravljanje o pravici do zasebnosti zadeva predvsem obseg te pravice, včasih pa se avtorji celo sprašujejo, ali je zasebnost sploh pravica, ali ne gre zgolj za interes. Gre za vprašanje koliko je možno »trgovanje« z zasebnostjo. Ta vidik je še posebej pomemben pri informacijski zasebnosti. (Kovačič 2006, 38)

Pravica do zasebnosti je sicer pogosto določena kot meja, do katere družba lahko vdre v posameznikove zadeve. (Laurant v Kovačič 2006, 38)

Kot ugotavljajo številni avtorji, je zasebnost zelo slabo definirana, dodaten problem pa predstavljajo še kolizije drugih pravic z zasebnostjo ter posledično vprašanje pod- in nadrejenosti posameznih pravic. Prav tako zasebnost prihaja v kolizijo z različnimi interesi, zaradi česar zasebnost ne more biti varovana zaradi pravnih in družbenih razlogov. Poleg tega je dojemanje zasebnosti s strani posameznika relativno – njeno dojemanje se razlikuje tako med posamezniki kot tudi glede na dani kontekst. (Wagner v Kovačič 2006, 38)

Nekateri avtorji so prepričani, da zasebnosti sploh ni, temveč gre le za pojem, za katerim se skrivajo različne bolj ali manj nepovezane pravice, oziroma da zasebnosti sploh ni mogoče definirati, saj naj bi bil problem zasebnosti v osnovi stvar vrednot, interesov in moči. (Gellman v Kovačič 2006,40)

Pri definiranju pravice do zasebnosti oziroma njenega obsega gre za regulacijo posegov v zasebnost, ne pa za določitev neke absolutne meje, ki je ni dovoljeno prestopiti. Zato pravo vedno le sledi razvoju tehnologije, ki omogoča nove in nove posege v zasebnost, hkrati pa sledi tudi razpoloženju v družbi, ki daje zasebnosti enkrat večjo, drugič manjšo težo. Kljub manjšim nihanjem meje v to ali ono smer pa družba zasebnost praviloma zgolj oži. (Lampe v Kovačič 2006, 40)

#### 4.1 VAROVANJE OSEBNIH PODATKOV NA INTERNETU

Kot navaja Kovačič (2006, 61), je glede varstva zasebnosti najprej potrebno ločiti različne akterje, ki sodelujejo v procesu izmenjevanja podatkov in informacij na internetu. Akterji so operater telekomunikacij, ponudnik dostopa do interneta, ponudnik internetnih storitev in uporabnik. Vsak od njih ima na voljo svoje mehanizme nadzora. (Kovačič 2003, 61)

Zakonodaja, ki ureja varovanje zasebnosti v realnem svetu, načeloma velja tudi v virtualnem svetu. Vendar pa se je treba zavedati, da internet ni prostorsko zamejen, kar ima lahko pri uveljavljanju uporabnikovih pravic zelo konkretne posledice. Posebej v primerih, kjer zakonodaja med državami ni usklajena, uporabnik pa se med uporabo interneta giblje na območju jurisdikcije različnih držav ali vstopa v interakcijo z globalno razpršenimi subjekti. (Kovačič 2003, 61)

Ker se je ustrezna regulativna zakonodaja interneta v 90. letih prejšnjega stoletja šele začela razvijati, so se nekateri uporabniki hitro zavedali pomena samozaščitnega ravnanja in razvoja ustrezne varnostne kulture. Kot navaja Kovačič (2006, 61) organizacija International Working Group on Data Protection in Telecommunications ugotavlja, da samozaščitno ravnanje samo po sebi ne more zagotoviti zasebnosti na internetu, pač pa je potreben tudi celovit pravni okvir, ki zagotavlja učinkovito varovanje osebnih podatkov na internetu. (Kovačič 2003, 61)

Problem varnosti in s tem tudi zasebnosti ni samo tehnični, pač pa tudi družbeni problem. To tudi pomeni, da bi se mogli uporabniki računalnikov bolj zavedati nevarnosti različnih zlorab, predvsem pa, kako se proti njim kar najbolje zavarovati. Predvsem pa se je treba zavedati, da varnost ni izdelek oziroma nekaj kar lahko kupimo, pač pa je proces. Varnostno kulturo je treba razvijati in gojiti neprestano. Pri tem si lahko pomagamo že z razumnim ravnanjem in s specializiranimi programi, ki so na internetu dostopni tudi brezplačno. (Kovačič 2003, 62)

## 5 KONCEPT JAVNOPOLITIČNEGA OMREŽJA

Omrežje v splošnem smislu pojmuje kot skupek vseh enot, povezanih z določenim tipom odnosov, oblikovanih prek povezav med igralci, ki (npr. na ravni javne politike) sodelujejo v procesih oblikovanja in izvajanja javnih politik. (Kustec-Lipicer 2002, 68)

Ključno pri opredeljevanju koncepta javnopolitičnega omrežja je zavedanje, da s konceptom spoznavamo, preučujemo omrežja odnosov med tistimi igralci, ki se vključujejo in oblikujejo proces oblikovanja in izvajanja politik. (Kustec-Lipicer 2002, 69)

Kot nujne in potrebne izhodiščne pogoje oziroma dimenzije za vzpostavitev javno političnega omrežja določamo:

PROBLEM: na osnovi določenega javnega problema neka javna politika šele začne nastajati, v smislu njenega oblikovanja. (Kustec-Lipicer 2002, 70)

IGRALCI: lahko prihajajo iz sfere državne ter civilne družbe. V okviru klasifikacije igralcev je treba upoštevati tudi njihovo medsebojno soodvisnost, kajti igralci državne narave pogosto potrebujejo igralce civilno družbene ravni, da jim slednji priskrbijo informacije, ki jih prvi nimajo. Nasprotno pa civilno družbeni igralci s pomočjo državnih lahko dobijo dovolj vpliva, ki ga potrebujejo za sam vstop v proces oblikovanja in izvajanja javnih politik. (Kustec-Lipicer 2002, 70)

VIRI: s katerimi igralci razpolagajo, kot denimo znanje, finančna sredstva, dohodki, stopnja izobrazbe, vpliv in moč, ne nazadnje pa tudi stopnja urbanizacije. (Kustec-Lipicer 2002, 70)

ODNOSI: med igralci, ki se večinoma vzpostavljajo na podlagi razpolaganja z viri in močjo. (Kustec-Lipicer, 70)

MEJE OMREŽIJ: omrežja pogosto prehajajo druga v druga. Zaradi nejasne določitve prostora delovanja posameznih javnih problemov se pogosto dogaja, da se omrežja različnih problemskih okolij na določenih točkah srečujejo oziroma prepletajo. (Kustec-Lipicer 2002, 71)



## **5.1 OPREDELITEV JAVNOPOLITIČNIH IGRALCEV IN AREN**

V vsakem procesu odločanja in oblikovanja javnih politik nastopajo javno politični igralci, arene in omrežja, s pomočjo katerih se javne politike izpeljejo do zelenega cilja.

Velikokrat zasledimo tudi tipološko razlikovanje med državnimi in civilno-družbenimi igralci. (Pal v Kotar 2007, 70)

Poimenovanje vsebinsko podobnih tipologij so sicer različna: institucionalni/neinstitucionalni igralci (Cahn v Kotar 2007, 50), ter uradni in neuradni oblikovalci politik (Anderson v Kotar 2007, 50). Razlika med naštetimi tipologizacijami leži v formalnem zakonitem pooblastilu, ki ga imajo državne strukture, da odločajo o javnih politikah.

Kot pravita Howlett in Ramesh (1995, 52) so igralci v policy procesu lahko posamezniki ali skupine. Za lažje razumevanje strukture igralcev v policy procesu, sta avtorja javno politične igralce razdelila v 5 kategorij:

- izvoljeni uslužbenci,
- imenovani uslužbenci,
- interesne skupine,
- raziskovalne organizacije (centri),
- množični mediji.

Prvi dve kategoriji se nanašata na državo, ostale tri kategorije pa se nanašajo na civilno družbo, skupaj pa oblikujejo osnovne elemente za policy analizo. (Howlett in Ramesh 1995, 52)

### **5.1.1. Nedržavni javnopolitični igralci**

Nedržavni javnopolitični igralci navadno sodelujejo pri oblikovanju politik, vendar pa njihove dejavnosti nimajo oblike zavezujoče odločitve za druge javnopolitične igralce, kajti sprejetje odločitve ali rešitve za določen javni problem je v rokah državnih javnopolitičnih igralcev. (Kotar 2007, 70)

Pri problemu varovanja osebnih podatkov na Facebooku gre za področje telekomunikacij, kjer v političnem omrežju delujejo različni igralci:

*Med nedržavne igralce bi lahko štela:*

- uporabnike svetovnega spleta,
- neodvisna združenja in interesne skupine, ki se jih omenjena problematika dotika (projekt SAFE, v organizaciji Centra za varnejši internet),
- ustanovitelje spletnih strani, ki od uporabnikov na takšen ali drugačen način zbirajo osebne podatke,
- civilna družba, saj je skoraj vsak žrtev kršenja informacijske zasebnosti na svetovnem spletu, sploh zaradi tega, ker smo se znašli v informacijski družbi, na katero nihče v svetovni ali slovenski skupnosti ni imun,
- SI-CERT, Slovenski center za posredovanje pri omrežnih incidentih.

### **5.1.2. Državni igralci (državne strukture)**

Državni igralci so predstavniki legalnih državnih organov in institucij. Za njih je značilno neko formalno zakonito pooblastilo, s katerim oblikujejo javne politike. (Kotar 2007, 50)

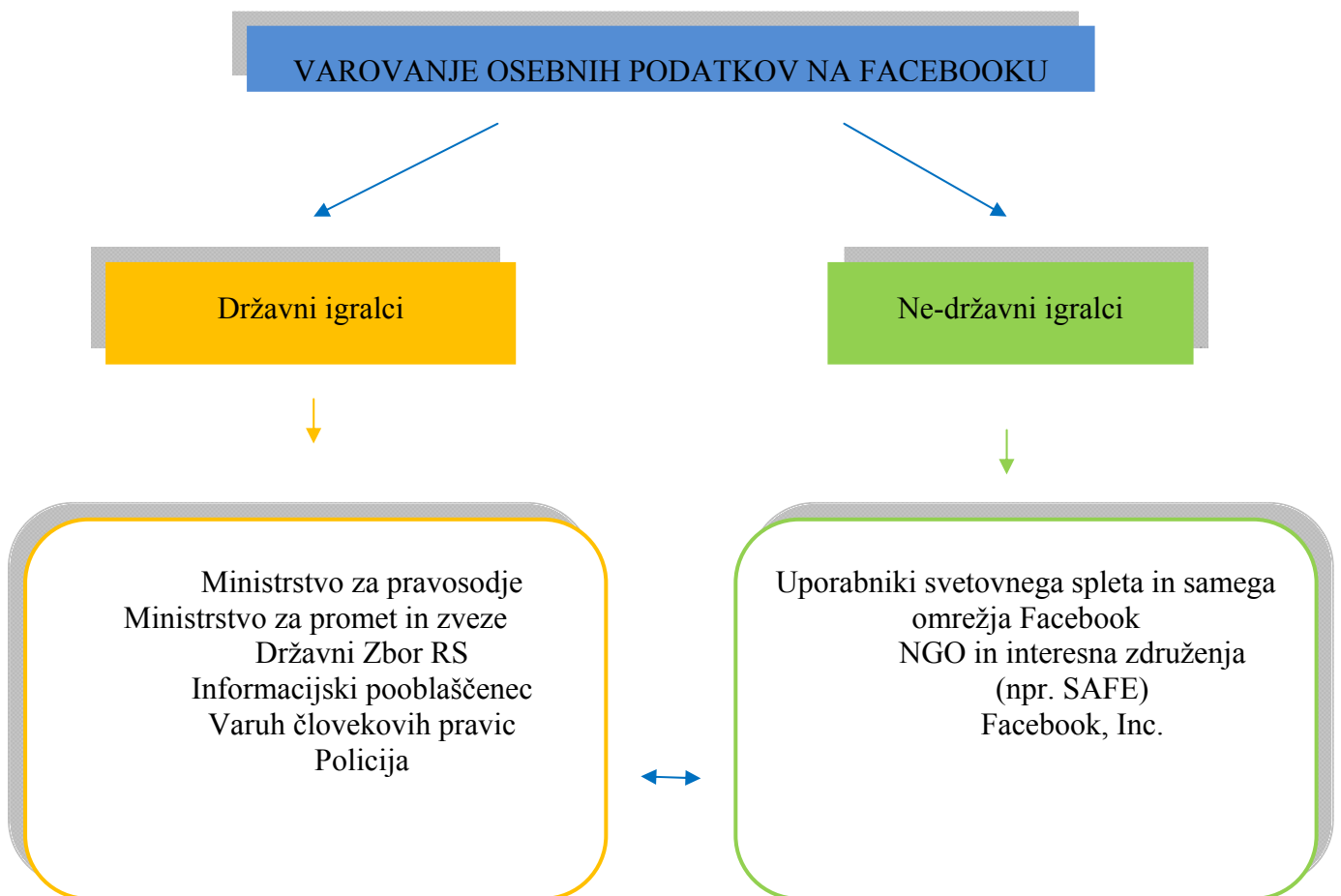
Kot javnopolitični igralec ima država veliko vlogo, kajti ljudje pričakujejo, da se država vpleta, angažira, sodeluje pri reševanju javnih problemov. V primerjavi z nedržavnimi javnopolitičnimi igralci so sredstva in pooblastila, ki jih ima na voljo država obsežnejša, kar nosi tudi večjo odgovornost. (Kotar 2007, 85)

*Med državne igralce bi lahko štela:*

- Informacijski pooblaščenec,
- Varuh človekovih pravic,
- Vlada RS, kot oblikovalka zakonov,
- Policija,
- Ministrstvo za promet in zveze,
- Ministrstvo za pravosodje.

Časovni potek interakcij, ter njihov prispevek je podan v prilogi E.

**Slika 5.1: Predstavitev policy omrežja, ki deluje na področju varovanja osebnih podatkov na primeru spletne skupnosti Facebook – tipologija igralcev**





## **Interpretacija sheme 5.2:**

V zgornji shemi je prikazan potek odnosov in interakcij med akterji, ki delujejo v javnopolitičnem omrežju varovanja osebnih podatkov na Facebooku.

Najprej sem akterje, ki prihajajo iz iste sfere barvno klasificirala. Državni javnopolitični igralci so opredeljeni v okvirjih oranžne barve, nevladne organizacije oziroma projekti nevladnih organizacij se nahajajo v okvirjih zelene barve, modro obarvani sta skupini, ki igrata, na področju varovanja osebnih podatkov na Facebooku, ključno vlogo; torej uporabniki spletnega omrežja ter ustvarjalci oziroma snovalci same spletne skupnosti, Facebooka. Vijolično obarvani okvirji pa predstavljajo ponudnike internetnih storitev, oziroma vse, ki so na kakršen koli drugi način povezani s samim delovanjem ter omogočanjem dostopa do svetovnega spleta.

Kot je razvidno iz sheme, je zgoščenost interakcij skoncentrirana na desnem predelu polja, kjer so prisotne nevladne organizacije, uporabniki in snovalci spletnega omrežja ter ponudniki internetnih storitev. Levi del polja, kot rečeno, predstavljajo državne institucije, ki pa, kot je že nakazano, v samem omrežju ne igrajo velike vloge. Nevladne organizacije poskušajo sodelovati z vsemi vpletenimi stranmi, a povratne komunikacije, razen z uporabniki Facebooka, ni. Razlog za takšno obnašanje tiči v tem, da so prav uporabniki spletnega omrežja tarče zlorab, ki so kakorkoli povezane z varovanjem osebnih podatkov.

Kot lahko opazimo, je komunikacija med upravljavci spletnega omrežja in ostalimi akterji šibka. Sodelujejo le z uporabniki, katere obveščajo o spremembah in dopolnitvah varnostnih pogojev in pogojev uporabe. Razlog za to je potrebno iskati v sami zakonodaji in obveznostih, ki jih spletno omrežje ima do drugih akterjev. Glede na to, da je bilo spletno omrežje ustanovljeno v ZDA, kjer, kot mi je povedal sogovornik Matej Kovačič (glej prilogo B), velja drugačna zakonodaja in drugačni predpisi glede same problematike.

Konflikt, ki samo tematiko opredeljuje kot problem, je torej ta, da je komunikacija in razvijanje odnosov v samem omrežju tako šibka, da omrežje ne more delovati oziroma, če že deluje, je njegovo delovanje zelo šibko in neučinkovito.

## 6 FACEBOOK – Spletno socialno ali javnopolitično omrežje?

Diplomska naloga temelji na predpostavki, da lahko rezultati oziroma končni produkt (v nadaljevanju osebni podatki) objavljeni na socialnem omrežju Facebook vplivajo na samo oblikovanje policy omrežja oz. dinamiko med igralci, ki so v posameznem omrežju vključeni.

### ***Definicija socialnega omrežja:***

Kot navaja Johnson (Johnson 2000, 207) pomeni termin socialno omrežje, kot osrednji pojem sociologije, zbirko odnosov, ki povezujejo ljudi, socialne statuse ali druge enote analize, kot so skupine ali formalne organizacije. (Johnson 2000, 207)

Na podlagi zgornje definicije lahko pojem socialno omrežje razširimo in povežemo s pojmom spletno socialno omrežje, saj Facebook prav tako združuje ljudi, skupine in organizacije.

### ***Definicija spletnega socialnega omrežja:***

Kot navaja Jernej Huber (2007), avtor članka »*Socialne mreže na internetu*« je spletno socialno omrežje širok pojem. Pomeni vsako spletno stran, ki ponuja komuniciranje z drugimi uporabniki ter pridobivanje novih stikov. Med socialne mreže lahko prištevamo najrazličnejše spletne storitve, od blogov pa do portalov za objavljanje slik. Pravi, da se najpogosteje s pojmom internetna socialna mreža označuje spletne storitve, na katerih je poudarek predvsem na pridobivanju oziroma širjenju socialnega kapitala bodisi v privatnem ali poslovnem življenju.

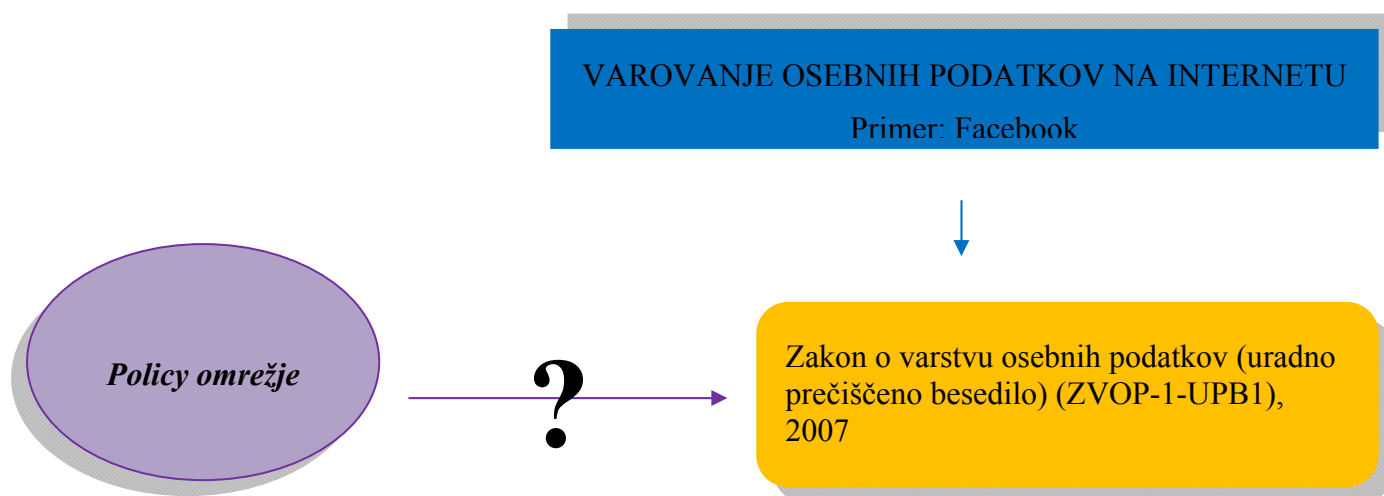
V socialnem omrežju torej sodelujejo uporabniki samih spletnih strani (primer uporabnikov Facebooka), ustvarjalci spletnih omrežij, ponudniki internetnih storitev ter vsi drugi akterji, omenjeni v poglavju 5.1.

### ***Definicija javnopolitičnega omrežja:***

»Omrežje v splošnem smislu pojmuje kot skupek vseh enot, povezanih z nekim določenim tipom odnosov, oblikovanih prek povezav med igralci, ki (npr. na ravni javne politike) sodelujejo v procesih oblikovanja in izvajanja javnih politik.« (Kustec Lipicer 2007, 88)

Torej kot navajajo Scharpf, Marin in Mayntzova (Marin in drugi v Kustec Lipicer 2007, 89) je javnopolitično omrežje koncept, ki s svojim obstojem predstavlja nove kvalitete v naravi odnosov med državo in civilno družbo, hkrati pa je tudi proces delovanja javnih politik.

**Slika 6.1: Prikaz poteka raziskave policy omrežja in odnosa, ki ga ima na proces urejanja in reguliranja problema varovanja osebnih podatkov na internetu, primer Facebooka.**



Zgornja shema prikazuje vprašanje povezave, če le-ta obstaja, med policy omrežjem in samim problemom varovanja osebnih podatkov na spletni mreži Facebook.

Na podlagi prebrane literature, ki je v diplomski nalogi le delno povzeta, sem prišla do zaključka, da policy omrežje obstaja, saj je omenjena tematika del že obstoječega policy problema, torej področja varovanja osebnih podatkov.

Če povzamem gospoda Kovačiča, ki je strokovnjak na področju informacijske zasebnosti lahko zapišem naslednje: »Država se je vedno trudila zbirati (osebne) podatke o posameznikih, vendar v preteklosti ni bilo na voljo posebne tehnologije za procesiranje, klasificiranje in povezovanje podatkov, ne nazadnje pa tudi avtomatsko (rutinsko) zbiranje le-teh. To se je spremenilo z razvojem informacijsko komunikacijske tehnologije (IKT), ki zaznamuje moderno družbo.« (Kovačič 2000, 1021.)

Čebulj (1992, 16) pa ugotavlja, da je bila zasebnost posameznika sicer ogrožena že pred uvedbo IKT in računalniških zbirk podatkov, da pa je nova tehnologija ogroženost zasebnosti še potencirala in privedla do tega, da so se ljudje nevarnosti pričeli zavedati bolj kot v času ročno vodenih evidenc.

Iz pravnega vidika za posameznika pomeni največjo nevarnost v zvezi z zbiranjem podatkov nenatančnost, napačnost, nepopolnost ali neažurnost zbranih podatkov. (Čebulj 1992, 8)

Drži, da sta omenjena avtorja svoje prispevke objavila že davno pred tem kot je bil Facebook sploh poslan na medmrežje, a določene trditve veljajo še danes.

## **6.1 FACEBOOK KOT SOCIALNO OMREŽJE**

Facebook je socialno omrežje, ki uporabnikom omogoča ustvarjanje svojega uporabniškega profila, povezovanje s prijatelji, pošiljanje sporočil, objavljanje fotografij ter igranje različnih iger. Je največje tovrstno omrežje z milijoni uporabniki iz celega sveta.

Tako organizacije kot posamezniki lahko uporabljajo Facebook, tako da ustvarjajo svoje strani, ki so neodvisne od njihovega osebnega profila. Ustvarjanje Facebook strani, z razliko od osebnega profila, služi promociji, navezovanju poslovnih stikov, ki so drugačni od druženja in komunikacije s prijatelji. Ustvarjanje takšne strani je mogoče tudi brez osebnega uporabniškega računa, saj ni potrebno navesti osebnih podatkov, tako kot je to obvezno pri kreiranju lastnega, osebnega profila. (Briggs 2011)

Kot socialno omrežje, Facebook svojim uporabnikom ponuja različne načine, kako ohraniti stike z ljudmi, ki niso v naši neposredni bližini. Vse to je mogoče prek sporočil, podobnih elektronski pošti, ali direktnega stik preko takojšnjega sporočanja, podobnega spletnim klepetalnicam. Kot dodatno možnost pa Facebook ponuja storitev, kjer se uporabniki lahko pridružujejo ali ustvarjajo skupine, ki združujejo uporabnike z istimi ali podobnimi interesi. (Briggs 2011)

Poleg tega, da je Facebook socialno omrežje, je tudi platforma za razvijalce programov. Pogosto se takšni programi odražajo v obliki spletnih iger, ki so se razvile v zelo dobičkonosno industrijo. Facebook kot platforma je pogosto tarča kritik, saj spodbuja uporabnike, da s skupnostjo delijo vedno več informacij, ki tako postanejo javne. Če uporabniki svojih podatkov ne želijo javno razkriti, je za to potrebno veliko časa, da preučijo



vse varnostne mehanizme in tako podatke, katere ne želijo javno objaviti, tudi primerno zaščitijo. (Briggs 2011)

## **6.2 FACEBOOK KOT JAVNOPOLITIČNO OMREŽJE VAROVANJA OSEBNIH PODATKOV**

Ključno pri opredeljevanju koncepta javnopolitičnega omrežja je zavedanje, da s konceptom spoznavamo, preučujemo omrežja odnosov med tistimi igralci, ki se vključujejo in oblikujejo proces oblikovanja in izvajanja politik. (Kustec-Lipicer 2002, 69)

Kot sem teoretično prikazala že v petem poglavju, bo v spodnjem sestavku sledila še praktična razlaga zakaj lahko omrežje, v procesu izvajanja javne politike varovanja osebnih podatkov na primeru Facebooka, obravnavamo kot javnopolitično omrežje.

Kot nujne in potrebne izhodiščne pogoje oziroma dimenzije za vzpostavitev javno političnega omrežja določamo:

*PROBLEM: V mojem primeru gre tukaj za problem varovanja osebnih podatkov na internetu, aplicirano na primer Facebooka.*

*IGRALCI: Facebook: državni igralci oziroma oblikovalci politik potrebujejo civilno družbo, torej same uporabnike socialnega omrežja, ki jim posredujejo podatke o tem, ali in kako so bile kršene njihove pravice in njihovi osebni podatki zlorabljeni v primeru socialnega omrežja. Civilna družba, torej uporabniki, pa potrebujejo državne igralce, preko katerih pridobivajo vpliv in izvajajo pritisk glede omenjenega problema, in lahko problem tudi javnopolitično zaznajo in ga regulirajo.*

*VIRI: Facebook: Problem je v tem, da sami uporabniki socialnega omrežja nimajo zadosti virov, interesa ter niso dovolj ozaveščeni, da bi lahko izvajali pritisk na državne igralce, preko katerih bi omenjeni problem lahko postal tudi javna politika.*

*ODNOSI: Facebook: Gre predvsem za to, da odnosi med dvema sferama niso vzpostavljeni, saj se v zvezi z omenjeno problematiko le malo dogaja.*

*MEJE OMREŽIJ: Facebook: Gre za problem ločitve med realnim in virtualnim svetom.*

Kot sem predstavila zgoraj, je Facebook socialno omrežje, preko katerega se v informacijski družbi, v kateri živimo, opazi določene probleme, ki bi lahko vplivali na delovanje ali vsaj na oblikovanje nekega javnopolitičnega omrežja, glede na to, da razpolaga z vsemi pogoji (predstavljenimi v poglavju številka 5), ki so potrebni za vzpostavitev odnosov.

Glede na to, da Facebook, kot socialno omrežje ne moremo opredeliti kot javnopolitični problem, je bistvenega pomena zavedanje, da preko njega izhaja problematika, ki močno posega v našo zasebnost - varovanje osebnih podatkov.

**Tabela 6.2: Prikaz razlik med javnopolitičnim omrežjem varovanja osebnih podatkov ter socialnim omrežjem Facebook**

	<b>JAVNOPOLITIČNO OMREŽJE VAROVANJA OSEBNIH PODATKOV</b>	<b>SPLETNO SOCIALNO OMREŽJE (primer: FACEBOOK)</b>
<b>IGRALCI</b>	Državni in civilno družbeni (IP-RS, Varuh ČP, civilna družba....)	Uporabniki Facebooka, oblikovalci spletnega omrežja, IP-RS, Varuh ČP (glej poglavje 5.1.)
<b>SFERA OZ. PODROČJE DELOVANJA</b>	Javna sfera	Zasebna sfera
<b>PRAVNI OKVIR</b>	Zakonodaja RS (ZVOP)	Zakonodaja Združenih Držav Amerike (glej prilogo 12.1.2. za obrazložitve)
<b>VLOGA DRŽAVE OZ. DRŽAVNIH IGRALCEV</b>	Država ukrepa ob kršitvah, nadzoruje, oblikuje ter izvaja javno politiko	Država lahko poseže le, ko pride do zlorabe na slovenskih tleh in ko krši slovensko zakonodajo
<b>PROBLEM</b>	V prvem omrežju je prisotnih veliko državnih igralcev, medtem ko v drugem omrežju država nima velike vloge. Kljub enaki tematiki igralci v omrežjih niso enaki oz. gre pri Facebooku samo za vzorec tistih, ki so v omrežju o varovanju osebnih podatkov večinsko zastopani (civilna družba).	

## 7 FACEBOOK IN VAROVANJE ZASEBNOSTI

Facebook, kot socialno omrežje, je prava zakladnica osebnih podatkov uporabnikov. Ker gre za spletno omrežje, ki ga uporabniki sami oblikujejo in s tem oblikujejo svoje predstavitevne strani, tako imenovane uporabniške profile, je tudi raven zasebnosti na samih profilih v rokah uporabnikov. Glede na to, da Facebook ponuja ogromno mehanizmov in varnostnih postopkov kako zaščititi osebne podatke, so le-ti mnogokrat preveč kompleksni in težavni, da bi jih povprečen Facebook uporabnik sam razumel. Gre za obilico varnostnih mehanizmov, ki kljub svoji dostopnosti uporabnikom predstavljajo oviro oziroma se teh mehanizmov niti ne zavedajo in jih ne poznajo.

Kot je razvidno iz raziskave, ki sta jo izvedla Alessandro Acquisti in Ralph Gross (2006, 13), z naslovom *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, objavljeni leta 2006, se uporabniki ob vprašanju: Katere informacije uporabniki Facebooka objavijo ter v kakšnih razsežnostih?, prišla do ugotovitev, da je veliko uporabnikov kar selektivnih pri obliki in razsežnosti informacij, ki jih na omenjenem omrežju ponudijo. Kot sta ugotovila, veliko uporabnikov ponudi svoje ime in priimek, ampak prikrijejo številke mobilnih telefonov. Uporabniki so v raziskavi poudarili tudi to, da so tiste informacije, ki so na Facebooku objavljene, v večini primerov resnične, torej popolne in natančne.

Avtorja omenjene raziskave kot težavo socialnega omrežja vidita tudi dejstvo, da se vsak uporabnik Facebooka pojavi v iskalniku vsakega drugega uporabnika. Ugotavljata tudi, da Facebook omogoča zelo široko politiko varovanja zasebnosti ter ponuja zelo natančen nadzor nad tem, katere informacije uporabnik objava ter komu dovoli vpogled v svoje podatke. Uporabniški profil uporabnika lahko vidijo prijatelji, prijatelji prijateljev, uporabniki, ki niso nikakor povezani s samim uporabnikom, sledilci določenim stranem oziroma uporabniki, ki prihajajo iz iste geografske enote. Vse to je pa odvisno od tega katerim omrežjem se pridružimo ter kako sami opredelimo nastavitve zasebnosti. (Acquisti in Gross 2006, 16)

Avtorica članka »Če nimaš svojega profila, skoraj ne obstajaš« Mojca Finc (2008), v svojem članku citira dr. Tanjo Oblak Črnič, ki množično uporabo Facebooka med drugim razlaga z občutkom uporabniške svobode in navidezne varnosti. Pravi da uporabljati medije danes pomeni, bolj kot kdajkoli prej, prejemati in oblikovati vsebine z visoko ravno lastnega

nadzora, kaj bo objavljeno. Facebook je po njenem mnenju nekakšen magnet, saj deluje kot resen, zaupanja vreden prostor izražanja in druženja, s privlačno vizualizacijo oseb in preprostim načinom vpogleda v omrežja »prijateljev od prijateljev«. Avtorica članka navaja, da čeprav snovalci Facebooka trdijo, da jim je zaščita oziroma ohranjanje zasebnosti ena od glavnih prioritet, za katero se močno zavzemajo, se poraja vprašanje, koliko je uporabnikova zasebnost sploh zasebna.

## **7.1 KAKO JE MOGOČE ZBIRANJE OSEBNIH PODATKOV NA FACEBOOKU?**

Družba Sophos Security razkriva, da je Facebook, kot pravijo na spletni strani projekta SAFE, postal raj za prevarante. Pravi, da se mnogi tega zavedajo, drugi si pa ob tem dejstvu zatiskajo oči. Kot navajajo na omenjeni spletni strani, naj bi Facebook postal poln lažnih vprašalnikov, aplikacij, ki niso tisto, kar so videti na prvi pogled, in lažnih povezav na dvomljive strani. Večina takšnih potegavščin naj bi bila namenjena temu, da si nepridipravi tako ali drugače polnijo žepe, navadno na račun klikov. Večjo težavo pa vidijo v temu, da lahko preko takšnih aplikacij določene osebe dobijo vpogled v bančne račune in jih na takšen način tudi izpraznijo. Pri Sophosu navajajo predvsem tri načine goljufanja na Facebooku. (SAFE-SI 2011b)

### *»Likeme« črvi*

Prevaranti postavijo lažno spletno stran z naslovom, ki obljublja veliko. Ob takih straneh brez težav najdejo več tisoč ljudi, ki bodo odkljukali »všeč mi je« gumb. Vsak obisk takšne strani, prevarantom prinaša zaslužek. (SAFE-SI 2011b)

### *Potegavščine z lažnimi vprašalniki*

Privabijo nas z neko super zgodbo. Da bi prebrali zgodbo moramo najprej klikniti gumb »všeč mi je«. Če želimo nadaljevati moramo nato izpolniti še kratek vprašalnik. Najprej so na podlagi našega interesa zaslužili, nato bodo podobno stvar poslali še vsem našim prijateljem. (SAFE-SI 2011b)

### *Lažne aplikacije*

Z aplikacijami, ki pravijo, da je mogoče ugotoviti kdo si ogleduje naš profil nepridipravi zopet služijo, saj kaj takšnega na Facebooku trenutno še ni mogoče. (SAFE-SI 2011b)

Kot navajajo na spletni strani, pri Facebooku pravijo, da se je ob povečanem številu prevarantov in vdorov, povečala tudi učinkovitost boja proti njim. Še posebej učinkoviti so bili pri tožbah proti nekaj »spamerjem«, ki so razpošiljali nadležna sporočila. Poznavalci spletne varnosti trdijo, da bodo uporabniki Facebooka še bolj na udaru, v kolikor bo Facebook povečal dostop aplikacij do naslovov in telefonskih števil uporabnikov. (SAFE-SI 2011b)

## **7.2 HRANJENJE OSEBNIH PODATKOV NA FACEBOOKU**

Avtor članka »Facebook hrani izbrisane slike več kot poldrugo leto«, Matej Huš (2010) pravi, da so leta 2009 na Ars Technici izvedli eksperiment, v katerem so raziskovali, kako dolgo izbrisane slike vztrajajo na družbenih omrežjih, kot je na primer Facebook. Odkrili so, da če imamo neposredni naslov slike, lahko do nje dostopamo še precej časa po izbrisu. Facebook je dejal, da slike ostanejo v obliki varnostnih kopij na strežnikih še nekaj časa, medtem ko naj bi bile neposredno s spleta z direktno povezavo takoj nedosegljive (kar se je izkazalo za laž). Posnetek, ki so ga izbrisali iz Facebooka 21. maja 2009, je bil čez eno leto še vedno dosegljiv, če smo poznali direktno povezavo do njega. To pomeni, da v več kot enem letu Facebook ni storil tistega, kar so obljubili, da se zgodi v trenutku izbrisa. Facebook je uporabil staro zvijačo, ko s podizvajalcem rešujejo problem prekomernega hranjenja izbrisanih podatkov in navajajo, da pa so podatki za vse praktične potrebe izbrisani, saj se nikjer ne pojavi nobena povezava do njih.

Težava, ki jo izpostavljata tudi avtorici članka »Facebook, MySpace Confront Privacy Loophole«, Emily Steel in Jessica E. Vascellaro (2010), se kaže predvsem v tem, da mnoge spletne strani, ki ponujajo socialno povezovanje, pošiljajo podatke oglaševalskim agencijam, ki bi lahko uporabnikove podatke izrabile za namene, za katere niso bili pridobljeni. Metode, ki so v stalni praksi takšnih podjetij, dokazujejo, da uporabnik že ko klikne na oglas, ki se pojavi na socialnem omrežju, pridobi uporabnikovo uporabniško ime oziroma naslov.

## 8 LEGISLATIVNA ZGODOVINA

Čebulj (1992, 42) v svoji knjigi omenja da pravni vidik zasebnosti zaradi svoje subjektivnosti ni nedvoumno ali jasno definiran. Zaradi morebitnega preozkega definiranja se pri vsakem posameznem primeru sodnega spora tehta pravica do zasebnosti nasproti drugi pravici. Pravica do zasebnosti je definirana kot osebna pravica, v kateri se združuje vrsta pravic v zvezi s človekovo osebo in njegovimi osebnimi razmerji. Tudi zanjo je značilno, da pripada posamezniku kot sestavni del njegove zasebnosti, ki jo sočasno varuje, pri čemer je varovan tudi njegov odnos do drugih.

Prvi predlog za izdajo zakona o zaščiti podatkov v družbenem sistemu informiranja je bil podan konec leta 1983. Ta predlog je v grobem bolj varoval subjekte, ki zbirajo in uporabljajo podatke, kot pa posameznike. Drugi predlog zakona, z današnjo vsebino je bil sprejet 7. marca 1990 in dopolnjen 24. aprila 1991. Ta zakon temelji na načelih, ki so vsebovana v Smernicah OCED, zlasti v Konvenciji Sveta Evrope. (Čebulj 1992, 42)

»Področje telekomunikacij je danes največja gospodarska veja v svetovnem merilu, eno najhitreje razvijajočih se tehnologij in ključni faktor za uspešno poslovanje.« (Kustec – Lipicer 2000, 85)

Osredotočila sem se predvsem na področje strokovnega nadzora, ki ga Zakon o varovanju osebnih podatkov opredeljuje v svojem 8. členu.

*(1) Osebni podatki se lahko obdelujejo le, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev posameznika. (ZVOP-1-UPB1)*

*(2) Namen obdelave osebnih podatkov mora biti določen v zakonu, v primeru obdelave na podlagi osebne privolitve posameznika pa mora biti posameznik predhodno pisno ali na drug ustrezen način seznanjen z namenom obdelave osebnih podatkov. (ZVOP-1-UPB1)*

Moj drugi fokus pa je 16. člen prej omenjenega zakona, ki pravi:

»Osební podatki se lahko zbirajo le za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, če zakon ne določa drugače.« (ZVOP-1-UPB1)

ZVOP – 1 določa, da je varovanje osebnih podatkov namenjeno preprečevanju nezakonitih in neupravičenih posegov v informacijsko zasebnost posameznika na vseh relevantnih področjih. Pravi, da je smisel varstva osebnih podatkov varovanje pravic posameznika, ne glede na njegove vsesplošne značilnosti, in ne varovanje osebnih podatkov kot takih. Osebni podatek je vsakršen podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen. (Pirc Musar 2006, 39–41)

Iz tega lahko sklepamo in zaključimo, da je osebni podatek tudi naslov elektronske pošte, ki ga kot obvezno sestavino moramo navesti vsakokrat, ko se prijavimo na Facebook.

Objava določenih vsebin na spletu je lahko protipravna in ima za posledico sankcije. Vsebine, ki so protipravne kot take so: otroška pornografija, žaljive vsebine, spodbujanje sovraštva in nestrpnosti. (Antić 2011)

Bolj kot ta vidik, nas pri proučevanju Facebooka zanima, druga oblika protipravnosti, ki se kaže v kršitvi intelektualne lastnine drugih in protipraven poseg v zasebnost druge osebe. (Antić 2011)

Glede na vsa omenjena izhodišča je Facebook opredelil nastavitve zasebnosti v svojih pogojih uporabe, ki pravijo naslednje:

»Uporabnik si lahko nastavi stopnjo zasebnosti. Kar je spornega tukaj, je to, da Facebook ne odgovarja za nobeno zlorabo ali prevaro pri samih nastavitvah. Stopnje zasebnosti pa so različne, od najmanjše do največje.« (Facebook 2011)

## 8.1 KLJUČNI PRAVNI AKTI

Zaradi razvoja informacijske tehnologije se je tako pojavila potreba po učinkoviti zaščiti zasebnosti, ta potreba pa je prioriteta tudi v današnjem času. Leta 1974 je generalni sekretar OZN v poročilu z naslovom »Človekove pravice in znanstveni in tehnološki razvoj - Uporaba elektronike, ki lahko vpliva na pravice oseb in omejitve, ki bi morale biti podane v demokratični družbi ob takih uporabah«, vsem državam, ki še nimajo zakonske ureditve varstva informacijske zasebnosti, priporočil, naj tako ureditev čim prej sprejmejo. Poleg tega je priporočil tudi načela, ki naj bi se jih države pri sprejemanju tovrstne zakonodaje držale: načelo relevantnosti, ki predstavlja zahtevo, da se o posamezniku zbirajo samo tisti podatki, ki so nujno potrebni za doseg namena, zaradi katerega se zbirajo; načelo notifikacije, ki pomeni, da naj bo posameznik predhodno seznanjen o podatkih, ki se o njem zbirajo, shranjujejo in obdelujejo; ter načelo privolitve, ki pravi, da naj se zbirajo samo tisti podatki, glede katerih je posameznik v njihovo zbiranje privolil. (Čebulj 1999,19)

Od omenjenih načel so izjeme dopustne v specifičnih primerih, ki pa morajo biti določene z zakonom (Čebulj 1992, 12). Na podlagi tega je OZN predstavila Smernice o avtomatiziranih zbirkah osebnih podatkov, ki se v bistvu zgledujejo po načelih, ki so se izoblikovala v drugih pravnih aktih. Organizacija za ekonomsko sodelovanje in razvoj je leta 1980 sprejela Smernice OECD, ki vsebujejo načela za pošteno in zakonito ravnanje z osebnimi podatki (Raab 1992, 90), na podlagi 8. člena Evropske konvencije o človekovih pravicah (Čebulj 1992, 13) - leta 1953 jo je sprejel Svet Evrope - je bila leta 1981 sprejeta Konvencija o varstvu posameznikov z vidika avtomatskega procesiranja osebnih podatkov. Le-ta vsebuje načela, ki naj bi zagotovila poenotenje nacionalnih zakonodaj na področju varstva posameznikove informacijske zasebnosti. Omeniti je potrebno še predloge treh direktiv, ki jih je leta 1990 sprejela Evropska skupnost. Le-te se nanašajo na varstvo posameznikov iz vidika procesiranja osebnih podatkov, na specifične zahteve glede varstva zasebnosti v okviru javnih digitalnih telekomunikacijskih omrežij ter na razvoj globalne strategije na področju zavarovanja podatkov oz. informacij. (Čebulj 1992, 13)

Vsi omenjeni pravni akti se ukvarjajo predvsem z naslednjimi načeli: načelo ažurnosti, načelo določitve namena zbiranja in uporabe osebnih podatkov, načelo vpogleda prizadete osebe v zbirko, načelo preprečevanja diskriminacije, načelo zakonitosti pri omejitvah pravic in izjem



od varstva informacijske zasebnosti načelo zavarovanja podatkov, načelo nadzora in sankcioniranja ter načelo svobodnega prenosa podatkov preko državnih meja.

*Na kratko pa bi lahko rekli, da je vodilna misel vseh omenjenih pravnih aktov, pa tudi načel, ki jih zagovarjajo ta, da se z večjo transparentnostjo uporabe osebnih podatkov ogroženost informacijske zasebnosti zmanjša. Moderna zakonodaja za zaščito zasebnosti se tako ukvarja predvsem z transparentnostjo uporabe osebnih podatkov. Zakonodajalec torej ščiti posameznikovo informacijsko zasebnost predvsem z uzakonjanjem postopkov za zagotavljanje transparentnosti uporabe posameznikovih osebnih podatkov. (Kovačič 2000)*

Vasja Ocvirk (2003) je v članku, z naslovom *Zasebnost na internetu ni zgolj tehnološko vprašanje*, objavljenem septembra 2003, zapisal tako:

*Posebno poglavje, ki se ukvarja s slovensko zakonodajo, postane posebej zanimivo v točkah, kjer opozarja na nedoslednosti ali preohlapne formulacije posameznih zakonov. Tako na primer Zakon o kazenskem postopku dovolj natančno in nedvoumno določa, v katerih primerih je moč posegati v zasebnost (151. člen), medtem, ko se pri Zakonu o Slovenski obveščevalno-varnostni agenciji (24. člen) stvar zaplete pri definiciji »tajnih aktivnosti zoper strateške interese Republike Slovenije«. Ti »strateški interesi« so namreč ravno dovolj raztegljiv pojem, da bi lahko omogočili morebitno zlorabo. (Ocvirk 2003)*

## **9 RABA INTERNETA V SLOVENIJI – Spletne skupnosti 2010**

Projekt Raba interneta v Sloveniji (v nadaljevanju RIS) je opravil raziskavo o vključenosti in aktivnostih prebivalcev Republike Slovenije v spletnih skupnostih, ki temeljijo na telefonski anketi, izvedeni v decembru 2003 na reprezentativnem vzorcu prebivalcev Slovenije (n=1209), starih od 10 do 75 let. V zadnjem času, ki ga avtorji Vehovar Vasja, Tina Činkole, Petrovčič Andraž in Saša Mašič označujejo kot obdobje spleta 2.0, uporabniško generiranih vsebin in družbenih medijev, so spletne skupnosti doživele dodatni vzpon in dokončno prodrle iz prostora subkulturnega udejstvovanja v množično obliko povezovanja ljudi na svetovnem spletu. (Činkole, Mašič, Petrovčič in Vehovar 2010)

Omenjeni proces je v tem desetletju moč zaznati tudi v slovenskem prostoru.

Avtorji so v raziskavi ugotovili, da je v Sloveniji rednih uporabnikov interneta, v populaciji 10-75 let, 74 %. Redni uporabniki interneta vsaj enkrat mesečno najpogosteje obiskujejo video in foto skupnosti (45%), ter spletna socialna omrežja (44%). Med rednimi uporabniki interneta v Sloveniji je ena izmed najpogosteje obiskanih skupnosti prav Facebook. (Činkole, Mašič, Petrovčič in Vehovar 2010)

### **9.1 FACEBOOK IN SLOVENCİ – vidik varovanja zasebnosti**

Na spletnem portalu RIS so objavili raziskavo in podatke pridobljene preko portala SocialBakers, ki pravi, da je sredi marca 2011 bilo v Sloveniji 627.360 uporabnikov Facebooka. To število uporabnikov Facebooka predstavlja 37% slovenske populacije v starosti od 10 do 74 let, ki po podatkih Statističnega urada RS za leto 2010 šteje 1. 700. 729 ljudi. Rezultati dobljeni s strani portala SocialBakers so grafično prikazani med prilogami, in sicer v grafu 12.2.1. (RIS 2011)

Število uporabnikov Facebooka se je pri nas v primerjavi z majem 2010 povečalo za skoraj 50 tisoč. Takšno stanje nas glede na rast uporabnikov Facebooka med 213 opazovanimi državami uvršča na 172. mesto. Podatki portala SocialBakers kažejo, da med slovenskimi uporabniki Facebooka prevladuje starostna skupina od 25 do 34 let (33%), ki ji tesno sledi segment od 18

do 24 let (31%). Izstopa predvsem podatek, da med slovenskimi uporabniki Facebooka najdemo zelo malo posameznikov, starih 45 let ali več. (glej prilogo D) (RIS 2011)

Slovenska točka ozaveščanja o varni uporabi interneta SAFE-SI je v sodelovanju s podjetjem iPROM pripravila raziskavo o varni uporabi interneta, kjer so ugotovili, da nekaj več kot polovica (58%) slovenskih uporabnikov socialnih spletnih omrežij skrbi, da bi drugi o njih objavljali podatke, slike in posnetke, za katere ne želijo, da pridejo v javnost. Skoraj petini (17%) uporabnikov se je že zgodilo, da je njihov bližnji izrabil njihovo zaupanje in na svojem profilu objavil informacije, za katere niso želeli, da bi bile javno objavljene; med mladimi med 10 in 20 let se je to zgodilo skoraj četrtini (23%). (SAFE-SI 2010)

Kot navajajo, gesla za dostop do profila v socialnem omrežju ne bi smeli zaupati nikomur, tudi najbližjim ne. Če geslo zaupamo neki osebi, nam ta lahko ukrade identiteto in v našem imenu počne, kar želi. Več kot petina (22%) slovenskih uporabnikov socialnih omrežij geslo za dostop do svojega profila deli še z eno ali več osebami. Najpogosteje s sorodniki, prijatelji, partnerji. Svoj profil in s tem vpogled v svoje življenje je pametno zaščititi z nastavitvami zasebnosti, ki jih ponuja socialno omrežje. Najbolj zasebne informacije ter kontaktne podatke je dobro omejiti tako, da jih lahko vidijo le naši prijatelji in ne tudi prijatelji prijateljev ali celo vsi uporabniki omrežja. Omenjena raziskava je sicer pokazala, da je med Slovenci več (37%) takih uporabnikov, ki jih ne skrbi, da bi kdo zlorabil njihove podatke na profilu, kot takih, ki jih to skrbi (29%). Kljub temu ima večina (71%) svoj profil viden samo prijateljem, 14 odstotkov ima profil odprt vsem uporabnikom socialnega omrežja, 13 odstotkov pa vsem uporabnikom interneta. (SAFE-SI 2010)

V omenjeni raziskavi lahko zasledimo tudi, da smo Slovenci pri objavi kontaktnih podatkov previdni: Le 7% vprašanih ima svoj naslov bivanja objavljen tako, da ga lahko vidijo vsi, 17% ga ima objavljenega le za prijatelje, ostali pa imajo ta podatek skrit. Podobno je s telefonsko številko in MSN kontaktom, Svoj e-poštni naslov javno objavlja nekoliko več uporabnikov (15%), s prijatelji ga deli 47%, skritega ima le dobra četrtina uporabnikov. (SAFE-SI 2010)

Podatki, ki jih najbolj odprto delimo z vsemi, so ime, priimek, spol ter prikazna fotografija. Ostale slike na profilu z vsemi deli 14% uporabnikov, večina (67%) pa dovoli ogled slik le prijateljem. Ob tem ne gre zanemariti podatka, da ima kar 32% uporabnikov družabnih omrežij med prijatelje dodane tudi popolne neznance. (SAFE-SI 2010)

## 10 ZAKLJUČEK IN LASTNA ANALIZA

V diplomski nalogi sem obravnavala tematiko varovanja osebnih podatkov na internetu; analizirala sem primer spletnega omrežja Facebook. Osredotočala sem se predvsem na javnopolitičen vidik, kjer sem raziskovala obstoj javnopolitičnega omrežja oziroma dejavnost le-tega, v kolikor takšno omrežje sploh obstaja.

Varovanje osebnih podatkov na internetu sem definirala kot javnopolitični problem, saj kot pravi Grdešič (1995, 57–58) je temeljni kriterij za obstoj problema razkorak med obstoječim družbenim stanjem in želenim stanjem. Definirati javnopolitični problem pa pomeni poiskati razliko med tistim kar je, in tistim do česar želimo priti s svojim udejstvovanjem. (Grdešič 1995, 57–58)

Problem varovanja osebnih podatkov je, po mojem mnenju, vsekakor javnopolitični problem, saj obstaja zakonodaja, ki se s področjem varovanja osebnih podatkov ukvarja in skuša problematiko regulirati. Problem nastane predvsem v tem, kot sta mi to zaupala sogovornika Matej Kovačič in Nataša Pirc Musar, da gre pri regulaciji problema varovanja osebnih podatkov, zlasti v socialnih omrežjih, za to, da je prakse in pravila iz realnega sveta zelo težko prenesti na virtualni svet. (glej prilogo B ter C)

Po mnenju Kovačiča (2003, 62) problem varnosti in s tem tudi zasebnosti ni samo tehnični, pač pa tudi družbeni. Povedano pomeni, da bi se mogli uporabniki računalnikov bolj zavedati nevarnosti različnih zlorab, predvsem pa, kako se proti njim mogoče kar najbolje zavarovati.

V poglavju pod zaporedno številko 8 sem omenila 8. člen Zakona o varovanju osebnih podatkov, ki pravi, da se osebni podatki lahko obdelujejo le, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon, ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev posameznika.

Kar je spornega pri tem je, da je Facebook objavil naslednje: uporabnik si lahko nastavi stopnjo zasebnosti. Facebook pa ne odgovarja za nobeno zlorabo ali prevaro pri samih nastavitvah. Stopnje zasebnosti pa, na omrežju, označujejo kot najmanjše ali največje.

Drži, da si uporabnik sam določa stopnjo zasebnosti oziroma samo varnost in zaščitenost svojega osebnega profila, a kaj ko se večina ne zaveda zlorab, ga le-te ne zanimajo ali pa so same nastavitve tako zapletene, da jih večina uporabnikov niti ne razume (glej poglavje številka 9). (SAFE-SI 2009)

Kot navaja prvi odstavek 8. člena Zakona o varovanju osebnih podatkov mora biti za obdelavo le-teh zagotovljena pisna privolitev posameznika. Pri Facebooku vsak uporabnik preden ustvari svoj osebni profil sprejme pogoje uporabe, s katerimi Facebooku dovoljuje obdelavo podatkov v namene, za katere so bili pridobljeni. Gre za problematiko nezakonitega zbiranja podatkov, za katere pa Facebook ne odgovarja in nima nadzora, kdo te podatke obdeluje.

Kot mi je v intervjuju pojasnil Kovačič, se mu samo zbiranje podatkov na Facebooku zdi problematično, saj omrežja na ta način uporabnika silijo v razkrivanje osebnih podatkov, če želi biti vključen v samo omrežje. Pravi, da so osebni podatki danes tržno blago, zato je interes za njihovo obdelavo in zbiranje zelo velik. Gre torej za vprašanje »trgovanja z zasebnostjo«. (Kovačič 2006, 38)

Kar zadeva zakonodajo Kovačič pravi, da je potrebno narediti še korak naprej. Zgolj normativno urejanje področja zasebnosti ni dovolj. Meni, da so danes za regulacijo problematike potrebni proaktivni pristopi.

Informacijska pooblaščenka Pirc-Musarjeva se prav tako strinja, da Zakon o varstvu osebnih podatkov določa, da je v zasebnem sektorju (kamor spadajo ponudniki spletnih mrež) pravna podlaga za obdelavo osebnih podatkov lahko tudi privolitev posameznika. Enako velja tudi v primeru obdelave občutljivih osebnih podatkov. Pri tem so upravljavci sicer omejeni z namenom obdelave, vendar pa lahko namen obdelave določijo precej široko – če se posameznik s tem strinja in torej privoli v tako širok namen obdelave njegovih osebnih podatkov oz. celo v posredovanje njegovih osebnih podatkov tretjim osebam – takšna obdelava torej ni protipravna (v kolikor seveda upravljavec upošteva tudi ostale določbe zakonodaje – ustrezno zavarovanje osebnih podatkov, dolžnost obveščanja posameznikov ipd.). (glej prilogo C)

Po mnenju pooblaščenke zakonodaja lahko pomaga regulirati področje, predvsem z uzakonitvijo pravil, ki se jih morajo držati upravljavci zbirk osebnih podatkov. Izjemno pomembna so osnovna načela varstva osebnih podatkov, med njimi načelo sorazmernosti (»Obdeluj točno toliko podatkov, kot jih potrebuješ za dosego cilja.«) in načelo sledljivosti, ki

pri upravljavcih preprečuje radovednost zaposlenih in na ta način zlorabe osebnih podatkov. Največja težava pa je zagotovo ta, da pravo vedno zaostaja za modernimi informacijskimi tehnologijami, zato je ozaveščanje upravljavcev in posameznikov toliko bolj pomembno.

Pri vprašanju, ali imajo državne institucije oziroma državni akterji kakšno vlogo pri regulaciji problematike, Kovačič odgovarja pritrdilno. Zelo pomembni so organi, ki se strokovno ukvarjajo s področjem zasebnosti. Pri nas je to informacijski pooblaščenec, po Evropi pa njemu sorodni organi, ki so povezani na ravni EU. Informacijska pooblaščenka izjavo Kovačiča dopolnjuje s tem, da ima država predvsem nalogo varovati posameznika in njegove človekove pravice (kamor sodi tudi pravica do varstva osebnih podatkov). Da bi dosegla in uresničila te naloge, mora država predvsem poskrbeti za ustrezno zakonodajo in za ustrezno izvrševanje te zakonodaje. Ukrepati mora tako represivno (s sankcioniranjem kršiteljev) kot tudi preventivno (z izobraževanjem posameznikov in upravljavcev).

Po mnenju Kovačiča je bistven problem Facebooka zakonodaja ZDA, ki je bistveno drugačna od zakonodaje v Evropi. Napoveduje, da žal kakšnih hitrih sprememb na tem področju v ZDA ni pričakovati. Omenjeno trditev utemelji tudi v svojem delu, kjer pravi, da zakonodaja, ki ureja varovanje zasebnosti v realnem svetu, načeloma velja tudi v virtualnem svetu. Vendar pa se je treba zavedati, da internet ni prostorsko zamejen, kar ima lahko pri uveljavljanju uporabnikovih pravic zelo konkretne posledice. Posebej v primerih, kjer zakonodaja med državami ni usklajena, uporabnik pa se med uporabo interneta giblje na območju jurisdikcije različnih držav ali vstopa v interakcijo z globalno razpršenimi subjekti. (Kovačič 2003, 61)

Kot temeljno vprašanje za dokončanje diplomskega dela, v prilogi B, vprašanje št. 10, sem Mateja Kovačiča spraševala zakaj v Sloveniji ni potrebne iniciative za regulacijo problema oziroma za oblikovanje omrežja, ki bi se s problematiko ukvarjalo. Le-ta odgovarja, da deloma zato, ker za to področje profesionalno skrbijo ustrezne uradne institucije (v mislih imam informacijskega pooblaščenca, pa tudi projekte kot Safe.si, itd.), deloma pa tudi zato, ker večina ljudi groženj zasebnosti ne vidi kot problem, ki bi bil vreden političnega angažiranja.

Prav slednje potrjuje izsledke raziskave SAFE.SI, (glej poglavje 9.1.), kjer pravijo, da je med Slovenci več (37%) takih uporabnikov, ki jih ne skrbi, da bi kdo zlorabil njihove podatke na profilu, kot takih, ki jih to skrbi (29%). Kljub temu ima večina (71%) svoj profil viden samo prijateljem, 14 odstotkov ima profil odprt vsem uporabnikom socialnega omrežja, 13 odstotkov pa vsem uporabnikom interneta. (SAFE-SI 2010)

**Kot raziskovalno vprašanje, v diplomski nalogi, sem si zastavila sledeče:**

**R1:** *Zakaj v primeru varovanja osebnih podatkov na internetu (primer: Facebook), ni javnopolitičnega omrežja oziroma je le-to tako šibko in brez vpliva, da na omenjenem področju ne prihaja do sprememb?*

Odgovor na R1 lahko utemeljim z izjavo Mateja Kovačiča, ki pravi, da je problem zelo kompleksen in težaven, saj ni odvisen samo od slovenske zakonodaje, ampak je podrejen zakonodaji ZDA, glede na to, da platforma Facebooka ustvarjena prav v Združenih državah Amerike. Za regulacijo problema so potrebni proaktivni ukrepi in ne le sprememba zakonodaje, tako da v primeru obstoja javnopolitičnega omrežja, le-to ni zmožno regulirati problema samostojno. Zaključim lahko, da javnopolitično omrežje obstaja, saj sem v poglavju 5 definirala igralce in interakcije med njimi, a le-ti nimajo pristojnosti za samostojno reagiranje. Delujejo lahko samo na podlagi slovenske zakonodaje, ki virtualni svet le delno opredeljuje.

**R2:** *Zakaj ni potrebne javnopolitične pobude za regulacijo omenjenega problema, glede na to, da število afer na področju zlorabe uporabniških vsebin v omenjeni spletni skupnosti narašča?*

Javnopolitične pobude ni, ker gre za relativno nov problem in dokler se zakonodaja ne uredi in na omenjenem področju ne pride do sprememb, ne glede na število in razsežnosti afer, slovensko javnopolitično omrežje ne more reagirati. Opaziti je tudi zelo šibko zavedanje problema med samimi uporabniki, ki so pa igralci in bi morali problem najprej zaznati.

**Hipotezo sem oblikovala na naslednji predpostavki:**

**H1:** *Na področju varovanja zasebnosti na internetu ne obstaja omrežje, ki bi se ukvarjalo z omenjeno tematiko, oziroma je tako šibko, da nima nikakršnega vpliva.*

Prvi del H1 lahko zavrnem, saj obstaja omrežje, ki se ukvarja z tematiko varovanja osebnih podatkov (informacijska pooblaščenka, SAFE.SI in drugi). Drugi del H1 pa lahko potrdim na podlagi trditve, da imajo igralci res tako malo moči in pristojnosti, da bi tematiko lahko regulirali.

**H2:** *Kljub naraščanju in vedno večjemu problemu varovanja osebnih podatkov in zlorabi le teh, javnopolitična pobuda na omenjenem področju, ki bi problem tudi zakonsko uredila, še vedno ne obstaja.*

H2 lahko potrdim, saj iniciativa še vedno ne obstaja, kljub temu, da se razsežnosti problema vsak dan večajo. To pa je pogojeno s tem, da se tudi uporabniki spletne skupnosti ne zavedajo vseh nevarnosti, kot so mi potrdili tudi vsi trije sogovorniki. V tem torej tiči razlog zakaj ne pride do javnopolitične pobude, ki bi problem tudi zakonsko regulirala.

Kot navajajo na spletni strani *What is social networking?* je dovolj le to, da se zavedamo okolja okrog sebe in nevarnosti spletnih omrežji. Le tako lahko uživamo in se prepustimo prednostim, ki jih socialno povezovanje prinaša. (*What is social networking?*)

Kot navaja avtor članka »ABC poslovne rabe interneta«, Mitja Mavsar (2008):

*Če za svojo spletno identiteto ne poskrbimo sami, bodo zelo mogoče, in morda ne ravno dobronamerno, to storili drugi. Povsem vsakdanji problem nastane, ko v splet naložimo slike in druge osebne informacije. Do nedavna tako ločevanje ni bilo mogoče, a pred kratkim je Facebook omogočil prav to. Vsak uporabnik zdaj sam nadzira dostopnost svojih osebnih informacij. Določen »osebni artefakt«, kot je fotografija, lahko torej »odpremo« po želji.*  
(Mavsar 2008, 36)

Če povzamem vse kar sem v diplomski nalogi zapisala in raziskala, je Facebook svet zase, v katerem ne veljajo pravila, ki so nekaj splošno znanega v realnem svetu. Gre za virtualno skupnost, kjer nam ne more pomagati nihče drug, kot pa le mi sami. Zavedati se moramo, da je svetovni splet globalna vas, kjer moramo biti nadvse pozorni koga in kaj spustimo v naš zasebni prostor.



## 11 LITERATURA

1. Acquisti, Alessandro in Ralph Gross. 2006. *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*. Dostopno prek: <http://privacy.cs.cmu.edu/dataprivacy/projects/facebook/facebook2.pdf> (1. september 2011).
2. Antić, France. 2011. *Pravni vidiki spletnega portala*. Dostopno prek: <http://mladipodjetnik.si/podjetniski-koticek/internet/pravni-vidiki-spletnega-portala> (15. maj 2011).
3. Briggs, Dave. 2011. *What is Facebook?* Dostopno prek: <http://davepress.net/2011/08/01/what-is-facebook/> (5. september 2011).
4. Čebulj, Janez. 1992. *Varstvo informacijske zasebnosti v Evropi in v Sloveniji*. Ljubljana: Inštitut za javno upravo pri Pravni fakulteti v Ljubljani.
5. Činkole, Tina, Saša Mašič, Andraž Petrovčič in Vasja Vehovar. 2010. *Spletne skupnosti 2010*. Dostopno prek: <http://www.ris.org/index.php?fl=2&lact=1&bid=11719&parent=13?> (5. september 2011).
6. Dunn, William. 1994. *Public Policy Analysis*. Englewood Cliffs: Prentice-Hall, Inc.
7. Facebook. 2011. *Pogoji uporabe*. Dostopno prek: <http://www.facebook.com/terms.php> (15. maj 2011).
8. Finc, Mojca. 2008. *Če nimaš svojega profila, skoraj ne obstajaš*. Dostopno prek: <http://www.delo.si/clanek/70196> (1. september 2011).
9. Fink Hafner, Danica, ur. 2007. *Uvod v analizo politik: teorije, koncepti, načela*. Ljubljana: Fakulteta za družbene vede.
10. Gredešić, Ivan. 1995. *Političko odločevanje*. Zagreb: Alinea.
11. --- 2006. *Osnove analize javnih politik*. Zagreb: Fakultet političkih znanosti.
12. Howlett, Michael in M. Ramesh. 1995. *Studying Public policy. Policy Cycles and Policy Subsystems*. Oxford: Oxford University Press.

13. Huber, Jernej. 2007. *Socialne mreže na internetu*. Dostopno prek: <http://revija.mojedelo.com/karierni-razvoj/socialne-mreze-na-internetu-294.aspx> (7. september 2011).
14. Huš, Matej. 2010. *Facebook hrani izbrisane slike več kot poldrugo leto*. Dostopno prek: <http://slo-tech.com/novice/t435841/0> (5. september 2011).
15. Informacijski pooblaščenec RS. 2009a. *Varstvo osebnih podatkov in mediji*. Dostopno prek: [http://www.ip-rs.si/fileadmin/user\\_upload/Pdf/smernice/OP\\_in\\_mediji.pdf](http://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/OP_in_mediji.pdf) (16. maj 2011).
16. --- 2009b. *Smernice Informacijskega pooblaščenca za oblikovanje izjave o varstvu osebnih podatkov na spletnih straneh*. Dostopno prek: [http://www.ip-rs.si/fileadmin/user\\_upload/Pdf/smernice/Smernice-za-oblikovanje-izjave-o-varstvu-osebnih-podatkov-na-spletnih-straneh.pdf](http://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice-za-oblikovanje-izjave-o-varstvu-osebnih-podatkov-na-spletnih-straneh.pdf) (16. maj 2011).
17. Kotar, Mirjam. 2007. Država kot javnopolitični igralec. V *Uvod v Analizo politik: Teorije, koncepti, načel*, ur. Danica Fink Hafner, 69–86. Ljubljana: Fakulteta za družbene vede.
18. Kovačič, Matej. 2000. *Zasebnost v informacijski družbi*. Dostopno prek: <http://dk.fdv.uni-lj.si/tip/tip20006kovacic.PDF> (5. september 2011).
19. --- 2003. *Zasebnost na internetu*. Ljubljana: Mirovni inštitut.
20. --- 2006. *Nadzor in zasebnost v informacijski družbi: filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu*. Ljubljana: Fakulteta za družbene vede.
21. Kustec Lipicer, Simona. 2002. Javnopolitična omrežja. V *Analiza politik*, ur. Danica Fink-Hafner in Damjan Lajh, 67–81. Ljubljana: Fakulteta za družbene vede.
22. --- 2007. Javnopolitična omrežja. V *Uvod v analizo politik: teorije, koncepti, načela*, ur. Danica Fink-Hafner, 87–101. Ljubljana: Fakulteta za družbene vede.
23. Mavsar, Mitja. 2008. *ABC poslovne rabe FACEBOOKA*. Dostopno prek: [http://www.mavsar.si/wp-content/uploads/2011/02/Poslovna\\_raba\\_facebooka\\_mitjamavsar\\_2006.pdf](http://www.mavsar.si/wp-content/uploads/2011/02/Poslovna_raba_facebooka_mitjamavsar_2006.pdf) (1. september 2011).

24. Ocvirk, Vasja. 2003. *Zasebnost na internetu ni zgolj tehnološko vprašanje*. Dostopno prek: <http://www.nasvet.com/zasebnost-internet/> (5. september 2011).
25. Pirc Musar, Nataša, ur. 2006. *Zakon o varstvu osebnih podatkov s komentarjem*. Ljubljana: GV Založba.
26. Raab, Charles D. 1997. Privacy, democracy, information. V *The Governance of Cyberspace*, ur. Brian D. Loader, 155–174. London, New York: Routledge.
27. RIS. 2011. *Na Facebooku skoraj 630.000 prebivalcev Slovenije*. Dostopno prek: [http://www.ris.org/db/27/11980/Raziskave/Na\\_Facebooku\\_skoraj\\_630000\\_prebivalcev\\_Slovenije/](http://www.ris.org/db/27/11980/Raziskave/Na_Facebooku_skoraj_630000_prebivalcev_Slovenije/) (5. september 2011).
28. SAFE-SI. 2010. *Slovence skrbi kaj drugi o njih objavljajo na spletu*. Dostopno prek: [http://www.safe.si/db/6/2161/Slovence\\_skrbi\\_kaj\\_drugi\\_o\\_njih\\_objavljajo\\_v\\_druzabnih\\_omrezjih](http://www.safe.si/db/6/2161/Slovence_skrbi_kaj_drugi_o_njih_objavljajo_v_druzabnih_omrezjih) (5. september 2011).
29. --- 2011a. Dostopno prek: [http://www.safe.si/c/712/O\\_projektu/](http://www.safe.si/c/712/O_projektu/) (15. maj 2011).
30. --- 2011b. *Kako vas goljufajo na Facebooku?* Dostopno prek: [http://www.safe.si/db/6/2331/Novice/Kako\\_vas\\_goljufajo\\_na\\_Facebooku/?p1=670&p2=1204](http://www.safe.si/db/6/2331/Novice/Kako_vas_goljufajo_na_Facebooku/?p1=670&p2=1204) (5. september 2011).
31. SI-CERT. Dostopno prek: <http://www.cert.si/o-centru.html> (15. maj 2011).
32. Steel, Emily in Jessica E. Vascarello. 2010. *Facebook, MySpace Confront Privacy Loophole*. Dostopno prek: [http://online.wsj.com/article/SB10001424052748704513104575256701215465596.html?mod=WSJ\\_Tech\\_LEFTToPNews](http://online.wsj.com/article/SB10001424052748704513104575256701215465596.html?mod=WSJ_Tech_LEFTToPNews) (5. september 2011).
33. *Varni na internetu*. Dostopno prek: <http://www.varninainternetu.si/nosilci-projekta/> (16. maj 2011).
34. Walters, Chris. 2009. *Facebook's New Terms of Service: »We Can Do Anything We Want Eith Your Content. Forever«*. Dostopno prek: <http://consumerist.com/2009/02/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever.html> (1. september 2011).

35. *What is social networking?* Dostopno prek: <http://www.whatissocialnetworking.com/>  
(1. september 2011)
36. *Zakon o varstvu osebnih podatkov (ZVOP-1-UPB1)*. Uradni list RS 94/2007. Dostopno prek: <http://www.uradni-list.si/1/objava.jsp?urlid=200794&stevilka=4690> (15. maj 2011).

## **PRILOGE**

### **Priloga A**

**Intervju z gospodom Sašo Samardžićem, zaposlenim pri podjetju SAOP, celostne informacijske rešitve, Šempeter pri Novi gorici.** (intervju opravljen pri gospodu na domu, dne 19.4.2009)

**1. Zanima me predvsem Vaš pogled na pridobivanje in zbiranje osebnih podatkov v spletnih mrežah, primer Facebooka, MySpace in ostalih podobnih aplikacijah?**

»Ne vidim problema tukaj, saj podatke predajaš tiste za katere se sam odločiš, noben te ne prisili v to.«

**2. Je Facebook kot družbena spletna stran, ki jo danes uporablja že preko 200 milijonov uporabnikov, nevaren zaradi kopičenja osebnih podatkov, ustvarjanja neverjetno širokih podatkovnih baz? In je kajpak zelo "priročen" za vse možne zlorabe.**

»Tudi tukaj ne vidim problema, saj sam moreš poskrbet kaj objavljaš na spletu. Je pa nevaren, in tudi škodljiv. Vsak naj poskrbi zase oziroma naj se ljudje ustrezno izobražujejo o zlorabah na spletu. Spletne aplikacija kot je Facebook sigurno ni bila ustvarjena z namenom zbiranja podatkov in je precej zaščitena. Same ustvarjalce spletnih aplikacij ne zanimajo naši podatki, za vdore pa ustrezno poskrbijo, kar pa seveda ne more vedno delovati. Tudi najboljši sistemi včasih padejo.«

**3. Se ljudje sploh zavedamo, da so takšne "nedolžne" stvari, kot so razne povezovalne mreže, nov korak v odpiranju vrat v našo spalnico, zasebnost, intimo, ali smo za te situacije sami krivi?**

»Večini ljudi je to všeč, da jih zunanji svet vidi. (primer Youtube). Za vse so ljudje sami krivi, zdaj pa je vprašanje ali je to neizobraženost ali ignoranca na vse to.«

**4. Ali mislite, da bi se ta fenomen, ki je izbruhnil ravno zaradi "Facebook afere", lahko zakonsko uredil in omejil? Ali bi na ta način bili uporabniki zaščiteni pred možnimi zlorabami ter ali bi spletne mreže zaradi zakonskih ureditev postale uporabnikom manj prijazne in bi jih pri tem omejevale?**

»Še vedno menim, da te noben ne prisili, da se prijaviš na Facebook in da se ljudje sami kažejo navzven. Z zakonom bi kvečjemu škodili spletnim aplikacijam kot je Facebook in njihovim lastnikom, omejili pa nebi ničesar. Samo poučevanje o spletnih aplikacijah lahko uporabnike zaščiti, ne pa zakon. Facebook je že dobro zaščiten, saj imaš celo paleto dovoljenj in prepovedi za nastaviti. Tega se ne more urediti z zakonom. Odločitev je pri vsakem posamezniku.«

**5. Pri nas obstajajo zakoni in evropske direktive, ki jih ustvarjalci spletnih strani "morajo" upoštevati, primer Konvencije Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, Zakon o varstvu osebnih podatkov, Zakon o elektronskih komunikacijah, itd. Mislite, da je to dovolj, oz. ali je to korak, ki bi lahko pripomogel k boljšemu nadzoru nad omenjeno problematiko, ali je potrebno narediti še veliko več?**

»Ne poznam vsebine teh zakonov. Treba ljudi izobraževati, ne pa spletne aplikacije omejevat. Ker nekdo potrebuje ravno takšne spletne aplikacije, da se izkaže (primer Susan Boyle - Britains Got Talent 2009 - milijon klikov na Youtube-u v nekaj dneh). Zato sem proti omejevanju spletnih aplikacij. Vsak naj poskrbi za svoje podatke, tako kot skrbijo za svojo denarnico, v kateri imajo vozniški izpit, osebno, kreditno kartico, itd.....«

**6. Kakšno vlogo ima pri vsem tem, po vašem mnenju, država, saj vemo, da si nekatere države želijo prilastiti tudi podatke pridobljene na spletnih omrežjih?**

»Nisem proti, prej ko slej se bo to zgodilo. Na navadne smrtnike ne vpliva veliko, saj smo nepomembni za njih, se zna pa na tak način zajezi kriminal, kriminal vseh vrst.«

**7. Za konec še vprašanje, ali se vam omenjena situacija v Sloveniji, v tem trenutku, zdi alarmantna, ali še nismo prišli do točke, kjer bi nas moralo skrbeti, kje in na kakšen način bodo naše osebne stvari (podatki, slike, itd.) končale, ter ali lahko uporabniki sami kaj pripomoremo za boljše in varnejše brskanje po svetovnem spletu?**

»Še vedno ponavljam, to je samo psiha ljudi, ki sami želijo objaviti svoje fotografije in jih pokazati ostalemu svetu, večino ljudi to ne moti. Vsak se mora sam zamisliti, kaj se lahko objavi in kaj ne. Do osebnih podatkov noben na spletu nima dostopa, če jih sam ne objaviš, za osebne podatke shranjene na osebni računalnik pa ravno tako mora vsak posameznik sam poskrbeti, saj tudi ko izstopiš iz hiše, stanovanja, za sabo zakleneš vrata, tako je treba zakleniti tudi svoj računalnik. Tu pa nastopi slaba izobraženost ljudi o svetovnem spletu.«

**Najlepša hvala za Vaše odgovore.**

## **Priloga B**

**Intervju z gospodom doktorjem Kovačič Matejem, avtorjem knjige Nadzor in zasebnost v informacijski družbi.** (Intervju opravljen 2. september, 2011, prek elektronske pošte)

**1. Zanima me predvsem Vaš pogled na pridobivanje in zbiranje osebnih podatkov v spletnih skupnostih, primer Facebook?**

To se mi zdi precej problematično in sicer zato, ker na ta način ta omrežja uporabnika silijo v razkrivanje svojih osebnih podatkov, če žel biti vključen v ta omrežja, hkrati pa ta omrežja omogočajo tudi razkrivanje osebnih podatkov tretjih oseb. Poleg tega je Facebook znan po svoji slabi skrbi za zasebnost oz. po svojih invazivnih praksah. To je tudi razlog, da Facebooka ne uporabljam.

**2. Je Facebook kot družbena spletna stran, ki jo danes uporablja že preko 200 milijonov uporabnikov, nevaren zaradi kopičenja osebnih podatkov ter ustvarjanja neverjetno širokih podatkovnih baz? In je kajpak zelo "priročen" za vse možne zlorabe.**

Vsekakor.

**3. Se ljudje sploh zavedamo, da so takšne "nedolžne" stvari, kot je Facebook, nov korak v odpiranju vrat v našo spalnico, zasebnost, intimo, ali smo za te situacije sami krivi?**

Večinoma se ljudje tega premalo zavedajo, če pa že, pa se s tem pogosto sprijaznijo brez ugovorov. Posegi v zasebnost namreč ne bolijo takoj oz. neposredno, njihove posledice se lahko pojavijo šele čez daljši čas, ko pa je pogosto že prepozno kaj storiti.

**4. Zakaj so po vašem mnenju osebni podatki tako lahko dostopni in ali bi se jih po vašem mnenju dalo bolje zaščititi, ter kakšne so vse možne zlorabe?**



Osebni podatki so danes tržno blago, zato je interes za njihovo zbiranje zelo velik. Posledično je tudi pritisk na posameznike, da dajejo svoje osebne podatke zelo velik.

**5. Ali mislite, da bi se ta fenomen, ki je izbruhnil ravno zaradi "Facebook afere", lahko zakonsko uredil in omejil? Ali bi na ta način bili uporabniki interneta zaščiteni pred možnimi zlorabami ter ali bi spletne mreže zaradi zakonskih ureditev postale uporabnikom manj prijazne in bi jih pri tem omejevale?**

Odgovor ni tako enostaven. Konec koncev gre za vprašanje svobodne volje. Posamezniki imajo pravico da "naredijo neumnost". Pomembno pa je, da se zavedajo vseh posledic in da niso zavedeni.

**6. Pri nas obstajajo zakoni in evropske direktive, ki jih ustvarjalci spletnih strani "morajo" upoštevati, primer Konvencije Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, Zakon o varstvu osebnih podatkov, Zakon o elektronskih komunikacijah, itd. Mislite, da je to dovolj, oz. ali je to korak, ki bi lahko pripomogel k boljšemu nadzoru nad omenjeno problematiko, ali je potrebno narediti še veliko več?**

Vsekakor je potrebno narediti še korak naprej. Zgolj normativno urejanje področja zasebnosti ni dovolj, poleg tega je praviloma reaktivno. Danes pa so na tem področju potrebni proaktivni pristopi.

**7. Kakšno vlogo ima pri vsem tem, po vašem mnenju, država, saj vemo, da si nekatere države želijo prilastiti tudi podatke, pridobljene na spletnih omrežjih?**

Državni nadzor je seveda problematičen, mislim, pa da je danes bistveno bolj problematičen zasebni sektor, ki ima pogosto večja sredstva za zbiranje in obdelavo osebnih podatkov kot

države, poleg tega je nad zasebnim sektorjem pogosto manjši nadzor, kot na državnim zbiranjem osebnih podatkov.

**8. Kdo so po vašem mnenju igralci oz. akterji, ki bi zlorabe osebnih podatkih na medmrežju, predvsem Facebooku, lahko preprečili ali vsaj pomagali pri ozaveščanju samih uporabnikov?**

Bistven problem Facebooka je zakonodaja ZDA, ki je bistveno drugačna od zakonodaje v Evropi. Žal kakšnih hitrih sprememb na tem področju v ZDA ni pričakovati.

**9. Ali imajo, po vašem mnenju, državne institucije oz. državni akterji lahko kakšno vlogo pri regulaciji same problematike; če DA, kdo so?**

Vsekakor. Zelo pomembni so organi, ki se strokovno ukvarjajo s področjem zasebnosti. Pri nas je to Informacijski pooblaščenec, po Evropi pa njemu sorodni organi, ki so povezani na ravni EU.

**10. Zakaj po vašem mnenju, kljub znani problematiki varovanja osebnih podatkov na medmrežju, v Sloveniji ni potrebne iniciative za oblikovanje nekega javnopolitičnega omrežja, ki bi se z problematiko intenzivno ukvarjalo?**

Deloma zato, ker za to področje profesionalno skrbijo ustrezne uradne institucije (v mislih imam Informacijskega pooblaščenca, pa tudi projekte kot Safe.si, itd.), deloma pa tudi zato, ker večina ljudi groženj zasebnosti ne vidi kot problem, ki bi bil vreden političnega angažiranja.

**11. Za konec še vprašanje, ali se vam omenjena situacija v Sloveniji, v tem trenutku, zdi alarmantna, ali še nismo prišli do točke, kjer bi nas moralo skrbeti, kje in na kakšen**

**način bodo naše osebne stvari (podatki, slike, itd.) končale, ter ali lahko uporabniki sami kaj pripomoremo za boljše in varnejše brskanje po svetovnem spletu?**

Do te točke smo prišli že zdavnaj, dejstvo pa je, da je od uporabnikov težko pričakovati, da bodo sposobni slediti nevarnostim, ki jih za zasebnost in varnost na internetu prinaša tehnološki razvoj. Delno zagotovo lahko vsak poskrbi za svojo varnost, del problema pa je potrebno reševati z drugimi ukrepi - zakonodajo in drugimi, zlasti proaktivnimi pristopi za zaščito zasebnosti.

**Najlepša hvala za Vaše odgovore.**

## **Priloga C**

**Intervju z Gospo Natašo Pirc Musar, univ. dipl. prav., informacijska pooblaščenka.  
Intervju opravljen prek elektronske pošte, dne 25. 4. 2009.**

### **1. Zanima me predvsem Vaš pogled na pridobivanje in zbiranje osebnih podatkov v spletnih mrežah, primer Facebooka?**

Z izdelavo profila na spletiščih za socialno druženje uporabnik (lahko) javno objavi nekatere svoje osebne podatke. Ker pa gre za **objavo podatkov s soglasjem** – uporabnik dovoli spletišču, da uporablja, obdeluje in objavi njegove podatke, je nadzor nad morebitno nezakonito uporabo podatkov s strani spletišča običajno precej omejen (največkrat le na uporabo podatkov izven namena, s katerim je bil posameznik seznanjen).

Zakon o varstvu osebnih podatkov npr. določa, da je v zasebnem sektorju (kamor spadajo ponudniki spletnih mrež) pravna podlaga za obdelavo osebnih podatkov lahko tudi privolitev posameznika. Enako velja tudi v primeru obdelave občutljivih osebnih podatkov. Pri tem so upravljavci sicer omejeni z namenom obdelave, vendar pa lahko namen obdelave določijo precej široko – če se posameznik s tem strinja in torej privoli v tako širok namen obdelave njegovih osebnih podatkov oz. celo v posredovanje njegovih osebnih podatkov tretjim osebam, takšna obdelava torej ni protipravna (v kolikor seveda upravljavec upošteva tudi ostale določbe zakonodaje – ustrezno zavarovanje osebnih podatkov, dolžnost obveščanja posameznikov ipd.).

### **2. Je Facebook kot družbena spletna stran, ki jo danes uporablja že preko 200 milijonov uporabnikov, nevaren zaradi kopičenja osebnih podatkov, ustvarjanja neverjetno širokih podatkovnih baz? In je kajpak zelo "priročen" za vse možne zlorabe.**

Nedvomno. Posledično je večja možnost zlorabe profilov in podatkov na profilih – npr. kraja identitete,<sup>1</sup> kopiranje profila ali velike količine podatkov iz profila, ki se jih nato uporabi v

---

1 Glej tudi novice o kraji identitete v primeru spletišča Facebook na spletni strani [www.safe.si](http://www.safe.si).

druge namene (»googlanje« za potrebe zaposlovanja...), ipd. Možnosti zlorabe se večajo s prihodom novih aplikacij (npr. aplikacija za sledenje preko mobilnega telefona) in z uporabo ne dovolj varnih spletnih struktur s strani ponudnikov spletišč. Pri tem je pomembno tudi dejstvo, da podatki pogosto ostanejo na spletu tudi potem, ko uporabnik svoj profil npr. izbriše, bodisi se avtomatsko shranijo na strežniku (npr. pri arhiviranju, cachiranju) bodisi jih shrani nekdo tretji.<sup>2</sup>

Vendar pa je bistvenega pomena sam **način uporabe** socialne mreže. Posameznik namreč lahko z lastnim ravnanjem precej zlorab prepreči (npr. da profila nima odprtega za vse, da posreduje čim manj svojih osebnih podatkov ali pa da si ustvari profil pod namišljenim imenom, da je previden pri posredovanju svojih osebnih podatkov, da temeljito prebere splošne pogoje in preveri, s čim vse se mora strinjati, da si ustvari profil, da upošteva vse varnostne napotke ipd.).

### **3. Se ljudje sploh zavedamo, da so takšne "nedolžne" stvari, kot je Facebook, nov korak v odpiranju vrat v našo spalnico, zasebnost, intimo, ali smo za te situacije sami krivi?**

Kot že omenjeno v prejšnjem odgovoru, lahko posameznik veliko naredi za to, da se prepreči zlorabo njegovih osebnih podatkov. Težava pa je predvsem v **ne zavedanju uporabnikov o možnih posledicah razkrivanja svojih podatkov**. Povprečen uporabnik se pogosto ne zaveda, da je tudi npr. fotografija osebni podatek in da se lahko tudi ta (predvsem v povezavi z osebnim imenom) lahko zlorabi. Povprečni uporabnik tudi ne bere splošnih pogojev, opozoril o varstvu osebnih podatkov ipd. Zato se pogosto ne zaveda, kakšna pooblastila daje ponudniku storitev spletišča. Pri tem je nevarnost toliko večja v primeru **uporabe s strani mlajših generacij** (ne nujno mladoletnikov!). Gre za generacije, ki so se z računalniki in internetom dodobra seznanile že v zelo mladih letih in jim zato uporaba ni tuja. Posledično so pri svoji uporabi spleta brezskrbni – prepričani, da se jim ne more nič zgoditi, saj okolje dobro poznajo. Poleg tega imajo drugačen odnos do zasebnosti in so pripravljene razkriti več kot pripadniki starejših generacij. Še največja pa je nevarnost zlorab v primerih uporabe s strani

---

<sup>2</sup> Ponudnik spletišča Facebook npr. sprva svojim uporabnikom ni omgočal trajne ukinitve računa, ampak le deaktivacijo. Njihovi profili sicer potem na spletni strani niso bili več vidni, vendar pa so ostali na strežniku.

mladoletnikov, saj ti pogosto veliko bolj obvladajo uporabo računalnika in spleta kot njihovi skrbniki, kar slednje zelo omejuje pri njihovi vlogi nadzora in uveljavljanja "pametne" uporabe.

Bistvenega pomena je torej (kot že rečeno), **kako previden je uporabnik in kako vesten je pri prebiranju določb** pogodbe, preden jo sklene s ponudnikom socialne mreže (ustvarjanje profila je namreč ravno to – sklenitev pogodbe!).

**4. Ali mislite, da bi se ta fenomen, ki je izbruhnil ravno zaradi "Facebook afere", lahko zakonsko uredil in omejil? Ali bi na ta način bili uporabniki zaščiteni pred možnimi zlorabami ter ali bi spletne mreže zaradi zakonskih ureditev postale uporabnikom manj prijazne in bi jih pri tem omejevale?**

Po mnenju Pooblaščenca je nemogoče pripraviti takšno (hermetično) zakonodajo, ki bi onemogočila možnost zlorab pri uporabi socialnih mrež oz. pri posredovanju osebnih podatkov v splet. Tudi če bi takšna možnost obstajala, je treba upoštevati, da je najboljša zakonodaja tista, ki omogoča **vzpostavitev ravnovesja med varnostjo in svobodo**, med interesom javnosti in interesom posameznika. Treba je namreč upoštevati, da vsaka nova tehnologija, vsako novo orodje pomeni hkrati lahko tudi nevarnost (internet npr. pomeni tako zelo koristno orodje pri širjenju informacij, vsebin – tudi znanja, vendar hkrati nevarnost za zlorabo podatkov, nelegalno reprodukcijo in distribucijo avtorskih del ipd.). To pa ni dovolj dober razlog, da bi uporabo takšnih orodij prepovedali.

Bistvo torej ni v pripravi bolj striktno in omejevalne zakonodaje, ampak predvsem v **izobraževanju uporabnikov o pravilni in priporočljivi rabi** socialnih mrež in interneta nasploh ter o **previdnosti pri razkrivanju oz. posredovanju svojih osebnih podatkov**.

**5. Pri nas obstajajo zakoni in evropske direktive, ki jih ustvarjalci spletnih strani "morajo" upoštevati, primer Konvencije Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, Zakon o varstvu osebnih podatkov, Zakon o elektronskih komunikacijah, itd. Misli, da je to dovolj, oz. ali je to korak, ki bi lahko**

**pripomogel k boljšemu nadzoru nad omenjeno problematiko, ali je potrebno narediti še veliko več?**

Zakonodaja lahko pomaga regulirati področje, predvsem z uzakonitvijo pravil, ki se jih morajo držati upravljavci zbirk osebnih podatkov. Izjemno pomembna so osnovna načela varstva osebnih podatkov, med njimi načelo sorazmernosti (»Obdeluj točno toliko podatkov, kot jih potrebuješ za doseg cilja.«) in načelo sledljivosti, ki pri upravljavcih preprečuje radovednost zaposlenih in na ta način zlorabe osebnih podatkov. Največja težava pa je zagotovo ta, da pravo vedno zaostaja za modernimi informacijskimi tehnologijami, zato je ozaveščanje upravljavec in posameznikov toliko bolj pomembno.

**6. Kakšno vlogo ima pri vsem tem, po vašem mnenju, država, saj vemo, da si nekatere države želijo prilastiti tudi podatke, pridobljene na spletnih omrežjih?**

Država ima predvsem nalogo varovati posameznika in njegove človekove pravice (kamor sodi tudi pravica do varstva osebnih podatkov). Da bi dosegla in uresničila te naloge, mora država predvsem poskrbeti z ustrezno zakonodajo in z ustreznim izvrševanjem te zakonodaje. Ukrepati mora tako represivno (s sankcioniranjem kršiteljev) kot tudi preventivno (z izobraževanjem posameznikov in upravljavcev).

V kolikor pa bi država želela postati upravljavec osebnih podatkov posameznikov, je pri tem zelo omejena. Samo soglasje posameznika namreč v takšnem primeru ne zadošča, saj se lahko v javnem sektorju obdelujejo osebni podatki le, če tako določa zakon. Lahko pa določen zakon dovoli, da država obdeluje osebne podatke posameznikov na podlagi njihove privolitve. To seveda v primeru spletišč za socialno druženje ne velja. V kolikor pa bi kakšen organ iz javnega sektorja kršil določbe veljavne zakonodaje s področja varstva osebnih podatkov, bi se proti njemu (tako kot proti entiteti zasebnega sektorja) lahko uvedli ustrezni postopki in v primeru ugotovitve kršitve tudi ustrezne sankcije. Res pa je, da države postajajo vse bolj »požrešne« in z izgovorom, da želijo povečati našo varnost, obdelujejo vse več naših podatkov. Da bi ujeli 5 % ljudi, ki jih vodijo zli in kriminalni nameni, posega v zasebnost 95

% (kolikor toliko) poštenih ljudi. To pa so nevarnosti, ki na koncu pomenijo konec svobode (in efekt velikega brata oz. če povem bolj po domače »Trumanov show«).

Morda lahko to ilustriram z znamenitim stavkom nekdanjega ameriškega predsednika Thomasa Jeffersona:

“Kdor žrtvuje delček svobode zato, da bi si zagotovil delček varnosti, bo na koncu izgubil oboje.”

**7. Za konec še vprašanje, ali se vam omenjena situacija v Sloveniji, v tem trenutku, zdi alarmantna, ali še nismo prišli do točke, kjer bi nas moralo skrbeti, kje in na kakšen način bodo naše osebne stvari (podatki, slike, itd.) končale, ter ali lahko uporabniki sami kaj pripomoremo za boljše in varnejše brskanje po svetovnem spletu?**

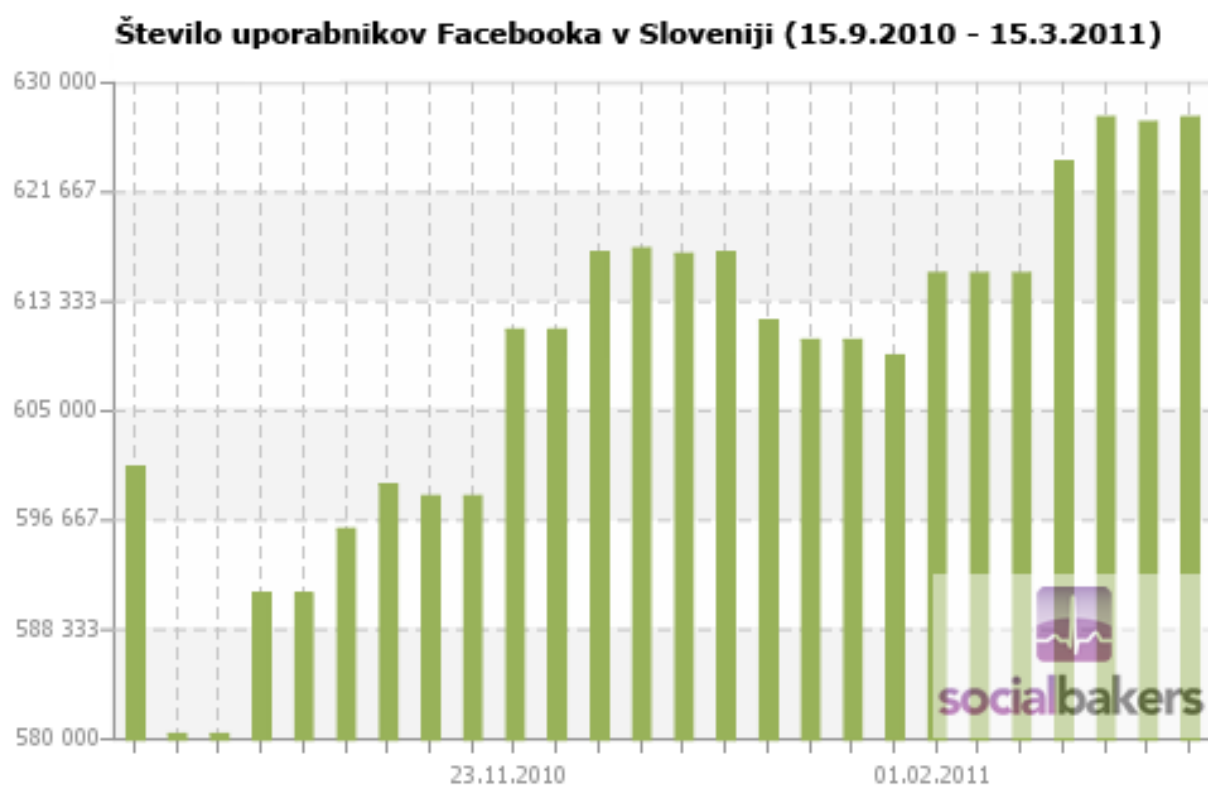
Vedno nas mora skrbeti, že zato, da ne postanemo brezskrbni. Zavedati se moramo, da poti nazaj ni več ( v čase, ko ni bilo zbirk osebnih podatkov in interneta), zato moramo vsi skupaj storiti vse, kar je v naših močeh, da stvari ne uidejo iz rok.

Mi varuhi zasebnosti na svojem področju, ko poskušamo generalno za vse in vsakogar doseči določene standarde zavarovanja in varovanja osebnih podatkov, in vsak posameznik za svojo lastno zasebnost.

**Najlepša hvala za Vaše odgovore!**



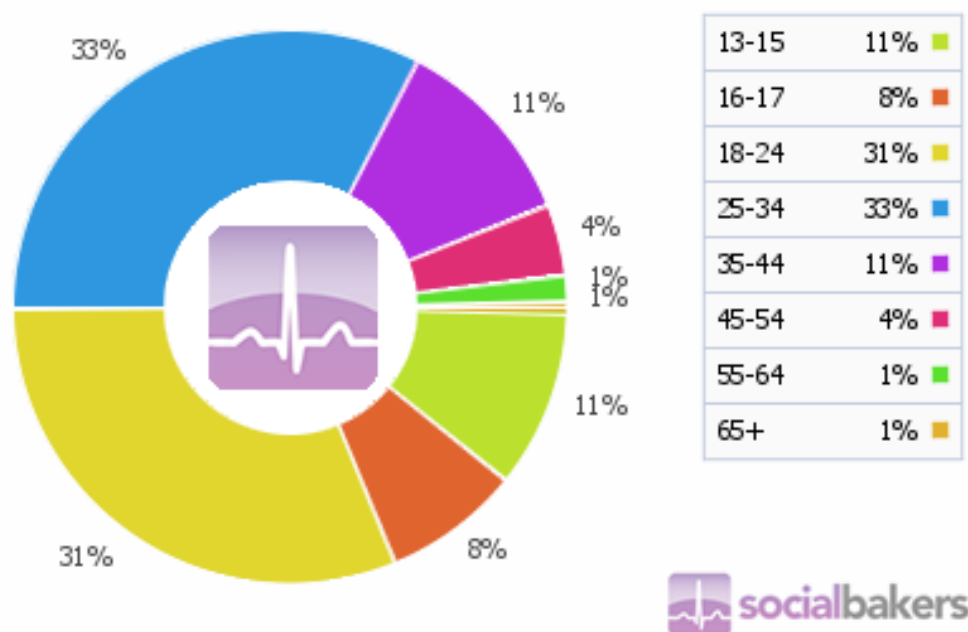
**Priloga Č: Število uporabnikov Facebooka v Sloveniji (15.9.2010 – 15.3.2011)**



Vir: RIS (2011)

**Priloga D: Starostna sestava uporabnikov Facebooka v Sloveniji (marec 2011).**

**Starostna sestava uporabnikov Facebooka v Sloveniji (marec 2011)**



*Vir: SocialBakers*

Vir:RIS (2011)

## Priloga E

### ČASOVNI POTEK INTERAKCIJ MED AKTERJI IN NASTAJANJE POLICY OMREŽJA

1999:

- Prvič sprejet Zakon o varovanju osebnih podatkov (ZVOP)
- Ustanovi se Slovenski center za posredovanje pri omrežnih incidentih, v okviru Arnesa (Akademske in raziskovalne mreže Slovenije), ki rešuje varnostne probleme v računalniških omrežjih v Sloveniji. (SI-CERT)

2001:

- Prva sprememba ZVOP, oblikuje in sprejme se ZVOP-A

2005:

- Ustanovi se SAFE: Projekt Center za varnejši internet SAFE-SI izvajajo Fakulteta za družbene vede, ARNES in Zveza potrošnikov Slovenije, financirata pa ga Generalni direktorat za informacijsko družbo in medije pri Evropski komisiji in Ministrstvo za visoko šolstvo, znanost in tehnologijo.

Aktivnosti Centra so namenjene štirim ciljnim skupinam: otrokom, mladostnikom, staršem in učiteljem. Vizija projekta je, da med izbranimi ciljnimi populacijami s sprotnim zagotavljanjem preverjenih informacij in nasvetov za varno rabo novih tehnologij v Sloveniji doseže visoko stopnjo osveščenosti o teh temah. (SAFE.SI)

2007:

- Objavi se uradno prečiščeno besedilo ZVOP-1-UPB1

2009:

- Informacijski pooblaščenec izda smernice o Varstvu osebnih podatkov in medijih (Informacijski pooblaščenec 2009)

- Informacijski pooblaščenec izda Smernice Informacijskega pooblaščenca za oblikovanje izjave o varstvu osebnih podatkov na spletnih straneh (Informacijski pooblaščenec 2009)
- Informacijski pooblaščenec ustvari profil na Facebooku, preko katerega komunicira z uporabniki in odgovarja na morebitna vprašanja.

2010:

- Projekt varni na internetu, pod okriljem SI-CERT. Projekt je zastavljen dolgoročno in naslavlja precej široko področje problematike informacijske varnosti. Dvig stopnje informiranosti o varni rabi interneta definiramo kot ključen cilj projekta osveščanja slovenske javnosti. (Varni na internetu)

Kot lahko opazimo so vse aktivnosti, ki so se odvijale od leta 2009 naprej plod preišljene analize in raziskovanja interneta in njegovih pasti. Prav zaradi novih problematik, ki se pojavljajo ob vsakdanji rabi interneta je napredovala tudi interakcija med samimi akterji in tako povzročila oblikovanje nekega omrežja, ki deluje na zelo zakonsko krhkih temeljih.