UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

Diplomsko delo

ZLORABA OSEBNIH PODATKOV V SPLETNIH SOCIALNIH OMREŽJIH

Urška Tavželj

Ljubljana, september 2011

UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

DIPLOMSKO DELO

ZLORABA OSEBNIH PODATKOV V SPLETNIH SOCIALNIH OMREŽJIH

Kandidatka: Urška Tavželj
Vpisna številka: 04036535
Študijski program: univerzitetni študijski program Uprava prva stopnja
Mentor: prof. dr. Mirko Vintar

Ljubljana, september 2011

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisana Urška Tavželj, študentka univerzitetnega študijskega programa Uprava prva stopnja, z vpisno številko 04036535, sem avtorica diplomskega dela z naslovom:« Zloraba osebnih podatkov v spletnih socialnih omrežjih.«

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega lastnega raziskovalnega dela;
- sem poskrbela, da so dela in mnenja drugih avtorjev oz. avtoric, ki jih uporabljam v predloženem delu, navedena oz. citirana v skladu s fakultetnimi navodili;
- sem poskrbela, da so vsa dela in mnenja drugih avtorjev oz. avtoric navedena v seznamu virov, ki je sestavni element predloženega dela in je zapisan v skladu s fakultetnimi navodili;
- sem pridobila vsa dovoljenja za uporabo avtorskih del, ki so v celoti prenesena v predloženo delo in sem to tudi jasno zapisala v predloženem delu;
- se zavedam, da je plagiatorstvo – predstavljanje tujih del, bodisi v obliki citata bodisi v obliki skoraj dobesednega parafraziranja bodisi v grafični obliki, s katerim so tuje misli oz. ideje predstavljene kot moje lastne – kaznivo po zakonu (Zakon o avtorstvu in sorodnih pravicah, Ur. list RS št. 21/95), prekršek pa podleže tudi ukrepom Fakultete za upravo v skladu z njenimi pravili;
- se zavedam posledic, ki jih dokazano plagiatorstvo lahko predstavlja za predloženo delo in za moj status na Fakulteti za upravo;
- je elektronska oblika identična s tiskano obliko diplomskega dela ter soglašam z objavo dela v zbirki »Dela FU«.

Diplomsko delo je lektorirala: Mateja Kržišnik.

V Ljubljani, 14. 9. 2011

Podpis avtorice: Urška Tavželj

POVZETEK

V diplomskem delu obravnavam problematiko zlorabe osebnih podatkov pri uporabi spletnih socialnih omrežij. Cilji zlorabe osebnih podatkov v spletnih socialnih omrežij so različni, vendar pa lahko izpostavimo skupen cilj, ki je, da od uporabnikov, ki so tarča napada, pridobijo zaupne podatke, do katerih niso upravičeni. V delu omenjam mnoga obstoječa spletna socialna omrežja, največ pozornosti pa je namenjene najpopularnejšemu na našem območju, to je Facebook. V prvem delu se ukvarjam z vprašanjem opredelitve varstva osebnih podatkov ter uporabo spletnih socialnih omrežij. Velik poudarek pripisujem predstavitvi zlorabe osebnih podatkov ter nevarnostnim zlorabe osebnih podatkov v spletnih socialnih omrežjih.

S hitrim razvojem informacijske tehnologije se širijo nevarnostni zlorab osebnih podatkov, od katerih jih nekaj predstavljam v zaključnem delu. V nalogi poudarjam, da je varnost osebnih podatkov posameznika v veliki meri odvisna od njega samega, zato so predstavljeni tudi nekateri ukrepi in opozorila. Zloraba osebnih podatkov v spletnih socialnih omrežjih je ključna smernica celotnega diplomskega dela. V njem preučujem zlorabo osebnih podatkov, ali se uporabniki spletnih socialnih omrežij zavedajo nevarnosti na spletu, kakšne so možnosti nastavitev zasebnosti. V ta namen so bili opravljeni intervjuji z različnimi vodilnimi osebami na tem področju.

Ključne besede: osebni podatki, spletna socialna omrežja, Facebook, nevarnosti na spletu, zloraba osebnih podatkov, intervju.

SUMMARY

ABUSE OF PERSONAL DATA WITHIN WEB SOCIAL NETWORKS

I deal with problems of abuse of personal data over use of web social networks in a dissertation. Goals of abuse of personal data are different, however we can emphasise common goal, only-this is, he gives of users, that they are target of a attack, they gain confidential data, they aren't justified until which. I am mentioning many existent web social networks within work, any more attention is assigned most popular on our range, he is eating Facebook-u's this. I engage in question of definition of protection of personal data and use of web social networks within first work. I am ascribing large emphasis to a presentation of abuse of personal data and nevarnostnim abuse of personal data in web social networks.
With quick development of information technology expand nevarnostni abuses of personal data, I am introducing them some since which within completed work. I am emphasising in task, that is safety of personal data individual in large degree dependent from him alone, therefore also some measures and warnings are introduced. Abuse of personal data within web social networks is key guideline of a entire dissertation. I was looking into abuse of personal data in a dissertation, or users of web social networks are aware of danger online, possibilities of settings of privacy are some. V this intention finished interviews with different management people on this field.

Key words: personal data, web social networks, Facebook, dangers on web, interview, abuse of personal data.

KAZALO

KAZALO PONAZORITEV

KAZALO SLIK

KAZALO PRILOG

1 UVOD

Osnovni namen spletnih socialnih omrežij je vzpostavljanje medsebojnih povezav in komuniciranje uporabnikov, zato le-ta uporabnike spodbujajo, da objavijo čim širši nabor svojih zasebnih in osebnih podatkov. Razlogov za nepremišljeno navedbo osebnih podatkov je več. Eden izmed njih je (lažen) občutek anonimnosti ter varnostni. Uporabniki, ki objavljajo podatke o sebi le za svoje prijatelje, se ne zavedejo (pasti in nevarnostni), da jih tako lahko preberejo tudi drugi. Internet je postal nekakšna ječa, ki je posameznika zaprla v 'zlato' kletko personaliziranih spletnih izkušenj. Zloraba osebnih podatkov v spletnih socialnih omrežjih je čedalje bolj pogost pojav, ljudje pa se premalo zavedamo negativnih učinkov in škodljivih posledic njihove uporabe. Zbiranje podatkov oziroma zloraba zasebnosti je v virtualnem svetu mogoča na več načinov. Ne zavedamo se, da z uporabo računalniške in telekomunikacijske tehnologije v virtualnem prostoru puščamo sledove, tako namerno kakor tudi nevede. S hitro rastjo uporabe informacijsko-komunikacijskih tehnologij se povečujejo tudi možnosti zlorab osebnih podatkov. Pri tem je ena ključnih varovalk večja osveščenost uporabnikov, zato želim z opisi nekaterih pasti in priporočili za varno uporabo prispevati k večji skrbi in boljšemu varovanju osebnih podatkov.

Namen diplomskega dela je povečati zavedanje uporabnika glede zlorabe osebnih podatkov, medtem ko ta uporablja spletna socialna omrežja. Posebno pozornost namenjamo spletnim socialnim omrežjem, z uporabo katerih se problematika zlorabe osebnih podatkov pokaže še bolj občutljiva. Predstavili bomo izhodišča in možnosti zlorabe osebnih podatkov, ki so večini uporabnikom neznane. Ob tem bomo dodatno pozornost namenili spletnim socialnim omrežjem. Izpostavili bomo pomen zlorabe osebnih podatkov pri uporabi v spletnih socialnih omrežjih ter hkrati raziskali nevarnosti v spletnem raziskovalnem okolju. S pomočjo analize literature in virov ter na podlagi že opravljenih raziskav na tem področju želimo predstaviti zlorabo osebnih podatkov.

Facebook je v zelo kratkem času postal eno najbolj priljubljenih spletnih socialnih omrežij po celem svetu, zadnjih nekaj let tudi v Sloveniji. Prav hiter razvoj in njegova popularnost med množicami ljudi sta nas navdihnila, da raziščemo fenomen Facebooka. Predvsem pa se poleg njega osredotočamo tudi na zlorabo osebnih podatkov v spletnih socialnih omrežjih.

Glavni cilji diplomskega dela so tako:

1. seznanitev s področjem zlorabe osebnih podatkov v spletnih socialnih omrežjih,
2. predstaviti vse razsežnosti pojma zloraba osebnih podatkov,

3. predstaviti varno rabo osebnih podatkov v spletnih socialnih omrežjih,
4. opisati značilnosti delovanja nevarnosti v spletnih socialnih omrežjih.
5. opisati značilnosti delovanja nevarnosti v spletnih socialnih omrežjih.

Omenjene cilje bomo preverjali s pomočjo naslednjih hipotez:

1. Zloraba osebnih podatkov v spletnih socialnih omrežjih se povečuje.
2. Z razcvetom socialnih omrežjih postaja zloraba osebnih podatkov enostavnejša.
3. Razvoj informacijske tehnologije vpliva na zlorabo osebnih podatkov.

Kot osnovno tezo postavljamo trditev, da lahko z upoštevanjem premišljene uporabe osebnih podatkov in pravilnih varnostnih nastavitvah uporabnik sam zmanjša možnost zlorab osebnih podatkov v spletnih socialnih omrežjih. V diplomskem delu se bomo opirali na že obstoječa spoznanja, opredeljena v domači in tuji literaturi, celotno delo pa bo temeljilo na metodi deskripcije, na opisu in predstavitvi zlorabe osebnih podatkov v spletnih socialnih omrežjih. Uporabljena bo najpogostejša sociološka metoda spraševanja – intervju, ki omogoča kvalitativno obdelavo podatkov. V ospredje so bila postavljena stališča, videnja in prepričanja ljudi, ki so eksperti na tem področju.

V raziskavi je bila uporabljena tudi teoretično-deskriptivna metoda za uporabo študije in interpretacije že napisane literature, ki zajema:

- komparativno metodo (metoda primerjave),
- metodo deskripcije (metoda opisovanja),
- metodo kompilacije (metoda navedb drugih avtorjev).

Uporabljena pa je bila tudi eksperimentalno-kavzalna metoda za pridobivanje informacij iz naslova eksperimentiranja (pregledovanje spletnih strani).

Diplomsko delo je strukturirano v deset poglavij. Uvodnemu delu sledi poglavje o varstvu osebnih podatkov, v katerem so na kratko opredeljeni osnovni pojmi zasebnosti na internetu, varstvo osebnih podatkov in zaščita zasebnosti. Drugo poglavje se nanaša na pomen množičnih medijev, predvsem medijev kot sredstva manipulacije. V četrtem poglavju, ki obsega štiri podpoglavja, so predstavljena poglavitna spletna socialna omrežja. Sledi peto poglavje, razdeljeno na tri postavke, ki zajema primere potencialnih nevarnosti za zlorabo osebnih podatkov, zasebnost, razkrivanje osebnih podatkov in krajo identitete in se nadaljuje v predstavitev pregleda varnostnih nastavitev na spletnih socialnih omrežjih. Šesto poglavje temelji predvsem na nevarnostih in morebitnih kršitvah osebnih podatkov pri uporabi spletnih socialnih omrežij. V sedmem poglavju preverjamo postavljene hipoteze in podrobno

analiziramo intervjuje. Osmo poglavje je namenjeno zaključku diplomskega dela. V devetem poglavju so navedeni literatura in viri. Celotno delo se zaokroži v desetem poglavju, kjer so zbrane priloge.

Nobena spletna aktivnost ne omogoča popolne zasebnosti. Ne samo, da pri brskanju po spletu puščamo elektronske sledi, še več: mnogo spletnih storitev in aktivnosti je zasnovanih tako, da nas spodbujajo, da na spletu razkrijemo čim več o sebi.

Številni ponudniki spletnih vsebin zbirajo osebne podatke o uporabnikih interneta (imena, naslovi, telefonske številke, e-poštni naslovi), ob tem pa pogosto ne navedejo, s kakšnim namenom bodo zbrani podatki uporabljeni. Poleg takšnega odkritega zbiranja podatkov se osebni podatki zbirajo tudi s pomočjo t. i. piškotkov (ang. cookies).

Nove tehnologije so omogočile, da tudi sami objavljamo informacije, nad čimer so seveda najbolj navdušeni mladi. S tem se odpirajo velike priložnosti za kreativnost: slike in videoposnetke lahko s pomočjo mobilnega telefona posnamemo v vsakem trenutku in prav tako hitro jih lahko pošljemo svojim prijateljem v imeniku ali naložimo na spletno stran, blog, svoj profil v socialnem omrežju itd. Slike, ki smo jih enkrat objavili, ostanejo na spletu, kjer jih lahko vidi kdorkoli, še leta po tem, ko so bile objavljene. Možnost označevanja oseb na slikah, ki jih ponuja večina socialnih omrežij, pa precej olajša delo tistemu, ki se na spletu loti iskanja fotografije nekoga. Otroci in najstniki, ki veliko uporabljajo spletne strani socialnih omrežij in drugih novih spletnih storitev, prek njih izražajo svojo identiteto, hkrati pa so lahko tudi zelo dovzetni in hitro prizadeti zaradi žaljenja, zmerjanja in opravljanja, saj šele razvijajo svojo osebnost in samopodobo.

Mladi se ne zavedajo dovolj, da lahko do osebnih informacij, ki jih objavljajo na spletu, dostopajo vsi, vključno z njihovimi starši, učitelji, bodočimi delodajalci, ljudmi s slabimi nameni. Mnogi delodajalci preverjajo, kakšne informacije lahko o kandidatu za službo najdejo na spletu. Osebne informacije, ki so objavljane v spletnih socialnih omrežjih, lahko uporabijo tudi ljudje z namenom spolne zlorabe, izsiljevanja ipd.

Tudi če sami ne objavljamo neprimernih fotografij, se moramo zavedati, da jih lahko objavi nekdo drug in jih prikaže v popolnoma drugem kontekstu, kjer postanejo za nas žaljive. Ker so fotografije digitalne, jih ni težko kopirati, združiti z drugimi ali kako drugače spremeniti, predrugačiti.

Z diplomskim delom želimo natančno preučiti pojem zlorabe osebnih podatkov v spletnih socialnih omrežjih ter pojavljanje le-teh v Sloveniji in približati uporabnikom spletnih socialnih omrežij nevarnosti uporabe osebnih podatkov na spletnih socialnih omrežjih.

2 VARSTVO OSEBNIH PODATKOV

Problem zasebnosti ni več samo tehnični, ampak je tudi družbeni problem. Uporabniki interneta bi se morali bolj zavedati nevarnostni različnih zlorab in tudi, kako se proti njim zavarovati, saj je s samozaščitnim ravnanjem varnost mogoče precej povečati (Kovačič, 2003, str. 62).

Pomemben del zaščite informacijske zasebnosti sta nadzor pretoka in posredovanje podatkov, ki se nanašajo na nekega posameznika. Mellours ugotavlja, da najboljša zaščita ni ta, da oni vedo manj o nas, ampak da mi vemo več o njih, s tem da vemo, kaj oni vedo o nas in kako te informacije uporabljajo (Mellors v Raab v Kovačič, 2003, str. 37).

Uporabniki interneta se na splošno ne zavedajo, da vsak prispevek, ki ga pošljejo na kakšen forum, vsak delček elektronske pošte, ki jo pošiljajo, vsako spletno stran, ki jo obiščejo, ter vsako stvar, ki jo kupijo v spletnih trgovinah, lahko opazuje tretja oseba, ki je ne vidimo. Vpliv na zasebnost je zelo velik, saj obstajajo baze podatkov, ki dajejo ali prodajajo zbirke osebnih informacij, ta praksa pa postaja vedno bolj pogosta z rastjo povpraševanja po informacijah. Grožnjo zasebnosti na internetu lahko razdelimo na dva dela. Kot prvo so naše aktivnosti na internetu opazovane s strani neavtoriziranih oseb, kot drugo pa se informacije shranjujejo in so dostopne še mnogo let (Goldberg, 2000, str. 2–5).

2.1 ZASEBNOST NA INTERNETU

Na zasebnost lahko gledamo z različnih perspektiv, ki vključujejo pravice državljanov ter varovanje potrošnikov. Zasebnost je pravica ljudi, da nadzorujejo, katere informacije o njihovem življenju ostanejo pri njih doma, katere gredo lahko v javnost (Barnes, 2006).

Kovačič (2006, str. 12) pravi, da je zasebnost pomembna, ker ščiti svobodo posameznika, kar pomeni, da omogoča svobodo odločanja, torej odločanje brez vmešavanja in prisile drugih. Prisila ni nujno samo neposredna in fizična, ampak gre lahko tudi za manipulacijo in pritiske; internet pa je te probleme zasebnosti prenesel tudi v virtualni prostor.

Čebulj (v Kovačič, 2000, str. 121) navaja tri elemente zasebnosti:

- zasebnost prostora (možnost posameznika, da je sam),
- zasebnost osebnosti (svoboda izražanja),
- informacijska zasebnost (možnost posameznika, da ima nadzor nad svojimi osebnimi informacijami).

V informacijski družbi je najbolj ogrožena informacijska zasebnost, kamor sodi tudi varstvo osebnih podatkov, ostala dva elementa pa sodita med temeljne človekove pravice.
Poročilo Privacy and Human Rights 2003 ločuje zasebnost v štiri kategorije (Laurant, 2003):

- informacijska zasebnost – zajema pravila o zbiranju in obdelavi osebnih podatkov, kot so informacije o plačilnih karticah, zdravstvene in vladne informacije ter druge;
- zasebnost telesa – ščiti človeška telesa pred invazivnimi posegi, kot so genetsko testiranje, testiranje drog in drugo;
- zasebnost komunikacije – vključuje varovanje in zasebnost elektronske pošte, navadne pošte, telefonskih številk in ostalih načinov komunikacije;
- prostorska zasebnost – določa mejo vdora v domače, delovno in javno okolje, kamor sodi tudi videonadzor.

En vidik razumevanja zasebnosti je pravica biti puščen v miru, kar je tudi vzrok za razumevanje problema nezaželene elektronske pošte ali 'spama' in neposrednega trženja kot nečesa, kar vdira v zasebnost posameznikov, čeprav pri teh vdorih v zasebnost ne gre za odtekanje informacij (Kovačič, 2006, str. 43).

Katz in Rice (v Barnes, 2006) opisujeta internet kot panoptikon[1]. Idejo panoptikona vidita v neprestanem nadzoru nad posamezniki s parasocialnimi mehanizmi, ki vplivajo na vedenje posameznikov samo zaradi možnosti, da nas nekdo opazuje. Internet je lahko uporabljen kot parasocialni mehanizem za opazovanje spletnih interakcij.

Trije glavni trendi, ki pripomorejo k vdoru v zasebnost so (Banisar, 1999):

- globalizacija – odpravlja geografske omejitve pretoka podatkov. Internet je najbolj znan primer globalne tehnologije;
- konvergenca – vodi v odpravo tehnoloških ovir med sistemi. Moderni informacijski sistemi vedno bolj sodelujejo z drugimi, medsebojno si lahko izmenjujejo in obdelujejo različne oblike podatkov;
- multimediji – informacije, zbrane v določene oblike, se lahko pretvorijo v drugačne oblike.

[1] Filozofa in pravnika Jeremyja Benthama poznamo predvsem po načrtu zapora Panoptikon, ki ga je predstavil leta 1791. Panoptikon je bil zamišljen kot krožna zgradba, v središču katere se nahaja inšpektor, v celicah na obodu pa so zaporniki. Bentham si je zapor zamislil tako, da bi inšpektor zapornike vedno lahko videl in slišal, obratno pa to ne bi bilo mogoče.

2.1.1 OSEBNI PODATKI

Cilj informacijske zasebnosti je kontrola nad lastnimi osebnimi podatki, zato je treba natančno definirati pojem osebni podatki.

Evropska direktiva o varstvu podatkov (95/46/ES) podaja naslednjo opredelitev pojma osebni podatek (Delovna skupina za varstvo podatkov, 2007): »Osebni podatek pomeni katerokoli informacijo, ki se nanaša na določeno ali določljivo fizično osebo (posameznik, na katerega se nanašajo osebni podatki); določljiva oseba je tista, ki se lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali socialno identiteto.«

Zakon o varstvu osebnih podatkov od večine pravnih oseb in samostojnih podjetnikov zahteva, da ustrezno varujejo osebne podatke ter da ukrepe za zavarovanje predpišejo v notranjem aktu. Po tem zakonu je osebni podatek katerikoli podatek, ki se nanaša na posameznika (fizično osebo), ne glede na obliko, v kateri je izražen. Fizična oseba mora biti določena ali vsaj določljiva; šteje se, da je določljiva, če se jo lahko neposredno ali posredno identificira, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa. Široka zakonska definicija pojma osebnega podatka pomeni, da osebni podatki niso le tisto, kar si 'tradicionalno' predstavljamo pod tem pojmom (npr. le podatki, izpisani na osebnih dokumentih), pač pa je število možnih osebnih podatkov, ki se zbirajo o določeni osebi, praktično neomejeno (ZVOP-1, 6. člen).

2.1.1.1 Varstvo osebnih podatkov in zaščita zasebnosti

Leta 1955 je Evropska unija (EU) sprejela Direktivo o varovanju podatkov (Delovna skupina za varstvo podatkov, 2007), da bi se s tem uskladila zakonodaja držav članic pri zagotavljanju zaščite državljanov in prostega pretoka osebnih podatkov znotraj EU. Direktiva se nanaša na obdelavo osebnih podatkov v elektronskih kot tudi v fizičnih datotekah in določa skupno izhodiščno raven zasebnosti, ki ne krepi zgolj sedanje zakonodaje o varovanju podatkov, temveč določa vrsto novih pravic (Laurant, 2003, str. 5).

Osnovna načela, ki jih vsebuje direktiva, so: pravica vedeti, od kod podatki izvirajo, pravica do zahteve, da se popravi netočne podatke, pravica do povračila v primeru nezakonite obdelave in pravica do odvzema dovoljenja za uporabo v določenih okoliščinah. Direktiva vsebuje okrepljeno zaščito v primeru uporabe občutljivih osebnih podatkov, kot so informacije o zdravju, spolnem življenju ter verskem ali filozofskem prepričanju. Za komercialno ali vladno uporabo takšnih informacij je na splošno zahtevana eksplicitna in nedvoumna privolitev posameznika (Laurant, 2003, str. 6).

Evropska direktiva o varovanju podatkov določa, da morajo imeti vse države članice neodvisen organ pregona. V Sloveniji je to Urad informacijske pooblaščenke. V skladu z direktivo je tem organom dana znatna moč, saj se mora vlada pri oblikovanju zakonodaje, ki se nanaša na obdelavo osebnih podatkov, posvetovati s tem organom. Organi imajo pristojnost za vodenje preiskav in pravico do dostopa do informacij, pomembnih za njihove preiskave. Lahko izdajajo tudi ukrepe, kot je uničenje podatkov ali prepoved obdelave, kršitelje lahko sodno preganjajo, razrešujejo pritožbe in izdajajo poročila. Prav tako je organ odgovoren za javno izobraževanje in mednarodno povezovanje na področju varovanja in prenosa podatkov. Slovenija je leta 2001 dopolnila zakon o zaščiti podatkov, da bi lahko vzpostavila neodvisen nadzorni organ in si s tem zagotovila skladnost z Evropsko direktivo o varovanju podatkov, ki je bila pred tem v pristojnosti Ministrstva za pravosodje (Laurant, 2003, str. 8).

Obstajajo štirje glavni modeli za zaščito zasebnosti. V večini držav jih uporabljajo več hkrati.
V državah, ki zasebnost ščitijo najučinkoviteje, pa se hkrati uporabljajo vsi modeli (Laurant, 2003):

- nadzorni zakon – v večini držav po svetu obstaja splošni zakon o zbiranju, uporabi in obdelavi osebnih podatkov v zasebnem in javnem sektorju, nadzorno telo pa nadzira njegovo izvajanje. Ta model je priporočljiv za vse države, ki sprejemajo zakon o zaščiti podatkov, in je bil sprejet v Evropski uniji;
- sektorski zakoni – nekatere države, recimo ZDA, so se izognile vpeljavi enotnega zakona o zaščiti podatkov, vendar so sprejele zakone, ki se nanašajo na posamezne sektorje, kot sta finančni sektor in sektor informacijske tehnologije. Slabost tega modela je, da je treba za vsako novo tehnologijo vpeljati nov zakon, zato dejanska zaščita zasebnosti velikokrat zaostaja. V večini držav so sektorski zakoni sprejeti le kot dopolnilo nadzornega zakona, saj vključujejo podrobnejše informacije glede določene kategorije informacij;
- samoregulacija – teoretično je lahko zaščita zasebnosti določena z vrsto samoregulativ. Z njihovo pomočjo komercialni in javni sektorji sprejmejo pravila, s katerimi se samo nadzorujejo. Takšen model žal ni preveč uspešen, saj obstaja le malo dokazov o tem, da so podjetja res sposobna slediti samoregulacijskim zakonom;
- tehnologija za zaščito zasebnosti – tehnologija za zaščito osebnosti je postala dostopna širši javnosti, s tem pa je bila posameznikom dana možnost, da lahko sami zaščitijo svojo osebnost. Uporabniki interneta imajo na voljo vrsto programov in sistemov, ki do neke stopnje zagotavljajo zasebnost in varno komunikacijo. Sem sodijo šifriranje, anonimni strežniki, strežniki Proxy in drugi.

V tem poglavju smo se osredotočili na varstvo osebnih podatkov ter kako pomemben del zaščite zasebnosti je nadzor pretoka in posredovanja podatkov, ki se nanašajo na nekega posameznika. V nadaljevanju bomo spoznali množične medije kot pomemben dejavnik v sodobni družbi ter kako vplivni so na občinstvo.

3 MNOŽIČNI MEDIJI

Današnji čas zlahka poimenujemo tudi medijski čas. Množični mediji imajo v sodobni družbi pomembno vlogo. Omogočajo namreč javno komunikacijo in vplivajo na oblikovanje vrednot in družbenih norm. Tako so vsaj posredno vir moči in nadzora v družbi. Tudi komunikološki raziskovalci so bili mnenja, da so mediji v sodobni družbi vedno pomembnejši dejavnik. McQuail (1994, str. 1) trdi, da je temu tako zato, ker so mediji:

- potencialno sredstvo vpliva, nadzora in inovacij v družbi; služijo kot primarno sredstvo za prenos in obenem tudi kot vir informacij, ki so potrebne za delovanje večine družbenih institucij;
- arena, kjer potekajo številne afere iz javnega življenja, tako na nacionalni kot na mednarodni ravni;
- osnovna pot do slave in statusa javne osebe kot tudi do učinkovitega nastopa v areni javnosti.

Definicijo množičnih medijev je opredelil tudi Slavko Splichal, ki ugotavlja, da so mediji v večini definirani kot sredstva, ki kvantitativno omogočajo povečanje obsega produkcije sporočil in tako razširjajo krog sočasno komunicirajočih s premagovanjem časovnih in prostorskih ovir med ljudmi (Splichal, 1981).

Wright Mills (1990, str. 37) množičnim medijem pripisuje zmožnost, da:

- povedo človeku, kdo je, in mu s tem podeljujejo identiteto,
- povedo človeku, kaj hoče biti, in s tem usmerjajo njegova prizadevanja,
- povedo človeku, kako doseči te cilje, dajejo mu tehniko,
- povedo človeku, kako naj si dopove, da je na cilju, kadar v resnici ni, pokažejo mu, kako zbežati od resnice.

Množični mediji so nosilci pomembnih funkcij. France Vreg (2000, str. 60) razdeli funkcije na: funkcijo vzpostavljanja in artikuliranja javnosti, socializacijsko funkcijo, funkcijo javnega nadzora ter legitimacijsko funkcijo. Izpostavili bi socializacijsko funkcijo, za katero omenjeni avtor meni, da v času sodobne industrijske in postindustrijske družbe prevladuje nad primarno (družina) in sekundarno (prijatelji, šola, cerkev, društva) socializacijo.

3.1 MEDIJI KOT SREDSTVO MANIPULACIJE

Navdušenju ob prihodu novih medijev v začetkih 20. stoletja (knjige, časopisi, radio, televizija itd.) in kasneje interneta je sledila zaskrbljenost nad njihovim vplivom na

uporabnike. Pojavilo se je vprašanje, kakšni škodljivi vplivi se skrivajo za (na videz) dobrimi lastnostmi medijev. Raziskovanje le-teh je bilo zelo raznovrstno, saj je izhajalo iz različnih predpostavk in je zato dajalo različne zaključke o vplivni moči, vendar so se avtorji v vseh raziskavah strinjali, da je vpliv precejšen. Raziskave morebitnih vplivov potekajo že desetletja, vendar jih je težko oziroma skoraj nemogoče dokazati. Spremljanje vremenske napovedi, nakup izdelka iz oglasa, ogled filma, katerega recenzija je bila objavljena v dnevnem časopisu – vse to McQuail navaja kot vsakodnevne učinke medijev. Mediji so po njegovem mnenju »velik skupek sporočil, ki ne izvirajo iz medijev, ampak iz družbe in so preko medijev samo poslani nazaj družbi« (McQuail, 1987, str. 250). Prav zaradi tega je težko definirati, kdaj učinek prihaja iz medijev, kdaj pa iz družbe.

Prvi začetki raziskovanja množičnega komuniciranja so se pričeli v Združenih državah Amerike. Prva teorija preučevanja vpliva množičnih medijev je bila *teorija hipodermične/podkožne igle*. V začetkih raziskovanja so raziskovalci termin množično občinstvo enostavno povezali z množičnimi mediji, saj so posplošili, da se med njimi vrši proces množičnega komuniciranja (Dolničar in Nadoh, 2004, str. 6). Strokovnjaki so si v tem obdobju zamišljali učinke množičnih medijev kot iglo, ki vbrizga sporočila občinstvu pod kožo, občinstvo pa naj bi se takoj in z enakimi občutji odzvalo na medijsko vsebino ter spremenilo svoje obnašanje in delovanje (Erjavec in Volčič, 1999, str. 23). Občinstvo je torej po tej teoriji popolnoma pasivno in je obravnavano kot množica s slabim okusom in nizko inteligenco. Kritika te teorije je zanemarjanje dejstva, da je občinstvo sestavljeno iz več posameznikov, ki se na medijske vsebine ne odzivajo pasivno, temveč aktivno, tako čustveno kot miselno. Druga slabost se nanaša na sprejemanje medijskih besedil. Teorija trdi, da člani občinstva sprejemajo medijska besedila kot izolirani in neodvisni individuumi, kritiki pa trdijo, da je vsak človek pripadnik različnih družbenih skupin in da pripada določenemu kulturnemu okolju (Ang v: Dolničar in Nadoh, str. 204)

Naslednja teorija, za katero je značilno popolno zanikanje moči in učinkov množičnih medijev, je bila *teorija zadovoljevanja potreb (uses and gratifications)*. Njen utemeljitelj je Elihu Katz. Izhodišče raziskovalcev te teorije je, da so mediji za ljudi uporabni in da njihova uporaba zadovoljuje posameznikove potrebe in želje. Torej za množično komuniciranje ni glavnega pomena ustvarjanje in pošiljanje sporočil, temveč izbira, sprejemanje in način odgovora s strani publike (Volčič, 2008, str. 79). Za razliko od občinstva iz teorije hipodermične igle je občinstvo iz teorije zadovoljevanja potreb videno kot aktivno, saj aktivno izbira in interpretira medijska besedila, da zadovolji želje po informiranju, razvedrilu in s tem pobegne od svojih problemov. Pomanjkljivost

teorije se je pokazala v poudarjanju pomembnosti občinstva na eni in zapostavljanju pomena medijskih vsebin na drugi strani (Blumer in Katz, 1975, str. 10).

Tretjo teorijo sta leta 1972 utemeljila Malcom McCombs in Donald Shaw in jo poimenovala *model prednostnega tematiziranja (aganda setting)*. Empirične raziskave so
pokazale sovpadljivost tem, ki jih publika zazna kot pomembne, in tem, ki so se pogosto
pojavljale v medijih. Vreg meni, »*da množični mediji povedo ljudem v javnosti, kaj naj si
mislijo o stvari in kako naj si jo razložijo*« (Vreg, 2000, str. 43). Po teoriji prednostnega
tematiziranja mediji sicer nimajo neposrednega vpliva na oblikovanje mnenj o neki temi, a
imajo moč, da določajo dnevni red razprave z določanjem tem, ki se bodo pojavljale. McQuail (1987, str. 275) trdi, »da dokazi kažejo, da ljudje razmišljajo o tistem, kar jim je povedano, vendar ne na način, kot ga je predstavil pripovedovalec«. To pomeni, da ljudje v svoje vsakdanje pogovore vključujejo teme, ki so v zvezi z določenim dogodkom predstavljene v medijih.

Vsem teorijam je skupno, navkljub kritikam in različnim pogledom, da imajo množični mediji vpliv na občinstvo. Eden izmed množičnih medijev, ki mu lahko pripišemo omenjene vpliva, je internet. Spletna socialna omrežja se nahajajo na spletu in so sestavni del interneta.

4 UPORABA SPLETNIH SOCIALNIH OMREŽIJ IN NEVARNOSTI ZLORABE OSEBNIH PODATKOV

V človekovi naravi je, da se želi zaščititi pred nevarnostmi. Večina ljudi želi del svojih navad in značilnosti skriti pred drugimi, da bi se izognila nadzoru, nezaželenim dejavnostim, kritiziranju, zasledovanju, izrabljanju itd. Vendar želijo po drugi strani ti isti ljudje vzpostaviti odnos z drugimi posamezniki ali skupinami. Da bi to lahko dosegli, morajo druge opozoriti nase. Torej ne smejo biti popolnoma nevidni. To pomeni, da morajo drugim posredovati tudi določeno mero informacij o (samih) sebi. Družbeno življenje je potemtakem nenehno krmiljenje in izogibanjem v iskanju zadovoljitev (Lahlou, 2008, str. 311–312).

Z razvojem interneta in različnih možnosti komuniciranja, ki jih ponuja, so se pojavile tudi nove varnostne dileme in grožnje. En vidik teh tveganj je nevarnost kraja identitete. Kot že sam termin nakazuje, ne gre zgolj za odtujitev materialne resnice, temveč so na udaru intimne informacije, ki posameznika opredeljujejo kot svojevrstno entiteto in ga ločujejo od drugih (Caeton, 2007, str. 12). Krajo identitete lahko razumemo kot skupek dejanj, katerih cilj je kraja osebnih informacij določenega posameznika. Do tega pride zaradi morebitnega profila, ki ga lahko kraja identitete prinese, kar je bolj poznano kot *finančna kraja identitete*. Primer take kraje sta vdiranje v računalniške sisteme in kraja podatkov PIN številke preko bankomatov itd. Druga oblika je t. i. *kriminalna kraja identitete*, pri kateri osumljenec kaznivega dejanja ob identifikaciji navede lažne podatke in se pretvarja, da je nekdo drug. Tretja oblika pa je t. i. *prevzem identitete*, kjer nekdo prevzame identiteto drugega, da na novo začne življenje z novo identiteto, ali pa zato, da ustvari virtualno osebnost z identiteto nekoga drugega (Lavi, Wall, Cole in Pontelli v Monahan, 2009, str. 156–157).

Kot ugotavlja Monahan (2009, str. 167), so ljudje prepričani, da je treba prevzeti in aktivno uporabljati zadnje tehnologije za ohranjanje stika s prijatelji in sorodniki, za uspešnost na poslovnem področju, ohranjanje konkurenčnosti in prednosti pred drugimi. Veliko ljudi tako verjame, da so tehnološki sistemi sinonim za napredek. Vendar so si po mnenju Monahana družbe pri tem pozabile zastaviti vprašanje o tem, kako ti informacijski sistemi povečujejo ranljivost njihovih uporabnikov, kar vključuje tudi nevarnost kraja identitete.

Med tehnološke sisteme zadnjih nekaj let, pri katerih se pojavlja tudi vprašanje ranljivosti in varnostni uporabnikov, spadajo družbeni mediji na spletu. Po mnenju Seppä (2008, str. 3) težava spletnih družbenih medijev ni le v vprašanju zasebnosti in varovanju osebnih podatkov, temveč tudi v ranljivosti, ki so ji lahko podvrženi. Informacije, posredovane v interesu interakcije, so lahko zlorabljene na različne načine – od posredovanja podatkov razpošiljevalcem neželene pošte, nadlegovanja

uporabnikov, spletnega in fizičnega zasledovanja, diskriminacije uporabnikov, izsiljevanja in celo kraje identitete (Seppä 2008, str. 3; Gross in Acquisti, 2005, str. 3). Kraja identitete na spletnih družbenih medijih se lahko pojavi v obliki prevzema identitete v dobesednem pomenu: da se nekdo registrira na spletni družbeni medij z lažno identiteto oz. identiteto nekoga drugega. Uporabniki lahko zaradi objav različnih osebnih informacij v okviru svojega profila na spletnih družbenih medijih postanejo žrtve tako prevzema identitete izven virtualnega sveta kot tudi t. i. finančne kraje identitete.

Spletna socialna omrežja so najnovejša generacija 'posredne javnosti'. To so okolja, kjer se ljudje zberejo javno s posredovano tehnologijo. V nekem smislu je posredovana javnost enaka neposredni, ki jo najdemo v parkih, gostinskih lokalih, nakupovalnih centrih itd. Najstniki pridejo na internet, da se povežejo s svojimi prijatelji, najverjetneje so zraven prisotni tudi drugi ljudje, ki sledijo pogovoru dveh prijateljev, če sta zanimiva, v nasprotnem primeru pa ju ignorirajo (Boyd, 2007, str. 2–3).

Medtem ko obe javnosti, posredna in neposredna, igrata podobni vlogi v življenju ljudi, pa ima posredna javnost štiri lastnosti, ki so značilne samo zanjo (Boyd, 2007, str. 2–3):

- vztrajnost (kar rečeš ostane, kar rečeš danes, bo še vedno tam čez 10 let),
- iskanost (danes lahko na internetu najdemo, kje je kdo bil nekoč),
- kopiranje (pogovor z enega mesta lahko skopiraš na drugo mesto),
- nevidno občinstvo (Ne samo, da so v posredni javnosti lurkerji[2] nevidni, ampak tudi vztrajnost, iskanost in kopiranje predstavljajo naše izraze občinstvu, ki ni bilo nikoli prisotno, ko so ti izrazi nastajali).

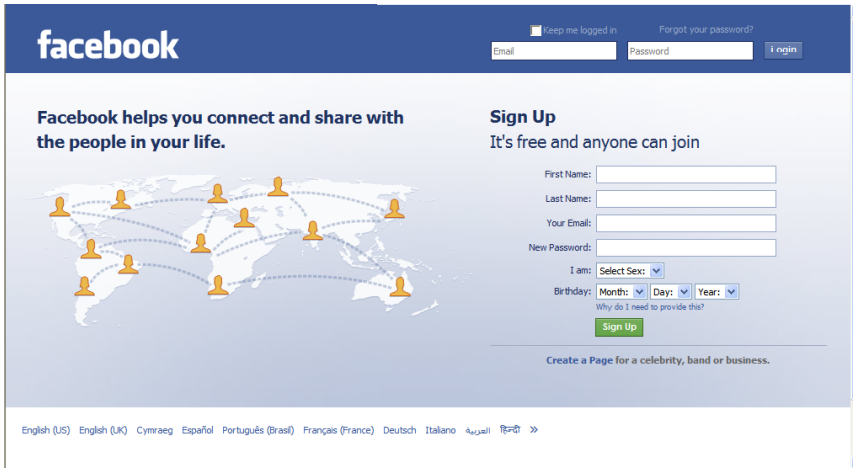
4.1 OPREDELITEV IN ZNAČILNOSTI SPLETNIH SOCIALNIH OMREŽJIH

Spletna socialna omrežja lahko definiramo kot individualne internetne strani, ki omogočajo vzpostavitev spletnega prijateljstva s pomočjo deljenja in zbiranja koristnih informacij s specifičnimi oz. nepoznanimi ljudmi (Kwon in Wen, 2009). Ta omrežja predstavljajo nov socialni in ekonomski fenomen, ki je privabil že na milijone uporabnikov, hkrati pa so poskrbela za nov način komuniciranja ter uvedbo nove vrste medosebnih odnosov. Sem uvrščamo spletne strani, kot so najbolj razširjeni Facebook (Slika 1), Hi5, Myspace, Netlog, Google+ itd. Profili uporabnikov ponujajo vpogled v njihove osebne podatke, od datuma rojstva, spola, verskega prepričanja, kraja bivanja pa vse do najljubših filmov, knjig, glasbe. Uporabniki lahko poleg informacij, ki jih puščajo na voljo, kreirajo tudi izgled svojega profila, nalaganje slik, filmčke ter

[2] Lurkanje pomeni obliko pasivne participacije, pri kateri uporabniki sicer redno pregledujejo prispevke ostalih članov, vendar nikoli ali zelo redko objavljajo svoje lastne.

glasbene datoteke, pridobijo omrežje stikov, ki so nato predstavljeni kot njihovi prijatelji. Pomen prijateljstva v spletnih socialnih omrežjih je precej drugačen od prijateljstva, ki ga poznamo v tradicionalni obliki v resničnem svetu. V spletnih socialnih omrežjih ni treba, da neko osebo sploh poznaš, da jo šteješ za svojega prijatelja, medtem ko za resnično življenje tega ne moremo trditi (Ofcom, 2008).

Slika 1: Spletno socialno omrežje- Facebook



Vir: Facebook (2011, str. 1)

Raziskava Ofcom[3] je ugotovila, da se uporabniki spletnih socialnih omrežjih razlikujejo po obnašanju in namenu uporabe spletnih socialnih omrežij. Prioritete uporabnikov so različne, zato jih razvrščamo v pet različnih skupin glede na namen uporabe spletnih socialnih omrežij (Ofcom, 2008):

- alfa uporabniki za druženje – ljudje, ki uporabljajo spletne skupnosti predvsem za zabavo, spogledovanje in spoznavanje novih ljudi;
- iskalci pozornosti – ljudje, ki iščejo pozornost in od drugih uporabnikov pričakujejo, da bodo komentirali njihov profil ter objavljene fotografije;
- pripadniki – ljudje, ki si ustvarijo profil zato, da so na tekočem z dogajanjem svojih prijateljev;
- zvesti – ljudje, ki uporabljajo spletna socialna omrežja za to, da obnovijo stike s starimi prijatelji, pogosto sošolci;
- funkcionarji – ljudje, ki so osredotočeni na to, da uporabljajo spletna socialna omrežja s točno določenim namenom.

Ravno tako lahko v različne skupine razdelimo neuporabnike spletnih socialnih omrežij, saj se razlogi za njihovo nečlanstvo med seboj razlikujejo (Ofcom, 2008):

[3] Ofcom Social Networking research je kvalitativna raziskava, ki je bil izvedena leta 2007 z namenom proučevanja obnašanja ter odnosa uporabnikov in ne uporabnikov do spletnih socialnih omrežij. V njej je sodelovalo 39 uporabnikov in 13 neuporabnikov spletnih socialnih omrežij.

- zaskrbljeni za varnost – ljudje, ki so zaskrbljeni zaradi varnostni na internetu, še posebej jih skrbi dejstvo, da lahko postanejo njihovi osebni podatki javno dostopni;
- tehnično neizkušeni – ljudje, ki se ne čutijo dovolj sposobnih za uporabo interneta ali računalnika;
- intelektualni zavrnitelji – ljudje, ki nimajo niti najmanjšega interesa za članstvo v spletnih skupnosti in se jim zdi potrata časa.

4.1.1 FACEBOOK

Odkritost in zaupanje med uporabniki Facebooka izhajata iz njegove kratke zgodovine, ki se je začela pred tremi leti na ameriški elitni univerzi Harvard. Takrat je Mark Zuckerberg izumil spletno mesto, na katerem so se povezovali harvardski študentje. Sčasoma se je dostop razširil na študente drugih elitnih univerz (Ivy League), ki so imeli univerzitetni elektronski naslov, kasneje pa so se Američanom pridružili angleški študenti. Eden izmed uporabnikov je tudi Igor Cesarec, ki je v času čezoceanskega širjenja Facebooka študiral na London School of Economics (LSE). Prav ta fakulteta je bila ena prvih angleških fakultet, ki so dobile dostop do Facebooka. »Takrat je bila uporaba Facebooka kot del neke underground scene in seveda si bil zelo kul, če si to uporabljal. Ker je bil dostop omejen, so bili študenti pripravljeni v svojih profilih izdati marsikaj. Znotraj fakultete ni težav, če kdo izve tvoje ime in priimek ali dobi tvojo telefonsko številko. Stvar postane problematična, ko se v fakultetno socialno omrežje prikradejo zunanji obiskovalci,« pove Cesarec (Crnović, 2007, str. 50). Enajstega septembra 2006 se je Facebook odprl za vse uporabnike z veljavnim elektronskim naslovom, tako da so se študentom in dijakom zgolj nekaterih šol in univerz pridružili še drugi. Pa ne samo študenti, Facebook je zaradi resnega videza in zaupanja, ki ga z navedbo imena in priimka izkažemo drugim uporabnikom, postal priljubljen tudi med tistimi, ki so šolanje že končali (Crnović, 2007).

»*Živijo, moje ime je Žiga in na Facebooku sem že pol leta. Ne vem, kako naj prekinem to odvisnost. Situacija je težka.*«

Tako se je napol v smehu začel pogovor z enim od nekaj tisoč slovenskih uporabnikov, ki so se zadnje mesece prijavili na Facebook. Študent Žiga ima na svojem seznamu prijateljev približno 130 ljudi, s katerimi se poveže večinoma le takrat, ko kaj potrebuje. Priznava pa, da lahko na Facebooku »nadaljuješ osvajalsko sago, tako da dekle, ki ti je všeč, dodaš na seznam prijateljev«. Facebook omogoča uporabnikom, da opredelijo tudi svoj stan. Žiga opaža, da ko kdo stan spremeni iz 'v razmerju' v 'samski', navadno sledi naval na to osebo, in to z osebnimi in javnimi sporočili. Znane so anekdote, da so s spremembo stanu nekateri tudi razdrli razmerje.

Facebook je trenutno eno najbolj priljubljenih spletnih mest, ki jih strokovnjaki uvrščajo med tako imenovana spletna mesta socialnih omrežij. Pred njim je

prijateljskih stikov željne ljudi privabljalo že več strani. Te danes še zdaleč niso pozabljene, a migracije na Facebook, ki smo ji bili nedavno priča, ni bilo mogoče spregledati. Facebook je v tandemu z bolj glasbeno naravnanim Myspaceom postal hkrati priložnost in grožnja za sodobno grajenje socialnih omrežij. Pred njim svari britanska informacijska pisarna, zaradi njega so padali v šolah ukori in v službah disciplinske kazni. Kljub temu število uporabnikov, tudi slovenskih, eksponentno narašča (Crnović, 2007).

Pri Facebooku je stvar še toliko kočljivejša, saj uporabniki praviloma uporabljajo prava imena in priimke in ne vzdevkov, kot je navada pri večini oblik spletne participacije. Anonimnosti je še manj, ko ljudje poleg svojega imena in priimka objavijo tudi fotografijo. Prav zato, ker je razmeroma jasno, kdo se skriva za katerim profilom, so stran v škodo uporabnikov že uporabile izobraževalne ustanove in delodajalci. Slišati je govorice, da so zaradi Facebooka iz ameriške srednje šole izključili nekaj dijakov, ki so v svojem profilu objavili fotografije z zabave, na kateri pijejo alkohol ali kadijo marihuano. Prav tako naj bi bila zaradi objave fotografij s službene zabave ogrožena delovna mesta. Zaradi tega je britanska informacijska pisarna mlade pozvala, naj bodo pri uporabi previdni, saj si z nepremišljenim objavljanjem podatkov in fotografij lahko uničijo kariero.

Facebook je po številu obiskovalcev leta 2008 prehitel tekmeca MySpace in tako postal največje družabno omrežje na svetu. Januarja 2009 je dosegel 150 milijonov aktivnih uporabnikov po svetu, v začetku leta 2010 pa je ta številka narasla na 400 milijonov (Slika 2). Inside Facebook poroča, da je bilo 1. marca 2010 v Evropi 129, v ZDA pa 113 milijonov aktivnih uporabnikov Facebooka (RIS, 2011).

Slika 2: Facebook uporabniki po svetu

Vir: Facebook (2011, str. 2)

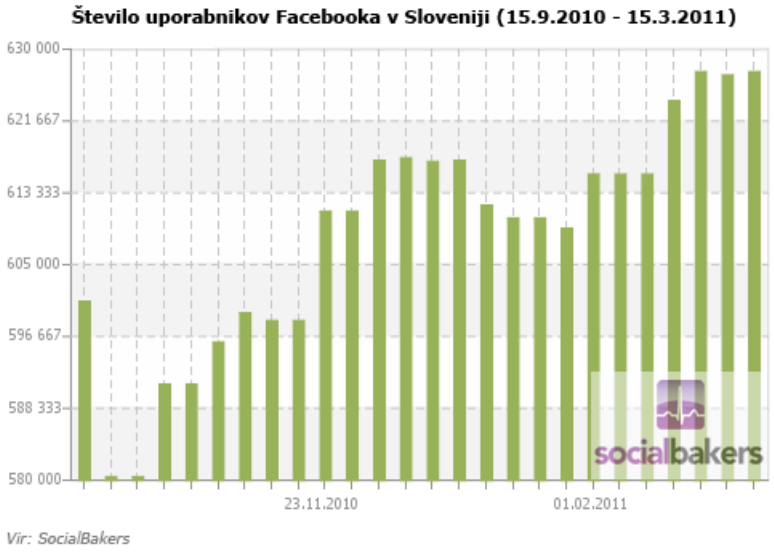
Kot kažejo podatki portala SocialBakers, je bilo sredi marca 2011 v Sloveniji 627.360 uporabnikov Facebooka (Slika 3). To število predstavlja 37 % slovenske populacije v starosti od 10 do 74 let, ki po podatkih Statističnega urada RS za leto 2010 obsega 1,700.729 ljudi.

Med tistimi, ki so že uporabljali internet (ne glede na pogostost uporabe), znaša delež uporabnikov Facebooka 51 %. Statistični urad RS je leta 2010 v Sloveniji zabeležil 1,238.114 posameznikov od 10 do 74 let, ki so že uporabljali internet (SocialBakers, 2011).

Seveda se ob vseh podatkih, ki jih pošljemo v svetovni splet, postavlja vprašanje zasebnosti. Čeprav mnogi uporabniki pri pisanju blogov ali sodelovanju na spletnih forumih in tudi na Facebooku mislijo, da delujejo v zasebnem prostoru, ki je omejen z uporabniškimi gesli, stvar ni tako preprosta. "*Dejansko delujejo v javnem prostoru, kjer nastane velik problem zasebnosti, ker se ti zelo zasebni tokovi prepletajo z delovnimi, profesionalnimi in posledično tudi denarnimi tokovi, ko Facebook podatke s profilov prodaja oglaševalcem. Nekateri pravijo, naj to ne bi bilo sporno. Ampak stvar lahko postane še resnejša, če se vmeša politični interes,*" meni Petrič (Petrič, 2005).

Število uporabnikov Facebooka pri nas se je v primerjavi z majem 2010 povečalo za skoraj 50 tisoč. Rast uporabnikov v zadnjih 6 mesecih je bila 4,4 %, kar predstavlja približno 27 tisoč posameznikov. Takšno stanje nas glede na rast uporabnikov Facebooka med 213 opazovanimi državami uvršča na 172. mesto, kar nakazuje saturacijo tega trga v Sloveniji (Facebook, 2010).

Slika 3: Facebook uporabniki v Sloveniji



Vir: Facebook (2010, str. 2)

Število uporabnikov Facebooka pri nas se je v primerjavi z majem 2010 povečalo za skoraj 50 tisoč. Rast uporabnikov v zadnjih 6 mesecih je bila 4,4%, kar predstavlja približno 27 tisoč posameznikov. Takšno stanje nas glede na rast uporabnikov Facebooka med 213 opazovanimi državami uvršča na 172. mesto, kar nakazuje saturacijo tega trga v Sloveniji (Facebook, 2010).

4.2 KOMUNIKACIJA V SPLETNIH SOCIALNIH OMREŽJIH

Za Facebook, MySpace, Hi5, Google+, Netlog in podobna omrežja je značilno, da je komunikacija v veliki meri odvisna od obligacije, da se komunicira. Komunikacija pa ni samo verbalna, ampak tudi neverbalna in vizualna. Na MySpaceu se za komunikacijo uporabljajo slike in videoposnetki, na Facebooku so zelo razširjene aplikacije, ki jih naredijo uporabniki sami in služijo kot virtualna darila. Pogosto prihaja do kombinacij verbalnih in neverbalnih sredstev komunikacije, velikokrat pa so besedila že integrirana v samo digitalno sliko ali videoposnetek. Druga značilnost komunikacije na spletnih socialnih omrežij je hkratna možnost sinhrone (v realnem svetu) in asinhrone (odložene) komunikacije.

Janez Strehovec (v: Anđelković, 2008) pravi: »Splet zato vedno bolj spominja na globalno areno, v kateri se uresničuje sumljivo geslo vsi smo ustvarjalci in domneva o posamezniku kot vsestransko razviti osebnosti. To seveda implicira pojav novega množičnega ljubiteljstva, ki skriva tudi veliko pasti. Implicitna predpostavka spleta je prepričanje, da ima vsakdo kaj zanimivega povedati, kar drži samo deloma.«. Komunikacija na spletnih socialnih omrežjih se poleg kombiniranja sinhronosti in asinhronosti razlikuje od komunikacije v virtualnih klepetalnicah ali forumih po tem, da pogosto predstavlja nadaljevanje komunikacije v fizičnem svetu ali pa pripravo nanjo. Kar pomeni, da internet kot okolje ne ponuja več kot neko drugo, temveč predstavlja sestavni del vsakdanjega življenja posameznikov (Anđelković, 2008).

Pionirja raziskovanja spleta Robert Burnett in David Marshall sta v svoji študiji večkrat opozorila na eno ključnih značilnosti spleta – omogočanje konvergence na ravni komuniciranja. Splet namreč različne medijske formate povezuje v medsebojne mreže in tako simultano tvori različne oblike komuniciranja (Oblak in Petrič, 2005, str. 55). Na spletu lahko brskamo za informacijami na nekem spletnem portalu, lahko izberemo elektronsko pošto in tako komuniciramo z natančno določenim seznamom oseb, lahko objavljamo vsebine, fotografije in bloge. In prav ta živahna, dinamična in raznolika komunikacija dela splet pomemben družbeni prostor, v katerem potekajo različne oblike računalniško posredovanega komuniciranja (Oblak in Petrič, 2005, str. 55).

Spletna socialna omrežja lahko uvrstimo v tako imenovane komunikacijske modele, in sicer v model imenovan eden-z-enim (one-to-one), za katerega je značilno neposredno medosebno komuniciranje oziroma komuniciranje iz oči v oči (face-to-

face) in ki poteka med dvema osebama, ki se nahajata v istem prostoru (Oblak in Petrič, 2005, str. 59).

Rheingold trdi, da smo ljudje po naravi izrazito prosocialno naravnani. V vsakem posamezniku je prisotna želja po druženju in po pripadnosti, kar pripomore k temu, da vzpostavljamo odnose tudi v kibernetskem prostoru. Posamezniki lahko z manjšim vložkom časa in manjšo frekvenco stikov vzpostavijo konkretne stike in jih po drugi strani ravno zaradi te plitkosti enostavno prekinejo. In to doživijo manj 'travmatično' kot v fizičnem okolju (Brodnik, 2007).

4.3 NADZOR ZASEBNOSTI V SPLETNIH SOCIALNIH OMREŽJIH

V spletnih socialnih omrežjih obstaja nadzor, za katerega ni treba imeti posebne tehnologije, saj se sam nadzor izvaja le zaradi tega, ker se lahko: torej ker nadzorovani uporabnik iz različnih razlogov v svojem profilu ni uredil nastavitev za zaščito zasebnosti.

Med spletnimi socialnimi omrežji po množičnem članstvu ter po podatkih, ki so edinstveni in identificirajo osebe, izstopa Facebook. Večina članov je precej selektivna glede tega, katere osebne podatke bo razkrila. Večina uporabnikov razkrije datum rojstva, na pa tudi npr. telefonske številke. Če je določen tip informacije sploh razkrit, potem obstaja večja verjetnost, da je podatek točen in zanesljiv, v nasprotnem primeru pa osebne informacije raje ostanejo nerazkrite (Acquisti in Gross, 2006, str. 13). Facebook ponuja svojim uporabnikom precejšno kontrolo nad tem, komu in katere osebne podatke bodo člani razkrili. Uporabniki lahko izberejo tako vidnost svojega profila (kdo lahko vidi njihov profil) kot tudi iskanje profila (kdo lahko najde njihov profil s pomočjo iskalnika glede na tip uporabnika), žal pa veliko članov ne ve, da take možnosti sploh obstajajo (Acquisti in Gross, 2006, str. 16).[4]

Za boljše razumevanje, kako uporabniki Facebooka (zlasti mlajši od 3O let) razumejo zasebnost, je Rayes-Goldie v januarju 2008 opravila leto dni dolgo etnografsko raziskavo. Eden od njenih ciljev je bil razkriti uporabniški odnos do zasebnosti. Avtorica je ugotovila, da uporabnike skrbi njihova zasebnost, predvsem pa so bolj zaskrbljeni za tako imenovano socialno zasebnost[5] kot za institucionalno[6].

Socialna zasebnost pomeni, da uporabnike bolj skrbi, da na svojih profilih nadzorujejo dostop do svojih podatkov, kot to, da bodo podjetja, ki stojijo za Facebookom, v

[4] Ugotovitev izhaja iz raziskave, v kateri je sodelovalo 294 posameznikov: 209 jih ima Facebook profil, 78 profila ni imelo nikoli, 7 sodelujočih pa je nekoč imelo profil, vendar so ga deaktivirali.
[5] Urejanje vidnosti uporabniških profilov, onemogočanje dostopa do podatkov izbranim uporabnikom.
[6] Onemogočanje dostopa do podatkov različnim korporacijam, ki zbirajo podatke v marketinške namene.

vsakem primeru uporabila njihove podatke. Skrbi ji predvsem, kako bi najbolje zaščitili svoje profile pred 'prijatelji', kot so njihovi šefi ali učitelji, ter kako bi zaščitili profile, da jih ljudje, ki jim niso všeč, sploh ne bi našli, in zato ne bi mogli poslati prošenj za 'prijateljstvo'. Uporabniki svojo socialno zasebnost večajo s tem, da namesto pravih imen uporabljajo vzdevke, čeprav je to v nasprotju s pogoji uporabe Facebooka, ki od svojih uporabnikov zahteva uporabo pravih imen in identitete, v nasprotnem primeru je njihov profil lahko izbrisan. Druga metoda večanja socialne zasebnosti je brisanje z zidu in oznak na slikah (Rayes-Goldie, 2010).

Naslednji primer lepo ponazori, kako zelo so pomembne nastavitve zasebnosti v spletnih socialnih omrežjih. Facebook je decembra 2009 prosil uporabnike, da ponovno razmislijo o svojih nastavitvah zasebnosti. Uporabniki naj bi razmislili o različnih vrstah vsebin in nato izbrali, ali naj bi bile te vsebine vidne vsem ali pa bodo ohranili svoje stare nastavitve. Privzeta nova nastavitev je bila izbira 'vsi'. Mnogi uporabniki so se med prijavljanjem na Facebook srečali s 'pop-up' okencem in ga samo zaprli, ker so želeli priti do samega Facebooka, pri tem pa so nevede spremenili vse nastavitve v javne. Mnogi se tega niso niti zavedali. Če so nekateri mnenja, da nikogar ne skrbi za zasebnost, potem bi lahko verjeli, da so uporabniki Facebooka svoje vsebine prostovoljno spremenili v javne. Da temu ni tako, lahko pokažemo s primerom, ki se je zgodil v Ameriki. Nasilni oče neke najstnice je bil izpuščen iz zapora. Ob spoznanju, da prepoved približevanja ne bo zadosten ukrep, ki bi lahko zagotavljal varnost, sta se najstnica in njena mati preselili tisoče kilometrov stran od očeta. Ko je najstnica pričela pridobivati krog prijateljev v novi šoli, je prosila mamo za Facebook račun. Njena mati je prošnji ugodila, zato sta previdno delali na tem, da bi bil Facebook profil zaseben, kolikor je to mogoče, saj se nobena od njiju ni želela soočiti s posledicami, če bi bili najdeni. Ko je Facebook v decembru spremenil nastavitve zasebnosti, najstnica in njena mati nista vedeli, kaj te spremembe nastavitve zasebnosti sploh pomenijo, dokler ju na to ni opozoril nekdo drug (Boyd, 2010).

Raziskava Ofcom (2008) je razkrila, katera so potencialno najbolj tvegana in nevarna ravnanja uporabnikov spletnih skupnosti:

- nespreminjanje varnostnih nastavitev – uporabniki puščajo varnostne nastavitve takšne, kot so jih dobili ob pričetku uporabe spletne skupnosti, s tem pa dopuščajo, da je njihov profil odprt in viden vsem uporabnikom;
- objavljanje občutljivih osebnih informacij in fotografij;
- objavljanje vsebin, zlasti fotografij, ki lahko škodujejo njihovemu ugledu;
- kontakt z ljudmi, ki jih ne poznajo – uporabniki pogosto sprejmejo povabilo za prijateljstvo od ljudi, ki jih sploh ne poznajo ali pa jih ne poznajo dovolj dobro.

Da do takšnega potencialno nevarnega obnašanja uporabnikov v spletnih skupnostih sploh prihaja, so krivi naslednji razlogi: pomanjkanje ozaveščenosti o problematiki

zasebnosti na internetu, prepričanje, da so za varnost in zasebnost na internetu poskrbele že spletne strani same, nizka raven samozavesti med uporabniki, da lahko sami spreminjajo varnostne nastavitve, težko dostopne informacije o varnostni in zasebnosti na internetu, občutek med mlajšimi uporabniki, da so nepremagljivi, miselnost, da so spletne strani s socialnimi omrežji manj škodljive, kot je internetno bančništvo (Ofcorm 2008).

4.4 PRIJATELJSTVO V VIRTUALNEM SVETU

Možnost samostojne izbire prijateljev je ena izmed prednosti spletnih socialnih omrežij. Ker (pa) je potencialnih virtualnih prijateljev na tisoče, jih uporabniki izberejo na podlagi različnih razlogov. Uporabniki se lahko poznajo že iz realnega sveta ali jih družijo skupni interesi oziroma hobiji – lahko jih pritegne zgled oziroma slika bodočega virtualnega prijatelja ali pa samo njegov grafično urejen profil.

Težko je določiti glavne kriterije, po katerih bi določali pomen prijateljstva. V različnih življenjskih situacijah gledamo prijatelje različno in tudi v posameznih družbah definiramo prijateljstvo različno. Bellah (v Doyle in Smith, 2002) trdi, da »prijatelji morajo uživati v družbi drug drugega, morajo biti drug drugemu v pomoč in morajo biti zavezani k skupni dobroti«. Cicero (v Skrinah, 2007, str. 38) pravi, da je »prijateljstvo močnejše kot sorodstvene vezi. Z modrostjo je največji dar, kar jih je narava podarila človeku. Brez njega ni vredno živeti: polepša srečno življenje in lajša nesreče, ker srečo ali nesrečo delimo z drugimi. Na prijateljstvu temelji civilna družba.«

V sodobni informacijski družbi vse več ljudi išče in sklepa prijateljstva na spletnih socialnih omrežjih. Dolušićeva (2008) deli uporabnike spletnih socialnih omrežij na pet skupin:

- *nostalgiki*: so uporabniki, ki si silno želijo obuditi šolske dni in iščejo svoje sošolce ter z enim klikom takoj izvedo ali so se poročili, ali imajo otroke, ali so pridobili kakšen kilogram. Omrežja omogočajo tudi komuniciranje celotne družbe posameznikov, ki so se nekoč družili, sedaj pa jim čas tega ne dopušča in jim tako preostane le virtualna zabava;
- *osamljeni*: sem sodijo tisti, ki si v resničnem življenju še niso uspeli najti prijateljev ali partnerja. Internet je idealno mesto za sklepanje prijateljstev, vendar Dolušićeva opozarja, da je virtualno druženje le privid, ki ga je treba preveriti s srečanjem v živo in tako ugotoviti, ali ti je prijatelj všeč ali ne;
- *zlomljena srca*: sem sodijo posamezniki, ki jim internet služi kot sredstvo za pozabljanje nesrečne ljubezni;
- *željni promocije*: pevci ali igralci v vzponu, ki s pomočjo fotografij in samohvale ustvarjajo samopromocijo;

- *lažniv*ci: glede na to, da se ta prijateljstva nahajajo v spletnem okolju, ne smemo pozabiti, da so lahko nekateri profili lažni oziroma uporabniki niso to, za kar se izdajajo.

Prijateljstvo na spletnih socialnih omrežjih Rosenova (2007) poimenuje hipertekst. Prijateljstvo je javno, fluidno, promiskuitetno in birokratizirano, kajti uporabniki z njim upravljajo. Prijatelje lahko spreminjajo, brišejo, dodajajo in blokirajo. In vse to le s klikom na miško. Nekatera spletna socialna omrežja, na primer MySpace, težijo k čim večjemu številu prijateljev na uporabnikovem profilu. Če ima uporabnik malo prijateljev, ga sistem MySpacea opozori z belim praznim kvadratkom, v katerem naj bi bile slike njegovih prijateljev. To opozorilo je podano z namenom, da se zave malega števila prijateljev (Rosen, 2007). Komunikacija ni množična, temveč gre zgolj za komunikacijo med prijatelji. Uporabniki se sami odločijo, s kom se bodo pogovarjali, s kom delili fotografije in koga bodo sprejeli na svojo listo prijateljev. Veliko virtualnih prijateljstev bazira na starih poznanstvih iz resničnega življenja. Petrič (Crnović, 2007, str. 45) meni, da »gre pri Facebooku za ohranjanje dejanskega socialnega omrežja oziroma za ponovno grajenje takega omrežja. Med sabo se povežejo ljudje, ki so lahko vsak dan v neposrednem stiku, ali pa so nekoč bili v kratkotrajnejšem ali dolgotrajnejšem začasnem socialnem krogu. Hkrati se vzpostavljajo nova poznanstva, šibke vezi – prijatelji prijateljev ali zanimivi neznanci, ki lahko zelo učinkovito pomagajo pri grajenju socialnega kapitala«.

Med uporabniki divja prava vojna za čim večje število prijateljev. Zbirke prijateljev tako postanejo zbirke elektronskih naslovov in osebnih podatkov, preko katerih uporabniki ohranjajo medsebojne stike in sledijo življenjsko pomembnim dogodkom svojih znancev (Crnović, 2007). Rosenova (2007) meni, da »ta impulz, zbrati čim več prijateljev, kolikor je možno, ni odraz človekove potrebe po druženju, temveč potrebe po statusu«. Takšne uporabnike imenuje iskalci statusa (status seekers). Prav zaradi težnje po velikem številu prijateljev oziroma stikov prihaja do problema preobilja prijateljstva.

Iz raziskave sociologa Camerona Marlowa (v Kečanović, 2009) razberemo, da ima povprečen uporabnik spletnega socialnega omrežja Facebook v svojih seznamih 120 stikov, redni kontakt pa vzdržuje le s štirimi ali šestimi. Na nekaterih profilih uporabnikov je možno najti tudi 500 prijateljev in izmed teh ženske uporabnice vzdržujejo redne kontakte s šestnajstimi, moški pa z desetimi uporabniki. Pri obravnavi virtualnega prijateljstva ne moremo mimo čustev. Jones (Završnik, 2007) meni, da je čustvena inflacija kibernetičnega prostora fenomen, ko ima udeleženec kiberprostora veliko poznanstev, ki jih lahko sklepa z ostalimi udeleženci. Za ta poznanstva je značilna čustveno ohlapna povezava. Možnost hitro najti novega znanca namreč udeležence vzpodbuja k hitremu sklepanju, a po drugi strani prav tako k hitremu opuščanju novih poznanstev. To možnost omogoča narava same skupnosti, ki je določena le z besedno ravnjo. Položaj in vloga udeleženca, ki vstopa v skupnost,

nista prej določena, zaradi česar se generira občutek, da posameznik ne pripada skupnosti, temveč da skupnost pripada njemu. Nasprotno pa ravno ta množičnost osebnih vezi onemogoča sklepanje pravih osebnih vezi, kajti za osebno vez je temeljna ravno njena izključevalna narava – ko smo z vsemi hkrati, v bistvu nismo z nikomer (Završnik, 2007).

Primarni namen spletnih socialnih omrežij je iskanje oziroma vzpostavljanje novih ali obnavljanje starih poznanstev. Vendar kaj kmalu ugotovimo, da je komunikacija med uporabniki skopa in da jih vse več teži le k čim večjemu številu prijateljev, ne pa k poglobitvi stikov in tkanju pristnih vezi. Virtualna prijateljstva na spletnih socialnih omrežjih rastejo z neverjetno hitrostjo. Vsak lahko postane prijatelj skoraj s komerkoli. Negativna posledica je prav v tej nagli hitrosti in dostopnosti, ki vsakomur omogoča dostop do okolja drugih (Kečanović, 2009).

4.5 PRIMERI POTENCIALNIH NEVARNOSTI ZA ZLORABO OSEBNIH PODATKOV

Enostaven registracijski postopek je prva izmed možnih nevarnosti za krajo identitete. Podatki, ki so potrebni za registracijo, namreč puščajo veliko možnosti za posameznikovo eksperimentiranje, morebitno zlorabo in prevzem identitete. Kako preprosto je prevzeti identiteto za potrebe registracije in oblikovanje profila na spletnih družbenih medijih, kažejo primeri mnogih javno izpostavljenih posameznikov[7].

Druga izmed potencialnih nevarnosti za krajo identitete je *širjenje socialnega omrežja z dodajanjem novih 'prijateljev'*. Primer tega, kako nevarno je lahko sprejemanje neznancev med spletne 'prijatelje', je eksperiment, ki so ga izvedli v eni izmed oddaj na britanski medijski mreži BBC (Finance, 2007). Avtorji oddaje o pravicah potrošnikov so na spletnem družbenem mediju Facebook ustvarili lažni uporabniški profil mladega dekleta, preko katerega so potem povabili 100 naključnih uporabnikov, da bi postali njeni spletni 'prijatelji'. 35 uporabnikov se je povabilu odzvalo, čeprav o tej izmišljeni uporabnici niso vedeli ničesar. S tem so ustvarjalci dobili dostop do vseh osebnih podatkov, ki so jih ti uporabniki imeli na svojem profilu. Na podlagi podatkov, ki so jih pridobili na profilu enega izmed teh uporabnikov, so ustvarjalci oddaje pridobili še nekaj javno dostopnih informacij o njem ter na njegovo ime odprli elektronski bančni račun in zaprosili za kreditno kartico. Tako je ta uporabnik zgolj s tem, da je sprejel neznanko za svojo spletno 'prijateljico', postal žrtev finančne kraje identitete.

Tretjo potencialno nevarnost predstavlja *dodajanje in uporaba aplikacij*. Kakšno nevarnost lahko predstavljajo aplikacije, kaže eksperiment, ki ga je izvedla britanska medijska mreža BBC (Kelly, 2008). Avtorji eksperimenta so najprej ustvarili lažen profil na Facebooku in nato ustvarili posebno aplikacijo za ta spletni družbeni medij. Aplikacija se je imenovala Miner in je bila narejena tako, da se je lahko zamaskirala kot igra, kviz ali šala dneva, v resnici pa je bila namenjena nelegalnemu in trajnemu pridobivanju podatkov s profila drugih uporabnikov. Kljub videzu nedolžne aplikacije je le-ta zbirala osebne podatke, tako od uporabnikov profila, ki je aplikacijo dodal, kot tudi od njegovih 'prijateljev'. Zbrane podatke je potem preko elektronske pošte posredovala avtorjem aplikacije. Ko so avtorji aplikacijo dodali na lažni profil, niso mogli pridobiti vseh podrobnosti, vendar so pridobivali informacije o uporabnikovem imenu, domačem mestu, šoli, interesih in fotografijah.

[7] Na spletnem družbenem mediju Facebook imajo mnogi slovenski politiki več kot en profil. Tudi mnogi znani iz sveta zabave se na tem družbenem mediju pogosto srečujejo s prevzemom identitete (npr. Angelina Jolie). Do ustvarjanja lažnih profilov oz. do prevzema identitete prihaja tudi na spletnem družbenem mediju Twitter, kjer sta bili žrtvi kraje že igralki Emma Watson in Evan McGregor ter celo Dalajlama.

4.6 ZASEBNOST, RAZKRIVANJE OSEBNIH PODATKOV IN KRAJA IDENTITETE

Boydova (2008, str. 18) definira zasebnost kot občutek nadzora nad informacijami, kontekstom, v katerem poteka izmenjava le-teh in občinstvom, ki ima lahko dostop do teh informacij. Dejstvo, da nihče ne ve določene informacije, slednje ne naredi zasebne. Informacija je zasebna zato, ker je njeno poznavanje omejeno in nadzorovano (Boyd 2008, 18). Uporabniki spletnih družbenih medijev lahko do določene mere sicer regulirajo, koliko in kateri podatki bodo dostopni tudi drugim in ne zgolj njihovim 'prijateljem'. Vendar pa je težava v tem, da mnogi uporabniki, ki svoje osebne podatke naredijo javne in dostopne na svojem profilu na spletnih družbenih medijih, ne pomislijo na varovanje zasebnosti in podatkov ter se ne zavedajo nevarnostni kraje identitete (Seppä 2008, str. 3).

Kot ugotavlja Seppä (2008, str. 3), je leta 2008 samo 25 odstotkov uporabnikov Facebooka dejansko uporabljalo varnostne nastavitve o zasebnosti profila in spremenilo privzete nastavitve, ki največkrat omogočijo tudi neznancem dostop do profila in vsebino objavljenih na njem. Podatki iz leta 2005 (Gross, 2005, str. 9) kažejo, da je bilo 30 odstotkov od 250.000 uporabnikov Facebooka, ki so jim poslali vabilo za 'prijateljstvo', pripravljenih sprejeti in razkriti vse informacije s profila popolnim neznancem in njihovim spletnim 'prijateljem'. Veliko uporabnikov tako na svojemu profilu povsem javno objavi veliko podatkov o sebi (ime, rojstni datum, domači naslov, elektronski naslov, telefonska številka itd.) in dodaja različne aplikacije, ki so lahko potem na različne načine zlorabljene. Tako kljub nevarnostim zlorabe osebnih podatkov, ki jih uporabnik objavi na spletnem družbenem mediju, uporabniki prostovoljno in zavestno posredujejo svoje podatke (Gross, 2005, str. 3).

Razlogi za tako ravnanje so po mnenju Grossa (2005, str. 3) različni: a) predvidevanje uporabnika, do bodo koristi, ki jih lahko pridobi s selektivnim razkrivanjem podatkov neznancem, večje kot pa potencialna nevarnost vdora v njegovo zasebnost; b) pritisk vrstnikov ali sledenje in posnemanje vedenja drugih; c) pretirano sproščen odnos ali nezainteresiranost za osebno varnost in varovanje podatkov; d) nepoznavanje in neinformiranost o nevarnostih razkrivanja osebnih podatkov na spletnih družbenih medijih; e) zaupanje v spletne družbene medije in njihove uporabnike; f) nezadostne ocene nevarnostni, ki je lahko rezultat razkrivanja podatkov na spletu.

4.7 PREGLED VARNOSTNIH NASTAVITEV NA SPLETNIH SOCIALNIH OMREŽJIH

Kot poudarja Lahlou (2008, 318), vdor v zasebnost in zloraba osebnih podatkov nista odvisna od tega, kaj nekdo stori ali razkrije, temveč od tega, komu te podatke razkrije. Vdor v zasebnost, prav tako pa tudi kraja identitete, torej vedno vključujeta

nekoga 'drugega'. Uporabnikom spletnih družbenih medijev nadzor nad tem, komu bodo razkrili osebne podatke, omogočajo varnostne nastavitve. Z njimi uporabnik regulira dostop do informacij, ki jih objavi na svojem profilu. Kakšne možnosti ima uporabnik pri oblikovanju svojega profila in s kakšnimi varnostnimi nastavitvami ga lahko zaščiti, pa je odvisno od posameznega družbenega medija na spletu.

5 NEVARNOSTI IN MOREBITNE KRŠITVE OSEBNIH PODATKOV PRI UPORABI SPLETNIH SOCIALNIH OMREŽIJ

Zloraba osebnih podatkov in kraja identitete sta v veliki meri povezani z razvojem informacijsko-komunikacijskih tehnologij. V nadaljevanju so podani razlogi najpogostejših načinov za pridobitev osebnih podatkov iz internetnega omrežja, to so socialni inženiring, piškotki, vohunska programska oprema ali spyware.

5.1 SOCIALNI INŽENIRING

Eden od pojavov modernega časa, ki je zlasti uspešen v povezavi z uporabo modernih tehnologij, je socialni inženiring. Gre za prakso, ki bo najverjetneje vse bolj pogosta, predvsem zaradi možnosti hitrega zaslužka s pomočjo internetnih goljufij in počasnih reakcij zakonodajalca. Kevin Mitnick (2000, str. 15), svetovno znani heker in avtor knjige o socialnem inženiringu *Umetnost prevare* (*Art of Deception*), je zapisal: »Socialni inženiring pomeni uporabljanje vpliva in prepričevanja z namenom zavajanja ljudi, da verjamejo, da je socialni inženir nekdo, ki to ni, ali z manipulacijo. Posledica tega je, da lahko socialni inženir izkoristi ljudi tako, da od njih pridobi informacije z ali brez uporabe tehnologij.«

Socialni inženiring velikokrat poteka po principu izrabe že obstoječih informacij o posamezniku za pridobitev še več in bolj pomembnih podatkov. Glede na to, da se skoraj o vsakem izmed nas na internetu pojavljajo določeni podatki, socialni inženir zlahka pridobi podatke o naši preteklosti (o naših hobijih, obiskovanih šolah, profesionalnem življenju in ostalih aktivnostih). Nemalokrat se zgodi celo, da so na internetu pomotoma objavljeni določeni osebni podatki (v obliki seznamov, tabel …), saj za velikimi strežniki in računalniškimi ekrani seveda sedijo ljudje, uredniki spletnih strani, ki lahko objavijo na internetu nekaj, česar pravzaprav niso nameravali. Bistvo socialnega inženiringa so ravno informacije – več kot jih napadalec ima, lažje bo izvedel svoj napad (Pirc Musar, 2009, str. 5). V nadaljevanju so opisani najbolj značilni primeri za socialni inženiring.

5.1.1 SPLETNO RIBARJENJE

Spletni goljufi želijo s pomočjo lažnih spletnih strani in elektronskih sporočil od ljudi na takšen ali drugačen način izvabiti osebne podatke, kot so številke kreditnih kartic, uporabniška imena in gesla, digitalna potrdila in ostali osebni podatki. Pri tem uporabljajo različne tehnike, ki spadajo v domeno tako imenovanega socialnega inženiringa (s tem, da poskušajo od uporabnika na zvit način izvabiti osebne

podatke). Praviloma najprej postavijo lažno spletno stran, ki je zelo podobna pravi, nato pa z lažnim elektronskim sporočilom poskušajo izvabiti bodisi obisk te strani ali kar takoj pridobiti osebne podatke z odgovorom uporabnika na to sporočilo. Število poizkusov prevar (predvsem kraj denarja preko interneta) s pomočjo nenaročene oglasne pošte (spam) v kombinaciji s ponarejenimi spletnimi stranmi se je v zadnjem letu povzpelo do alarmantnih številk. Te so že primerljive s tistimi ob epidemijah računalniških virusov. Najpogostejša oblika te prevare je, ko elektronsko pismo ali pa spletna stran od uporabnika zahteva, da vanjo vnese svoje bančne podatke ali pa gesla. Tako goljufiva spletna stran kot elektronsko pismo sta lahko na pogled popolnoma enaka spletni strani ali pismu legitimnega podjetja (npr. banke), vendar bosta vaše finančne podatke posredovala tretjim osebam, ki se bodo z njimi okoristile. Za tovrstne prevare se v svetu uporablja izraz 'phishing'.

Za uporabnika, ki takšni goljufiji nasede, so posledice lahko relativno majhne (odtujitev na primer računa brezplačne elektronske pošte), lahko pa tudi zelo velike (na primer kraja večjih vsot denarja z bančnih računov). Ogroženost zaradi spletnega ribarjenja podatkov se še vedno povečuje; v svetu namreč dnevno nastane med 100 in 200 novih strani za ribarjenje podatkov, pri enem zadnjih bolj odmevnih primerov januarja 2007 pa je 250 uporabnikov neke švedske banke izgubilo skupaj 850.000 EUR (Pirc Musar, 2009, str. 8).

5.1.2 TROJANSKI KONJI, VIRUSI IN ČRVI

Virusi so predstavniki škodljive kode, ki živijo znotraj datotek, kot so datoteke urejevalnika besedil Word, urejevalnika preglednic Excel in ostalih. Ob odprtju okužene datoteke se virus razširi in okuži ostale datoteke na računalniku. Črvi so ravno tako samorepliciraječi se programi, ki pa so za razliko od virusov nekoliko bolj inteligentni, saj znajo samodejno iskati primerne tarče za okužbo. Tako črvi kakor tudi virusi prinašajo s seboj breme (*payload*), ki jim omogoča prevzem nadzora nad okuženim računalnikom, brisanje datotek ali tatvino osebnih podatkov. Bežen pregled tovrstnega področja nam pove, da se vsak teden pojavi okrog 500 novih virusov in črvov. Njihovo število se vsako leto poveča za 400 %, pri čemer postajajo njihovi avtorji (kriminalci) vse bolj iznajdljivi. Tovrstni predstavniki zlonamerne kode so pogosto doma ravno v nezaželenih elektronskih sporočilih (spam), zato je treba biti pri odpiranju tovrstne pošte še posebno pazljiv (Pirc Musar, 2009, str. 9).

5.1.3 SPLETNI ISKALNIKI

Informacije, ki so prosto objavljene na internetu, lahko napadalec uporabi najprej za izbiro najustreznejše žrtve in nato za pridobivanje njenih podatkov s pomočjo psihološke manipulacije oziroma uporabe ene od tehnik socialnega inženiringa. Če socialni inženir pridobi imena in priimke naročnikov revije o luksuznih avtomobilih,

lahko naročnika pokliče, se izdaja za predstavnika revije ter z lažno anketo denimo pridobi podatke o tem, kakšno varnost namenja naročnik svojemu avtomobilu. Druga možnost zlorabe interneta pa je vzpostavitev tako imenovanih lažnih spletnih strani; v skrajnem primeru gre za lažne strani spletnih bančnih poslovalnic, pa tudi vseh ostalih strani, ki za vstop zahtevajo registracijo oziroma prijavo. Napadalec pridobiva osebne podatke od obiskovalcev spletnih strani tako, da jih pravzaprav prelisiči, da vpišejo svoje podatke na spletno stran, za katero so prepričani, da je 'prava' oz. da pripada osebi ali podjetju, ki so mu pripravljeni zaupati (Pirc Musar, 2009, str. 8).

5.2 PIŠKOTKI

Piškotki so majhne tekstovne datoteke, ki se shranijo na uporabnikovem računalniku ob obisku spletne strani. Njihov namen je poenostavitev uporabnikovega dela. Nekatere spletne storitve zahtevajo uporabniško ime in geslo. Da pa nam ob ponovnem obisku ni treba znova vpisovati teh podatkov, nam lahko ob pripadajoči izbiri pomagajo prav piškotki. Spletne trgovine tako kar same ponujajo artikle, ki so bili izbrani ob zadnjih obiskih teh strani. Poznamo časovno omejene in trajne piškotke. Razlikujejo se po svoji obstojnosti, ki je določena s strani spletne aplikacije, ki jih je ustvarila. Nekateri poidejo že ob zaprtju brskalnika, nekateri po določenem času. Piškotki lahko tudi kršijo zasebnost, če posameznik o njih ni ustrezno obveščen in npr. lastniki spletnih strani zaznajo uporabnikovo nakupovalno obnašanje na spletu in tako sestavijo uporabniški profil (Pirc Musar, 2009, str. 11).

5.3 VOHUNSKA PROGRAMSKA OPREMA ALI »SPYWARE«

Med vohunsko programsko opremo spadajo vsi programi, ki omogočajo pošiljanje zasebnih podatkov brez privolitve ali vednosti uporabnika. Za pošiljanje raznih statističnih podatkov, kot so seznami obiskanih spletnih mest, elektronski poštni naslovi z uporabnikovega seznama stikov ali seznami uporabnikovih udarcev tipk, uporabljajo funkcije sledenja. Avtorji vohunske programske opreme trdijo, da želijo s temi tehnikami izvedeti več o uporabnikovih potrebah in interesih ter da zagotavljajo boljše ciljno oglaševanje. Težava je v tem, da ni mogoče jasno razlikovati med uporabnimi in zlonamernimi programi in da nihče ne more biti povsem prepričan, da pridobljeni podatki ne bodo zlorabljeni. Med podatki, pridobljenimi z vohunsko programsko opremo, so lahko varnostne kode, PIN-i, številke bančnih računov itn. Vohunska programska oprema je pogosto v paketu brezplačne različice programa avtorja, ki želi ustvariti nek dobiček ali spodbuditi uporabnika k nakupu programske opreme. Pogosto so uporabniki med nameščanjem programa obveščeni o prisotnosti vohunske programske opreme, da bi jih njeni avtorji tako spodbudili k nadgradnji programa v plačljivo različico brez nje (Pirc Musar, 2009, str. 12).

6 RAZISKOVALNI OKVIR

V predhodnih poglavjih sem predstavila izhodišča in možnosti zlorabe osebnih podatkov, ki so večini uporabnikom neznane. Ob tem sem dodatno pozornost namenila spletnim socialnim omrežjem. Izpostavila sem pomen zlorabe osebnih podatkov pri uporabi v spletnih socialnih omrežjih ter hkrati raziskala nevarnostni v spletnem raziskovalnem okolju. S pomočjo analize literature in virov ter na podlagi že opravljenih raziskav na tem področju želim predstaviti zlorabo osebnih podatkov.

V diplomskem delu sem zastavila štiri temeljne cilje: seznanitev s področjem zlorab osebnih podatkov v socialnih omrežjih, predstaviti vse razsežnosti pojma zloraba osebnih podatkov, predstaviti varno rabo osebnih podatkov v spletnih socialnih omrežjih, opisati značilnosti delovanja nevarnosti v spletnih socialnih omrežjih, ki so bili upoštevani.

Opirala sem se na že obstoječa spoznanja, opredeljena v domači in tuji literaturi, celotno delo pa je temeljilo na metodi deskripcije, opisu in predstavitvi zlorabe osebnih podatkov v spletnih socialnih omrežjih. Uporabljena je bila tudi eksperimentalno-kavzalna metoda za pridobivanje informacij iz naslova eksperimentiranja (pregledovanje spletnih strani). Pri izdelavi diplomskega dela sem uporabila tudi teoretično-deskriptivno metodo za uporabo študije in interpretacijo že napisane literature. Slednja metoda zajema komparativno metodo (metoda primerjave), metodo deskripcije (metoda opisovanja) in metodo kompilacije (metoda navedb drugih avtorjev).

Za podkrepitev že obstoječih spoznanj sem uporabila kvalitativno metodo – intervju, ki velja za najpogostejšo uporabljeno sociološko metodo spraševanja in omogoča kvalitativno obdelavo podatkov. Zanimala so me stališča, videnja in prepričanja ljudi, ki so eksperti na tem področju. Intervju sem opravila z gospodom Vukom Ćosićem, gospodom Gorazdom Božičem, gospodom Francijem Mulcem in gospo Evo Kalan. Intervjuje sem izvedla preko elektronske pošte, saj je bil tako moj interes in interes imenovanih, da se hitreje opravijo.

Različni avtorji vseskozi poudarjajo, da se uporabniki spletnih socialnih omrežij ne zavedajo dovolj zlorab oz. nevarnosti, ki jim preži na spletnih socialnih omrežij. Na podlagi predhodno opravljene analize obstoječe literature o tej problematiki postavljam naslednje hipoteze:

1. Zloraba osebnih podatkov v spletnih socialnih omrežjih se povečuje.
2. Z razcvetom spletnih socialnih omrežij postaja zloraba osebnih podatkov enostavnejša.
3. Razvoj informacijske tehnologije vpliva na zlorabo osebnih podatkov.

6.1 ANALIZA INTERVJUJEV

Vsem štirim intervjuvancem sem zastavila enaka vprašanja, kot pričakovano, pa so se odgovori med seboj zelo razlikovali (glej Priloge). Udeleženci intervjuja so bili:

- **Vuk Ćosić**, pionir na področju spletne umetnosti – NET.ARTA,
- **Franci Mulec**, vodja informacijske tehnologije in informacijske varnostni v Službi Vlade RS za razvoj in evropske zadeve,
- **Gorazd Božič**, vodja slovenskega centra za posredovanje pri omrežnih incidentih (SiCERT),
- **Eva Kalan**, svetovalka pri Informacijskemu pooblaščencu RS.

Zelo zanimiv intervju sem opravila z gospodom **Vukom Ćosićem**, slovenskim spletnim interaktivnim umetnikom, znanem po projektih, v katerih uporablja splet za umetniške inštalacije, ASCII umetnost, projektu Slovenija in drugih. Zanimalo me je, kakšno je njegovo mnenje o brezskrbnem dajanju osebnih podatkov v spletna socialna omrežja, o odgovornosti uporabe osebnih podatkov, zasebnosti na internetu, o osveščenosti o uporabi orodij oziroma tehnologije za izboljševanje zaščite osebnih podatkov in kako bi izboljšali to osveščenost ter kaj svetuje tako starim kot novim uporabnikom spletnih socialnih omrežij.

Ćosić meni, da glavni pritisk prihaja od državnega aparata ter iz medijev, oba akterja pa sta dobila nov zagon najprej s pojavom digitalnih medijev, potem pa tudi s pojavom socialnih medijev. »Zaradi implicitnega dogovora, ki je jedro samega obstoja države kot organizacijske oblike skupnosti ima državna uprava pravico do posedovanja in nenadzorovanega križanja osebnih podatkov o 'podložnikih'. Koncept Big Brotherja je z razlogom še vedno povezan z državo in ne z mediji v zasebni lasti. Torej, prisiljeni smo imeti zaupanje v državo, ki bi po implicitnem dogovoru morala skrbno in vestno ravnati z našimi podatki, da bi bolje koordinirala delovanje skupnosti za splošno dobro (javni interes)«.

Mediji so tekom zadnjih nekaj generacij močno spremenili naše čutenje privatnosti. V našem času smo se morali naučiti, da je vsakdo javna oseba, da je osebni podatek vsakega od nas lahko javen. Socialni mediji so se pojavili kot logično nadaljevanje tega trenda, oziroma so delno formirani izhajajoč iz te miselnosti.

Ćosič je povedal, do so spletna socialna omrežja v lasti gospodarskih subjektov, ki imajo za cilj ustvarjanje dobička. Glavni oziroma praktično edini poslovni model teh spletnih podjetij je prodajanje spletnega prometa oglaševalcem. »Ne pričakujem, da bodo FB in TW šli zelo daleč v ščitenju pravic posameznika, če bo to v navzkrižju z njihovim razlogom obstoja. Seveda obstajajo tudi razlike med podjetji – če se spomnimo reakcij na pritisk State Departmenta ob aferi Wikileaks – in te bodo morda pomemben vhodni podatek za etičnega potrošnika, ki izbira s kom posluje«.

Poudaril je, da bo človeštvo organsko sprejelo in modificiralo to medijsko tehnologijo. »Nekateri bodo bolj, nekateri manj vešče izkoristili ta prvi val, nekatere bodo dogodki celo prizadeli, in edino interesantno je, kaj bo v seštevku tista ireverzibilna družbena sprememba, ki ji bomo priča. Ne morem napovedati, ali bomo dejansko doživeli dobo povečane transparentnosti in odgovornosti, ali bodo morda nove okoliščine samo pripeljale do bolj subtilnih oblik vzajemnega izkoriščanja. Od tega širokopoteznega ozadja je odvisno, kako bo izgledalo življenje posameznih uporabnikov.
Varnost bo na mikro ravni – razen od opisanih civilizacijskih dejavnikov – odvisna od kombinacije osebne inteligence in afinitet uporabnika. Morda je dobro biti pozoren pri branju medijskih zgodb pobarvanih z moralno paniko«.

Franci Mulec, vodja informacijske tehnologije in informacijske varnostni v službi Vlade RS za razvoj in evropske zadeve, je mnenja, da se uporabniki socialnih omrežij še premalo zavedajo, da bodo razkriti podatki in napisana mnenja dosegljiva upraviteljem sistema, javnosti, različnim ameriškim in drugim državnim organom in različnim gospodarskim subjektom še mnogo let, saj je diskovni prostor vse cenejši. Možno je, da bo najstnik čez mnogo let mogoče pomembna javna osebnost ali direktor uspešnega podjetja in bo nekdo uporabil te podatke proti njemu.

Mulec je povedal, da moderne računalniške tehnologije noben uporabnik ne more več 100-odstotno obvladovati. To velja tudi za upravitelje in lastnike socialnih omrežij. »Kar vedno pomeni, da je 'pot' podatkov, ki jih razkrivate ali posredujete v računalniškem svetu čedalje bolj nepredvidljiva. Zasebnosti na internetu nikoli ni bilo, niti nikoli ne bo. Torej vse, kar pišete na vaš računalnik in/ali na internet, se lahko pojavi kadarkoli in kjerkoli«.

Opozoril je, da uporabniki spletnih socialnih omrežij še niso dovolj osveščeni o uporabi orodij oz. tehnologije za izboljšanje zaščite osebnih podatkov na internetu, in dodal, da sta za slednjo pomembni vloga in odgovornost staršev, šole in državnih organov. Na vprašanje, ali lahko poda kakšen poseben ali najbolj odmeven primer zlorabe osebnih podatkov v spletnih socialnih omrežjih, je odgovoril pritrdilo. Povedal je za primer kandidatke za visoko uradnico v slovenski državni upravi (ministrstvu), ki se je v svoji prijavi za delovno mesto predstavila bistveno drugače, kot se je predstavljala na socialnem omrežju. Seveda ni prišla v ožji izbor za zaposlitev.

Po mnenju **Gorazda Božiča** se premalo zavedamo, da podatke dajemo zasebnemu podjetju v ZDA in da nas v primeru morebitnih zapletov ne morejo varovati naša lokalna zakonodaja in pristojne inštitucije. Naši podatki pomenijo Facebooku zaslužek, in to je razlog, zakaj to storitev dobimo 'zastonj'. »Menim, da smo danes v situaciji, kjer stare rešitve ne funkcionirajo več. Koncentracija podatkov pri velikih ponudnikih, kot sta Facebook in Google, obračajo model porazdelitve hranjenja podatkov na glavo. Ne samo da jih centraliziramo, to počnemo tudi z iznosom v državo, ki ima

popolnoma drugačno stališče do te teme, kot je to običajno v Evropi. Tu ne gre le za posameznike, v imenu optimizacije stroškov se 'v oblak' selijo cela podjetja in univerze«.
Družabna omrežja se spreminjajo, nastajajo nova, zato moramo vedno znova razmišljati, komu dajemo podatke in pod kakšnimi pogoji. Starim in novim uporabnikom zato svetuje, da se zavedajo, da smo z objavo na teh omrežjih verjetno nekaj pravic do svojega materiala izgubili. »Dosedanje izkušnje kažejo, da se lahko pravila igre čez noč spremenijo. Nekaj previdnosti torej, po drugi strani pa so družabna omrežja dandanes dejstvo in vedno več ljudi jih uporablja, zato kakšna abstinenca ni vedno smiselna«.

Božič je povedal tudi, da je najpogostejši primer še vedno kraja profila (npr. posameznik ugrabi profil nekdanjemu ljubezenskemu partnerju in na njem objavlja neprimerne vsebine).

Eva Kalan, svetovalka za področje zlorab osebnih podatkov na spletnih socialnih omrežjih pri Informacijski pooblaščenki, je svoje izkušnje pridobivala na različnih področjih. Z njo sem se pogovarjala o lahkomiselnem dajanju osebnih podatkov na spletna socialna omrežja, posledicah razkritja osebnih podatkov na spletu, o osveščenosti uporabnikov spletnih socialnih omrežij v zvezi z orodji oziroma tehnologijo za izboljšanje zaščite osebnih podatkov ter morebitni odgovornosti za izboljšanje zasebnosti na spletu ter priporočilih o uporabi osebnih podatkov na spletnih socialnih omrežjih.

Kalanova pravi, da vsa spletna socialna omrežja (Facebook, Netlog, MySpace…) temeljijo na vzpostavljanju medsebojnih povezav, zato uporabnika spodbujajo, da objavi čim širši nabor svojih osebnih podatkov. »In ravno nepremišljeno objavljanje prevelike količine (svojih) osebnih podatkov ter slabo varovana zasebnost uporabnikov je tisti vidik spletnih omrežij, ki lahko potencialno za posameznika pomeni tudi veliko nevarnost. Posameznik lahko v zvezi s tem največ stori sam, in sicer tako, da vedno dvakrat premisli, kaj bo objavil in kaj lahko taka objava zanj pomeni v prihodnosti«.

Kalanova meni, da se zavedanje s pomočjo akcij ozaveščanja, ki jih v Sloveniji na primer pripravlja tudi Informacijski pooblaščenec, počasi veča, vendar pa na žalost še vedno ni niti približno zadovoljivo. To opaža tudi pri svojem delu, saj tedensko prejme veliko vprašanj v zvezi z nepremišljenim razkrivanjem osebnih podatkov na spletu in posledično zlorabo le-teh s strani raznih nepridipravov (od škodoželjnih vrstnikov, pa vse do tatov identitete). Opozarja, da marsikdo sploh ne vidi težav z vidika zasebnosti, saj je mnenja, da se vsak uporabnik zase odloči, kaj bo objavil in komu bo omogočil vpogled. Vendar ob tem opomni, da je ponudnik spletnega socialnega omrežja upravljavec velike zbirke osebnih podatkov, ki mu Zakon o varstvu osebnih

podatkov predpisuje, da mora podatke obdelovati v zakonite in poštene namene in da jih brez ustrezne pravne podlage ne sme posredovati tretjim osebam.
Intervjuvanja je poudarila ključnost premišljene uporabe. Uporabnikom svetuje, da vedno dvakrat premislijo, kaj bodo objavili na spletnih družabnih omrežjih in na spletu na splošno in kaj lahko taka objava pomeni za njih čez na primer 30 let. Posameznik lahko namreč za varnost svojih osebnih podatkov in ohranitev zasebnosti največ stori sam s premišljenim ravnanjem.

6.2 PREVERJANJE HIPOTEZ

1. Prva hipoteza: *Zloraba osebnih podatkov na spletnih socialnih omrežjih se povečuje.*

Število uporabnikov spletnih socialnih omrežij se iz dneva v dan povečuje, s čimer se veča tudi število objavljenih osebnih podatkov in s tem njihova zloraba na spletu. Spletna socialna omrežja posamezniku ne služijo le kot vir informacij o tem, kaj se dogaja po svetu, ampak ga tudi informirajo o ljudeh, ki jih želi spoznati oziroma imeti za prijatelje. Na Facebooku in MySpaceu se na zavihku 'Domov' uporabniku izpiše celotna spletna aktivnost njegovih 'prijateljev'. Posameznik lahko izve, kdo se je s kom 'spoprijateljil', katerega dogodka se bo kdo udeležil, kdo je komu kaj sporočil. Vsak uporabnik omrežij ima možnost, da svoj profil omeji in tako določi, kateri podatki bodo vidni in kateri ne. Ti vmesniki služijo kot nekakšni majhni vohunski sistemi, kjer vsak profil čuva in gleda na druge, ne da bi jih ti drugi opazili. Od posameznika je torej odvisno, ali se udejstvuje aktivno ali pasivno, kot uporabnik ali kot producent.

Med uporabniki divja prava vojna za čim večje število prijateljev. Zbirke prijateljev tako postanejo zbirke elektronskih naslovov in osebnih podatkov, preko katerih uporabniki ohranjajo medsebojne stike in sledijo življenjsko pomembnim dogodkom svojih znancev. Vsi omenjeni intervjuvanci so se strinjali s to hipotezo in jo tudi potrdili.
Prva hipoteza je v celoti potrjena.

2. druga hipoteza: *Z razcvetom spletnih socialnih omrežij postaja zloraba osebnih podatkov enostavnejša.*

Spletna socialna omrežja so sestavljena iz profilov uporabnikov. Profil je individualna spletna stran uporabnika, na katerem se nahajajo fotografije, tekst, video materiali, komentarji drugih uporabnikov ter javni seznam prijateljev. Primaren namen spletnih socialnih omrežij je iskanje oziroma vzpostavljanje novih ali obnavljanje starih poznanstev. Vendar kaj kmalu ugotovimo, da je komunikacija med uporabniki skopa in da jih vse več teži le k čim večjemu številu prijateljev, ne pa k poglobitvi stikov in tkanju pristnih vezi. Virtualna prijateljstva na spletnih socialnih omrežjih rastejo z

neverjetno hitrostjo. Vsak lahko postane prijatelj skoraj s komerkoli. Negativna posledica je prav v tej nagli hitrosti in dostopnosti, ki vsakomur omogoča dostop do okolja drugih. Z razširjeno uporabo spletnih socialnih omrežij, kot je Facebook, glede na nedavno raziskavo uporabniki vse težje ohranjajo svojo anonimnost.

Čeprav snovalci Facebooka poudarjajo, da jim je ohranjanje zasebnosti ena od glavnih prioritet, za katero se močno zavzemajo, se kljub temu poraja vprašanje, koliko je uporabnikova zasebnost pravzaprav sploh zasebna. Osnovni namen spletnih socialnih omrežij je vzpostavljanje medsebojnih povezav in komuniciranje uporabnikov, zato jih spodbujajo k objavi čim širšega nabora svojih zasebnih in osebnih podatkov. Tudi to hipotezo so v celoti vsi omenjeni intervjuvanci potrdili.
Druga hipoteza je v celoti potrjena.

3. tretja hipoteza: *Razvoj informacijske tehnologije vpliva na zlorabo osebnih podatkov*.

Sodobne tehnologije so v vsakdanje življenje vnesle izjemno preprostost obdelave podatkov, posebej tistih, ki so shranjeni v elektronski obliki. To pomeni, da so v vsakdanje življenje vnesle tudi nevarnost, da je možno osebne podatke hitreje in lažje zlorabiti in jih ob pravi kombinaciji enostavno uporabiti za krajo identitete. Po nekaterih podatkih med prebivalci ZDA strah številka ena niso več teroristični napadi, pač pa zloraba osebnih podatkov in posledično kraja identitete. Tudi prebivalci EU nismo imuni pred zlorabo osebnih podatkov, kljub dokaj strogi zakonski uredbi, ki se nanaša na varstvo osebnih podatkov. Vendar noben zakon ne more nadomestiti tistega, kar je pri varovanju osebnih podatkov najpomembnejše – zavedanja prav vsakega posameznika o pomembnosti lastnih osebnih podatkov. Če sami ne bomo poskrbeli na zadostno zavarovanje, bomo lahko kmalu postali tarče tatov identitete. Vsi omenjeni intervjuvanci so se strinjali, da razvoj informacijske tehnologije vpliva na zlorabo osebnih podatkov.
Tretja hipoteza je v celoti potrjena.

7 ZAKLJUČEK

V času, ko sodobna informacijska tehnologija napreduje z izjemno hitrostjo, ljudje vsak dan žanjemo sadove teh dosežkov in novih pridobitev. Skoraj sočasno pa nastanejo nove nevarnostni in načini vdora v zasebnost, kar posledično pomeni nevarnost za posameznikove osebne podatke. Internet namreč predstavlja virtualen prostor, kjer se pretakajo ogromne količine osebnih podatkov, ki se obdelujejo s strani najrazličnejših akterjev. Pravna regulativa je na tem področju v zadnjih nekaj letih naredila pomembne korake v smeri varovanja osebnih podatkov, kar nekaj izzivov pa še ostaja.

Zloraba osebnih podatkov na spletnih socialnih omrežjih je postala nekakšen fenomen, katerega razsežnost je dosegla cel svet. Spletna socialna omrežja privlačijo na milijone ljudi in za marsikoga predstavljajo vsakodnevno rutino in prakso. S povečevanjem števila uporabnikov spletnih socialnih omrežij raste tudi problem varstva osebnih podatkov, kajti za včlanitev v spletno socialno omrežje je treba navesti kar nekaj osebnih podatkov. S tem pa se povečajo možnosti za zlorabo osebnih podatkov.

V prvem delu diplomske naloge sem obravnavala problem varstva osebnih podatkov na spletnih socialnih omrežjih. Pozornost sem namenila varstvu osebnih podatkov ter zasebnosti in zaščiti v spletnih socialnih omrežjih. Opredelila sem množične medije, opisala njihove funkcije ter predstavila najpomembnejše študije in avtorje v tradiciji medijskih učinkov. Definirala in podala sem kratko zgodovino interneta ter opisala njegovo rabo. Četrto poglavje je v celoti namenjeno spletnim socialnim omrežjem. Opredelila in poiskala sem značilnosti spletnih socialnih omrežij, predvsem najbolj obiskanega spletnega socialnega omrežja – Facebook. Raziskala sem, kakšna komunikacija poteka na njih, ter podrobneje raziskala nadzor zasebnosti ter prijateljstva v virtualnem svetu. V petem poglavju sem se posvetila uporabi spletnih socialnih omrežij in nevarnostim zlorabe osebnih podatkov. Podala sem primere potencialnih nevarnostni za zlorabo osebnih podatkov, podrobneje opisala zasebnost na spletnih socialnih omrežjih, razkrivanje osebnih podatkov ter krajo identitete. Nevarnosti in morebitne kršitve osebnih podatkov pri uporabi spletnih socialnih omrežij so bile temeljni cilj šestega poglavja. Pozornost sem namenila morebitnim pastem spletnih socialnih omrežij, kot so socialni inženiring, ribarjenje podatkov, trojanski konji, spletni iskalniki, piškotki ter vohunska programska oprema ali Spyware.

S pridobljenim znanjem sem se lotila raziskovalnega okvirja. Zastavila sem tri hipoteze, ki sem jih v celoti potrdila s pomočjo intervjuvancev in uporabljene literature. S pomočjo Vuka Ćosića, slovenskega spletnega interaktivnega umetnika, Francija Mulca, vodjo informacijske tehnologije in informacijske varnostni v Službi

Vlade RS za razvoj in evropske zadeve, Gorazda Božiča, vodjo slovenskega centra za posredovanje pri omrežnih incidentih (SiCERT), in Evo Kalan, svetovalko za področje zlorab osebnih podatkov v spletnih socialnih omrežij pri Informacijski pooblaščenki RS, sem podala nasvete za varno rabo spletnih socialnih omrežij.
Vsi omenjeni intervjuvanci so bili menja, da se uporabniki spletnih socialnih omrežij pogosto ne zavedajo, da so lahko njihovi osebni podatki objavljeni zelo dolgo in da jim morda čez nekaj časa lahko tudi škodijo. Zaskrbljujoč je podatek, koliko uporabnikov je pripravljenih deliti osebne podatke z drugimi uporabniki spletnih socialnih omrežij. Človeštvo bo organsko sprejelo in modificiralo to medijsko tehnologijo. Nekateri bodo bolj in nekateri manj vešče izkoristili ta prvi val, nekatere bodo dogodki celo prizadeli, in edino interesantno je, kaj bo v seštevku tista ireverzibilna družbena sprememba, ki ji bomo priča. Ne da se napovedati, ali bomo dejansko doživeli dobo povečane transparentnosti in odgovornosti, ali bodo morda nove okoliščine samo pripeljale do bolj subtilnih oblik vzajemnega izkoriščanja. Od tega širokopoteznega ozadja je odvisno, kako bo izgledalo življenje posameznih uporabnikov. Seveda je odločitev glede objave osebnih podatkov na njihovi strani, intervjuvanci pa vendar svetujejo temeljit premislek.

Glede na temeljni cilj diplomskega dela – raziskati področje zlorab osebnih podatkov v socialnih omrežjih, predstaviti vse razsežnosti pojma zlorabe osebnih podatkov ter varno rabo osebnih podatkov – lahko sklenem, da so zlorabe osebnih podatkov na spletnih socialnih omrežij zelo razširjene in se drastično povečujejo. Ljudje se poslužujejo socialnih omrežij zaradi ohranjanja prijateljskih stikov, nekaterim pa predstavljajo zabavo in način preživljanja prostega časa.

Ne zavedamo se, da živimo v družbi, v kateri po eni strani opažamo čedalje večje poudarjanje posameznikove individualnosti in zasebnosti, po drugi strani pa smo priča čedalje višji stopnji nadzorovanja. Prav tako ne moremo mimo tega, da je nadzor tesno povezan s tehnologijo. Informacijske tehnologije so namenjene zbiranju in obdelavi vseh vrst podatkov in informacij. Dvigovanje ozaveščenosti ter stalno izobraževanje in izpopolnjevanje že mnogo let veljajo za mantro varnega in uspešnega delovanja v informacijski družbi. To seveda velja tudi pri ravnanju z osebnimi in drugimi podatki. Kaj kmalu se namreč lahko zgodi, da od naše pravice do informacijske samoodločbe (komu, zakaj in kakšne osebne podatke bomo posredovali) ostane le še oddaljen spomin in veliko težav, ki jih moramo reševati, ne da bi bili zanje krivi sami. S premeteno uporabo tehnik socialnega inženiringa se lahko zgodi, da ostanemo brez sredstev na transakcijskem računu, da utrpimo poslovno škodo ali imamo kopico drugih nevšečnosti. Podatki kažejo, da so opisane možnosti zlorabe osebnih podatkov v porastu, vendar se jim lahko s proaktivnim delovanjem uspešno zoperstavimo.

Menim, da se uporabniki interneta premalo zavedajo oziroma premalo poznajo grožnje zasebnosti na spletnih socialnih omrežjih. Uporabnik dejansko ne upošteva

dejstva, da ne objavlja podatkov o sebi le za svoje prijatelje, temveč jih lahko preberejo tudi drugi. Internet je postal nekakšna ječa, ki je posameznika zaprla v 'zlato' kletko personaliziranih spletnih izkušenj. Velikokrat brez potrebe razkrivamo svoje osebne podatke in premalo poznamo orodja za zaščito zasebnosti na internetu. Kljub temu pa čutimo določen strah pred razkritjem osebnih podatkov ter nadzorom, ki ga nove tehnologije omogočajo. Upamo lahko, da se bo s pomočjo različnih predpisov, zakonov in sporazumov ter izobraževanjem dvignila ozaveščenost glede pomembnosti zlorabe osebnih podatkov na spletnih socialnih omrežjih. Veliko pozornosti bo treba nameniti informiranju in izobraževanju posameznikov, saj se v večini primerov le-ti ne zavedajo nevarnosti za osebne podatke in ukrepov, ki se jih lahko poslužujejo za zmanjšanje teh nevarnosti pri uporabi spletnih socialnih omrežjih. Poudarila bi, da se bo zaradi hitrega razvoja spleta pojavilo tudi vedno več novosti, pri katerih bo verjetno še večje tveganje za zlorabo osebnih podatkov, mi pa bomo morali znati ločiti med tem, kaj je zasebno in kaj je javno.

LITERATURA IN VIRI

ANĐELKOVIĆ, Boris, *Emplematične »identitete« in nadzorovana »komunikacija« darovanja na MySpacu in Facebooku.* Radio študent. 2008: Dostopno prek: http://www.radiostudent.si/print.php?sid=17023&lang=slovene

BOYD, Danah. 2007. *Social Network Sites. Public, Privat or What?* Dostopno prek: http://kt.flexiblelearning.net.au/tkt2007/edition-13/social-network-sites-public-private-or-what

BARNES, Susan. 2006. *A privacy paradoxs: Social networking in the United States. D*ostopno prek:http://www.digitallymediatedsurveillance.ca/2011/05/a-privacy-paradox-social-networking-in-the-united-states

BRODNIK, Tadej. 2007. *Vloga identitete v kiberprostoru*. Diplomsko delo Ljubljana. Fakulteta za družbene vede (FDV).

CAETON Daniel. 2007. *The Cultural Phenomenon of Identity Treft and the Domenstication of the World Wide Web, Bulletion of Science Tehnology and Society 27* (1): 11–23. Dostopno prek: https://login.nukweb.nuk.uni-lj.si/url=http://bst.sagepub.com/cgi/reprint/27/1/11 (20. januar 2011).

CRNOVIĆ Deja. 2007. Moj ego je težak 500 prijateljev. Mladina 50. Narodno Univerzitetna knjižnica, Ljubljana.

DALUŠIĆ, Sunčica. Virtualna prijateljstva. Vjesnik, 2009. Dostopno prek: http://www.vjesnik.hr/Search.aspx?text=virtualno%20prijateljstvo

GOLDBERG, Ian Avrum. 2000. A *Pseudonymous Communications Infrastructure for the Internet. Berkeley*. University of California

KWON, Ohbyung in WEN, Yixing 2009. *An empirical study of the factors affecting social network service use. Computers in Human Behaviour*

KOVAČIČ, Matej. 2003. *Zasebnost na internetu*, Ljubljana. Mirovni inštitut.

KEČANOVIČ, Sabina. 2009. Prijateljstvo in narcizem na spletnih socialnih omrežjih. Diplomsko delo, Ljubljana, Fakulteta za družbene vede.

KVAS, Bojan. 2009 Raziskava: Spletna omrežja so »zlata jama« osebnih podatkov. Dostopno prek: http://www.e-demokracija.si/2009/03/30/raziskava-spletna-omrezja-so-zlata-jama-osebnih-podatkov

LAHLOU Saadi. 2008*. Identity Social status, privacy and face-keeping and digital society. Social Sience Information* 47 (3): 299–330. Dostopno prek: https://login.nukweb.nuk.uni-lj.si/ url=http://ssi.sagepub.com/cgi/reprint/47/3/299

LAURANT Ceric. 2003. *Privacy nd Human Rights* An internation survay of privacy laws and developments. Dostopno prek: https://www.privacyinternational.org/survey/phr2003/overview.htm

MCQUAIL, Denis. 1994. Mass Communication Theory. London: Sage

MCQUAIL, Denis. 1987. Mass communication Theory. London: Sage

MONAHAN, Torin. (2009). *Identity treft vulnerability*. Theoretical Criminology. 13 (2) 155–176,

OFCOM. 2008. *Social Networking. A quantitative and qualitative research report into attitudes behaviours and use*. Dostopno prek: http://stakeholders.ofcom.org.uk/market-data-research/media-literacy/medlitpub/medlitpubrss/socialnetworking/

OBLAK, Tanja in PETRIČ Gregor. 2005. *Splet kot medij in mediji na spletu*. Fakulteta za družbene vede. Ljubljana.

PIRC MUSAR, Nataša. 2009. *Smernice za preprečevanje kraja identitete*. Informacijska pooblaščenka, Ljubljana.

PIRC MUSAR, Nataša. 2009. *Socialni inženiring in kako se pred njim ubraniti*. Informacijska pooblaščenka, Ljubljana.

ROSEN, Cherise. 2007. *Virtual Friendship and the New Narcisim*. Dostopno prek: http://www.thenewatlantis.com/publications/virtual-friendship-and-the-new-narcissism

SEPPA, Ville. 2008. The Future of Social Networking Seminar on Internetworking.

SPLICHAL, Slavko. 1991. *Množično komuniciranje med svobodo in odtujitvijo*. Obzorja. Ljubljana.

SPENCER, Kelly. 2008*. Identity 'at risk' on Facebook. BBC News, 1. maj*. Dostopno prek:
http://news.bbc.co.uk/2/hi/programmes/click_online/7375772.stm

ULE NASTRAN. Mirjana. 2000. *Temelji socialne psihologije*. Znanstveno in publicistično središče Ljubljana.

VREG, France. 2004. *Politično komuniciranje in prepričevanje*. Komunikacijska strategija, diskurzij, prepričevalni modeli, propaganda, politični marketing, volilna kampanja. Ljubljana, Fakulteta za družbene vede.

ZAVRŠNIK, Alojz. *Kibernetična kriminaliteta*: *(kiber)kriminološke in (kiber)viktimološke posebnosti »informacijske avtoceste«.* Revija za kriminalistiko.

Zakon o varstvu osebnih podatkov (ZVOP-1-UPB1), Uradni list Republike Slovenije, št. 86/2004 in 113/2005. Dostopno preko: http://www.uradnilist.si/1/objava.jsp?urlid=200486&stevilka=3836

Virtualni »prijatelji« lahko ukradejo vašo identiteto. 2007. Finance. Dostopno preko: http://www.finance.si/194604

PRILOGE

Priloga 1: Intervju z Vukom Ćosićem, pionirjem na področju spletne umetnosti *net.arta*

1. Spletna socialna omrežja so postala v današnjem svetu čedalje večji fenomen. Ustanovitelj Facebooka, Mark Zuckerberg meni, da se v Facebook dnevno včlani 450.000 novih uporabnikov, s tem tudi ogromno število osebnih podatkov. Kakšno je vaše mnenje o brezskrbnem dajanju osebnih podatkov v spletna sociala omrežja?

Naš občutek za privatnost občutno mutira že nekaj generacij. Glavni pritisk prihaja iz smeri državnega aparata in potem iz medijev. Oba akterja pa sta dobila nov zagon najprej s pojavom digitalnih medijev potem pa tudi s socialnimi mediji:

1. Državna uprava ima – zaradi implicitnega dogovora, ki je jedro samega obstoja države kot organizacijske oblike skupnosti – pravico do posedovanja in nenadzorovanega križanja osebnih podatkov o podložnikih. Koncept big brotherja je z razlogom še vedno povezan z državo in ne z mediji v zasebni lasti.
   Torej, prisiljeni smo imeti zaupanje v državo, ki bi po implicitnem dogovoru morala skrbno in vestno ravnati z našimi podatki, da bi bolje koordinirala delovanje skupnosti za splošno dobro (javni interes).
2. Mediji so v zadnjih nekaj generacijah časa močno spremenili naše čutenje privatnosti. V našem času smo se morali naučiti, da je vsakdo javna oseba, in je osebni podatek vsakega od nas lahko javen. Socialni mediji so se pojavili kot logično nadaljevanje tega trenda, oz. so delno formirani izhajajoč iz te miselnosti.

2. Razkritje osebnih podatkov na spletih socialnih omrežjih prinaša obilo tveganj in posledic. Menite, da se uporabniki spletnih socialnih omrežij zavedajo posledic?

Prav v slovenskem prostoru smo svojevrsten unikum, ker imamo besedi Družbeni in Družabni mediji. Z uporabo prevoda Družabni mediji smo povzročili javno percepcijo izmenjevanja osebnih podatkov kot nečesa za zabavo ipn... Uporabnikom je udeležba na FB predstavljena kot vir zabave in koncept tveganja je nezaželen, ker moti žur.

3. Kaj menite o odgovornosti uporabe osebnih podatkov, zasebnosti na internetu?

Vsi akterji v informacijski družbi se morajo naučiti nove strukture družbe in načina delovanja v njej. To med ostalim pomeni bistveno večjo vidljivost oz. najdljivost

vsakega akterja in posledično tudi potrebo po drugačnem ravnanju z zasebnostjo. Ta generacija se istočasno uči in postavlja pravila.
Moj osebni občutek je, da bomo nedvomno morali prisluhniti mladim, ki jim je raba mrežnega komuniciranja nekaj organskega in jih ne obremenjujejo pred-digitalna razmišljanja. Vloga nas starejših, ki še pomnimo čase izpred interneta, je, da nekatere morebitne površnosti nekoliko obogatimo z izkušenejšim pogledom. Zagovarjam torej neko permisivnost s fusnoto.

4. Lastniki spletnih socialnih omrežij zbirajo in nato prodajajo baze informacij, ki naj bi jih "očistili" osebnih podatkov, podjetjem za tržne raziskave. Vendar so znanstveniki razširili računalniški algoritem, s pomočjo katerega je moč identificirati uporabnika spletnega socialnega omrežja zgolj na podlagi anonimnega socialnega grafa. Bi morali lastniki spletnih socialnih omrežij kljub temu, da podatki, katere prodajajo ne vsebujejo osebnih podatkov, obvestiti uporabnike, da bodo njihove podatke razkrili podjetjem in jim ponudili možnost, da onemogočijo razkritje?

Spletna socialna omrežja so v lasti gospodarskih subjektov, ki imajo za cilj ustvarjanje dobička. Glavni, oz. praktično edini poslovni model teh spletnih podjetij je prodajanje spletnega prometa oglaševalcem. Ne pričakujem, da bodo FB in TW šli zelo daleč v ščitenju pravic posameznika, če bo to v navzkrižju z njihovim samim razlogom obstoja. Seveda, obstajajo tudi razlike med podjetji – če se spomnimo reakcij na pritisk State Departmenta ob aferi Wikileaks – in te bodo morda pomemben vhodni podatek za etičnega potrošnika, ki izbira s kom posluje.

5. Ali menite, da so uporabniki spletnih socialnih omrežij dovolj osveščeni o uporabi orodij oz. tehnologije za izboljšanje zaščite osebnih podatkov na internetu in kako bi po vašem mnenju izboljšali to ozaveščenost?

Menim, da bi bilo dobro razširiti razumevanje problematike, in opažam neko število projektov na to temo. Pri mlajši populaciji bi svojo vlogo morali odigrati starši in šola, a v veliki večini primerov niti sami nimajo razčiščenih pojmov in s tem ustvarjajo kolosalen vakuum v katerega so se naselili dušebrižniki mediji in trgovci s strahom oz. varnostnimi aplikacijami.

6. Kaj bi priporočali tako "starim" kot novim uporabnikom spletnih socialnih omrežij? Kakšen nasvet za varno uporabo socialnih omrežij bi podali?

Človeštvo bo organsko sprejelo in modificiralo to medijsko tehnologijo. Nekateri bodo bolj in nekateri manj vešče iskoristili ta prvi val, nekatere bodo dogodki celo prizadeli, in edino interesantno je, kaj bo v seštevku tista ireverzibilna družbena sprememba, ki ji bomo priča. Ali bomo dejansko doživeli dobo povečane transparentnosti in odgovornosti, ali bodo morda nove okoliščine samo pripeljale do bolj subtilnih oblik

vzajemnega izkoriščanja, tega ne morem napovedati. Od tega širokopoteznega ozadja odvisni kako bo izgledalo življenje posameznih uporabnikov.
Varnost bo na mikro ravni – razen od opisanih civilizacijskih dejavnikov - odvisila od kombinacije osebne inteligence in afinitet uporabnika. Morda je dobro biti pozoren pri branju medijskih zgodb pobarvanih z moralno paniko.

7. Ali razpolagate s kakšnimi posebnimi ali najbolj odmevnimi primeri zlorabe osebnih podatkov v spletnih socialnih omrežij?

Ne, nisem seznanjen z nobenim tovrstnim primerom, kar morda samo pove nekaj o moji informiranosti, morda pa je dejansko dobra novica.

Priloga 2: Intervju s Francijem Mulcem, vodjo informacije tehnologije in vodjo Informacijske varnosti v službi Vlade RS za razvoj in evropske zadeve

1. Spletna socialna omrežja so postala v današnjem svetu čedalje večji fenomen. Ustanovitelj Facebooka, Mark Zuckerberg meni, da se v Facebook dnevno včlani 450.000 novih uporabnikov, s tem tudi ogromno število osebnih podatkov. Kakšno je vaše mnenje o brezskrbnem dajanju osebnih podatkov v spletna socialna omrežja?

Uporabniki socialnih omrežij se premalo zavedajo, da bodo podatki, ki jih razkrivajo, mnenja, ki jih pišejo dosegljiva upraviteljem sistema, javnosti, različnim ameriškim in drugim državnim organom in različnim gospodarskim subjektom še mnogo let, saj je diskovni prostor vse cenejši. Možnost je, da bo sedaj najstnik čez mnogo let mogoče pomembna javna osebnost ali direktor uspešnega podjetja in bo nekdo uporabil te podatke proti njemu.

2. Razkritje osebnih podatkov na spletih socialnih omrežjih prinaša obilo tveganj in posledic. Menite, da se uporabniki spletnih socialnih omrežij zavedajo posledic?

Uporabniki se vse bolj zavedajo posledic, a še vedno premalo.

3. Kaj menite o odgovornosti uporabe osebnih podatkov, zasebnosti na internetu?

Odgovorni posamezniki in odgovorna podjetja računalnikov, ki so namenjeni za uporabo na internetu ne uporabljajo za obdelavo občutljivih podatkov. Za obdelavo občutljivih podatkov uporabljajo ločene računalnike, ki niso priključeni v internet.

4. Lastniki spletnih socialnih omrežij zbirajo in nato prodajajo baze informacij, ki naj bi jih "očistili" osebnih podatkov, podjetjem za tržne raziskave. Vendar so znanstveniki razširili računalniški algoritem, s pomočjo katerega je moč identificirati uporabnika spletnega socialnega omrežja zgolj na podlagi anonimnega socialnega grafa.
Bi morali lastniki spletnih socialnih omrežij kljub temu, da podatki, katere prodajajo ne vsebujejo osebnih podatkov, obvestiti uporabnike, da bodo njihove podatke razkrili podjetjem in jim ponudili možnost, da onemogočijo razkritje?

Moderne računalniške tehnologije ne more noben uporabnik niti več 100% obvladovati. To velja tudi za upravitelje in lastnike socialnih omrežij. To vedno pomeni, da je »pot« podatkov, ki jih razkrivate ali posredujete v računalniškem svetu čedalje bolj nepredvidljiva.

5. Ali menite, da so uporabniki spletnih socialnih omrežij dovolj osveščeni o uporabi orodij oz. tehnologije za izboljšanje zaščite osebnih podatkov na internetu in kako bi po vašem mnenju izboljšali to ozaveščenost?

Še niso. Tu je pomembna vloga in odgovornost staršev, šole in državnih organov.

6. Kaj bi priporočali tako "starim" kot novim uporabnikom spletnih socialnih omrežij? Kakšen nasvet za varno uporabo socialnih omrežij bi podali?

Zasebnosti v internetu nikoli ni bilo niti nikoli ne bo. Torej, vse kar pišete na vaš računalnik in/ali v internet se lahko pojavi kadarkoli in kjerkoli.

7. Ali razpolagate s kakšnimi posebnimi ali najbolj odmevnimi primeri zlorabe osebnih podatkov v spletnih socialnih omrežij?

Kandidatka za visoko uradnico v slovenski državni upravi (ministrstvu) je v svoji prijavi za delovno mesto predstavila bistveno drugače, kot se je predstavljala na socialnem omrežju. Seveda ni prišla v ožji izbor za zaposlitev.

Priloga 3: Intervju z Gorazdom Božičem, vodjo slovenskega centra za posredovanje pri omrežnih incidentih (sicert)

1. Spletna socialna omrežja so postala v današnjem svetu čedalje večji fenomen. Ustanovitelj Facebooka, Mark Zuckerberg meni, da se v Facebook dnevno včlani 450.000 novih uporabnikov, s tem tudi ogromno število

osebnih podatkov. Kakšno je vaše mnenje o brezskrbnem dajanju osebnih podatkov v spletna socialna omrežja?

Premalo se zavedamo, da podatke dajemo zasebnemu podjetju v ZDA in da nas v primeru morebitnih zapletov ne more varovati naša lokalna zakonodaja in pristojne inštitucije. Naši podatki pomenijo Facebooku zaslužek in to je razlog, zakaj to storitev dobimo "zastonj".

2. Razkritje osebnih podatkov na spletih socialnih omrežjih prinaša obilo tveganj in posledic. Menite, da se uporabniki spletnih socialnih omrežij zavedajo posledic?

Menim, da se stopnja zavedanja povečuje. Opazimo lahko, da se uporabniki vedno bolj zavedajo nevarnosti in da začenjajo razmišljati o tem, kaj objavljajo. Kot drugje, gre tudi tu za proces ozaveščanja. Nove storitve začnemo uporabljati bolj odprto, morda lahko rečemo celo naivno, potem pa se zaradi ovir in težav tudi naše stališče začne temu prilagajati.

3. Kaj menite o odgovornosti uporabe osebnih podatkov, zasebnosti na internetu?

Menim, da smo danes v situaciji, kjer stare rešitve ne funkcionirajo več. Koncentracija podatkov pri velikih ponudnikih, kot sta Facebook in Google obračajo model porazdelitve hranjenja podatkov na glavo. Ne samo, da jih centraliziramo, to počnemo tudi z iznosom v državo, ki ima popolnoma drugačno stališče do te teme, kot je to običajno v Evropi. Tu ne gre le za posameznike, v imenu optimizacije stroškov se "v oblak" selijo cela podjetja in univerze.

4. Lastniki spletnih socialnih omrežij zbirajo in nato prodajajo baze informacij, ki naj bi jih "očistili" osebnih podatkov, podjetjem za tržne raziskave. Vendar so znanstveniki razširili računalniški algoritem, s pomočjo katerega je moč identificirati uporabnika spletnega socialnega omrežja zgolj na podlagi anonimnega socialnega grafa.
Bi morali lastniki spletnih socialnih omrežij kljub temu, da podatki, katere prodajajo ne vsebujejo osebnih podatkov, obvestiti uporabnike, da bodo njihove podatke razkrili podjetjem in jim ponudili možnost, da onemogočijo razkritje?

Prav je, da ponudniki spletnih omrežij jasno opišejo v svojih pogojih, kako ravnajo z našimi podatki. Od nas samih kot uporabnikov pa je potem odvisno, ali na to pristanemo ali ne. Potem pa moramo v skladu s tem tudi prevzeti odgovornost za to, da smo takšno ravnanje na podlagi predočenih pogojev sprejeli.

Seveda pa včasih ponudniki izkoriščajo dejstvo, da pogojev nihče ne bere, ravno zato so napisana tako nepregledno. Menim torej, da se moramo zavedati dejstva, da ponudnik služi na podlagi naših osebnih podatkov. V njegovem interesu je, da zasluži čim več.

5. Ali menite, da so uporabniki spletnih socialnih omrežij dovolj osveščeni o uporabi orodij oz. tehnologije za izboljšanje zaščite osebnih podatkov na internetu in kako bi po vašem mnenju izboljšali to ozaveščenost?

Menim, da še nismo rekli zadnje na to temo in da gre bolj za proces, kot za neko zaključeno dejanje. Družabna omrežja se spreminjajo, nastajajo nova, zato moramo vedno znova razmišljati, komu dajemo podatke in pod kakšnimi pogoji.

6. Kaj bi priporočali tako "starim" kot novim uporabnikom spletnih socialnih omrežij? Kakšen nasvet za varno uporabo socialnih omrežij bi podali?

Predvsem to, da se moramo zavedati, da smo z objavo na teh omrežjih verjetno nekaj pravic do svojega materiala izgubili. Dosedanje izkušnje kažejo, da se lahko pravila igre čez noč spremenijo. Nekaj previdnosti torej, po drugi strani pa so družabna omrežja dandanes dejstvo in vedno več ljudi jih uporablja, zato kakšna abstinenca ni vedno smiselna.

7. Ali razpolagate s kakšnimi posebnimi ali najbolj odmevnimi primeri zlorabe osebnih podatkov v spletnih socialnih omrežij?

Kakšnih senzacionalističnih se ne spomnim. Večinoma gre za kraje profilov (kjer dostikrat bivši fant punci ugrabi profil in na njem objavlja neprimerne vsebine).

Priloga 4: Intervju z Evo Kalan, svetovalko pri informacijski pooblaščenki RS

1. Spletna socialna omrežja so postala v današnjem svetu čedalje večji fenomen. Ustanovitelj Facebooka, Mark Zuckerberg meni, da se v Facebook dnevno včlani 450.000 novih uporabnikov, s tem tudi ogromno število osebnih podatkov. Kakšno je vaše mnenje o brezskrbnem dajanju osebnih podatkov v spletna sociala omrežja?

Objava na internetu pomeni skoraj isto kot objava na oglasni deski sredi mesta, ki bo tam stala za vedno in ki jo bodo lahko videli vsi. Tega dejstva se predvsem mlajši uporabniki spletnih socialnih omrežij vse premalo zavedajo. Vsa spletna socialna omrežja (Facebook, Netlog, MySpace,…) temeljijo na vzpostavljanju medsebojnih povezav, zato uporabnika spodbujajo, da objavi čim širši nabor svojih osebnih podatkov. In ravno nepremišljeno objavljanje prevelike količine svojih osebnih

podatkov ter slabo varovana zasebnost uporabnikov je tisti vidik spletnih omrežij, ki lahko potencialno za posameznika pomeni tudi veliko nevarnost. Posameznik lahko tu največ stori sam in to s tem, da vedno dvakrat premisli kaj bo objavil in kaj lahko taka objava zanj pomeni v prihodnosti.

2. Razkritje osebnih podatkov na spletih socialnih omrežjih prinaša obilo tveganj in posledic. Menite, da se uporabniki spletnih socialnih omrežjih zavedajo posledic?

Menim, da se zavedanje s pomočjo akcij ozaveščanja, ki jih v Sloveniji na primer pripravlja tudi Informacijski pooblaščenec, počasi veča, vendar pa na žalost še vedno ni niti približno zadovoljivo, kar opažam tudi pri svojem delu, pri katerem tedensko prejmemo veliko vprašanj v zvezi nepremišljenim razkrivanjem osebnih podatkov na spletu in posledično zlorabi le-teh s strani raznih nepridipravov (od škodoželjnih vrstnikov pa vse do tatov identitete).

3. Kaj menite o odgovornosti uporabe osebnih podatkov, zasebnosti na internetu?

Kot že rečeno, posamezniki se teže posledic, ki jih lahko s seboj prinese neodgovorno razdajanje svojih osebnih podatkov na internetu, veliko premalo zavedajo. Ker namreč kršitve zasebnosti ne bolijo in ne puščajo krvi, se večini sploh ne zdijo nič takega… oziroma so takega mnenja, dokler se taka kršitev ne zgodi njim. Takrat pa se njihovo mnenje hitro spremeni, saj lahko pomeni vse od izgube ugleda, pa do izgube vsega premoženja. Prav zaradi tega moramo biti previdni in premišljeni, kar še posebej velja za dandanašnjo dobo informacijskih tehnologij, ko na spletu vede in nevede puščamo neskončno število elektronskih sledi.

4. Lastniki spletnih socialnih omrežij zbirajo in nato prodajajo baze informacij, ki naj bi jih "očistili" osebnih podatkov, podjetjem za tržne raziskave. Vendar so znanstveniki razširili računalniški algoritem, s pomočjo katerega je moč identificirati uporabnika spletnega socialnega omrežja zgolj na podlagi anonimnega socialnega grafa.
Bi morali lastniki spletnih socialnih omrežij kljub temu, da podatki, katere prodajajo ne vsebujejo osebnih podatkov, obvestiti uporabnike, da bodo njihove podatke razkrili podjetjem in jim ponudili možnost, da onemogočijo razkritje?

Osebni podatek je zelo širok pojem in po slovenski zakonodaji se nanaša na katerikoli podatek, ki se nanaša na določeno ali določljivo fizično osebo, ne glede na obliko, v kateri je izražen. Fizična oseba pa je določljiva, če se jo lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko,

kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa. Če je torej moč posameznika določiti brez nesorazmerno velikega napora, časa in stroškov že zgolj na podlagi anonimnega socialnega grafa, potem lahko tudi take podatke smatramo za osebne podatke. Če je temu tako, bi morali upravljavci spletnih omrežij posameznike obvestiti o tem, da bodo njihove podatke razkrivali tretjim osebam.
Seveda pa ob tem opozarjam, da zgornja določila izhajajo iz slovenske oziroma evropske zakonodaje, ter da je lahko zakonodaja drugih držav, ki zavezuje upravljavce določenega spletnega socialnega omrežja, drugačna.

5. Ali menite, da so uporabniki spletnih socialnih omrežij dovolj osveščeni o uporabi orodij oz. tehnologije za izboljšanje zaščite osebnih podatkov na internetu in kako bi po vašem mnenju izboljšali to ozaveščenost?

Z namenom dviga ozaveščenosti Informacijski Pooblaščenec veliko energije posveča izobraževanju o pasteh socialnih omrežij, saj sledimo razvoju dogodkov in se nam zdi izjemno pomembno, da predvsem mlade ozaveščamo o posledicah, ki jih lahko zaradi elektronskih sledi, ki jih puščamo v medmrežju, občutimo kasneje, ko nam bo morda že žal, da smo na zid nekaj napisali ali objavili občutljivo fotografijo. Akcijo ozaveščanja pa v Sloveniji vodita tudi Center za varnejši internet SAFE-SI (www.safe.si) ter Slovenski center za posredovanje pri omrežnih incidentih SI-CERT (www.varninainetrnetu.si).

6. Kaj bi priporočali tako "starim" kot novim uporabnikom spletnih socialnih omrežij? Kakšen nasvet za varno uporabo socialnih omrežij bi podali?

Svetovala bi zelo ozko omejeno nastavitev zasebnosti, kar pomeni ročno omejitev dostopa do objavljenih podatkov samo potrjenim »prijateljem«, ter tudi razlikovanjem med njimi samimi, ter spremljanje sprememb nastavitev zasebnosti s strani spletnih omrežjih. V tem kontekstu je na primer zanimiva
primerjava med privzetimi nastavitvami zasebnosti spletnega omrežja Facebook iz leta 2005, ko je bilo podjetje ustanovljen, in zadnjo spremembo, ki je bila narejena aprila 2010. Ta pokaže, da so bili na začetku obstoja omrežja, brez spreminjanja nastavitev zasebnosti, osebni podatki uporabnikov vidni le njihovim prijateljem, danes pa so vsi uporabnikovi podatki, razen rojstnega datuma in kontaktnih informacij, vidni vsem uporabnikom interneta. Če si torej ob tem, ko si ustvariš svoj Facebook profil, ne vzameš vsaj deset minut časa in privzetih nastavitev zasebnosti ne omejiš, bodo podatki, ki jih boš objavil na svojem profilu dostopni ne zgolj vsem uporabnikom omrežja, ampak tudi vsem uporabnikom interneta! Kot varuhi zasebnosti pa vsekakor zagovarjamo princip, da so zasebnosti prijazne že privzete nastavitve, ne pa da jih mora vsak uporabnik sam nastaviti.

Ključna pa je seveda premišljena uporaba. Uporabnikom bi tako svetovala, da vedno dvakrat premislijo, kaj bodo objavili na spletnih družabnih omrežjih in na spletu na splošno in kaj lahko taka objava pomeni za njih čez npr. 30 let. Posameznik lahko namreč za varnost svojih osebnih podatkov in ohranitev zasebnosti največ stori sam s premišljenim ravnanjem.

7. Ali razpolagate s kakšnimi posebnimi ali najbolj odmevnimi primeri zlorabe osebnih podatkov v spletnih socialnih omrežij?

O konkretnih primerih ne moremo govoriti, lahko pa rečem, da se primeri povezani s spletnimi socialnimi omrežji največkrat nanašajo na zlorabe osebnih podatkov na spletnem omrežju Facebook, predvsem v povezavi s krajo identitete, nedovoljeno objavo fotografij in spletnim nadlegovanjem.