

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Maja Gregl

**Varstvo osebnih podatkov in zasebnost v spletnih družbenih omrežjih – primer
Facebooka**

Diplomsko delo

Ljubljana, 2016

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Maja Gregl

Mentorica: red. prof. dr. Tanja Oblak Črnič

Somentorica: red. prof. dr. Tina Kogovšek

**Varstvo osebnih podatkov in zasebnost v spletnih družbenih omrežjih – primer
Facebooka**

Diplomsko delo

Ljubljana, 2016

ZAHVALA

Zahvaljujem se svoji mentorici red. prof. dr. Tanji Oblak Črnič in somentorici red. prof. dr. Tini Kogovšek za strokovno pomoč, dragocene nasvete ter potrpežljivost pri nastajanju mojega diplomskega dela.

Hvala Niki Plevnik za lektoriranje.

Hvala vsem, ki so si vzeli čas in izpolnili anketni vprašalnik.

Hvala vsem prijateljem, ki ste mi stali ob strani, me bodrili in vselej verjeli vame.

Hvala mami Barbari in očetu Iztoku za brezpogojno ljubezen, zaupanje in oporo vedno, ko sem jo potrebovala.

Posebna zahvala mojemu najboljšemu prijatelju, bratu Tiborju, ki mi že od malih nog stoji ob strani in pazi, da grem varno in srečno skozi življenje.

Varstvo osebnih podatkov in zasebnost v spletnih družbenih omrežjih – primer Facebooka

V diplomski nalogi sem se ukvarjala s tematiko varstva osebnih podatkov in zasebnostjo v spletnih družbenih omrežjih, s poudarkom na Facebooku, ki je najbolj priljubljeno omrežje med mladimi. Zanimalo me je, kako so mladi pa tudi starejši uporabniki Facebooka seznanjeni z varstvom zasebnosti in varstvom osebnih podatkov pri uporabi tega spletnega družbenega omrežja. To sem preverjala z anketnim vprašalnikom, s katerim sem zajela vzorec oseb, starejših od trinajst let. Vprašalnik je zajemal vprašanja glede poznavanja varnosti pri uporabi in zaščiti osebnih podatkov. Prek odgovorov sem poskušala ugotoviti, kako so uporabniki Facebooka seznanjeni z nastavitvami zasebnosti, kako varne se jim zdijo informacije, ki jih posredujejo na Facebook, ali spremljajo novosti v zvezi z varnostjo in ali se zavedajo nevarnosti, ki nanje prežijo ter na koga se lahko v primeru ogrožene zasebnosti obrnejo. Uporaba spletnih družbenih omrežij namreč iz dneva v dan narašča, število uporabnikov se večja, s tem pa tudi možnosti zlorab. Opravila sem tudi intervju z direktorico Pravnega centra za varstvo človekovih pravic in se tako seznanila z nevarnostmi, ki jih prinašajo nove tehnologije predvsem mladim, ter spoznala tudi s praktične primere zlorabe osebnih podatkov prek spleta.

Ključne besede: spletna družbena omrežja, varnost, zasebnost, osebni podatki, Facebook.

Privacy and Personal Data Protection in Online Social Networks - Facebook Example

In this thesis, the issue of privacy and personal data protection in online social networks, with the focus on Facebook, the most popular network among young people, has been researched. The main research focus was on how well the younger as well as older Facebook users are familiar with the protection of their privacy and personal data when using this online social network. The questionnaire covered a sample of Facebook users from the age of thirteen. It contained the questions about the user's awareness of safety and protection of personal data when used online. The answers revealed, how well Facebook users are familiar with the privacy settings, how safe they consider the information supplied to Facebook to be, and if the users follow the updates in regard to online safety. Moreover, it was checked, if the users are aware of the dangers and threats, and to whom they can turn to in the event of privacy being jeopardized or breached. The use of online social networks is increasing daily, especially the number of users, and thus the possibilities of abuse. The interview with the Director of the Legal Center for the Protection of Human Rights has been performed, which revealed real-life dangers posed by new technologies, particularly among young people, supported with practical examples of misuse of personal data in the Internet.

Keywords: online social networks, security, privacy, personal data, Facebook.

KAZALO

1	UVOD	8
2	SPLETNA DRUŽBENA OMREŽJA	10
2.1	DEFINICIJA SPLETNIH DRUŽBENIH OMREŽIJ	11
2.2	RAZVOJNA POT SPLETNIH DRUŽBENIH OMREŽIJ	14
2.2.1	Nastanek spleta 2.0.....	14
2.2.2	Pojav spletnih družbenih omrežij	15
2.3	PRILJUBLJENOST SPLETNIH DRUŽBENIH OMREŽIJ	16
2.4	VRSTE SPLETNIH DRUŽBENIH OMREŽIJ	18
2.5	MEDSEBOJNA KOMUNIKACIJA V SPLETNIH DRUŽBENIH OMREŽJIH.....	20
2.5.1.	Spletna družbena omrežja kot medij in vir informacij	21
3	FACEBOOK	23
3.1	ZGODOVINA FACEBOOKA.....	23
3.2	FACEBOOK DANES	24
4	PRAVICA DO ZASEBNOSTI IN PRAVICA DO VAROVANJA OSEBNIH PODATKOV	25
4.1	OSEBNI PODATKI	26
4.1.1	Varstvo osebnih podatkov v Ustavi RS	26
4.1.2	Zakonska ureditev varstva osebnih podatkov	28
4.1.3	Mednarodna ureditev varstva osebnih podatkov	28
4.2	PRAVICA DO ZASEBNOSTI	29
4.2.1	Vidiki pravice do zasebnosti	30
4.3	VARSTVO POSAMEZNIKA GLEDE OSEBNIH PODATKOV	31
4.4	PROBLEM VARSTVA OSEBNIH PODATKOV NA SPLETNIH DRUŽBENIH OMREŽJIH	32
5	ZASEBNOST NA SPLETNEM DRUŽBENEM OMREŽJU FACEBOOK.....	35
5.1	SPLOŠNI POGOJI UPORABE.....	35
5.2	NASTAVITVE IN ORODJA ZA ZASEBNOST	36
5.2.1	Uporabna orodja za upravljanje zasebnosti.....	36
6	NEVARNOSTI, ZLORABE IN ZAŠČITA PRED NJIMI	39
6.1	TIPI SPLETNIH KRIMINALCEV	39
6.2	MOŽNE NEVARNOSTI IN ZLORABE NA SPLETU	40
6.2.1	Odtujitev ali okužba profila uporabnika.....	40
6.2.2	Lažna predstavljanja, zloraba identitete in nadlegovanje.....	40
6.2.3	Ribarjenje ali »phishing«.....	42

6.2.4	Možne negativne posledice objav	43
6.3	ZAŠČITA ZASEBNOSTI V SPLETU	44
6.4	ZAŠČITA ZASEBNOSTI V SPLETNEM DRUŽBENEM OMREŽJU FACEBOOK.....	45
7	EMPIRIČNI DEL.....	46
7.1	OPREDELITEV PROBLEMA	46
7.2	METODOLOGIJA IN ZBIRANJE PODATKOV	46
7.3	REZULTATI: ANALIZA VPRAŠANJ	47
8	SKLEP.....	62
9	LITERATURA.....	65
PRILOGE		71
	PRILOGA A: Anketni vprašalnik	71
	PRILOGA B: Intervju z gospo Margerito Jurkovič, direktorico Pravnega centra za varstvo človekovih pravic (9. junij 2016).....	75

KAZALO SLIK

Slika 2.1:	Odstotek prebivalstva ZDA, ki ima ustvarjen najmanj en osebni profil v spletnih družbenh omrežjih, podatki zajemajo obdobje od leta 2008 do 2016	17
Slika 2.2:	Odstotek prebivalstva Združenega kraljestva (UK), ki ima ustvarjen najmanj en profil v spletnih družbenh omrežjih, podatki zajemajo obdobje od leta 2007 do 2015	17
Slika 2.3:	Število aktivnih mesečnih uporabnikov spletnega družbenega omrežja Facebook (v milijonih)	18
Slika 3.1:	Statistični podatki omrežja Facebook za prvo četrtino leta 2016	24

KAZALO GRAFOV

Graf 7.1:	Spol.....	47
Graf 7.2:	Starost.....	48
Graf 7.3:	Status.....	48
Graf 7.4:	Izobrazba.....	49
Graf 7.5:	Čas, dnevno preživet v spletu.....	49
Graf 7.6:	Čas, dnevno preživet na Facebooku.....	50
Graf 7.7:	Glavni razlog za obisk Facebooka.....	51
Graf 7.8:	Število prijateljev na Facebooku.....	51

Graf 7.9: Osebno poznanstvo s prijatelji na Facebooku.....	52
Graf 7.10: Sprejem prošnje za prijateljstvo neznane osebe.....	53
Graf 7.11: Zaščitenost osebnih podatkov, objavljenih na Facebooku.....	53
Graf 7.12: Nastavitve zasebnosti.....	54
Graf 7.13: Seznanjenost s politiko zasebnosti na Facebooku.....	56
Graf 7.14: Pogostost spremljanja politike zasebnosti na Facebooku.....	56
Graf 7.15: Posodobitve in varnostne nastavitve profila na Facebooku.....	57
Graf 7.16: Posodobitve in varnostne nastavitve profila na Facebooku po starostnih skupinah.....	57
Graf 7.17: Shranjevanje in obdelava osebnih podatkov na Facebooku.....	58
Graf 7.18: Nevarnosti objave osebnih podatkov na Facebooku.....	59
Graf 7.19: Prijava v primeru ogrožene zasebnosti.....	59
Graf 7.20: Pomembnost varnosti in zasebnosti na Facebooku.....	60
Graf 7.21: Informiranost o možnih nevarnostih Facebooka.....	61

1 UVOD

Življenja brez interneta si v današnjem času ne moremo predstavljati, saj ga uporabljamo tako doma kot v službi. Prebiramo novice, iščemo podatke, informacije, pa tudi stike s svojci, prijatelji, znanci, in sklepamo nova poznanstva. Predvsem pa je v zadnjem času v porastu uporaba vse številčnejših spletnih družbenih omrežij.

Spletna družbena omrežja so med uporabniki zelo priljubljena, saj jim omogočajo izražanje individualnosti in srečevanje z ljudmi s podobnimi interesi. Postala so del našega vsakdana tako z vidika osebne kot tudi poslovne rabe. Zaradi odprtosti in dostopnosti pa niso zanimiva zgolj uporabnikom, temveč tudi tako imenovanim kibernetiskim kriminalcem, ki izkoriščajo nevednost, lahkomišelnost in naivnost uporabnikov spletnih družbenih omrežij. Zato je bistvenega pomena, da se uporabniki zavedamo, da moramo poskrbeti za varnost svojih podatkov. Živimo v času informacijske družbe, zato virtualnost postaja naša vsakdanjost. Varnost in zasebnost sta velik problem že v realnem svetu, kaj šele virtualnem. Zaradi lažnega občutka varnosti namreč prihaja do številnih napak in tveganj v spletnih družbenih omrežjih.

S prihod interneta se je varovanje zasebnosti preneslo tudi v virtualni prostor, v katerem informacijsko-komunikacijska tehnologija omogoča številne nove tehnične načine zlorab zasebnosti (Kovačič 2006). Lahko bi rekli, da je zasebnost posameznika v informacijski družbi zelo »načeta«.

»Živimo v svetu, v katerem se »moramo« odpovedati delu svoje zasebnosti v imenu večje funkcionalnosti in udobja, sodobni Panoptikon pa je zasnovan tako, da se posamezniki nadzoru podreajo celo prostovoljno« (Kovačič 2006, 33). Zasebnost je v sodobni družbi postala tržno blago, s katerim lahko trgujemo, in ne več pravica, ki jo moramo varovati.

Cilj diplomske naloge je ugotoviti, kako so zaščiteni uporabniki spletnega družbenega omrežja Facebook in kakšna je varnost osebnih podatkov, ki jih uporabniki spletnih družbenih omrežij uporabljajo, kako je pri nas urejena zakonodaja glede varovanja osebnih podatkov in zasebnosti, ter kakšen odnos imajo uporabniki spletnega družbenega omrežja Facebook do varovanja osebnih podatkov in zasebnosti na omenjenem omrežju.

Diplomsko delo je razdeljeno na dva dela; prvi del je teoretični del, v katerem predstavljam spletna družbena omrežja, s posebnim poudarkom na Facebooku, kateremu sem namenila posebno poglavje, saj je glavni predmet raziskave moje diplomske naloge. V nadaljevanju

podrobneje obravnavam pravico do zasebnosti in pravico do varovanja osebnih podatkov ter izpostavljam problem varstva osebnih podatkov v spletnih družbenih omrežjih. Posebno pozornost namenjam zasebnosti na spletnem družbenem omrežju Facebook, potencialnim nevarnostim in zlorabam v spletu ter zaščito pred njimi. V empiričnem delu diplomskega dela pa predstavim rezultate analize ankete, ki sem jo izvedla med uporabniki Facebooka.

S pomočjo teoretičnega in empiričnega dela naloge bom skušala potrditi ali ovreči naslednje hipoteze:

1. HIPOTEZA: Za varnost in zasebnost v spletnem družbenem omrežju Facebook je dobro poskrbljeno.
2. HIPOTEZA: Mlajši uporabniki Facebooka bolj redno posodablajo svoje nastavitve zasebnosti na Facebooku.

2 SPLETNA DRUŽBENA OMREŽJA

Danes v spletu obstaja veliko družbenih oziroma socialnih omrežij. Njihova skupna značilnost je povezovanje posameznikov s podobnimi interesi širom sveta. Splet in vsa spletna družbena omrežja omogočajo različne oblike komuniciranja med ljudmi. »Splet namreč ni le ogromno skladišče informacij, temveč tudi prostor družabnega delovanja, interakcij, druženja, koordiniranja, spoznavanja, tekmovanja in reševanja konfliktov« (Oblak in Petrič 2005, 24).

Spletna družbena omrežja lahko opredelimo kot spletne storitve, na katerih posamezniki ustvarjajo osebni profil. Lahko je javen in dostopen vsem uporabnikom ali omejen in dostopen le določenim uporabnikom.

Splet in spletna omrežja nam omogočajo komunikacijo s točno določenimi osebami, lahko pa se vključimo v javne skupinske debate na številnih forumih, kjer razpravljajo o temah, ki nas osebno zadevajo ali nas zanimajo. Omogočajo nam, da objavljamo vsebine, fotografije, izbor naše najljubše glasbe ali priljubljene filme, ter se tako javno predstavimo širši javnosti. Je izrazito živahna, dinamična in raznolika komunikacijska platforma, na kateri se odvijajo različne oblike računalniško posredovanega komuniciranja (Oblak in Petrič 2005).

Uspeh spletnih družbenih omrežij je odvisen predvsem od števila uporabnikov, ki jih uporabljajo, ter od različnih možnosti uporabe, ki jih nudijo. S številom uporabnikov pa sorazmerno raste tudi materialna vrednost družbenega omrežja, kar lastnikom teh omrežij omogoča tudi promocijo različnih marketinških idej.

Biti uporabnik spletnega družbenega omrežja ima določene prednosti: z njimi si ustvarjamo nov način deljenja življenjskih izkušenj, čutimo povezanost z drugimi uporabniki, spoznavamo isto misleče ljudi in objavljamo osebne podatke, ki jih želimo deliti z drugimi uporabniki. Možnost upravljanja osebnih podatkov je velika prednost, saj uporabnik sam odloča, katere podatke želi deliti z drugimi in katerih ne, ter tako varuje svojo zasebnost. Hkrati se spletna družbena omrežja nenehno izboljšujejo, pojavljajo se nova, ki uporabnikom ponujajo nove in nove možnosti.

Za razliko od tradicionalnih medijev so spletni mediji dostopni širši javnosti veliko ceneje, večinoma pa kar zastonj. Prav tako od uporabnika ne zahtevajo posebnih znanj, ampak samo reinterpretacijo obstoječih veščin, kar pomeni, da lahko vsi, ki imajo dostop do družbenih

omrežij, z njimi tudi upravljajo. Tudi odzivni čas komunikacije v spletnih družbenih omrežjih je načeloma krajši, saj uporabniki sami odrejajo čas odgovora. Zato se tudi vse več tradicionalnih medijev poslužuje spletnih družbenih medijev, tako za produkcijo kot za promocijo. Dejstvo je, da lahko članke v spletnih družbenih omrežjih kadarkoli objavimo ali menjamo, sproti dopolnjujemo in hkrati tudi prejmemo komentarje, po navadi brez stroškov.

Družbena omrežja sama po sebi spodbujajo ljudi, da svoje zasebno življenje delijo z javnostjo. Ob tem je treba poudariti, da kar je enkrat objavljeno v spletu, bo za vedno tam tudi ostalo, zato je pri objavah potrebna previdnost. Lahko se zgodi, da posameznik objavi določeno sliko ali posnetek, ki se mu v tistem trenutki zdi povsem neškodljiv, je pa lahko v prihodnosti glavni razlog, da ga, na primer, potencialni delodajalec zaradi tega ne zaposli.

Potrebno se je zavedati, da lahko taka priložnostna in navidezno spontana povezava na internetu daje lažen občutek povezanosti z drugimi uporabniki. Tako družbena omrežja za vse svoje uporabnike zelo otežujejo razlikovanje med pristnimi in številnimi priložnostnimi odnosi, ki se oblikujejo na tovrstnih omrežjih (Medijska pismenost 2016).

Seveda pa je treba opozoriti na dejstvo, da imajo spletna družbena omrežja poleg mnogih pozitivnih lastnosti tudi mnoge slabosti. Naletimo lahko na morebitne zlorabe ali neprijetnosti. Najpogostejše gre za kršitve naše zasebnosti. Uporabniki namreč v svojih spletnih profilih objavljajo svoje osebne podatke, ki jih lahko zlikovci zlorabijo (npr. kraja identitete) (Wikipedia 2016c). Zato je treba biti pri objavi osebnih podatkov v spletu zelo previden. O negativni plati uporabe spletnih družbenih omrežij, in konkretno Facebooka, nekoliko pozneje.

2.1 DEFINICIJA SPLETNIH DRUŽBENIH OMREŽIJ

V literaturi najdemo veliko definicij spletnih družbenih omrežij. Angleški izraz za spletna družbena omrežja je »social network«, v slovenščini pa obstaja več različnih izrazov. Poleg izraza spletna družbena omrežja, ki ga bomo uporabljali v naši diplomski nalogi, so pri nas v uporabi tudi izrazi družabno omrežje, družabne spletne strani, socialno omrežje, socialni mediji, socialne spletne skupnosti in podobno.

Za definicijo spletnih družbenih omrežij se največkrat uporablja definicija avtoric Boyd in Ellison (2007), ki sta spletna družbena omrežja opredelili kot spletne storitve, ki posameznikom omogočajo:

- ustvarjanje javnega ali pol-javnega profila znotraj omejenega sistema,
- ustvarjanje seznama uporabnikov, s katerimi so povezani, in
- ogled in pregled seznama naših povezav ter sezname povezav drugih uporabnikov znotraj sistema.

Obar in Wildman (2015) sta v svojem članku povzela več definicij iz literature in poiskala skupne točke med aktualnimi družbenimi storitvami:

- družbene medijske storitve so (trenutno) Web 2.0, ki temelji na aplikacijah, osnovanih na internetu;
- za družbene medije je ključnega pomena vsebina, ki jo ustvarjajo uporabniki;
- posamezniki in skupine ustvarjajo uporabniško specifične profile za spletne strani ali aplikacije, ki jih oblikujejo in vzdržujejo družbeno medijske storitve,
- s povezovanjem profilov z drugimi posamezniki in skupinami, družbeno medijske storitve olajšajo razvoj spletnih družbenih omrežij.

Kietzmann (2011, 243–248) z vidika funkcionalnosti predstavi okvir sedmih temeljev, ki opredeljujejo družbena omrežja: *identiteta, pogovori, izmenjave, prisotnost, odnosi, ugled in skupine*. Ti temelji se med seboj ne izključujejo, niti ni treba, da bi bili vsi hkrati prisotni v družbeno medijski dejavnosti.

• **Identiteta**

Uporabniki družbenih omrežij razkrivajo svojo identiteto. To vključuje podatke, kot so njihova imena, starost, spol, poklic, kraj bivanja, kot tudi vse preostale podatke, ki jih na kakršen koli način opisuje. Z odkrivanjem teh podatkov uporabnik zavedno ali nezavedno odkriva subjektivne informacije o sebi, o tem, kar misli, občuti, ljubi ali ne ljubi. Obstaja veliko različnih spletnih družbenih omrežij (npr. Facebook), ki od uporabnikov zahteva, da ustvarijo svoj spletni profil. Ti profili postanejo leglo naših spletnih identitet in to privablja številna podjetja, da ustvarijo svoje družbene mreže in se povežejo z ostalimi omrežji (Kietzmann 2011).

Čeprav na spletnih družbenih omrežjih uporabniki prostovoljno delijo svojo identiteto, pa to ne pomeni, da jim ni mar, kaj se s temi podatki potem zgodi. Dejansko imajo uporabniki resne pomisleke o tem, kako sekundarna podjetja uporabljajo njihove podatke kot vir za podatkovno rudarjenje in nadzor. Uporabniki spletnih družbenih omrežij so razvili tudi osebne strategije in tako se prepletajo prave identitete in virtualne, nekateri pa so se osredotočili predvsem na lastno promocijo ali na promocijo svojega proizvoda oz. storitve (Kietzmann 2011).

● Pogovori

Pogovor v spletnih družbenih omrežjih služi za vzpostavitev komunikacije med uporabniki. Številna spletna družbena omrežja so bila ustanovljena ravno zato, da bi olajšala komunikacijo med posamezniki in skupinami. Razlogi za pogovore v spletnih družbenih omrežjih so različni. Ljudje tvitajo (ang. *tweet*), blogajo (ang. *blog*) in uporabljajo druge načine komunikacije, da bi spoznali nove ljudi s podobnim razmišljanjem, našli ljubezen, si izgradili svojo samozavest ter bili v trendu z novimi idejami in temami. Nekateri uporabniki v pogovoru vidijo priložnost, da spregovorijo o družbenih in ekonomskih problemih ali političnih temah. Skozi pogovore v spletu se lahko dosežejo tudi različni učinki in tako lahko pogovor služi tudi kot brezplačna kampanja za proizvode, osebe ali dogodke (Kietzmann 2011).

● Izmenjave

Izmenjave predstavljajo način, s katerim uporabniki izmenjujejo, distribuirajo in sprejemajo neko vsebino. Pojem *družbeno* dostikrat pomeni, da je izmenjava med ljudmi ključnega pomena, zato je druženje v spletnih družbenih omrežjih eden glavnih razlogov, zakaj se uporabniki povezujejo in si izmenjujejo različne vsebine (Kietzmann 2011).

● Prisotnost

Prisotnost predstavlja način, kako lahko uporabniki preverijo ali so drugi uporabniki dostopni. To pomeni, da uporabniki vidijo, kje so drugi uporabniki, v virtualnem in/ali realnem svetu, in ali so dosegljivi. Na spletnem družbenem omrežju Facebook se prisotnost na omrežju kaže s statusom dosegljiv (ang. *online*) ali nedosegljiv (ang. *offline*). Nekatera spletna družbena omrežja pa podpirajo aplikacije, preko katerih se uporabniki 'označijo' (ang. *check in*) in s tem drugim uporabnikom dajo vedeti, kje je njihova trenutna lokacija (Kietzmann 2011).

- **Odnosi**

Odnosi predstavljajo obseg, ki kaže, kako so uporabniki med sabo povezani. Dva ali več uporabnikov je lahko povezanih na različne načine, ki privedejo do tega, da se vključujejo v pogovore, izmenjujejo vsebine, se srečujejo ali pa se povežejo zgolj kot virtualni prijatelji (Kietzmann 2011).

- **Ugled**

Ugled označuje identificiranje in položaj uporabnika samega, kot tudi drugih uporabnikov v določenem spletnem družbenem omrežju. V večini primerov je ugled stvar zaupanja, s katerim uporabniki opredelijo svoj položaj v družbi. Različna spletna družbena omrežja imajo svoje indikatorje priljubljenosti, na Facebooku se ti lahko merijo s številom prijateljev, številom všečkov (ang. *likes*) ipd (Kietzmann 2011).

- **Skupine**

Skupine predstavljajo obseg, v katerem uporabniki lahko tvorijo skupnosti in podskupnosti. Večja kot je družbena mreža, večje so skupine prijateljev, sledilcev in stikov (Kietzmann 2011).

2.2 RAZVOJNA POT SPLETNIH DRUŽBENIH OMREŽIJ

Začetki spletnih družbenih omrežij segajo veliko dlje v zgodovino, kot si morda predstavljamo. Čeprav se zdijo kot nek nov trend, so naraven rezultat več stoletij dolgega razvoja družbenih medijev. Komunikacija je najprej potekala prek pisem, nato prek telegrafa, telefona in radia. Slednja sta v uporabi še dan danes, vendar v veliko modernejši obliki.

2.2.1 Nastanek spleta 2.0

Tehnologija se je v 20. stoletju hitro razvijala. Leta 1943 je inženir Tommy Flowers razvil prvi elektronski digitalni programabilni računalnik Colossus. Prve oblike interneta beležimo že konec 60. let prejšnjega stoletja, dejanski začetek interneta, kot ga poznamo danes, pa sega v leto 1983 (Wikipedia 2016).

Danes je v uporabi splet 2.0, ki ga imenujemo tudi splet druge generacije. Je izboljšana različica prejšnje različice spleta 1.0. Splet 1.0 se je pojavil z nastankom svetovnega spleta, a je poimenovan šele ob nastanku termina *splet 2.0*, torej je bil poimenovan za nazaj. Suhadolc (2007) poimenuje splet 1.0 *statični splet* (ang. *static web*), splet 2.0 pa *živi splet* (ang. *live web*). »V statičnem spletu smo bili pasivni uporabniki informacij s spletnih mest, ki so jih ustvarili drugi. V živem spletu pa vloge niso jasno razmejene in uporabniki postanemo tudi ustvarjalci vsebin« (Suhadolc 2007, 24).

Oblak in Petrič (2005) razumeta splet v tehničnem smislu kot najpomembnejšo in najbolj prevladujočo komponento interneta, saj se vse več storitev, ki jih spremljamo prek interneta, zlija na splet. Dodajata, da so se nekdanji servisni dostopi do podatkovnih zbirk, klepetalnic, elektronske pošte in novičarskih skupin, združili v enotni spletni format, ki je uporabniku dostopen prek brskalnika.

»Prejšnje samostojne sisteme nadomeščajo razne spletne aplikacije, ki so integrirane v brskalnik in omogočajo osebno, medosebno in skupinsko komunikacijo ter dostop do informacijskih baz prek enotnega vmesnika« (Oblak in Petrič 2005, 14).

»Splet namreč ni le ogromno skladišče informacij, temveč tudi prostor družbenega delovanja, interakcij, druženja, koordiniranja, spoznavanja, tekmovanja in reševanja konfliktov« (Oblak in Petrič 2005, 24). Z razvojem spleta so se prilagodile tudi različne spletne družbene aplikacije, katerih namen je bil povezovati ljudi s podobnimi interesi povsod po svetu.

2.2.2 Pojav spletnih družbenih omrežij

Prvo prepoznavno spletno družbeno omrežje SixDegrees¹ se je pojavilo leta 1997. Omogočalo je možnost ustvarjanja profila, seznama prijateljev, od začetka leta 1998 pa je nudilo tudi možnost pregleda seznama prijateljev naših prijateljev. Vsaka od teh možnosti je v določeni obliki obstajala že pred nastankom omrežja SixDegrees, predvsem na večjih spletnih straneh, namenjenim iskanju ljubezenskih partnerjev. Čeprav je omrežje SixDegrees privabilo milijone uporabnikov, so ga leta 2000 ukinili. Po besedah ustanovitelja, je bil glavni razlog

¹ Poimenovanje SixDegree se nanaša na teorijo šestih stopenj oddaljenosti (ang. *six degrees of separation*), ki pravi, da je vsak povezan s katero koli osebo na svetu preko verige šestih ali manj poznanstev, tako da se veriga »prijatelj od prijatelja« med katerima koli dvema osebama lahko vzpostavi v največ šestih korakih (Wikipedia 2016a).

najverjetneje ta, da je bilo omrežje SixDegrees za svoj čas preveč napredno (Boyd in Ellison 2007).

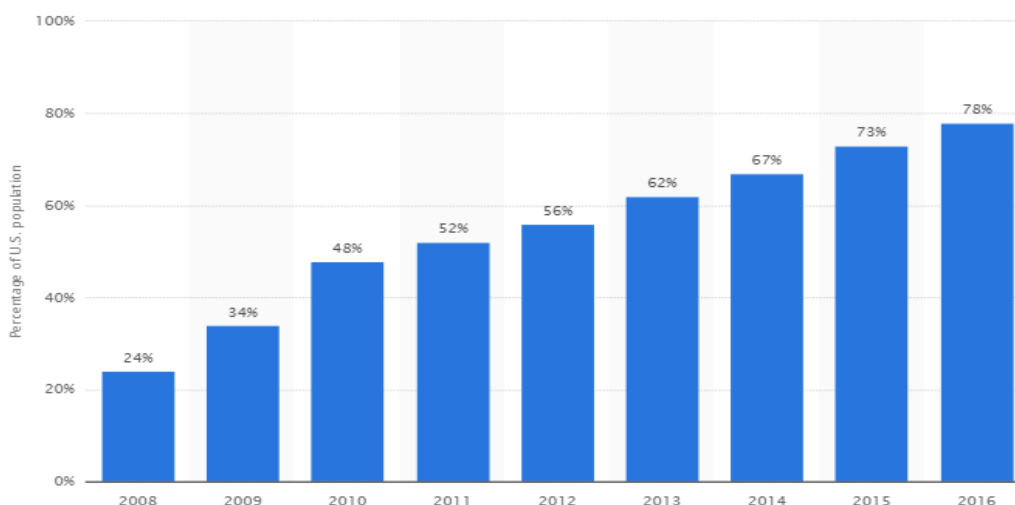
Pravi razmah spletnih družbenih omrežij pa se je začel v začetku tega desetletja. Leta 2002 se je pojavil Friendster. Podobno kot njegov predhodnik SixDegrees, je tudi Friendster sledil teoriji šestih stopenj oddaljenosti. Zrasel je na prepričanju, da lahko uspešna spletna skupnost obstaja le med ljudmi, ki imajo resnično močne prijateljske vezi in zagotavljal številne načine, da so uporabniki te vezi med seboj našli (Digital Trends 2016).

Leta 2003 se je pojavilo kar nekaj novih spletnih družbenih omrežij, ki so doživela velik uspeh. Med njimi Hi5, LinkedIn in MySpace. Slednji je leta 2004 izpodrinil Friendster s prestola najpopularnejšega spletnega družbenega omrežja in zasedel prvo mesto na lestvici priljubljenosti. Leta 2004 pa je bilo ustanovljeno, po številu uporabnikov, največje spletno družbeno omrežje vseh časov, Facebook (WebdesignerDepot 2007).

2.3 PRILJUBLJENOST SPLETNIH DRUŽBENIH OMREŽIJ

Po podatkih s spletne strani Statista (2016b) vidimo, kako zelo in kako hitro so se spletna družbena omrežja med letoma 2008 in 2016 razširila. Slika 2.1 prikazuje odstotek prebivalstva Združenih držav Amerike, ki je med letoma 2008 in 2016 v spletnih družbenih omrežjih ustvarilo vsaj en profil. Razvidno je, da ima v letu 2016 že kar 78 % prebivalstva Združenih držav Amerike ustvarjen vsaj en profil na enem od spletnih družbenih omrežij, razvidno pa je tudi, da se je v primerjavi z lanskim letom ta odstotek povečal za 5 % (Statista 2016b).

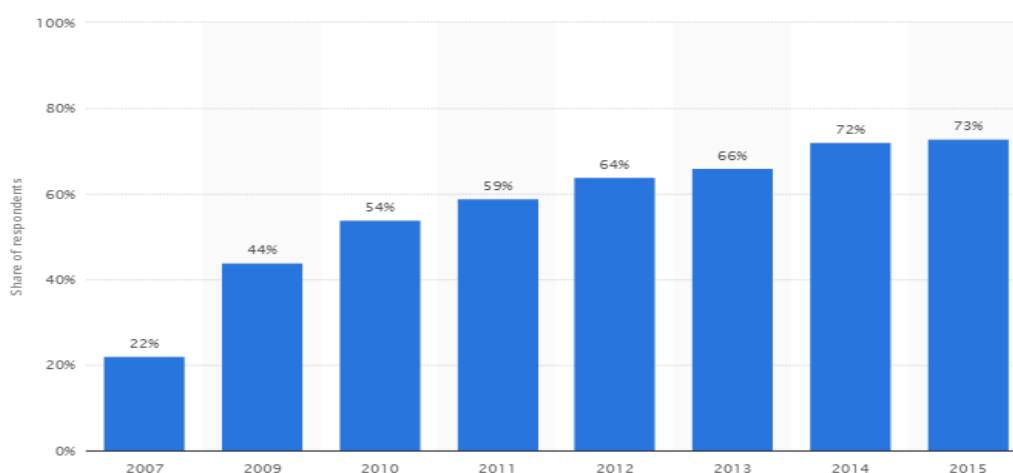
Slika 2.1: Odstotek prebivalstva ZDA, ki ima ustvarjen najmanj en osebni profil v spletnih družbenih omrežjih, podatki zajemajo obdobje od leta 2008 do 2016



Vir: Statista.com (2016b).

Spodnja slika (glejte Sliko 2.2) pa prikazuje statistične podatke raziskave o uporabnikih interneta v Združenem kraljestvu, ki so med letoma 2008 in 2015 v spletnih družbenih omrežjih ustvarili najmanj en osebni profil. V letu 2012 je 64 % vprašanih odgovorilo, da imajo v spletnih družbenih omrežjih ustvarjen vsaj en osebni profil. Od leta 2014 je v Združenem kraljestvu Facebook najbolj priljubljeno spletno družbeno omrežje. Sledita mu YouTube in Twitter (Statista 2015).

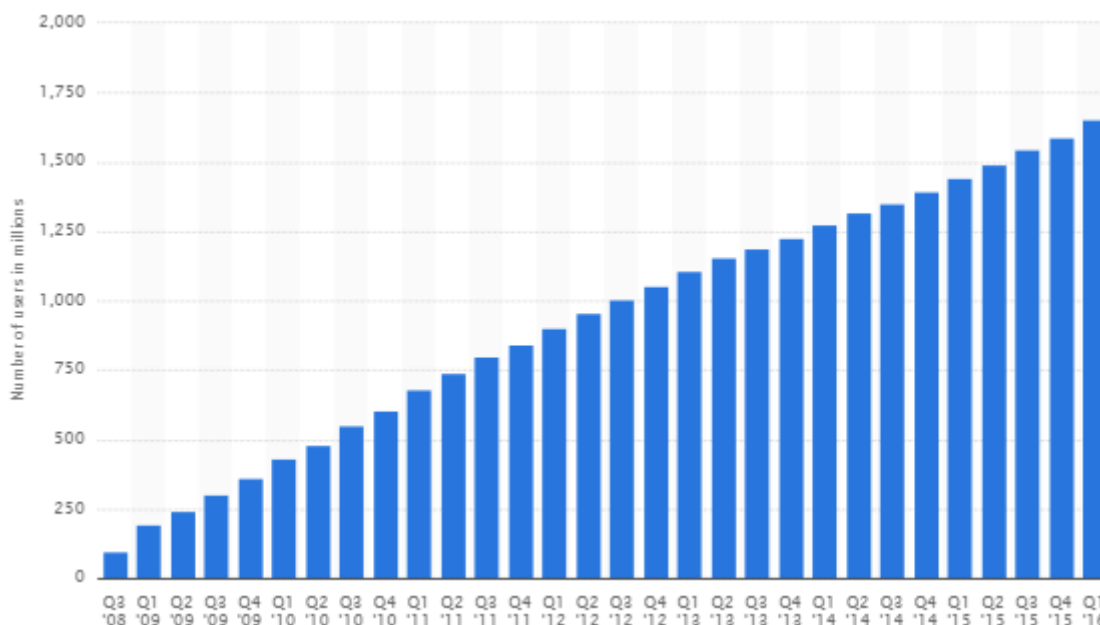
Slika 2.2: Odstotek prebivalstva Združenega kraljestva (UK), ki ima ustvarjen najmanj en profil v spletnih družbenih omrežjih, podatki zajemajo obdobje od leta 2007 do 2015



Vir: Statista.com (2015).

Na spletni strani Statista (2016a) najdemo tudi statistične podatke raziskave, v katerih so ugotavljali, kolikšno je število aktivnih mesečnih uporabnikov spletnega družbenega omrežja Facebook po vsem svetu. Statistika kaže časovni razpon od leta 2008 do 2016. Iz slike (glej Sliko 2.3) je razvidno, da je bilo v prvi četrtini leta 2016 na svetu vsak mesec 1,65 milijarde aktivnih uporabnikov spletnega družbenega omrežja Facebook. Slika prikazuje tudi podatek, da je v tretji četrtini leta 2012 število aktivnih mesečnih uporabnikov Facebooka preseglo eno milijardo. Omeniti je treba, da so aktivni uporabniki tisti, ki so se v zadnjih tridesetih dneh vpisali v svoj Facebook profil (Statista 2016a).

Slika 2.3: Število aktivnih mesečnih uporabnikov spletnega družbenega omrežja Facebook (v milijonih)



Vir: Statista (2016a).

2.4 VRSTE SPLETNIH DRUŽBENIH OMREŽIJ

Družbeni mediji so postali popularen način izmenjave informacij in podatkov z drugimi uporabniki. Spletna družbena omrežja so strani, ki gostijo družbene medije. Poznamo več vrst spletnih družbenih omrežij, Schrader (2010) jih deli na:

- **Forume**

Forumi so eno od prvih spletnih mest, ki so omogočala družbeno interakcijo. Običajno se tu združujejo uporabniki s podobnimi interesi, ki se pogovarjajo o določeni temi in gradijo medsebojne odnose. Forumi nudijo veliko informacij o določeni temi in so odličen način za izmenjavo znanja.

- **Bloge (spletne dnevnike)**

Blogi so primerni za uporabnike, ki radi pišejo dnevnike. Preko spleta delijo svoje spletne dnevnike z drugimi uporabniki. Še vedno obstajajo nekateri osebni dnevniki, medtem ko se na drugih blogih razpravlja o določenih temah ali interesih.

- **Mikro-bloge**

Podobno kot blogi, le da je to dnevnik, v katerem uporabniki poročajo o tem, kaj se dogaja v trenutku objave. Uporabniki lahko delijo kratke informacije o sebi, lahko pa delijo tudi informacije o dogajanjih oziroma novicah in dogodkih. Najbolj znan mikro-blog je Twitter.

- **Skupna raba fotografij**

Spletna družbena omrežja so znana po izmenjavi informacij, v tem primeru fotografij. Uporabniki naložijo sliko na spletna mesta za deljenje fotografij in namesto, da pošiljajo po eno sliko, enostavno pošljejo povezavo do spletnega albuma. Slike lahko uporabnik označi s ključnimi besedami, povezanimi s sliko, in omogoči drugim uporabnikom, da sliko komentirajo. Priljubljeno spletno omrežje za izmenjevanje fotografij sta Picasa in Flickr.

- **Skupna raba video posnetkov**

Eno najbolj priljubljenih spletnih mest za izmenjavo videoposnetkov je YouTube. Videoposnetkom se dodajo ključne besede, da drugi uporabniki lažje najdejo določen videoposnetek po teh ključnih besedah ali nazivu. Uporabnik, ki je videoposnetek objavil, lahko dovoli komentiranje le-tega.

- **Strokovna (poslovna) omrežja**

Mreženje je v strokovnih krogih že dolgo poznano in omogoča, da se prek spleta posameznik poveže z drugimi strokovnjaki z določenega področja. Če se uporabnik preseli, lahko še vedno ostane v stiku s svojimi bivšimi sodelavci in drugim osebam iz svoje stroke. Najbolj priljubljeno strokovno (poslovno) družbeno omrežje je LinkedIn.

- **Družabna omrežja**

Ko nekaj časa delamo z ljudmi, lahko ti postanejo naši prijatelji. Družabna omrežja pa omogočajo, da ostanemo z njimi v stiku. Najbolj priljubljeno družabno omrežje je Facebook.

- **Spletni zaznamki**

Glavni namen teh spletnih družbenih strani je izmenjava informacij. Če preberemo spletno stran, ki je zanimiva, inovativna ali navdihujoča, jo lahko označimo z zaznamki in s tem povemo drugim uporabnikom, da nam je ta spletna stran všeč. Strani, ki jih je veliko uporabnikov označilo z zaznamki, postanejo popularne in privabijo tudi druge uporabnike, da si jo ogledajo. Priljubljena družbena spletna omrežja za dodajanje zaznamkov so Digg, Delicious in StumbleUpon (Schrader 2010).

2.5 MEDSEBOJNA KOMUNIKACIJA V SPLETNIH DRUŽBENIH OMREŽJIH

Priklopiti se danes na internet v najširšem smislu pomeni »vstopiti na splet« in prek njega družbeno, kulturno ali politično delovati. Na ta način svetovni splet (world wide web) pridobiva pomembne razsežnosti kot družben in kulturni fenomen. Splet je namreč v komunikološkem jeziku platforma, ki »posreduje« – je medijski posrednik med družbenimi akterji, ki se prek svojih spletnih mest predstavljajo navzven (podjetja in javni zavodi, državni organi, nevladne organizacije in društva, umetniki, glasbeniki in »navadni« posamezniki itd.), in tistimi, ki nanj bolj ali manj naključno in bolj ali manj pogosto stopajo kot njegovi uporabniki (Oblak in Petrič 2005, 13).

Živimo v dobi računalniško posredovane komunikacije. Oblak in Petrič (2005) navajata, da:

...širjenje komunikacijskih poti ni zanimiva novost samo v luči tehnoloških inovacij, ki s sofisticirano računalniško podprto opremo premoščajo časovno prostorske ovire, temveč je pomembno tudi kot zametek nove komunikacijske kulture in nastajanja alternativnih javnih interakcijskih prizorišč. S širitvijo in družbenim utrjevanjem pomena računalniško posredovanega komuniciranja v sodobni družbi

se namreč oblikujejo pomembni prostori za vzpostavitev javnih razprav o javnih zadevah, ki zlahka presegajo dane nacionalne okvire. Poleg tega se porajajo tudi mnoga prizorišča, namenjena reševanju intimnih dilem in zasebnih problemov številnih posameznikov. S pomočjo interneta se tako oblikujejo dodatni družbeno-dialoški prostori, v katerih se posamezniki lahko na posebne načine srečujejo in med seboj združujejo, pogovarjajo in razpravljajo o zadevah, ki so v njihovem skupnem interesu, si izmenjujejo izkušnje, strahove, pričakovanja in želje (Oblak in Petrič 2005, 54).

Povezovanje uporabnikov v mnoga spletna družbena omrežja, vzpodbuja v njih željo po komuniciranju z ljudmi okoli sebe. Zato so na mnogih področjih uporaben pripomoček pospeševanja prodaje, izobraževanja, reklamiranja, povezovanja s prijatelji in poslovnimi partnerji. Področij spletnega mreženja je več:

- področje vlade (za enostavno pridobivanje javnega menja in ohranjanje publicitete),
- poslovno področje (ugoden način promocije in vzpostavljanja povezav za učinkovitejšo prodajo storitev ter način pridobivanja praks in poslovnih priložnosti),
- romantične zveze (lažje iskanje in spoznavanje partnerjev),
- področje izobraževanja (uporabniki se med seboj ali s profesorji lahko pogovarjajo o študijskih temah, delijo informacije ipd.),
- področje zdravstva (možnost povezovanja ljudi s podobnimi težavami ali boleznimi, možnost dodatne raziskave in medsebojno spodbujanje bolnikov) (Wikipedija 2016).

2.5.1. Spletna družbena omrežja kot medij in vir informacij

Spremenila se je komunikacija z občinstvom, ki ne sprejema več pasivno informacij in čaka na pregled dnevnih dogajanj popoldanske in večerne informativne oddaje. Velike količine informacij so danes občinstvu dostopne na številnih spletnih platformah, kar je spremenilo tudi proces iskanja, obdelovanja in posredovanja novic. V spletu najdemo milijone novic in občinstvo samo izbira novice in založnika. V takšnem okolju, kjer je uporabnikom dostopno veliko različnih virov informacij, model enosmerne komunikacije izgubi svojo vlogo, nadzor

pa prevzamejo uporabniki. Spremenila se je tudi dinamika poročanja, saj so se uporabniki navadili informacije dobiti takoj in biti del novinarskega procesa. Spletna družbena omrežja, kot sta Twitter in Facebook, so postala hitrejša in interaktivnejša od ostalih portalov, zlasti od televizije, radia in tiska. Možnost deljenja, komentiranja in ustvarjanja vsebine, je uporabnikom veliko bolj zanimiva od pasivnega sprejemanja informacij preko uveljavljenih (*mainstream*) medijev. Spletna družbena omrežja služijo novinarjem kot filter novic in kot storitev za iskanje informacij in oseb, najbolj pa služijo za odkrivanje in sledenje pomembnih dogajanj, saj spletna sfera daje vtis poročanja v živo (Volarević in Bebić 2013).

Danes se nemalokrat zgodi, da v poročilih preberemo ali slišimo novico, katere izvor je ravno Facebook. Za objavljanje novic prek spletnih družbenih omrežij so se odločili tudi številni politiki in politične stranke. Ko določene objave zberejo večje število všečkov, se pojavijo tudi v *mainstream* medijih in na ta način pridobijo dodatno vrednost. Seveda pa lahko pride tudi do negativnih posledic tovrstnih objav, saj novinarji dostikrat ne preverijo vira in resničnosti informacij. Novinarji ne bi smeli pozabiti na poglobljeno pravilo svojega poklica, to je, preverjanja informacij.

Druga negativna plat pa je, da mediji objavljajo necenzurirane novice iz spletnih družbenih omrežij, kot je bil lanski primer, ko so dijaki ene od mariborskih srednjih šol posneli ravnatelja in učiteljico pri spolnem odnosu in posnetek objavili na Facebooku. To nepremišljeno dejanje je imelo skrajno negativne posledice za vpletene. Pri poročanju o tem neljubem dogodku se večina osrednjih slovenskih medijev ni znala samoomejiti in spoštovati posameznikov in je s tem kršila Kodeks novinarjev Slovenije (Š.P. 2015). Kako hude so lahko posledice nepremišljenih objav v spletu in neprimerne poročanja v medijih o njih, je nazorno prikazal prej omenjeni dogodek.

Eno od najbolj priljubljenih in največjih spletnih družbenih omrežij je prav gotovo Facebook, zato sem se tudi odločila pisati o njem v diplomskem delu. V naslednjem poglavju sledi podroben opis Facebooka.

3 FACEBOOK

»Naša misija je dati ljudem moč, da delijo in ustvarjajo bolj odprt in povezan svet. Ljudje uporabljajo Facebook, da ostanejo povezani s prijatelji in družino, da odkrivajo kaj se po svetu dogaja ter da delijo in izražajo tisto, kar je njim pomembno« (Facebook 2016a).

3.1 ZGODOVINA FACEBOOKA

Spletno družbeno omrežje Facebook je ustanovil Mark Zuckerberg med študijem psihologije na univerzi v Harvardu. Kot navdušen računalniški programer je Mark pred tem za svoje študentske kolege že razvil več spletnih družbenih omrežij, med drugim Coursematch, ki je uporabnikom omogočal pregled nad napredkom študija drugih študentov, in Facemash, kjer so uporabniki lahko ocenjevali privlačnost drugih uporabnikov (Phillips 2007).

Po teh testnih poskusih je Mark Zuckerberg s še tremi soustanovitelji marca 2004 ustvaril spletno družbeno omrežje »The Facebook«. Ta je bil sprva mišljen za povezovanje študentov s Harvarda, a je že v 24-ih urah od ustanovitve dobil 1200 uporabnikov. Do konca meseca pa ga je uporabljala že več kot polovica dodiplomskih študentov s Harvarda. The Facebook se je hitro razširil tudi po ostalih elitnih univerzah v ZDA in avgusta 2005 spremenil ime v »Facebook«. Od septembra 2005 je postal odprt tudi dijakom srednjih šol v ZDA in nato še angleškim fakultetam (Phillips 2007).

Ker je bil vstop omejen, je bilo takrat zelo kul, če si ga uporabljal, in zaradi tega so bili študentje na svojih Facebook profilih pripravljeni marsikaj izdati. 11. septembra 2006 pa je Facebook postal odprt in dostopen vsem uporabnikom z veljavnim elektronskim računom. Zaradi svojega resnega videza in zaupanja je Facebook postal priljubljen tudi med tistimi, ki so šolanje že končali (Crnović 2007).

3.2 FACEBOOK DANES

Skoraj deset let pozneje je Facebook spletno družbeno omrežje z največ dnevno aktivnih uporabnikov. 27. avgusta 2015 je Mark Zuckerberg na svojem Facebook profilu naznanil, da je v ponedeljek, 24. avgusta 2015, Facebook prestopil velik mejnik, saj so v enem samem dnevu zabeležili milijardo aktivnih uporabnikov (Facebook 2015a). Marca letos pa je bilo v povprečju dnevno zabeleženih 1,09 milijarde aktivnih uporabnikov Facebooka (Facebook 2016a).

Slika 3.1: Statistični podatki omrežja Facebook za prvo četrtino leta 2016



Vir: Facebook (2016a).

Iz Slike 3.1 je razvidno, da je v prvi četrtini leta 2016 imelo spletno družbeno omrežje Facebook na mesec 1,65 milijarde aktivnih uporabnikov in s tem za več kot polovico prehitelo omrežje WhatsApp, ki je zabeležilo 1 milijardo aktivnih uporabnikov na mesec. Sledita jima Messenger z 900 milijoni uporabnikov in Instagram s 400 milijoni aktivnih uporabnikov na mesec. Zanimivo je, da si Facebook lasti vsa štiri omrežja.

S porastom spletnih družbenih omrežij se povečujejo tudi kršitve osebnih pravic in zasebnosti posameznikov. Ko pride do teh kršitev, se zatečemo k različnim pravno-formalnim sredstvom. Kako je to področje urejeno v Sloveniji, bomo pogledali v naslednjem poglavju.

4 PRAVICA DO ZASEBNOSTI IN PRAVICA DO VAROVANJA OSEBNIH PODATKOV

»Univerzalne definicije zasebnosti in pravice do zasebnosti ni«, pravi Kovačič (2006, 12). Razlog za to je, da je zasebnost relativna, kontekstualna in subjektivna in vsak ima različna pričakovanja o zasebnosti, ki se spreminjajo tudi glede na družbeni kontekst (Kovačič 2006).

Zasebnost je neizogibno težak koncept. Nanaša se namreč na nekaj, kar je subjektivno in jo je zato nemogoče dokončno opredeliti. Predstava zasebnosti se namreč spreminja od posameznika do posameznika, od skupine posameznikov do skupine posameznikov, od družbe do družbe in je pogojena s kulturo in tradicijo (Lampe 2004).

»Pravica do zasebnosti ali osebnega življenja temelji na človekovi potrebi, da nemoteno in v miru živi svoje intimno in osebno življenje, brez vsakega nezaželenega vmešavanja tujih oseb oz. javnosti« (Križaj 1989, 21).

V današnjem svetu informacijske tehnologije je vse težje zagotavljati pravico do zasebnosti in do varovanja osebnih podatkov. Vsakega posameznika namreč opisujejo številni podatki, ki se nanašajo zgolj nanj in se zato upravičeno sprašuje, ali se jih uporablja res samo za zakonsko določene namene, ali pa se njegovi podatki zbirajo tudi v druge namene. Dnevno smo namreč priča vse večjim posegom v našo zasebnost, ki se jih morda niti popolnoma ne zavedamo (Stare 2010).

V naši pravni ureditvi je varstvo osebnih podatkov urejeno že v Ustavi RS, gre torej za eno od ustavno zagotovljenih človekovih pravic in temeljnih svoboščin in sodi v okvir pravic s področja zasebnosti. V nadaljevanju bom predstavila, kako je varstvo osebnih podatkov urejeno s slovensko zakonodajo, pa tudi, kako to področje ureja mednarodna zakonodaja.

Drugi naziv za varstvo osebnih podatkov je podatkovna oziroma informacijska zasebnost, ki je širši del področja varstva zasebnosti. Namen varstva osebnih podatkov je tudi varstvo dostojanstva posameznika. Pravica do dostojanstva je v prvi vrsti obrambna pravica pred posegi državne oblasti in posameznika (Pirc Musar in ostali 2006).

Bistvo varstva osebnih podatkov oz. podatkovne zasebnosti posameznika ni v nekem kvazilastniškem konceptu osebnih podatkov, ampak v varstvu in nadzoru obdelave osebnih podatkov, za katero marsikateri uporabnik sploh ne ve, da poteka (Pirc Musar in ostali 2006).

V moderni informacijski družbi, v kateri živimo, je regulacija zasebnosti nujno potrebna, saj napredek znanosti omogoča vedno več posegov vanjo s strani posameznikov, hkrati pa državni oblasti daje vse večje možnosti nadzora. Zato je pravna ureditev tega področja zelo pomembna.

4.1 OSEBNI PODATKI

S pojmom osebni podatek se praktično srečujemo vsak dan. Definicij je zato več.

»To je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen. Tudi naslov e-pošte je lahko osebni podatek, če se z njim da določiti posameznika« (Antić 2011).

Osebni podatek je po določbah Zakona o varstvu osebnih podatkov katerikoli podatek, ki se nanaša na določeno ali določljivo fizično osebo, torej na posameznika, ne glede na obliko, v kateri je izražen. Določljiva fizična oseba pa je tista, ki se jo lahko neposredno ali posredno identificira s pomočjo njenih identifikacijskih števil (npr. EMŠO, davčna številka, številka zdravstvenega zavarovanja, telefonska številka, registrska številka vozila), ali s sklicevanjem na dejavnike, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto (npr. zaposlitev, naslov, funkcijo, položaj ali status v določenem subjektu ipd.) (ZVOP-1, 6. čl.).

4.1.1 Varstvo osebnih podatkov v Ustavi RS

Kot že zgoraj omenjeno, je v Sloveniji varstvo osebnih podatkov zagotovljeno že z samo Ustavo RS in sicer v poglavju o človekovih pravicah in temeljnih svoboščinah.

Izhodišče za urejanje osebnih podatkov je umeščeno v Ustavo Republike Slovenije, ki določa pravico do varstva zasebnosti in osebnostnih pravic:

»Zagotovljena je nedotakljivost človekove telesne in duševne celovitosti, njegove zasebnosti ter osebnostnih pravic« (Ustava RS, 35. čl.).

Informacijska zasebnost oziroma varstvo osebnih podatkov je kot ena od kategorij pravice do zasebnosti prav tako zagotovljena z Ustavo Republike Slovenije:

»Zagotovljeno je varstvo osebnih podatkov. Prepovedana je uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja.

Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon.

Vsakdo ima pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi.« (Ustava RS, 38.čl.).

Varstvo osebnih podatkov je del človekove zasebnosti. Ta pravica se navezuje na ostale človekove pravice, ki so opredeljene kot pravice človekove zasebnosti. Normativna ureditev Republike Slovenije področje varstva osebnih podatkov ureja s sistemskim zakonom, ki v splošnem določa obveznosti in ukrepe za preprečevanje nezakonitosti ter neupravičene posege v zasebnost posameznika na področju obdelave osebnih podatkov. Varstvo osebnih podatkov pa je poleg sistemske potrebno urediti tudi s področno zakonodajo (Pirc Musar in ostali 2006).

Ena izmed človekovih pravic in temeljnih svoboščin, ki jo določa 38. člen Ustave RS, je varstvo osebnih podatkov. Le-te je prepovedano uporabljati v nasprotju z namenom njihovega zbiranja, pri čemer iz drugega odstavka 38. člena Ustave RS izhaja zahteva po zakonski določenosti zbiranja, obdelovanja, namena uporabe, nadzora in varstva tajnosti osebnih podatkov. V posledici navedenega se ima tudi vsakdo pravico seznaniti z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi² (Čebulj in Žurej 2005).

² Enake zahteve vsebuje tudi Konvencija o varstvu osebnih podatkov glede na avtomatsko obdelavo podatkov (KonVOP). »Poleg tega, da morajo biti osebni podatki pridobljeni in obdelani pošteno in zakonito, konvencija terja sprejem ukrepov, ki bodo zagotovili, da bodo osebni podatki shranjeni za določene in zakonite namene ter da se bodo obdelovali le podatki, ki so primerni, ustrezni in niso pretirani glede na namen zbiranja« (Čebulj in Žurej 2005, 20).

Varstvo osebnih podatkov učinkuje nasproti državnim organom, organom lokalnih skupnosti, nosilcem javnih pooblastil, učinkuje pa tudi med zasebniki, torej med civilnopravnimi osebami. Sodno varstvo pravic, ki jih ima posameznik zaradi uresničevanja varstva osebnih podatkov, je zagotovljeno v upravnem sporu (Čebulj v Šturm 2002, 410).

4.1.2 Zakonska ureditev varstva osebnih podatkov

Varstvo osebnih podatkov je v Sloveniji urejeno z zakonom. Prvi Zakon o varstvu osebnih podatkov (ZVOP) smo dobili še pred osamosvojitvijo, ko ga je leta 1990 sprejela slovenska skupščina.

Ko je Slovenija leta 2004 postala članica Evropske unije, je morala varstvo osebnih podatkov uskladiti z določbami Direktive 95/46/ES Evropskega parlamenta in Sveta Evrope z dne 24. oktober 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem gibanju takih podatkov (Informacijski pooblaščenec 2009).

S 1. januarjem 2005 je začel veljati novi Zakon o varstvu osebnih podatkov (ZVOP-1), ki ga je DZ Republike Slovenije sprejel 15. julija 2004. S sprejetjem tega zakona je bila predvidena ustanovitev neodvisnega in samostojnega Državnega nadzornega organa za varstvo osebnih podatkov ter povečanje pristojnosti tega organa glede na pristojnosti, ki jih je imel v letu 2004 Inšpektorat za varstvo osebnih podatkov (Stare 2010).

ZVOP-1 je sistemski zakon, ki ureja pravice, obveznosti, načela in ukrepe, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika oziroma posameznice pri obdelavi osebnih podatkov (Informacijski pooblaščenec 2014).

4.1.3 Mednarodna ureditev varstva osebnih podatkov

Varstvo osebnih podatkov je predmet pravne ureditve in regulacije tudi številnih drugih mednarodnopravnih dokumentov. Med mednarodnimi oblikami varstva človekovih pravic je

najpomembnejša ureditev v Evropski konvenciji za človekove pravice in uredbah ter direktivah EU.

Na podlagi prvega odstavka 8. člena Evropske konvencije o varstvu človekovih pravic, ki določa, da ima vsakdo pravico do spoštovanja njegovega zasebnega in družinskega življenja, doma in dopisovanja, je bila v okviru Sveta Evrope sprejeta Konvencija o varstvu posameznikov glede na avtomatsko obdelavo podatkov, katere ratifikacijo je sprejel Državni zbor Republike Slovenije na seji dne 25.1.1994. Le – ta vsebuje načela varstva osebnih podatkov na katera se opira slovenska ustavna ureditev varstva osebnih podatkov (Evropska konvencija za človekove pravice, 8. čl.).

Načela Konvencije o varstvu osebnih podatkov so bistveno pridobila na pomenu junija 1994, ko je Evropska konvencija za človekove pravice (EKČP) postala del notranjega prava RS. To je pomenilo tudi to, da je Slovenija prišla pod jurisdikcijo Evropskega sodišča za človekove pravice. Z ratifikacijo Konvencije o varstvu posameznika glede na avtomatsko obdelavo podatkov (KonVOP) so postala njena načela merilo zakonskega urejanja vsakega zbiranja, procesiranja in uporabe osebnih podatkov. Leta 1995 so bila načela KonVOP povzeta tudi v evropsko direktivo - Direktivo o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku teh podatkov (DirVOP). Do 24. oktobra 1998 so morale vse države članice EU direktivo implementirati (Stare 2010).

4.2 PRAVICA DO ZASEBNOSTI

V Sloveniji, kakor tudi v večini evropskih držav, je pravica do zasebnosti ena od ustavno zagotovljenih pravic. Pojavlja se v dveh oblikah; kot mednarodna in ustavna človekova pravica javnopravnega značaja ter kot osebnostna pravica zasebnega značaja. Kot prva je pred posegi države in njenih organov varovana z ustavo in mednarodnopravnimi instrumenti v okviru ustavnega, upravnega in kazenskega prava. Njeni zasebnopravni vidiki pa so obravnavani v razpršenih disciplinah zasebnega prava in varovani z instrumenti civilnega prava.

»Zasebnost sodobna pravna teorija opredeljuje kot področje posameznika, v katerega ne sme nihče posegati brez posebnega zakonskega pooblastila« (Pravno-informacijski sistem 2001).

Natančne definicije pa tako pravna teorija kot praksa ne dajeta, saj je »pravna praksa zaradi družbene dinamike tako spreminjajoča in prožna, da bi preozka definicija ali pojmovanje pravice do zasebnosti lahko omejila ali ohromila določene dobrine, katerim gre v okviru pravice do zasebnosti pravno varstvo« (Lampe 2004, 41–42).

Pravica do zasebnosti varuje določene vidike, od katerih je nekaterim priznan status samostojne pravice. Na podlagi Ustave so nekateri aspekti te pravice varovani s »splošno« pravico do zasebnosti, nekateri pa so izpeljani iz le-te. Med slednje spada tudi varstvo osebnih podatkov, ki je v literaturi dostikrat označeno kot informacijska zasebnost (ang. *Information Privacy*) (Stare 2010).

4.2.1 Vidiki pravice do zasebnosti

»Zasebnost oziroma pravica do zasebnosti ima različno vsebino v različnih političnih ureditvah, na njeno opredelitev pa vpliva tudi časovni horizont. Ena prvih definicij se je izoblikovala že konec prejšnjega stoletja v Združenih državah Amerike. Po njej je to pravica posameznika, da se ga pusti pri miru. Takšna definicija za potrebe sodobnih družbenih sistemov, katerih najpomembnejšo značilnost in podlago za delovanje predstavljajo informacije, prav gotovo ni ustrezna. Zato se danes pravica do zasebnosti opredeljuje kot pravica posameznika, da zahteva, da se podatki in informacije o njegovih zasebnih razmerjih ne sporočajo komurkoli. Gre torej za kontrolo pretoka in posredovanja podatkov, ki se nanašajo nanj oziroma opisujejo njegove lastnosti« (Čebulj 1992, 7).

V mednarodnopravnih aktih se pojavljajo naslednja področja pravice do zasebnosti, iz 8. člena Evropske konvencije za človekove pravice (1994) lahko razberemo tri področja pravice do zasebnosti:

- *prostorska zasebnost*, ki jo lahko opredelimo tudi kot željo posameznika, da je ločen od fizične navzočnosti drugih ljudi, npr. nedotakljivost stanovanja in drugih zasebnih prostorov;
- *psihična/duševna zasebnost*, npr. pravica od imena, spolna integriteta, svoboda misli,

veroizpovedi; nanjo se navezuje tudi odločitvena zasebnost posameznika – npr. glede njegovega telesa, druženja z ljudmi;

- *informacijska zasebnost*, in sicer korespondenčna in komunikacijska zasebnost ter varstvo osebnih podatkov.

4.3 VARSTVO POSAMEZNIKA GLEDE OSEBNIH PODATKOV

Vsakemu posamezniku je glede varstva osebnih podatkov zagotovljen inšpekcijski nadzor, ki ga izvaja *Informacijski pooblaščenec* in sodno varstvo, ki ga izvršujejo sodišča. To pomeni, da ni treba posebej urediti inšpekcijskega nadzora nad osebnimi podatki na kateremkoli področju. Tako se zagotovi enaka raven varstva osebnih podatkov, ki mora biti enako kakovostna na vseh področjih. Inšpekcijski nadzor lahko poleg informacijskega pooblaščenca kot predstojnika organa opravljajo tudi državni nadzorniki za varstvo osebnih podatkov pri Informacijskem pooblaščenču (Pirc Musar 2006).

Z dnem 1.9.2003 je začel delovati Pooblaščenec za dostop do informacij javnega značaja, ki je bil ustanovljen z Zakonom o dostopu do informacij javnega značaja. Le – ta je v prvem odstavku 28. člena določal, da je Pooblaščenec za dostop do informacij javnega značaja samostojen državni organ, katerega skladno z drugim odstavkom istega zakona na predlog predsednika Republike Slovenije imenuje Državni zbor Republike Slovenije. Upoštevajoč določbi prvega odstavka 29. člena in drugega odstavka 30. člena Zakona o dostopu do informacij javnega značaja je bil Pooblaščenec za dostop do informacij javnega značaja državni funkcionar, ki je imel strokovno službo, ki sta jo do dne 15.7.2005 sestavljala največ dva svetovalca, med tem, ko je organizacijsko-administrativne naloge za Pooblaščenca za dostop do informacij javnega značaja zagotavljalo takratno Ministrstvo za informacijsko družbo. Z dnem uveljavitve Zakona o varstvu osebnih podatkov (ZVOP-1) je bila v slovenski pravni red prenesena Direktiva 95/46/ES Evropskega parlamenta in Sveta z dne 24.10.1995 o varstvu posameznikov pri obdelavi osebnih podatkov in prostem pretoku osebnih podatkov. Tako je ZVOP-1 predvideval glavni državni nadzorni organ za varstvo osebnih podatkov; postopek za imenovanje naj bi se začel 1.7.2005, državni nadzorni organ pa naj bi začel delovati najkasneje s 1.1.2006. Po določbi prvega odstavka 38. člena Zakona o varstvu osebnih podatkov (ZVOP-1) je državni nadzorni organ samostojni državni organ, ki ga v skladu z drugim odstavkom istega člena vodi glavni državni nadzornik, ki je državni

funkcionar. V tem delu je potrebno poudariti, da je pred uveljavitvijo ZVOP-1 skladno z določbo 26. člena ZVOP opravljal inšpekcijsko nadzorstvo nad izvajanjem določb ZVOP in drugih predpisov s področja varstva osebnih podatkov inšpektorat za varstvo osebnih podatkov kot organ v sestavi Ministrstva za pravosodje, ki je bil v razmerju do ministrstva organ prve stopnje. Z uveljavitvijo Zakona o informacijskem pooblaščenecu dne 31.12.2005 sta se združila Pooblaščenec za dostop do informacij javnega značaja in Inšpektorat za varstvo osebnih podatkov, s čimer je bila spoštovana določba prvega odstavka 108. člena ZVOP-1, ki je določala, da državni nadzorni organ za varstvo osebnih podatkov, ki ima položaj samostojnega državnega organa, začne z delom 1.1.2006. Z uveljavitvijo Zakona o informacijskem pooblaščenecu je bil ustanovljen Informacijski pooblaščenec in določene njegove pristojnosti in pooblastila (Informacijski pooblaščenec 2016b).

Informacijski pooblaščenec se ukvarja z dvema temeljnima ustavnima človekovima pravicama, to sta dostop do informacij javnega značaja in pa varstvo osebnih podatkov – na teh dveh področjih tudi izvaja številne pristojnosti (Informacijski pooblaščenec 2016a).

V določenih primerih pa je sodno varstvo edini način, da posameznik zavaruje svoje pravice v zvezi z varstvom osebnih podatkov. Pravica do sodnega varstva izhaja že iz Ustave RS, po katerem ima vsakdo pravico, da o njegovih pravicah in dolžnostih ter o obtožbah proti njemu brez nepotrebnega odlašanja odloča neodvisno, nepristransko in z zakonom ustanovljeno sodišče (Ustava RS, 23. čl.).

4.4 PROBLEM VARSTVA OSEBNIH PODATKOV NA SPLETNIH DRUŽBENIH OMREŽJIH

Oseba, ki želi uporabljati neko spletno družbeno omrežje, se mora vanj vključiti tako, da na tem omrežju ustvari svoj profil, prek katerega se potem povezuje z drugimi osebami, pridobiva podatke, jih tudi sama objavlja in tako stopa v interakcijo z drugimi. To je posebnost spletnih družbenih omrežjih, saj so nekatere stvari o uporabniku vidne vsem, odvisno od tega, kakšne nastavitve zasebnosti kdo uporablja. Prav to dejstvo namreč loči uporabnike spletnih družbenih omrežij od ostalih internetnih strani, na katerih lahko poljubno

dostopamo do novic, podatkov in podobno. Tukaj je naš »vstop« takorekoč pogojen z ustvarjanjem profila. Če profila ne ustvarimo, do podatkov ne moremo dostopati.

Vedno ko odpiramo profil na kateremkoli družbenem omrežju, se nam odpre nekakšen vprašalnik oziroma obrazec, v katerega vnesemo svoje podatke, kot so ime, priimek, spletni naslov, datum rojstva, fotografija, opis naših zanimanj ipd. S tem posredujemo svoje osebne podatke, za katere natančno ne vemo, če so ustrezno varovani pred morebitnimi vdori. Ob ustvarjanju profilov različnih uporabnikov spletnih družbenih omrežij tako nastaja nekakšna »široka baza osebnih podatkov«, za katere se upravičeno sprašujemo, komu je namenjena in kako je zavarovana pred posegi in zlorabo s strani drugih oseb.

Danes je naša zasebnost omejena na vsakem koraku; npr. če rešujemo križanko in rešitve pošljemo uredništvu revije ali časopisa, ki to edicijo izdaja, od nas želijo osebne podatke, telefonsko številko, internetni naslov, nekateri tudi datum rojstva, podpis, nekateri k temu dodajo še kratko anketo, za katero nas vljudno prosijo, da si vzamemo čas in jo izpolnimo. Včasih nehote o sebi posredujemo osebne podatke, za katere niti ne vemo, kdo jih bo uporabil. Zagotovo bi bilo za žrebanje nagrad pri nagradni križanki čisto dovolj samo ime in priimek in naslov. Če torej osebne podatke posredujemo takole mimogrede in brez razmišljanja, se moramo zavedati, da lahko takšnemu našemu ravnanju sledijo včasih zelo neprijetne posledice. Dejstvo je namreč, da s širjenjem našega informacijskega prostora vse težje ohranjamo svojo anonimnost. Podatki, ki jih enkrat posredujemo, so lahko posredovani drugim uporabnikom, drugim omrežjem in tako do naših osebnih podatkov lahko dostopa čedalje večje število uporabnikov spletnih družbenih omrežij. Še posebej pa velja previdnost pri objavljanju fotografij, saj lahko le-te drugi uporabniki kopirajo, jih objavljajo na svojem profilu, jih delijo, nas na fotografijah označujejo in fotografije komentirajo tudi brez naše privolitve.

V virtualnem prostoru so zlorabe zasebnosti in nadzor oziroma zbiranje podatkov mogoči na več načinov. Dostikrat se ne zavedamo, da z uporabo računalniške in telekomunikacijske tehnologije v virtualnem prostoru puščamo sledove, tako namerno kakor tudi nevede (Kovačič 2003).

Kot člani spletnega družbenega omrežja Facebook prav tako puščamo sledove, zato si bomo sedaj pogledali, kako je urejena zasebnost na družbenem omrežju Facebook in njegove splošne pogoje uporabe.

5 ZASEBNOST NA SPLETNEM DRUŽBENEM OMREŽJU FACEBOOK

5.1 SPLOŠNI POGOJI UPORABE

Ob prvi prijavi oziroma registraciji v spletno omrežje Facebook se moramo strinjati s pogoji uporabe na tem omrežju. Vse dokler ne potrdimo, da se strinjamo z vsemi navedenimi pogoji, nas Facebook ne spusti naprej in prijava ni mogoča. Splošne pogoje uporabe ima danes že vsako spletno družbeno omrežje, v katerega se je treba registrirati, in pri vseh so pravila enaka; če se želimo vpisati v omrežje, moramo te pogoje sprejeti.

Pod tretjo točko Pogojev uporabe na omrežju Facebooka je določena varnost. Prvi odstavek te točke navaja, da se ustvarjalci Facebooka trudijo za varnost na omenjenem omrežju, vendar je ne morejo zagotoviti. »Potrebujemo vašo pomoč, da ohranimo Facebook bolj varen« in navajajo obveznosti, ki se jih uporabniki Facebooka morajo držati (Facebook, 2015b):

- Ne boste objavljali nepooblaščenih reklamnih sporočil.
- Ne boste zbirali vsebine in podatke uporabnikov ali kako drugače dostopali do Facebooka brez našega dovoljenja.
- Na Facebooku ne boste sodelovali pri nezakonitem mrežnem marketingu, kot je piramidni sistem.
- Ne boste nalagali virusov in drugih zlonamernih kod.
- Od drugih uporabnikov ne boste zahtevali vpisnih podatkov in se vpisovali v profile drugih uporabnikov.
- Ne boste ustražovali in nadlegovali drugih uporabnikov.
- Ne boste objavljali vsebin, kot so: sovražni govor, grožnje, pornografija; spodbujanje nasilja; ali vsebine, ki vključujejo goloto ali nasilje.
- Ne boste razvijali ali upravljali z aplikacijami tretjih oseb, ki vsebujejo uživanje alkohola, zmenkarije ali drugo vsebino za odrasle (vključno z oglaševanjem), brez primernih starostnih omejitev.
- Facebooka ne boste uporabljali za nekaj nezakonitega, zavajajočega, zlonamernega ali diskriminatornega.
- Ne boste storili ničesar, kar bi lahko onemogočilo, preobremenilo ali oviralo pravilno delovanje ali videz Facebooka.

- Ne boste povzročali ali spodbujali kakršnih koli kršitev te Izjave ali naših politik.

Problem dostikrat nastane, ker uporabniki ne preberejo vseh pogojev uporabe, če sploh katere, in lahko se zgodi, da zaradi nepoznavanja le-teh, kršijo določena pravila. Če pri Facebooku ugotovijo, da je uporabnik kršil katerega od splošnih pogojev uporabe, ga opozorijo in mu zaprejo profil. Do težav pri seznanjanju s splošnimi pogoji uporabe pa lahko pride tudi zato, ker so ti pogoji večinoma pisani v tujem jeziku, najpogosteje v angleškem. Facebook do danes še ni prevedel svojih splošnih pogojev uporabe v slovenščino in za marsikoga je lahko to težava ali ovira za razumevanje teh pogojev.

5.2 NASTAVITVE IN ORODJA ZA ZASEBNOST

Facebook svojim uporabnikom omogoča, da sami določajo stopnjo zasebnosti svojih osebnih profilov. Uporabnik lahko podatek, na primer sliko, objavi tako, da je javna in vidna vsem, da jo vidijo samo prijatelji, ima pa tudi možnost, da vidijo sliko le izbrani prijatelji ali skupine. Privzete nastavitve so po navadi precej ohlapne, zato se uporabnikom priporoča, da jih ročno spremenijo in nastavijo tako, da bi bili objavljeni podatki čim boljše zaščiteni, in s tem možnost morebitnih zlorab profila čimmanjša.

5.2.1 Uporabna orodja za upravljanje zasebnosti

Po svoji meri lahko prilagodimo naslednje nastavitve (Facebook 2016b):

- *Kdo lahko vidi moje objave in podatke?* Ta nastavek omogoča, da prilagodimo, kdo bo v prihodnje videl naše objave na časovnici. Nastavimo jih lahko tako, da jih bomo videli samo mi, naši prijatelji, prijatelji naših prijateljev ali po meri (po meri pomeni, da sami določimo prijatelje ali skupine, katerim bodo naše objave vidne). Pri tej nastavitvi Facebook nudi možnost, da lahko pogledamo vse naše objave in vsebine, v katerih smo bili označeni. Omogoča tudi, da omejimo občinstvo za objave, ki smo jih v preteklosti delili s prijatelji prijateljev ali javnostjo.
- *Kdo lahko stopi v stik z mano?* Poljubno lahko nastavimo, kdo nam lahko pošlje prošnjo za prijateljstvo. Izbiramo lahko med vsemi uporabniki Facebooka ali samo prijatelji naših prijateljev.

- *Kdo me lahko poišče?* Na Facebooku nas lahko uporabniki poiščejo preko elektronskega naslova ali telefonske številke, ki smo ju navedli. Možne nastavitve so prijatelji, prijatelji naših prijateljev ali vsi. Facebook nas tudi vpraša, če želimo, da iskalniki zunaj Facebooka prikažejo povezavo do našega profila.
- *Kdo lahko objavlja na moji časovnici?* Objave na naši časovnici lahko omejimo tako, da jih dodajamo samo mi sami, ali naši prijatelji. Lahko pa tudi vključimo nastavev, ki nam omogoča predogled objave. Ta funkcija omogoča nadzor nad tem, ali želimo ročno odobriti objave, v katerih smo označeni, preden se le-te pojavijo na naši časovnici.
- *Kdo lahko vidi objave na moji časovnici?* Nastavljamo lahko, kdo lahko vidi objave na naši časovnici, v katerih smo bili označeni, in kdo lahko vidi objave naših prijateljev na naši časovnici. Lahko nastavimo tudi, kdo lahko komentira naše objave. Možne nastavitve so: vsi, prijatelji mojih prijateljev, prijatelji, samo jaz ali po meri.
- *Kako lahko upravljam z oznakami, ki jih dodajo drugi ljudje, in predlogi za oznake?* Za večji nadzor zasebnosti lahko vključimo predogled oznak, ki jih naši prijatelji dodajo našim vsebinam, preden se le-te prikažejo na Facebooku, in se sami odločimo, ali želimo, da smo označeni v tej vsebini, ali ne. Ta nastavev je še posebej koristna, ko nekdo objavi našo sliko z neprimerno vsebino.

Obstajajo tudi druge možnosti nastavev zasebnosti. Lahko nastavimo, kdo lahko komentirana naše objave, komu je viden podatek, s kom smo v razmerju, kdo je naša družina, pri datumu rojstva lahko nastavimo, da je vidna samo letnica ali pa je celoten podatek viden le nam; omejimo lahko povabila v aplikacije; obstaja tudi možnost, da ustvarimo seznam blokiranih oseb in osebe s tega seznama nam ne morejo več pošiljati sporočil ali objavljati na naši časovnici (Facebook 2016).

Facebook nudi tudi številna orodja, s katerimi lahko zavarujemo našo zasebnost. V spletu, s tem tudi v spletnem družbenem omrežju Facebook, moramo biti zelo previdni pri objavljanju naših vsebin. O tem se je na lastne oči prepričala najstnica Rebecca, ko je na Facebooku za svoj petnajsti rojstni dan želela povabiti le petnajst prijateljev na Facebooku. A najstnica ni bila pazljiva in je dogodek, v katerem je zapisala tudi svoj domači naslov in telefonsko številko, objavila kot javen. Na povabilo se je odzvalo 21.000 oseb in posredovati je morala celo policija (The Telegraph 2010).

V naslednjem poglavju si bomo ogledali, kakšne so nevarnosti, zlorabe in zaščite pred takimi incidenti.

6 NEVARNOSTI, ZLORABE IN ZAŠČITA PRED NJIMI

6.1 TIPI SPLETNIH KRIMINALCEV

Da bi lažje razumeli, kako se kriminalna dejanja in ostale nevarnosti pri uporabi spleta zgodijo, se najprej moramo seznani, kdo so storilci, ki stojijo za temi dejanji.

Tako kot v realnem svetu za kriminalnimi dejanji stojijo posamezniki ali skupine, so tudi v virtualnem svetu za kriminaliteto odgovorni posamezniki ali skupine, česar se dostikrat skoraj ne zavedamo. Ob »klasičnih« kaznivih dejanjih si predstavljamo dejanskega storilca, medtem ko o kibernetičnih storilcih to živo predstavo nekako izgubimo oziroma si je sploh ne ustvarimo (Bernik in Prislan 2012).

Splošni izraz za kibernetične kriminalce je »heker« (ang. *hecker*), obstaja pa več podskupin, ki se delijo glede na različne kriterije: npr. po stopnji tehničnega znanja, področju zanimanja, uporabi programske in strojne opreme. Te podskupine pa se nadalje delijo še na ožje kategorije. Bernik in Prislan (2012) navajata naslednje kategorije:

- novinci (ang. *Toolkit newbies*), ki imajo malo tehničnih veščin in uporabljajo že pripravljeno programsko opremo ter sledijo dokumentaciji, ki jih vodi skozi postopke uporabe programov.
- kiberpankerji (ang. *Cyber-punks*) – sami ustvarijo majhne programe, ki jih uporabljajo za defacing³, pošiljanje neželene pošte ali krajo kreditnih kartic.
- notranji (ang. *Internals*) – zaposleni ali nekdanji zaposleni, ki iz maščevanja želijo poškodovati sistem podjetja, pri napadu pa jim pomaga poznavanje varnostnih razmer v organizaciji, ne pa tehnično znanje.
- koderji (ang. *Coders*) – ustvarjalci kod, katerih namen je poškodovanje drugih sistemov.
- hekerji (ang. *Old-guard heckers*) – skrajšano hekerji, imajo visoko raven strokovnega znanja in v večini primerov nimajo kriminalnih namenov, ampak jih bolj zanima intelektualna in kognitivna stran hekerstva.

³ *Website defacement* (ang.) je napad na spletno stran, ki spreminja izgled spletne strani. Storitvi vdrejo v spletni strežnik in zamenjajo gostujočo spletno stran z eno od svojih strani (Wikipedia 2016č).

- profesionalci – njihovi nameni so kriminalne narave, zato so tudi najnevarnejša kategorija.

6.2 MOŽNE NEVARNOSTI IN ZLORABE NA SPLETU

Na vsakega uporabnika spleta prežijo številne nevarnosti. Dnevno brskamo po spletu, iščemo novice, podatke, stopimo v stik z mnogimi osebami, se vpisujemo v razna spletna družbena omrežja in posredujemo svoje osebne podatke.

Pred včlanitvijo v katerokoli družbeno omrežje, torej tudi v Facebook, se moramo seznaniti z možnimi nevarnostmi, ki prežijo na nas. In teh ni malo. V nadaljevanju predstavljam najpogostejše nevarnosti, ki na uporabnike prežijo v spletnih družbenih omrežjih.

6.2.1 Odtujitev ali okužba profila uporabnika

Če želimo dostopati do profila na Facebooku, pa tudi v drugih spletnih družbenih omrežjih, moramo vnesti uporabniško ime in geslo. Uporabniško ime je elektronski naslov, s katerim je profil povezan. Če se tretja oseba z uporabniškim imenom in geslom seznani, lahko dostopa do vseh podatkov, do katerih sicer lahko dostopa lastnik profila. Taka oseba lahko potem upravlja s profilom, pošilja zasebna sporočila, objavlja na zidu, lahko pa spreminja tudi nastavitve zasebnosti. Spremeni lahko tudi geslo za prijavo in elektronski naslov, ki je povezan s profilom ter tako lastniku onemogoči dostop do profila. Pri tem obstaja tudi možnost, da se tako odtujeni profil lahko uporabi za izvajanje različnih goljufij in pošiljanje spam-sporočil (Kaliopé 2011).

6.2.2 Lažna predstavljanja, zloraba identitete in nadlegovanje

Ko uporabnik ustvarja profil na Facebooku, mora navesti osebne podatke. Nastavi lahko tudi prikazno sliko, za katero pa ni nujno, da je njegova, pravzaprav lahko uporabi katerokoli sliko, ki jo dobi kjerkoli, tudi v spletu. Facebook nima mehanizmov, s katerimi bi lahko preverjal, ali so podatki resnični in točni, tako da se tisti, ki uporablja profil, lahko izdaja za kogarkoli, npr. za kakšno slavno osebo, politika, svojega prijatelja, znanca. Motivi za tako početje so različni, bodisi kdo to počne za šalo, huje pa je, če to počne iz maščevanja, takrat

ponavadi za prijatelje dodaja osebe, ki osebo, za katero se izdaja, poznajo. Na zidu potem lahko objavlja žaljive objave, fotografije ipd., kar ima lahko negativne posledice za dobro ime in čast osebe, na katere se objave nanašajo (Kaliopé 2011).

Prav o zlorabi identitete oziroma zlorabi osebnih podatkov prek spleta sem govorila tudi z gospo Margerito Jurkovič, direktorico Pravnega centra za varstvo človekovih pravic, ki je predstavila konkretni primer članice ženskega nogometnega kluba. Njena soigralka je dva meseca iz maščevanja zlorabljala njen Facebook profil in prek zasebnih sporočil in na zidu objavljala, da je uporabnica istospolno usmerjena. Prav tako jo je včlanjevala v različna društva, vdrla v njeno elektronsko pošto ter v njenem imenu pošiljala žaljiva sporočila njenim družinskim članom. Več o tem bo predstavljeno v intervjuju ob koncu diplomskega dela.

»Ukrasti« identiteto nekomu drugemu je na spletnem družbenem omrežju bistveno lažje kot v resničnem življenju. Če pa do tega vendarle pride, moramo o tem nemudoma obvestiti upravljalca strani.

Kako varna je moja identiteta, je najbrž vprašanje, ki si ga kdaj postavi vsakdo od nas. Zloraba identitete je namreč vedno pogostejši pojav in cena, ki jo plača žrtev take kraje, je lahko precej visoka. Včasih je namreč svoje dobro ime vse, kar imamo in če z njim ne ravnamo pametno in previdno, smo hitro lahko ob ves svoj sloves. Dober primer so številne znane in javne osebe, ki so za svoj status v družbi trdo garale, nato pa ga za vedno izgubile z eno samo nespametno potezo. Zloraba osebnih podatkov je naraščajoč pojav, ki ima mednarodne razsežnosti. K temu je zelo pripomogel razvoj in uporaba informacijsko-komunikacijskih tehnologij, ki so v vsakdanje življenje vnesle obdelavo velike količine podatkov, zlasti tistih, shranjenih v elektronski obliki, ki jih je mogoče najhitreje in najlažje zlorabiti. Nepridipravi se lahko dokopljejo do podatkov, s katerimi jim uspe zlorabiti bančne in kreditne kartice in podobno. Kraja identitete ni samo zloraba določenega osebnega podatka, saj je vedno povezana z namenom, da storilec s tem pridobi določeno korist. Pri nas kazenski zakonik kaznivega dejanja tatvine identitete ne pozna, jo pa inkriminira⁴ kot zlorabo osebnih podatkov. Kraja identitete je po navadi pripravljeno dejanje za kaznivo dejanje, lahko pa je tudi posledica že izvršenega kaznivega dejanja (Pirnat 2013).

4 **inkriminirati** inkriminirati –am dov. In nedov. (i) knjiž. obdolžiti, obtožiti: avtor inkriminira v svojem članku več oseb ♦ jur. določiti s kazenskim zakonom, da je kako dejanje kaznivo dejanje inkriminiran –a –o 1. Deležnik od inkriminirati: inkriminirana oseba / inkriminirano dejanje 2. napaden, grajan: inkriminirani članek; inkriminirana trditev

6.2.3 Ribarjenje ali »phishing«

Izraz ribarjenje podatkov (ang. *phishing*) izvira iz angleških besed za geslo (*password*) in ribarjenje (*fishing*). S pomočjo lažnih spletnih strani in elektronskih sporočil želijo spletni goljufi od uporabnikov izvabiti njihove osebne podatke, kot so npr. uporabniška imena in gesla, številke kreditnih kartic, digitalna potrdila in ostale osebne podatke. V ta namen uporabljajo različne tehnike. Praviloma najprej postavijo lažno spletno stran, ki je zelo podobna pravi, nato pa od uporabnika z lažnim elektronskim sporočilom poskušajo izvabiti obisk te spletne strani ali pa kar takoj pridobiti podatke uporabnika z njegovim odgovorom na to sporočilo. Za uporabnika, ki takšni goljufiji nasede, so posledice lahko relativno majhne ali pa tudi velike, npr. kraja denarja z bančnega računa (Informacijski pooblaščenec 2016a).

Obiskovalci spletnih strani morajo biti zelo previdni pri sporočanju podatkov. Če jih že pošiljajo po internetu, naj to počnejo le prek dobro zaščitene spletne povezave.

Priporočila Informacijskega pooblaščenca (2016a), kako se obraniti pred ribarjenjem podatkov:

- *naučiti se prepoznavati elektronsko pošto*, ki je namenjena prevari oziroma ribarjenju podatkov (uporaba imena in znanih oblikovnih elementov prave organizacije, npr. bank, podjetij; uporaba navidez resničnih imen zaposlenih v tej organizaciji, grožnja z izgubo podatkov, brisanjem računa ali podobnimi škodljivimi posledicami, če ne bi izvršili tistega, kar od nas zahtevajo, npr. sporočitev uporabniškega imena, ipd.);
- *preveriti vir prejetih sporočil* (banke svojim komitentom ne nagovarjajo prek e-pošte, predvsem pa od njih ne zahtevajo osebnih podatkov, kot so uporabniška imena in gesla oziroma ne pozivajo k izvozu digitalnega potrdila);
- *ne klikati povezav v e-pošti*, ki se na videz zdijo kot prava povezava do banke, prek katere poslujemo (bolje je uporabiti zaznamke oziroma bližnjice (ang. *bookmarks* ali *favourites*), ki smo jih predhodno shranili v naš brskalnik);
- *preveriti, ali smo na pravi strani* (predvsem moramo preveriti, ali je povezava do spletnega mesta varovana s tako imenovanim varnim http-protokolom – v tem primeru se ime domene začne s https: \\\..., v vrstici stanju na dnu okna v brskalniku pa mora biti prikazana zaklenjena ključavnica. Pri tem je treba biti pozoren na druga priporočila, saj v primeru, če se na našem

računalniku nahaja nevarna programska oprema, tudi ta korak ne more zavarovati pred izgubo podatkov in ostalimi posledicami. Razlike med pravimi in lažnimi stranmi so lahko minimalne, za nekatere organizacije pa poleg tega obstaja poleg prave domene tudi več deset zelo podobnih registriranih domen (npr. spletnabanka.com, spletna-banka.com, login-spletnabanka.com...);

– *poskrbeti je treba za varnost računalniškega sistema* (redno je treba nameščati varnostne popravke operacijskega sistema, uporabljati in redno posodabljati protivirusne programe, ni priporočljivo nameščati programov s sumljivih spletnih mest in prav tako ne odpirati sporočil neznanih pošiljateljev, še zlasti ne tistih, s priponkami izvršljivih programov, kot so npr. exe. ali .bat datoteke);

– *uporabljati je treba zadnje različice brskalnikov z zadnjimi varnostnimi popravki.*

6.2.4 Možne negativne posledice objav

Uporabniki na svojem profilu lahko objavljajo fotografije, videoposnetke, komunicirajo s prijatelji, objavljajo svoje aktivnosti. Uporabnik lahko svoje objave tudi sproti briše, lahko pa se zgodi, da na to pozabi. A rek, kar je enkrat na internetu, tam tudi ostane, še vedno velja. Za uporabnika lahko v primeru, da podatkov ne briše, nastanejo zelo negativne posledice.

Že nekaj časa na TV-sprejemnikih gledamo oglas mlade ženske na razgovoru za službo. Medtem ko se delodajalec z njo pogovarja, na računalniku gleda njen profil in njene fotografije, ki niso primerne za objavo, zato se odloči, da takšne osebe v svojem podjetju ne bo zaposlil. »Ne objavi, kar te lahko gnjavi« (Marketing magazin 2015), ker nikoli ne veš, kdaj ti bodo nespodobne fotografije, na katere si morda že pozabil, škodile. Pred objavljanjem v spletu moramo dobro premisliti, kaj bomo objavili, da se ne bomo kdaj soočali s posledicami svojih nepremišljenih objav.

6.3 ZAŠČITA ZASEBNOSTI V SPLETU

Zasebnost je nekaj, na kar smo vsi občutljivi. Uporabniki Facebooka in drugih spletnih družbenim omrežij imajo na svojem profilu vnesenih veliko osebnih podatkov. Le-ti pa niso namenjeni vsem, ampak samo tistim, za katere se tako odločijo lastniki profila.

Za zaščito varnosti v spletu lahko poskrbimo na različne načine:

- *uporabljamo dolga in zapletena gesla* (pri tem ne uporabljamo istih gesel za različne stvari, gesla naj bodo naša skrivnost);
- *poskrbimo za ustrezne nastavitve zasebnosti v spletnih družbenih omrežjih*;
- *vsake toliko časa preverimo naše podatke v spletu* (v Google vpišemo svoje ime in priimek in preverimo, kateri podatki so objavljeni v spletu);
- *v spletu objavljamo le stvari, ki jih lahko vidi kdorkoli, še posebej to velja za fotografije* (kar je enkrat objavljeno, je težko oziroma nemogoče izbrisati, saj ne vemo, kam vse se je že razširilo, kdo si je to skopiral, shranil, posredoval naprej in bo spet objavil);
- *spoštujemo in zaščitimo tudi zasebnost drugih* (objavljanje slik brez dovoljenja/označevanje oseb na slikah je groba kršitev);
- *v spletu ne objavljamo svojih podatkov za stik* (priimka, imena, naslova bivanja, telefonske številke, naslova elektronske pošte ter drugih osebnih podatkov, kot so davčna številka, datum rojstva, številka kreditne kartice ipd.)
- *ne odgovarjamo na elektronska pisma, ki od nas zahtevajo osebne in finančne podatke* (legitimna podjetja takšnih zahtev nikoli ne pošiljajo po elektronski pošti ali prek spleta) (Safe.si 2016).

Kovačič (2003) izpostavlja, da problem varnosti in s tem tudi zasebnosti ni samo tehnični, ampak je tudi družbeni problem. Kar pomeni, da se morajo uporabniki računalnikov bolj zavedati različnih zlorab, predvsem pa, kako se pred njimi kar se da dobro zavarovati. Čeprav noben sistem ni stoo odstotno varen, pa je mogoče varnost precej povečati s samozaščitnim ravnanjem. Potrebno se je zavedati, da varnost ni izdelek oziroma nekaj, kar lahko kupimo, pač pa je proces. Varnostno kulturo je treba razvijati in jo neprestano gojiti (Kovačič 2003).

6.4 ZAŠČITA ZASEBNOSTI V SPLETNEM DRUŽBENEM OMREŽJU FACEBOOK

Facebook uporabnikom nudi šest nasvetov, kako lahko zaščitijo svoj račun (Facebook 2016b):

- zavarujte svoje geslo – ne uporabljajte vašega Facebook-gesla na drugih spletnih mestih; ne izdajte gesla drugim, geslo naj bo znano samo vam; pri sestavljanju gesla se izogibajte uporabi vašega imena in besed v zvezi z vami, geslo mora biti kompleksno in težko uganljivo,
- uporabljajte dodatne nastavitve zasebnosti,
- poskrbite, da je(so) vaš(i) elektronski račun(i) varen(i),
- vselej ko uporabljate računalnik, ki ga delite z drugimi, se izpišite iz Facebook-računa. Če ste se pozabili izpisati, lahko naredite to na daljavo. Facebook nudi možnost vpogleda v seznam vseh naprav, na katerih ste prijavljeni vanj. Seznam prav tako beleži vse brskalnike in naprave, prek katerih ste se v preteklosti vpisovali v Facebook. Vsak vpis na seznamu vsebuje datum, čas in približno lokacijo ob prijavi (lokacija temelji na IP-naslovu naprave), kot tudi podatke o sami napravi, s katere ste se v Facebook prijavili. Na tem mestu se lahko uporabnik tudi izpiše iz teh naprav, bodisi iz računalnika, telefona ali tablice.
- uporabljajte protivirusne programe,
- dvakrat premislite, preden kliknete ali prenašate kakršne koli datoteke.

7 EMPIRIČNI DEL

7.1 OPREDELITEV PROBLEMA

Namen empiričnega dela je podrobneje raziskati seznanjenost uporabnikov spletnega družbenega omrežja Facebook z varnostjo in zasebnostjo pri uporabi tega omrežja. Zanimalo me je, kako varne se uporabnikom zdijo informacije, ki jih posredujejo na Facebook, ali spremljajo politike zasebnosti, ali posodablajo nastavitve svojega profila, ali so seznanjeni s tem, na koga se lahko obrnejo v primeru, če je ogrožena njihova zasebnost. Prav tako sem z anketo skušala zbrati podatke o tem, kako pomembna sta jim varnost in zasebnost in ali bi želeli izvedeti še več o nevarnostih, ki jih prinaša uporaba oz. če sploh poznajo nevarnosti, ki jih prinaša objava osebnih podatkov v spletu.

Za potrebe diplomskega dela sem uporabila metodo anketiranja prek spleta in v ta namen pripravila anketni vprašalnik. Anketni vprašalnik je obsegal 20 vprašanj in je bil razdeljen na splošni in vsebinski del. V prvem delu so bila anketirancem zastavljena demografska vprašanja o spolu, starosti, statutu in zaključeni izobrazbi. V drugem delu so anketiranci odgovarjali na vprašanja, na podlagi katerih sem potrdila oziroma ovrgla zastavljene hipoteze, in sicer:

1. HIPOTEZA: Za varnost in zasebnost v spletnem družbenem omrežju Facebook je dobro poskrbljeno.
2. HIPOTEZA: Mlajši uporabniki Facebooka bolj redno posodablajo svoje nastavitve zasebnosti na Facebooku.

7.2 METODOLOGIJA IN ZBIRANJE PODATKOV

Tematiko sem preučevala s kvantitativno metodo, s pomočjo anketnega vprašalnika.

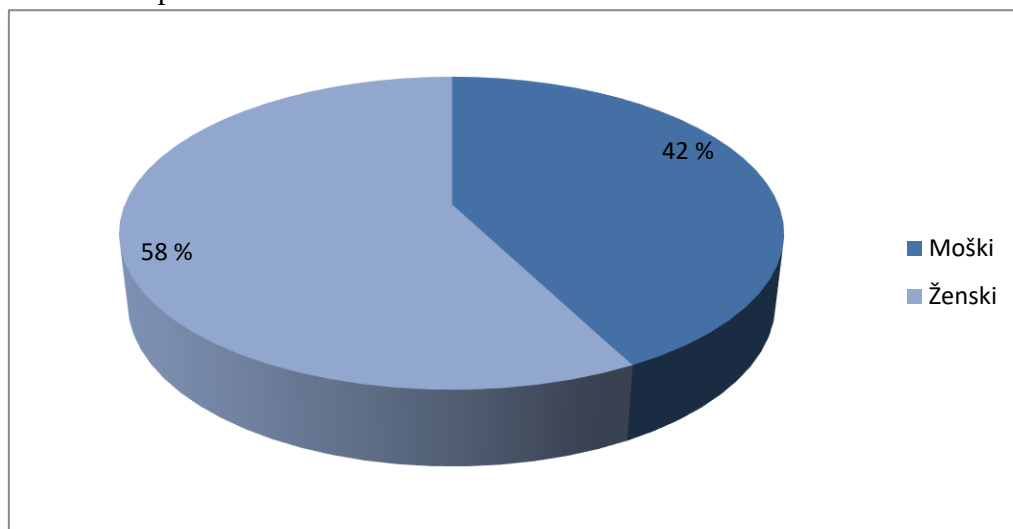
Anketo sem izvedla v obliki spletne ankete, povezava do nje je bila objavljena v spletnem družbenem omrežju Facebook, tako da so bili anketiranci dejanski uporabniki Facebooka. Med zasebnimi sporočili na Facebooku sem ustvarila skupino prijateljev, katerim sem poslala povezavo do ankete. Prednost spletnih anket je v anonimnosti, enostavnosti izpolnjevanja, podatke zberemo v relativno kratkem času, po drugi strani pa ima taka anketa tudi slabosti, saj

anketirancev ne poznamo, tudi jim ne moremo svetovati in pomagati pri izpolnjevanju ankete, vprašanje pa je seveda tudi, ali so odgovori na vprašanja (v primeru nejasnosti) resnično taki, kot jih anketiranci želijo podati. Anketa je bila odprta od 8. junija 2016 do 13. junija 2016, nanjo pa se je odzvalo oziroma jo je izpolnilo 151 anketirancev. V anketo so bile zajete osebe, stare od 13 pa do 40 let in več, in sicer po posameznih starostnih skupinah; od 13–18 let, 19–24 let, 25–31 let, 32–40 let in več kot 40 let. Spletno anketo je izpolnilo 151 oseb, kar zagotavlja dovolj reprezentativen vzorec za določitev posameznih značilnosti uporabnikov.

7.3 REZULTATI: ANALIZA VPRAŠANJ

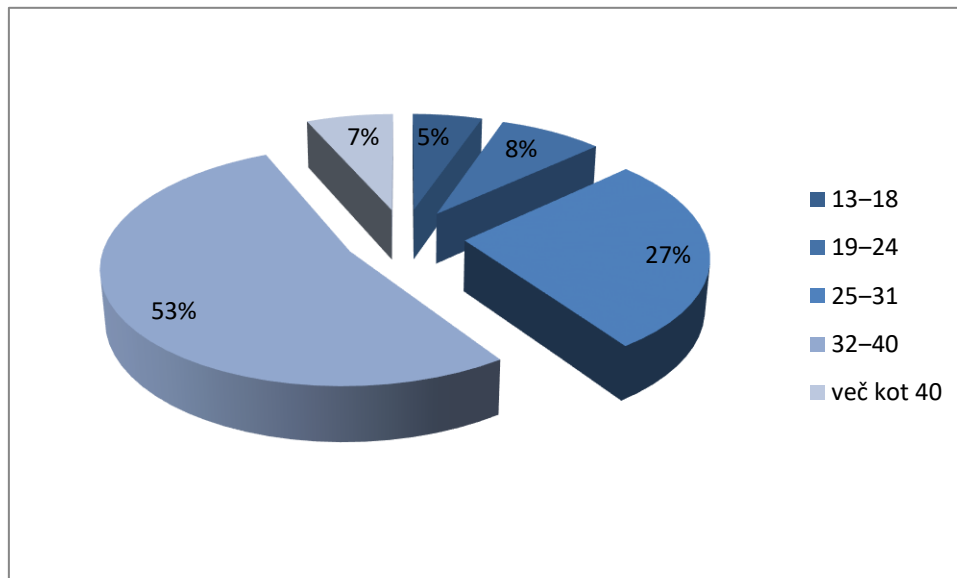
V raziskavi je sodelovalo 151 anketirancev, ki so aktivni uporabniki spletnega družbenega omrežja Facebook.

Graf 7.1: Spol



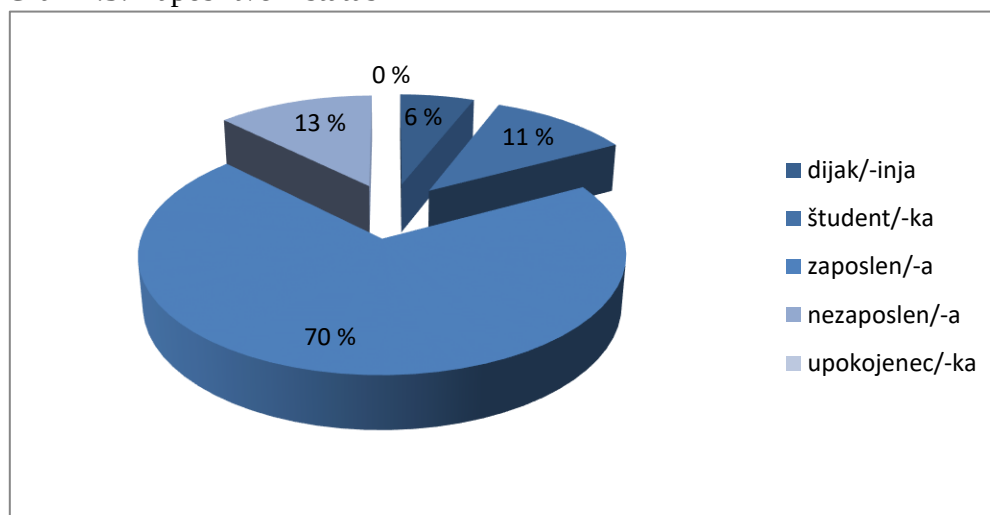
Od 151 anketirancev je bilo 87 (58 %) žensk in 64 (42 %) moških. Med tistimi, ki so izpolnili ankete, so torej prevladovalе ženske (Graf 7.1).

Graf 7.2: Starost



Več kot polovica anketirancev, kar 53 % (80), je bila starih med 32 in 40 let. S 27 % (41) sledi skupina anketiranih, starih od 25 do 31 let. Stari med 19–24 let predstavljajo 8 % (12) anketiranih, 7 % (10) anketiranih je starih od 32–40 let, samo 5 % (8) pa je takih, ki so stari nad 40 let (Graf 7.2).

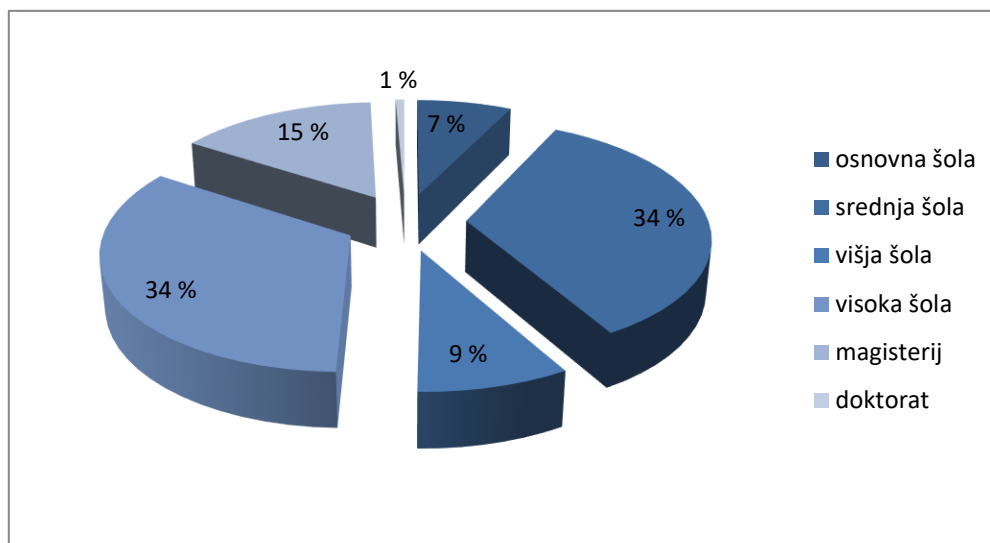
Graf 7.3: Zaposlitveni status



Glede na zaposlitveni status smo anketirance razdelili v 5 statusnih kategorij: dijak/-inja, študent/-ka, zaposlen/-a, nezaposlen/-a in upokojenec/-ka. Iz dobljenih podatkov je razvidno, da je kar 70 % zaposlenih (106), 13 % je brezposelnih (19), z 11 % sledijo tisti, ki imajo status študenta (17), 6 % jih ima status dijaka (9), nihče od anketiranih pa ni upokojenec ali

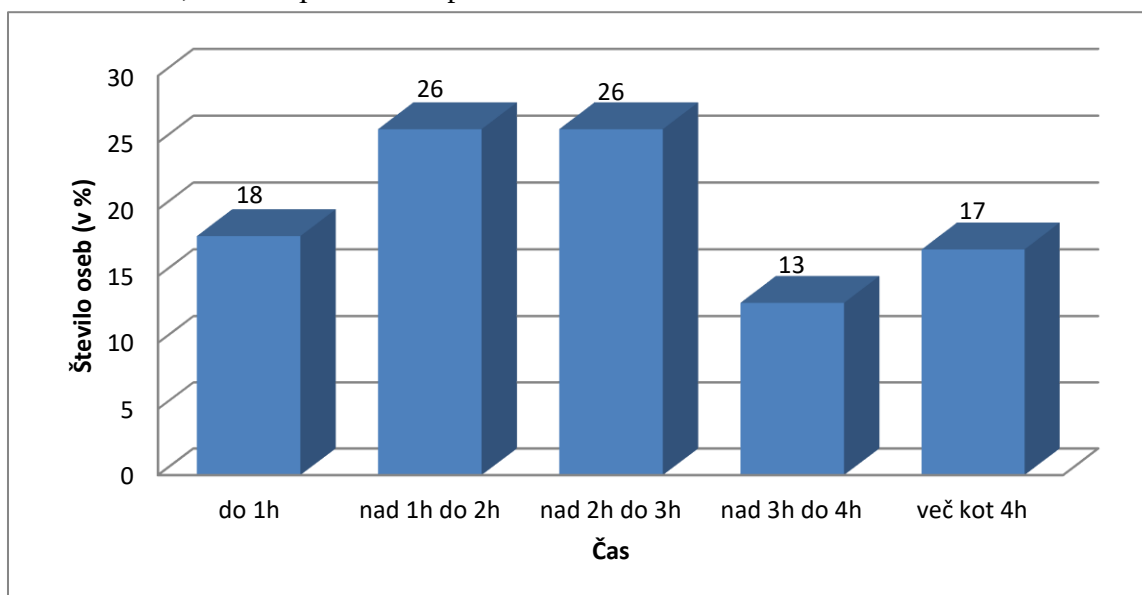
upokojenka (Graf 7.3).

Graf 7.4: Izobrazba



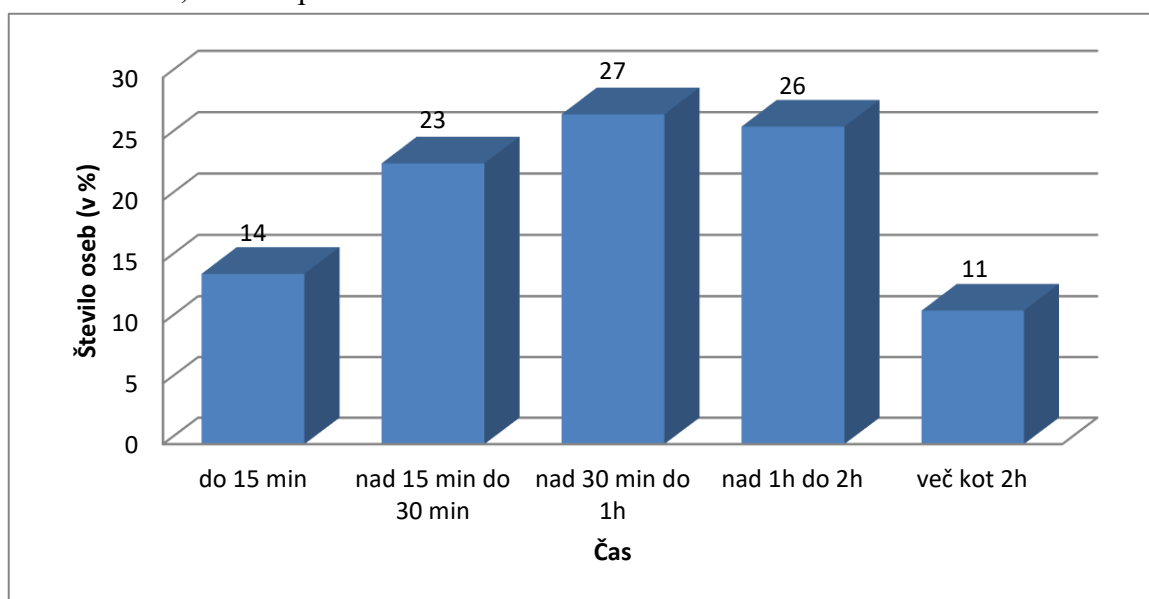
Anketirance smo spraševali tudi po stopnji izobrazbe. Ugotovili smo, da ima približno enako število anektiranih visoko ali srednjo izobrazbo. 34 % (52) jih ima zaključeno srednjo šolo, prav tako pb. 34 % (51) jih ima visokošolsko izobrazbo. S 15 % (23) sledijo tisti z magisterijem, 9 % (13) jih ima zaključeno višjo šolo. Nekoliko manj, 7 % (11) anketirancev, ima končano osnovno šolo, zgolj 1 % (1) pa ima doktorat (Graf 7.4).

Graf 7.5: Čas, dnevno preživet v spletu



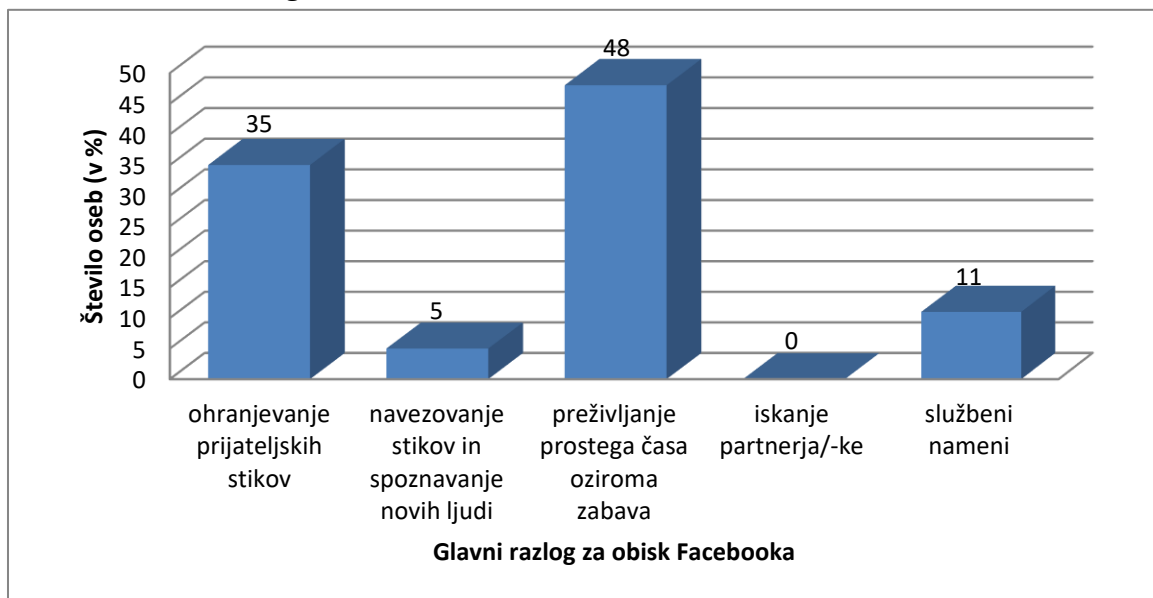
Pri naslednjem vprašanju nas je zanimalo, koliko časa povprečno anketirani uporabniki preživijo v spletu. Največ anketirancev, 40 (26 %), je odgovorilo, da v spletu preživijo na dan povprečno več kot 1 in manj kot 2 uri, eden manj, torej 39 (26 %), pa jih je odgovorilo, da povprečno dnevno brskajo po spletu več kot 2 in manj kot 3 ure. 27 (18 %) jih v spletu dnevno preživi do največ ene ure, 26 (17 %) od vseh anketirancev jih v povprečju na dan po spletu brska več kot 4 ure, 19 (13 %) pa več kot 3 in manj kot 4 ure dnevno. Večina anketiranih torej brska po spletu med eno in tremi urami dnevno, takih je skupno 52 % (Graf 7.5).

Graf 7.6: Čas, dnevno preživet na Facebooku



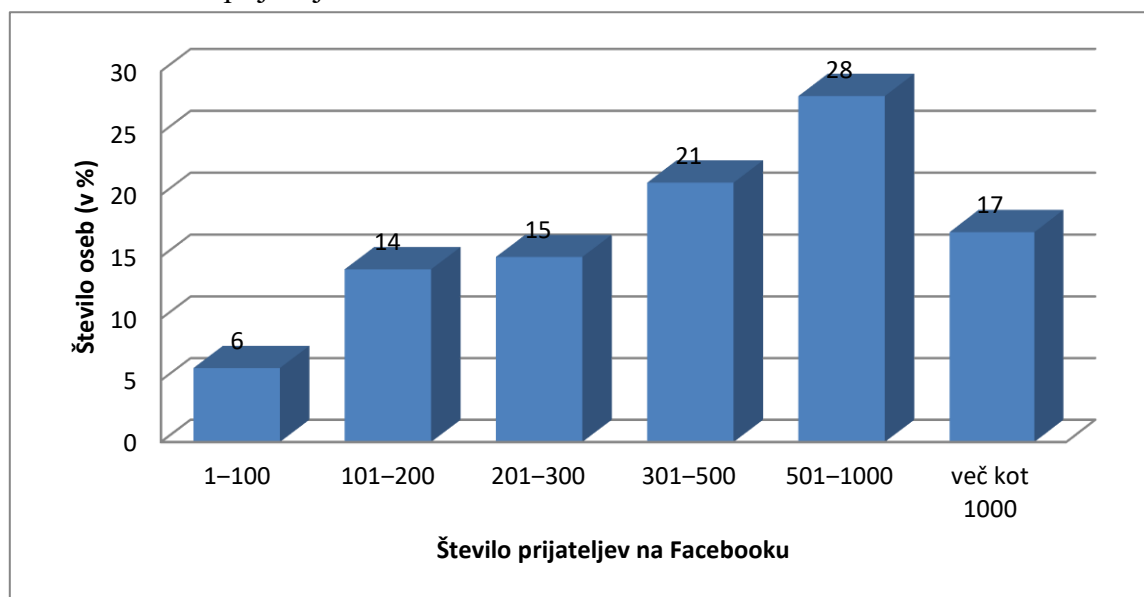
Kot šesto smo anketirancem zastavili vprašanje, koliko časa na dan v povprečju preživijo na Facebooku. Iz grafa 7.2 je razvidno, da 41 anektiranih (27 %) dnevno preživi na Facebooku od 30 minut do eno uro, sledijo tisti od ene do dve uri dnevno, takih je 39 (26 %). 34 anketiranih (22 %) na Facebooku preživijo povprečno od 15 do 30 minut, 21 (14 %) jih preživi na Facebooku do 15 minut, le 16 (11 %) pa je takih, ki dve uri ali več dnevno uporabljajo Facebook (Graf 7.6).

Graf 7.7: Glavni razlog za obisk Facebooka



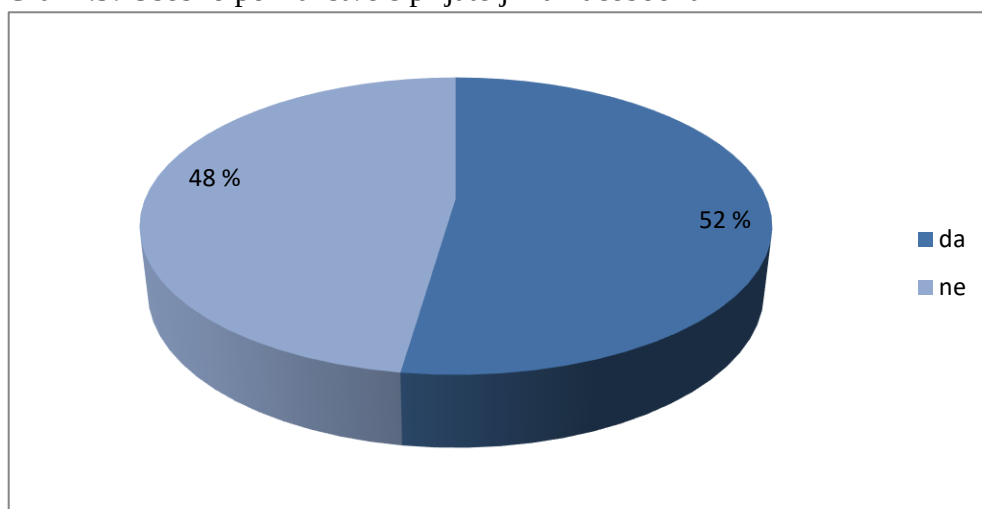
Zanimalo nas je tudi, kaj je pri anketiranih glavni razlog za obisk Facebooka. Dobili smo naslednje odgovore; največ, kar 73 anketiranih, to je skupno 48 %, uporablja Facebook za preživljanje prostega časa oziroma zabavo. Sledijo jim tisti, 53 jih je (35 %), ki preko Facebooka ohranjajo prijateljske stike. Zgolj 17 (11 %) jih uporablja Facebook za službene namene, 8 (5 %) pa za navezovanje stikov in spoznavanje novih ljudi. Zanimivo pa je, da nihče od anketiranih prek Facebooka ne išče partnerja ali partnerke; najverjetneje zato, ker za to obstajajo števila druga spletna družbena omrežja (Graf 7.7).

Graf 7.8: Število prijateljev na Facebooku



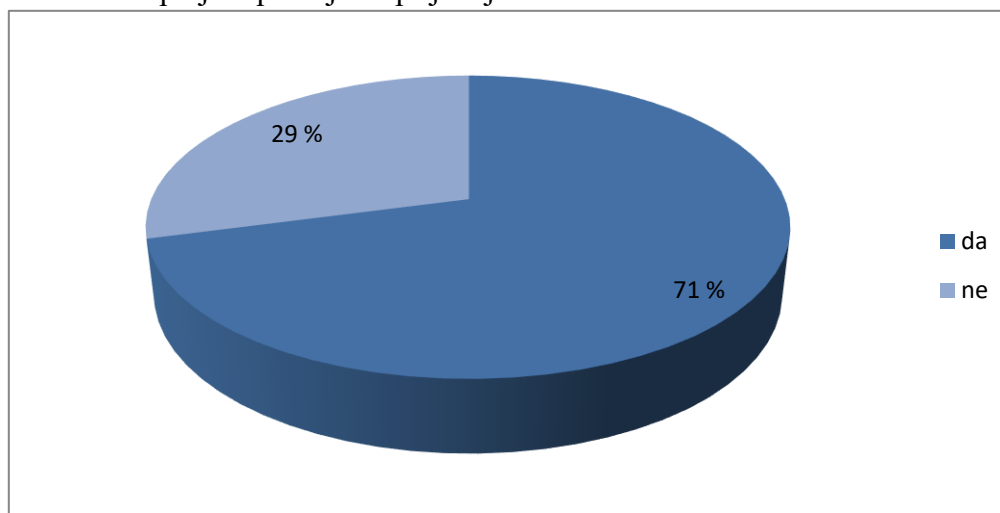
Anketirance smo spraševali, koliko prijateljev imajo na Facebooku. Večina med njimi, 42, ima na Facebooku med 501 in 1000 prijateljev, kar znaša 28 % anketiranih. Sledijo tisti, ki imajo med prijatelji 301–500 oseb, teh je 31, kar predstavlja 20 %, 25 anektiranih (17 %) je takih, ki imajo na Facebooku več kot 1000 prijateljev. 23 anketiranih (15 %) ima na Facebooku od 201 do 300 prijateljev, sledijo anketirani, 21 jih je (14 %), ki imajo med 101 in 200 prijateljev, le 9 (6 %) anketiranih pa ima med 1 in 100 prijateljev (Graf 7.8).

Graf 7.9: Osebno poznanstvo s prijatelji na Facebooku



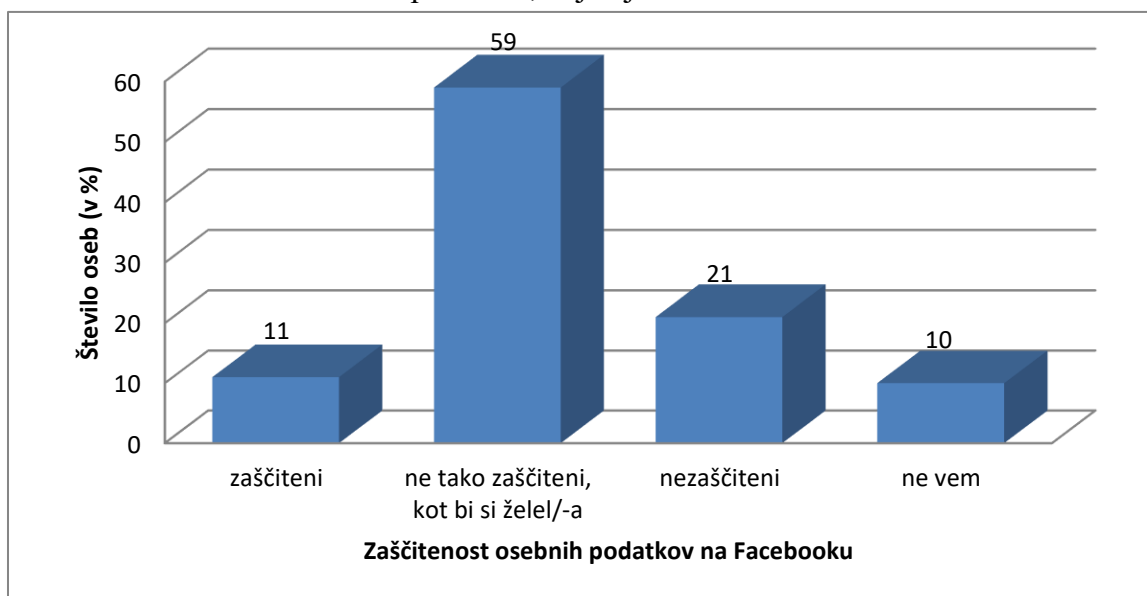
V devetem vprašanju smo anketirance spraševali, ali osebno poznajo vse prijatelje, ki jih imajo na Facebooku. Rezultat odgovorov je bil precej izenačen. 79 (52 %) anketirancev je odgovorilo, da osebno poznajo vse prijatelje, ki jih imajo na Facebooku, 72 (48 %) pa jih je odgovorilo, da vseh svojih prijateljev, ki jih imajo na spletnem družbenem omrežju Facebook, ne poznajo osebno (Graf 7.9).

Graf 7.10: Sprejem prošnje za prijateljstvo od neznane osebe



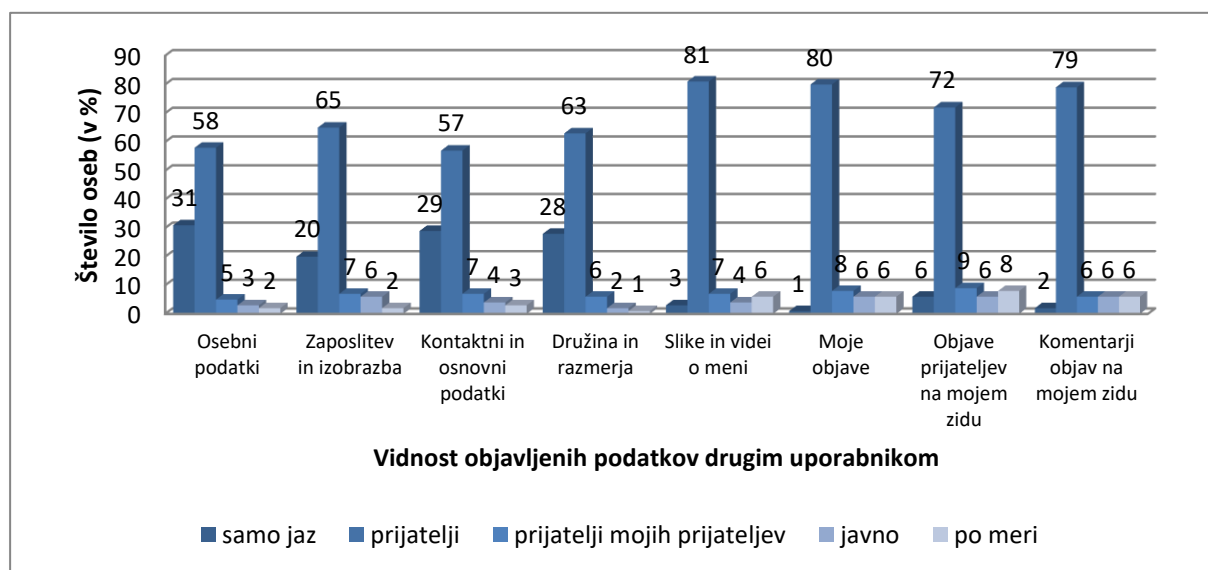
Na vprašanje, ali so že kdaj sprejeli prošnjo za prijateljstvo osebe, ki je ne poznajo, je večina anketiranih odgovorila pritrdilno, in sicer kar 71 % anketirancev (107), preostalih 29 % (44) pa je odgovorilo, da nikoli niso sprejeli prošnje za prijateljstvo osebe, ki je ne poznajo (Graf 7.10).

Graf 7.11: Zaščitenost osebnih podatkov, objavljenih na Facebooku



Ko smo anketirance spraševali, kako zaščiteni se jim zdijo podatki, ki jih objavljajo na Facebooku, smo dobili naslednje odgovore: velika večina vprašanih, kar 89 (59 %) jih meni, da niso tako zaščiteni, kot bi si želeli. 31 anketiranih (21 %) je mnenja, da podatki niso zaščiteni, 16 (11 %) jih meni, da so objavljeni podatki zaščiteni, 15 od 151 (11 %) pa tega ne ve (Graf 7.11).

Graf 7.12: Nastavitve zasebnosti



To vprašanje je bilo za anketirance najbolj kompleksno, zanimalo pa nas je, s kom delijo osebne podatke, podatke o zaposlitvi in izobrazbi, podatke za stik in osnovne podatke, podatke o družini in razmerju, slike in osebne videoposnetke, svoje objave, objave prijateljev na svojem zidu in komentarje objav na svojem zidu. Izbirali so lahko med odgovori: javno, prijatelji, samo jaz, prijatelji mojih prijateljev in po meri.

Osebne podatke s prijatelji deli 87 (58 %) anektiranih, 47 (31 %) anketiranih ima dostop do osebnih podatkov nastavljen tako, da jih vidijo le oni, 8 (5 %) vprašanih je odgovorilo, da so njihovi objavljeni osebni podatki vidni prijateljem njihovih prijateljev, samo 5 (3 %) ima podatke javno dostopne in 3 (2 %) imajo nastavitve po meri, 1 od vprašanih pa se ni opredelil, s kom deli osebne podatke v omrežju Facebook.

Podatke o zaposlitvi in izobrazbi deli s prijatelji 94 (65 %) vprašanih; da so njihovi podatki o zaposlitvi in izobrazbi vidni le njim, je odgovorilo 29 (20 %) anketiranih, sledijo tisti, ki te podatke delijo s prijatelji svojih prijateljev, takih je 10 (7 %), 9 oziroma 6 % je takih, ki le-te delijo z javnostjo, 3 (2 %) imajo pri teh podatkih nastavitve po meri. 6 anketirancev se ni opredelilo, s kom delijo podatke o zaposlitvi in izobrazbi.

Podatke za stik in osnovne podatke s prijatelji deli 84 (57 %) vprašanih, 43 (29 %) so taki podatki vidni samo njim samim, 10 (7 %) deli podatke s prijatelji svojih prijateljev, 6 (4 %) ima javno objavljene podatke za stik in osnovne podatke, 4 (3 %) ima nastavitve po meri, 4 pa se niso opredelili, s kom delijo podatke za stik in osnovne podatke v Facebooku.

Podatki o družini in razmerju so prijateljem vidni pri 9 (63 %) anketiranih, 41 (28 %) ima take nastavitve, da so vidni ti podatki samo njim, 8 (6 %) vprašanih te podatke deli s prijatelji svojih prijateljev, 3 (2 %) imajo te podatke vidne javnosti, 2 (1 %) imata nastavitve po meri, 6 se jih ni opredelilo, s kom delijo podatke o družini in razmerju.

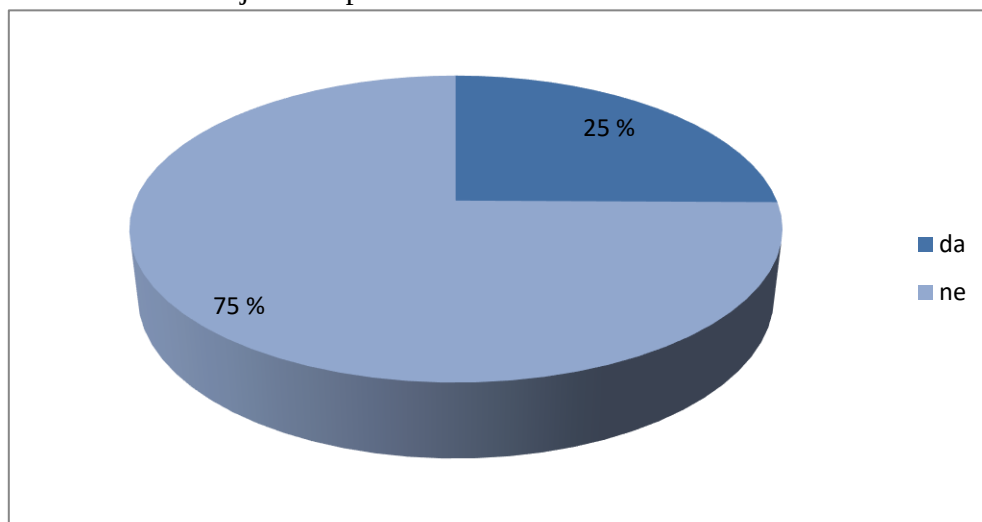
Fotografije in lastne videoposnetke s svojim prijatelji deli 117 (81 %) anketiranih, 10 (7 %) jih te podatke deli s prijatelji svojih prijateljev, 8 (6 %) ima nastavitve po meri, 6 (4 %) fotografije in lastne videoposnetke deli z javnostjo ter 4 (3 %) je takih, ki imajo take nastavitve, da to lahko vidijo le oni. 6 se jih ni opredelilo, s kom delijo fotografije in lastne videoposnetke v spletnem družbenem omrežju Facebook.

Lastne (svoje) objave s prijatelji deli 116 (80 %) anektiranih, sledijo jim tisti, takih je 11 (8 %), ki imajo take nastavitve, da to lahko vidijo prijatelji njihovih prijateljev, 8 (6 %) ima nastavitve javne, prav tako 8 (6 %) jih ima nastavitve po meri, le 2 (1 %) imata nastavitve nastavljene tako, da lahko samo ona vidita svoje objave v Facebooku. 6 vprašanih ni odgovorilo, s kom delijo svoje lastne objave.

Objave prijateljev na svojem zidu deli med prijatelje 105 (72 %) vprašanih, 13 (9 %) te podatke deli s prijatelji svojih prijateljev, 11 (8 %) jih ima nastavitve po meri, 8 (6 %) ima te podatke javno dostopne, prav tako je 8 (6 %) takih, ki zgolj sami dostopajo do teh podatkov, 6 pa se jih ni opredelilo, s kom delijo objave prijateljev na svojem zidu.

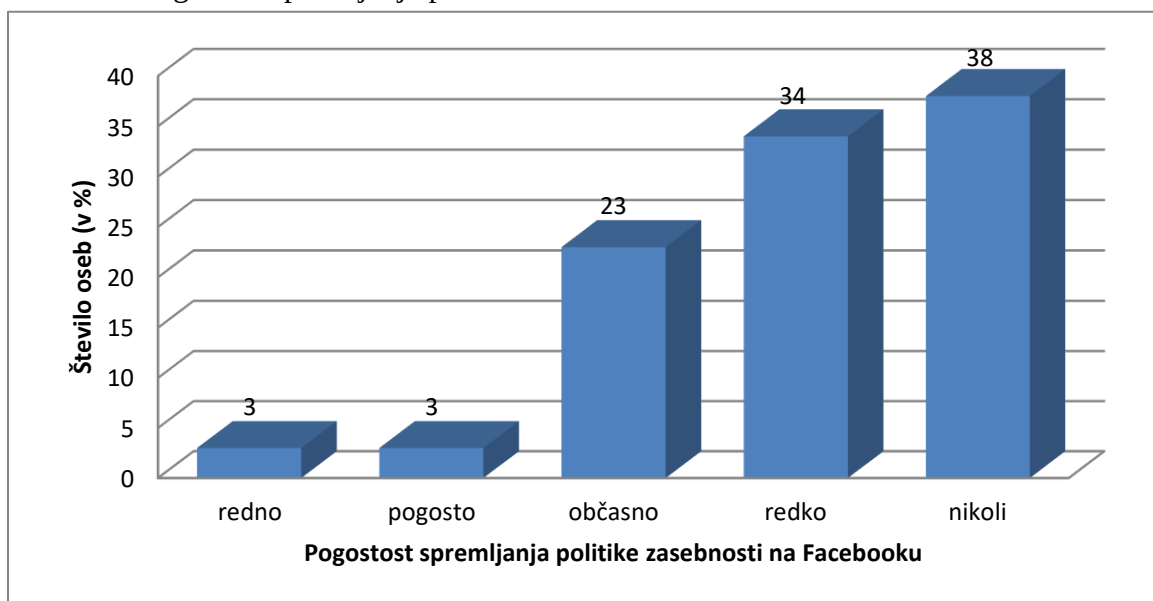
Komentarje objav na svojem zidu s prijatelji deli 115 (79 %) anketiranih, 9 (6 %) jih komentarje deli javno, 9 (6 %) jih ima nastavitve po meri, 9 (6 %) jih komentarje deli s prijatelji svojih prijateljev, le 3 (2 %) imajo take nastavitve, da so ti komentarji vidni le njim, 6 se jih ni opredelilo, s kom delijo komentarje objav na svojem zidu (Graf 7.12).

Graf 7.13: Seznanjenost s politiko zasebnosti na Facebooku



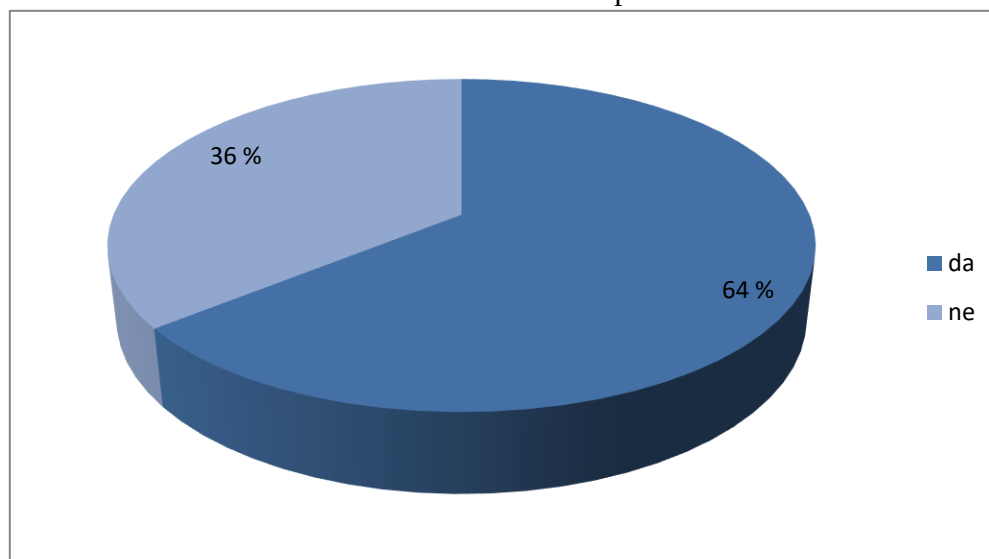
Na vprašanje, ali so prebrali politiko zasebnosti v spletnem omrežju Facebook, jih je velika večina, kar 113 (75 %) anketirancev, odgovorila, da je ni prebrala. Politiko o varovanju osebnih podatkov je prebralo le 38 (25 %) anketirancev (Graf 7.13).

Graf 7.14: Pogostost spremljanja politike zasebnosti na Facebooku



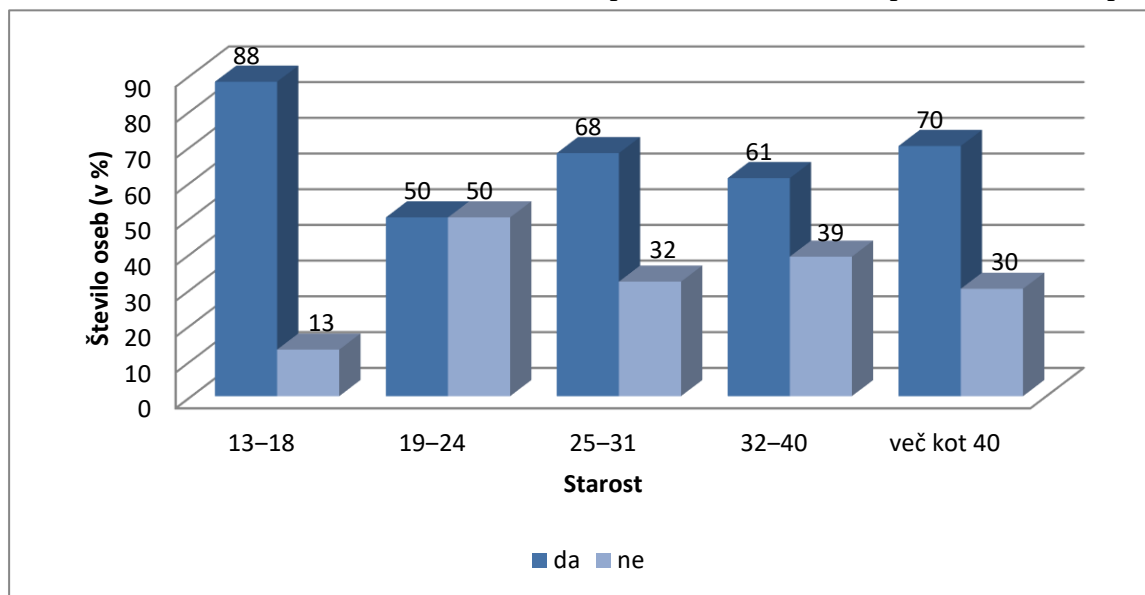
Pri tem vprašanju nas je zanimalo, kako pogosto anketiranci spremljajo politike zasebnosti, ki jih izdaja Facebook. Presenetljivo veliko je bilo takih, kar 57 (38 %), ki tega nikoli ne spremlja. Takih, ki to redno spremljajo, je bilo 51 (34 %), občasno se s tem seznani 34 (22 %) anketiranih, sledijo tisti, ki se s tem pogosto seznanjajo in jih je relativno malo, zgolj 5 (3 %), še manj, samo 4 (3 %) pa so tisti, ki se s tem redno seznanjajo (Graf 7.14).

Graf 7.15: Posodobitve in varnostne nastavitve profila na Facebooku



Na vprašanje, ali anketiranci posodablajo in spremljajo varnostne nastavitve profila na Facebooku, je večina le-teh, kar 64 % (97), odgovorila, da to počne, 36 % (54) pa je bilo takih, ki profila ne posodabljajo niti ne spremljajo varnostnih nastavitev profila (Graf 7.15).

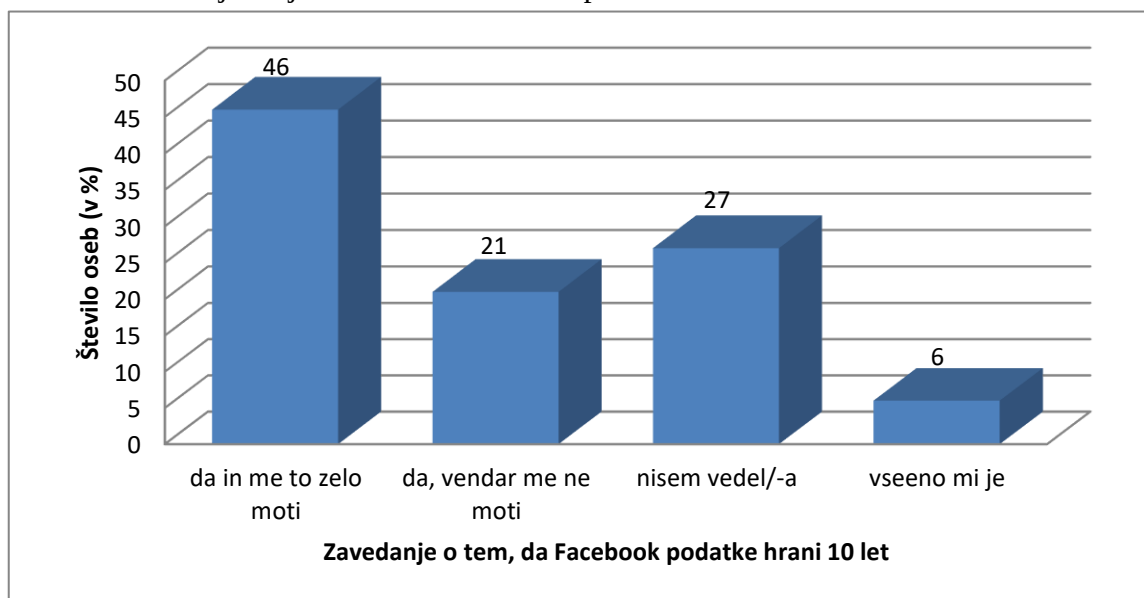
Graf 7.16: Posodobitve in varnostne nastavitve profila na Facebooku po starostnih skupinah



Graf 7.16 prikazuje, v kolikšni meri anketirani uporabniki spletnega družbenega omrežja Facebook različnih starostnih skupin posodabljajo in spremljajo varnostne nastavitve svojih profilov v omenjenem omrežju. Vidimo, da 7 (88 %) od vprašanih, starih od 13 in 18 let, redno posodablja in spremlja varnostne nastavitve svojih profilov na Facebooku, medtem ko 1

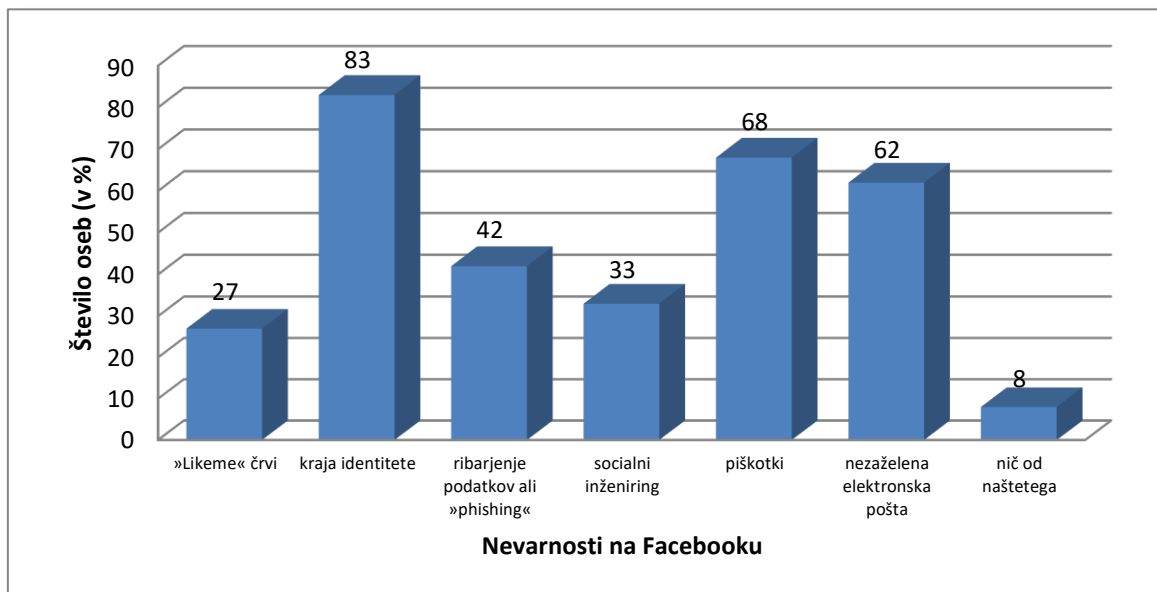
(13 %) tega ne počne. V starostni skupini od 19 do 24 let je razmerje izenačeno, saj jih 6 (50 %) posodablja svoj profil, 6 (50 %) pa jih tega ne počne. V skupini, starih od 25 do 31 let, 28 (68 %) od vprašanih posodablja in spremlja varnostne nastavitve, 13 (32%) pa jih tega ne počne. V skupini anketirancev, starih od 32 do 40 let, jih je 49 (61 %) odgovorilo, da to počne, 31 (39 %) pa, da tega ne počne. Med starejšimi od 40 let je 7 (70 %) anketirancev odgovorilo, da posodablja in spremlja varnostne nastavitve svojih profilov na Facebooku, 3 (30 %) anketiranci pa tega ne počno.

Graf 7.17: Shranjevanje in obdelava osebnih podatkov na Facebooku



Ko smo anketirance povprašali o tem, ali se zavedajo, da ima Facebook po izbrisu profila pravico vsaj še deset let hraniti in obdelovati njihove osebne podatke, nam je velika večina potrdila, da se tega zaveda in da jih to zelo moti, takih je bilo kar 69 (46 %). 41 vprašanih (27 %) tega ni vedela, 32 (21 %) je bilo takih, ki so to vedeli, a jih ne moti, 9 (6 %) pa je za to vseeno (Graf 7.17).

Graf 7.18: Nevarnosti objave osebnih podatkov na Facebooku



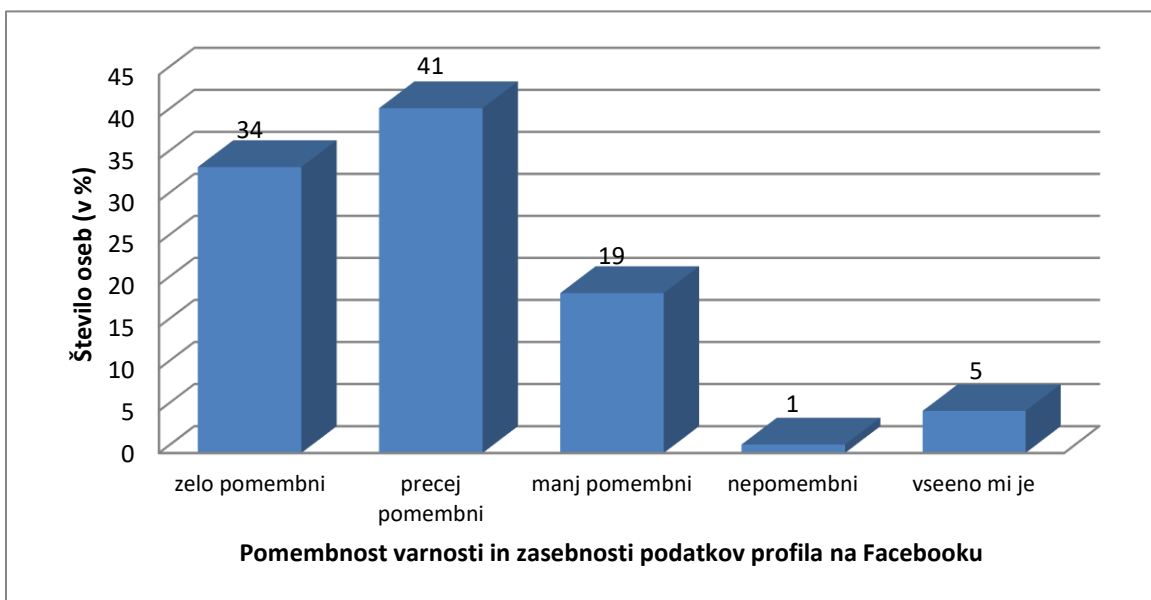
Pri tem vprašanju je bilo možnih več odgovorov. Skušali smo izvedeti, ali anketiranci poznajo nevarnosti, ki jih prinaša objavljanje osebnih podatkov na Facebooku. Največ, kar 125 od 151 (83 %) jih je seznanjenih z možnostjo kraje identitete. Prav tako veliko anketiranih pozna piškotke, takih je 102 (68 %). 94 od vprašanih (62 %) jih pozna možnost nezaželenih elektronskih sporočil oziroma pošte. Nekoliko manj, 64 anketiranih (42 %) je takih, ki so že slišali za ribarjenje podatkov oz. phishing, 50 (33 %) pa je takih, ki poznajo družbeni inženiring. Tako imenovane „črve“ pozna 41 od 151 anketiranih (27 %), le 12 (8 %), pa je takih, ki ne pozna ničesar od naštetega (Graf 7.18).

Graf 7.19: Prijava v primeru ogrožene zasebnosti



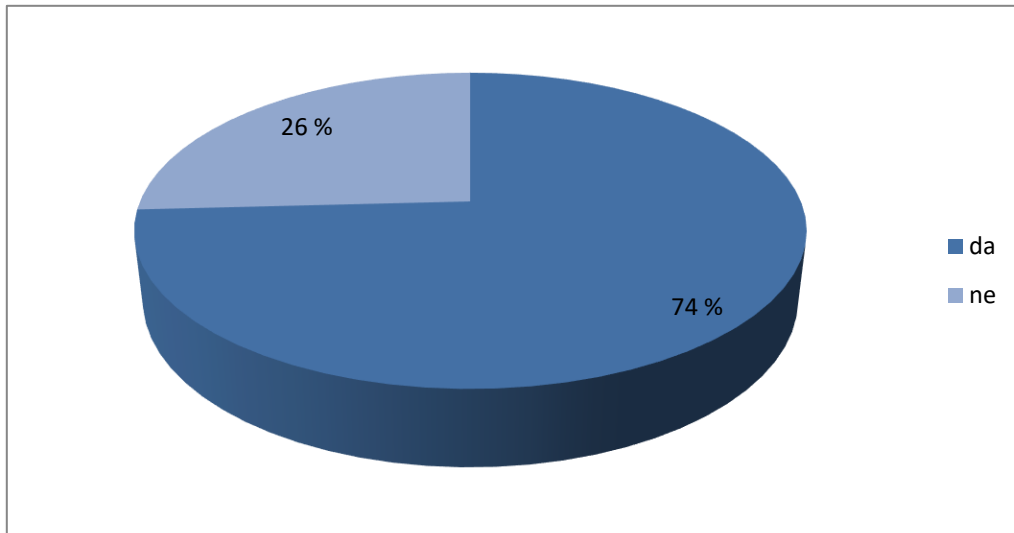
Tudi pri tem vprašanju so lahko anketiranci izbrali več odgovorov. Zanimalo nas je, ali vedo, na koga se lahko obrnejo v primere ogrožene zasebnosti. Od skupno 151 jih je bilo 65 oziroma 43 % mnenja, da se lahko v takem primeru obrnejo na Facebook, 53, torej 35 %, jih ne ve, na koga se lahko obrnejo v primeru, da je njihova zasebnost ogrožena. Da je Informacijski pooblaščenec pravi naslov za take primere, je bilo mnenja 51 anketirancev, kar znaša 34 %. 28, torej 19 % anektiranih, pa je prepričanih, da se je v takem primeru najbolje obrniti na razne organizacije, ki ozaveščajo uporabnike o nevarnosti v spletu. Na Ministrstvo za javno upravo bi se, sodeč po odgovorih, obrnilo 6 oziroma 4 % anketirancev, 5 oziroma zgolj 3 % pa se jih v takem primeru ne bi obrnilo na nobenega od naštetih organov oziroma organizacij (Graf 7.18).

Graf: 7.20: Pomembnost varnosti in zasebnosti na Facebooku



Kako pomembna je varnost in zasebnost profilu v omrežju Facebook, je bilo naslednje vprašanje, ki smo ga zastavili anketiranim. Da je oboje zelo pomembno, je bilo mnenja 62 (41 %) anketiranih. 51 oziroma 34 % jih meni, da sta varnost in zasebnost zelo pomembna, manj pomembna se je zdela 28 (19 %). Da jim je vseeno, je odgovorilo 8 oziroma 5 % vprašanih, zgolj dvema od vprašanih (1 %) pa se to zdi nepomembno (Graf 7.20).

Graf 7.21: Informiranost o možnih nevarnostih Facebooka



Na vprašanje, ali bi želeli več informacij o možnih nevarnostih Facebooka, je pritrdilno odgovorilo 74 % (112) vprašanih, 26 % (39) pa je takih, ki dodatnih informacij ne potrebujejo (Graf 7.21).

8 SKLEP

V diplomskem delu sem predstavila varstvo osebnih podatkov in zasebnost v spletnih družbenih omrežjih, na primeru Facebooka. Razširjenost in tudi priljubljenost spletnih družbenih omrežij narašča, zato je pomembno, da se uporabniki zavedajo, da je taka uporaba lahko zanje nevarna, če niso ustrezno seznanjeni z varstvom zasebnosti na takih omrežjih. Osebni podatki so lahko v primeru nepoznavanja varnostnih mehanizmov ogroženi, s tem pa je ogrožena tudi identiteta in dostojanstvo posameznika.

V uvodu diplomskega dela sem za raziskovalne namene predstavili naslednje hipoteze:

HIPOTEZA 1: Za varnost in zasebnost v spletnem družbenem omrežju Facebook je dobro poskrbljeno.

HIPOTEZA 2: Mlajši uporabniki Facebooka bolj redno posodablajo svoje nastavitve zasebnosti na Facebooku.

Diplomska naloga je obsegala teoretični in empirični del. V teoretičnem delu so predstavljena teoretična izhodišča, pridobljena s pomočjo domače in tuje literature, v empiričnem delu pa sem podatke, ki zadevajo preveritev hipotez, pridobila s pomočjo anketnega vprašalnika, objavljenega v spletu. Spletni vprašalnik je bil zasnovan tako, da sem lahko, tudi z njegovo pomočjo oziroma na podlagi odgovorov anketirancev, prišla do podatkov, ki so mi bili poleg teoretičnih znanj v pomoč pri preveritvi v uvodu postavljenih hipotez.

Prva hipoteza, ki sem si jo zastavila, je bila: *Za varnost in zasebnost v spletnem družbenem omrežju Facebook je dobro poskrbljeno.*

Že v teoretičnem delu diplomskega dela smo precej podrobno opisali delovanje spletnega družbenega omrežja Facebook, ki je postal priljubljen tako med mladimi, kot tudi med malo starejšimi uporabniki, saj zaradi svojega resnega videza spletno mesto vliva zaupanje uporabnikom. Precej podrobno sem predstavila tudi nasvete, s katerimi Facebook redno obvešča svoje uporabnike, kako naj ti najbolje zaščitijo svoj račun pred možnimi vdori. Ti nasveti so izčrpni, razumljivi in uporabniku pomagajo pri varni uporabi Facebooka.

Da uporabniki dobro poznajo nastavitve varnosti in zasebnosti na Facebooku, se je potrdilo tudi v odgovorih pri dvanajstem vprašanju spletne ankete, ki je pokazala, da so uporabniki s to tematiko zelo dobro seznanjeni, take nastavitve poznajo in se tudi sami odločajo, kako in

komu bo »viden« njihov profil oz. njihovi osebni podatki, fotografije, videoposnetki in ostalo. Ugotovimo lahko, da velika večina uporabnikov svoje podatke pretežno deli s svojimi prijatelji, delno tudi s prijatelji svojih prijateljev, nekateri imajo take nastavitve, da lahko te podatke vidijo zgolj oni, v manjšini so tisti, ki svoje osebne podatke delijo z javnostjo. A dejstvo je, da nastavitve varnosti in zasebnosti poznajo, uporabljajo pa jih tako, kakor se njim zdi prav.

Področje varnosti in zasebnosti na Facebooku je primerno urejeno že s samimi informacijami in mehanizmi, ki jih uporabnikom tega družbenega spletnega omrežja posreduje Facebook, pomembno pa je tudi zavedanje uporabnikov, da nekdo »skrbi za njihovo varnost in zasebnost«, zato sem se odločila, da hipotezo »*Za varnost in zasebnost v spletnem družbenem omrežju Facebook je dobro poskrbljeno*« potrdim.

Druga hipoteza, ki sem si jo zastavila, je bila: *Mlajši uporabniki Facebooka bolj redno posodablajo svoje nastavitve zasebnosti na Facebooku.* Za potrebe preveritve te hipoteze sem se oprla na odgovore anketirancev pri vprašanju številka 15 spletne ankete, v katerem sem preverjala, ali uporabniki posodablajo in spremljajo varnostne nastavitve profila na Facebooku. Večina vprašanih, kar 64 %, jih je odgovorilo, da to počne, v manjšini pa so bili tisti, ki tega ne počnejo. Starostno gledano je med njimi bilo 88 % mlajših oz. starih med 13–18 let, ki redno posodablajo in spremljajo varnostne nastavitve profila na Facebooku. Anketirani, še posebej mlajši od 18 let torej redno posodablajo svoje nastavitve in s tem sami odločajo, katere informacije o njih bodo vidne določenim ljudem, katere samo njim in katere samo njihovim prijateljem. Zanimiv je podatek, da kljub temu da redno posodablajo in spremljajo varnostne nastavitve svojega profila, je samo 12 % anketirancev mlajših od 18 let, prebralo politiko zasebnosti na spletnem družbenem omrežju Facebook. To kontradiktornost lahko pojasnim s teoretičnim delom diplomskega dela, kjer sem pisala o varstvu posameznikov glede osebnih podatkov. Posamezniki se namreč dobro zavedajo da imajo na voljo več orodij, če bi prišlo do kršitve ali zlorabe njihovih osebnih podatkov; od informacijskega pooblaščenca, do zakona o dostopu do informacij javnega značaja, vse do Ustave. Vsekakor pa dodatna osveščenost uporabnikov, naj redno posodablajo svoje nastavitve zasebnosti, ni odveč. Na podlagi zgoraj navedenega in ugotovitev, do katerih sem prišla skozi raziskovanje, sem se odločila, da hipotezo *Mlajši uporabniki Facebooka bolj redno posodablajo svoje nastavitve zasebnosti na Facebooku delno potrdim.* Čeprav večina mlajših uporabnikov v skupini od 13–18 let redno posodablja in spremlja varnostne nastavitve svojih profilov na Facebooku, jih v skupini starih od 19–24 let polovica to počne, polovica pa

ne, medtem ko v naslednjih treh starostnih skupinah zopet poraste število tistih uporabnikov, ki redno posodablja in spremlja varnostne nastavitve profila na Facebooku.

NASVETI UPORABNIKOM SPLETA IN FACEBOOKA ZA PRIHODNOST

Glede na to, da uporaba Facebooka narašča iz dneva v dan med različnimi uporabniki, bo tudi v prihodnje treba uporabnike sproti obveščati o vseh novostih, predvsem pa o tem, kako naj zavarujejo svoje podatke in zasebnost, da se bodo ob uporabi počutili varne.

Glede na izsledke spletne raziskave menim, da bo uporabnike Facebooka treba bolje obveščati o nevarnostih, ki nanje v spletu prežijo, o tem, na koga se lahko v primeru zlorabe podatkov obrnejo, kako se najučinkoviteje zavarujejo pred vdori v njihovo spletno zasebnost in na kakšen način lahko najbolje zavarujejo svoje osebne podatke, ki jih objavljajo.

Čeprav se osveščenost uporabnikov Facebooka iz leta v leto izboljšuje, je dejstvo, da popolnoma varnega spleta ni in ga najbrž tudi ne bo. Dejstvo je, da smo ljudje družabna bitja, ki nenehno iščemo stike in splet je eden od posrednikov, prek katerih lahko pridemo do številnih stikov, bodisi na zasebnem ali poslovnem področju. Splet je nenazadnje postal vir informacij in novih znanj ter medij za izmenjavo izkušenj.

Zaščitnost informacij, ki jih objavljajo v spletu, zaščita zasebnosti, spletna varnost in še kaj, so torej tista vprašanja, ki jim bo treba tudi v bodoče posvečati pozornost in na tem področju predlagati izboljšave, novosti, skratka vse tisto, kar nas bo še naprej vodilo v to, da bomo zadovoljni in varni uporabniki spleta.

9 LITERATURA

1. Antić, France. 2011. *Pravni vidiki spletnega portala*. Dostopno prek: <http://mladipodjetnik.si/podjetniski-koticek/poslovanje/pravni-vidiki-spletnega-portala> (17. junij 2016).
2. Bernik, Igor in Kaja Prislan. 2012. *Kibernetika kriminaliteta, informacijsko bojevanje in kibernetični terorizem*. Ljubljana: Fakulteta za varnostne vede.
3. Boyd, Danah M. in Nicole B. Ellison. 2007. Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication* 13 (1). Dostopno prek: <http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/full> (9. maj 2016).
4. Crnović, Deja. 2007. *Moj ego je težak 500 prijateljev*. Dostopno prek: <http://www.mladina.si/97212/moj-ego-je-tezak-500-prijateljev/> (11. maj 2016).
5. Čebulj, Janez. 1992. *Varstvo informacijske zasebnosti v Evropi in Sloveniji*. Ljubljana: Inštitut za javno upravo pri Pravni fakulteti.
6. --- in Jurij Žurej. 2005. *Varstvo osebnih podatkov in informacije javnega značaja*. Ljubljana: Nebra.
7. Digital Trends. 2016. *The history of social networking*. Dostopno prek: <http://www.digitaltrends.com/features/the-history-of-social-networking/> (9. maj 2016).
8. *Direktiva o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku teh podatkov*. Ur. l. Evropskih skupnosti L 281/31–50 (23. november 1995).
9. *Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin* (EKČP). Ur. l. MP 7/94.
10. *Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin* (EKČP) Ur. l. RS 33/94.
11. Facebook. 2015a. *Mark Zuckerberg Profile*. Dostopno prek:

<https://www.facebook.com/zuck/posts/10102329188394581> (11. maj 2016).

12. --- 2015b. *Statement of Rights and Responsibilities*. Dostopno prek: <https://www.facebook.com/legal/terms> (25. junij 2016).

13. --- 2016a. *Facebook company info*. Dostopno prek: <http://newsroom.fb.com/company-info/> (11. maj 2016).

14. --- 2016b. *Facebook Privacy Settings*. Dostopno prek: <https://www.facebook.com> (25. junij 2016).

15. Informacijski pooblaščenec. 2014. *Iskalnik po odločbah in mnenjih VOP*. Dostopno na: <https://www.ip-rs.si/vop/definicija-osebnih-podatkov-2427/> (18. junij 2016).

16. --- 2016a. *Varstvo osebnih podatkov na internetu*. Dostopno prek: <https://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/varstvo-osebnih-podatkov-na-internetu/#c410> (18. junij 2016).

17. --- 2016b. *Zgodovina Informacijskega pooblaščenca*. Dostopno prek: <https://www.ip-rs.si/o-pooblascencu/zgodovina/> (19. junij 2016).

18. Kaliopé, Klemen. 2011. *Zagotavljanje zasebnosti uporabnikov Facebooka*. Diplomsko delo. Maribor: Fakulteta za varnostne vede.

19. Kietzmann, Jan, Kristopher Hermkens, Ian P. McCarthy in Bruno S. Silvestre. 2011. Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons* 2011 (54). Dostopno prek: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2519365 (10. maj 2016).

20. Kovačič, Matej. 2003. *Zasebnost na internetu*. Ljubljana: Mirovni inštitut, Inštitut za sodobne družbene in politične študije.

21. --- 2006. *Nadzor in zasebnost v informacijski družbi*. Ljubljana: Znanstvena knjižnica, Fakulteta za družbene vede.

22. Križaj, Franc. 1989. *Osebnostne svoboščine in zasebnost v »informacijski družbi«*. Ljubljana: Gospodarska založba.
23. Lampe, Rok. 2004. *Sistem pravice do zasebnosti*. Ljubljana: Bonex založba.
24. MacQuail, Denis. 1994. *Mass Communication Theory: An Introduction*. London: Sage.
25. Marketing magazin. 2015. *Ne objavi, kar te lahko gnjavi*. Dostopno prek: <http://www.marketingmagazin.si/izbor-mmeseca/341/ne-objavi-kar-te-lahko-gnjavi> (20. junij 2016).
26. Obar, Jonathan A. in Steven S. Wildman. 2015. Social media definition and the governance challenge: An introduction to the special issue. *Telecommunications policy* 2015 39 (9): 745–750.
27. Oblak, Tanja in Gregor Petrič. 2005. *Splet kot medij in mediji na spletu*. Ljubljana: Fakulteta za družbene vede.
28. Phillips, Sarah. 2007. A brief history of Facebook. *The Guardian*, 25. julij. Dostopno prek: <https://www.theguardian.com/technology/2007/jul/25/media.newmedia> (14. junij 2016).
29. Pirc Musar, Nataša. 2006. Neodvisni nadzor in varstvo osebnih podatkov. *Pravna praksa* 25 (35): 6–10.
30. ---, Sonja Bien, Jože Bogataj, Mojca Prelesnik in Alenka Žaucer. 2006. *Zakon o varstvu osebnih podatkov (ZVOP-1) s komentarjem*. Ljubljana: GV Založba.
31. Pirnat, J. Andrej. 2013. *Kako varna je moja identiteta?* Dostopno prek: <http://siol.net/novice/slovenija/kako-varna-je-moja-identiteta-296680> (19. junij 2016).
32. Pismenost.si. 2016. *Kaj so socialna omrežja?*. Dostopno prek: <http://pismenost.si/kaj-so-socialna-omrezja/> (8. maj 2016).
33. Počkar, Mirjam in Marina Tavčar Krajnc. 2012. *Sociologija*. Ljubljana: DZS

34. Pravno-informacijski sistem. 2001. *Odločba o razveljavitvi sodb vrhovnega sodišča, Višjega sodišča v Ljubljani in Okrožnega sodišča v Ljubljani ter zavrnitvi tožbnega zahtevka*. Dostopno prek: <http://www.pisrs.si/Pis.web/pregledPredpisa?id=ODLU357#> (15. junij 2016).
35. Safe.si. 2016. *Zaščita zasebnosti na spletu – 10 naj nasvetov*. Dostopno prek: <http://www.safe.si/podrocja/moja-identiteta-in-zasebnost-na-spletu/10-naj-nasvetov-o-zasciti-zasebnosti-na-spletu> (18. junij 2016)
36. Savič, Domen. 2008. Raztrgane socialne mreže. *Monitor*, 27. maj. Dostopno prek: <http://www.monitor.si/clanek/raztrgane-socialne-mreze/123191/?xURL=301> (11. junij 2016).
37. Schrader, MJ. 2010. *Types of social networking sites*. Dostopno prek: <http://ezinearticles.com/?Types-of-Social-Networking-Sites&id=4019476> (8. maj 2016)
38. Stare, Jovita. 2010. *Položaj nadzornega organa na področju varstva osebnih podatkov*. Magistrsko delo. Kranj: Fakulteta za državne in evropske študije.
39. Statista. 2015. *Social network profile creation in the United Kingdom 2007-2015*. Dostopno prek: <http://www.statista.com/statistics/271849/social-network-profile-creation-in-the-uk/> (24. junij 2016).
40. --- 2016a. *Numbers of monthly active Facebook users worldwide as of 1st quarter 2016 (in millions)*. Dostopno prek: <http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/> (24. junij 2016).
41. --- 2016b. *Share of U.S. population with a social network profile 2008-2016*. Dostopno prek: <http://www.statista.com/statistics/273476/percentage-of-us-population-with-a-social-network-profile/>. (24. junij 2016).
42. Suhadolc, Jasna 2007. *Nove priložnosti e-komuniciranja*. Ljubljana: GV Založba.
43. Š.P. 2015. *Kodeks kršilo 48 novinarjev, urednikov in voditeljev*. Delo, 7. april. Dostopno prek: <http://www.delo.si/novice/slovenija/pedagogi.html> (4. julij 2016).

44. Šturm, Lovro. 2002. *Komentar ustave Republike Slovenije*, Ljubljana: Fakulteta za podiplomske državne in evropske študije.
45. The Telegraph 2010. *Girl, 14, fears 21,000 party guests after Facebook invite blunder*. Dostopno prek: <http://www.telegraph.co.uk/technology/facebook/8012043/Girl-14-fears-21000-party-guests-after-Facebook-invite-blunder.html> (25. junij 2016).
46. *Ustava Republike Slovenije* (Ustava RS) Ur. l. RS, 33/91-I. (28. december 1991).
47. *Ustava Republike Slovenije* (Ustava RS) Ur. l. RS, 42/97. (17. julij 1997).
48. *Ustava Republike Slovenije*. (Ustava RS) Ur. l. RS, 66/2000. (26. julij 2000)
49. *Ustava Republike Slovenije*. (Ustava RS) Ur. l. RS, 24/2003. (7. marec 2003).
50. *Ustava Republike Slovenije*. (Ustava RS) Ur. l. RS, 69/2004. (24. junij 2004).
51. Volarević, Marija in Domagoj Bebić. 2013. Društvene mreže kao izvor vijesti u najgledanijim središnjim informativnim emisijama u Hrvatskoj. *Medijske studije* 4 (8): 60–75.
52. WebdesignerDepot.com. 2007. *The history and evolution of social media*. Dostopno prek: <http://www.webdesignerdepot.com/2009/10/the-history-and-evolution-of-social-media/> (9. maj 2016)
53. Wikipedija. 2016a. *Social network service*. Dostopno prek: https://en.wikipedia.org/wiki/Social_networking_service (8. maj 2016).
54. --- 2016b. *Spamming*. Dostopno prek: <https://en.wikipedia.org/wiki/Spamming> (20. junij 2016).
55. --- 2016c. *Spletna socialna omrežja*. Dostopno prek: https://sl.wikipedia.org/wiki/Spletno_socialno_omre%C5%BEje (9. maj 2016).

56. --- 2016č. *Website defacement*. Dostopno prek:
https://en.wikipedia.org/wiki/Website_defacement (20. junij 2016).

57. *Zakon o informacijskem pooblaščenju* (ZinfP). Ur. l. RS 113–5005/2005 (16. december 2005).

PRILOGE

PRILOGA A: Anketni vprašalnik

1. Spol

- ☐ moški
- ☐ ženska

2. V katero starostno skupino spadate?

- ☐ 13–18
- ☐ 19–24
- ☐ 25–31
- ☐ 32–40
- ☐ več kot 40

3. Status

- ☐ dijak/-inja
- ☐ študent/-ka
- ☐ zaposlen/-a
- ☐ nezaposlen/-a
- ☐ upokojenec/-ka

4. Zaključena izobrazba

- ☐ osnovna šola
- ☐ srednja šola
- ☐ višja šola
- ☐ visoka šola
- ☐ magisterij
- ☐ doktorat

5. Koliko časa na dan v povprečju brskate po spletu?

- ☐ manj kot 1h
- ☐ od 1h do 2h
- ☐ od 2h do 3h
- ☐ od 3h do 4h
- ☐ več kot 4h

6. Koliko časa na dan v povprečju preživite na Facebooku?

- ☐ do 15 min
- ☐ nad 15 min do 30 min
- ☐ nad 30 min do 1h
- ☐ nad 1h do 2h
- ☐ več kot 2h

7. Navedite glavni razlog za obisk Facebooka. (izberite en odgovor)

- ☐ ohranjanje prijateljskih stikov
- ☐ navezovanje stikov in spoznavanje novih ljudi
- ☐ preživljanje prostega časa oziroma zabava
- ☐ iskanje partnerja/-ke
- ☐ službeni nameni

8. Koliko prijateljev imate na Facebooku?

- ☐ 1–100
- ☐ 101–200
- ☐ 201–300
- ☐ 301–500
- ☐ 501–1000
- ☐ več kot 1000

9. Ali osebno poznate vse prijatelje, ki jih imate na Facebooku?

- ☐ da
- ☐ ne

10. Ali ste že kdaj sprejeli prošnjo za prijateljstvo osebe, ki je ne poznate?

- ☐ da
- ☐ ne

11. Kako zaščiteni menite, da so vaši osebni podatki, ki jih objavljate na Facebooku?

- ☐ zaščiteni
- ☐ ne tako zaščiteni, kot bi si želel/a
- ☐ nezaščiteni
- ☐ ne vem

12. Preverite vaše nastavitve zasebnosti na svojem Facebook profilu in pri vsakem tipu informacij označite, komu so te informacije vidne:

	Samo jaz	Prijatelji	Prijatelji mojih prijateljev	Javno	Pomeri
Osební podatki	☐	☐	☐	☐	☐
Zaposlitev in izobrazba	☐	☐	☐	☐	☐
Kontaktni in osnovni podatki	☐	☐	☐	☐	☐
Družina in razmerja	☐	☐	☐	☐	☐
Slike in videi o meni	☐	☐	☐	☐	☐
Moje objave	☐	☐	☐	☐	☐
Objave prijateljev na mojem zidu	☐	☐	☐	☐	☐
Komentarji objav na mojem zidu	☐	☐	☐	☐	☐

13. Ali ste prebrali politiko o varovanju zasebnosti na omrežju Facebook? (ang. *privacy policy*)

- ☐ da
- ☐ ne

14. Kako pogosto, če sploh, spremljate spremembe politike zasebnosti družbenega omrežja Facebook?

- ☐ redno
- ☐ pogosto
- ☐ občasno
- ☐ redko
- ☐ nikoli

15. Ali posodabljate in spremljate varnostne nastavitve vašega profila na Facebooku?

- ☐ da
- ☐ ne

16. Ali veste, da lahko Facebook po tem, ko izbrišete svoj profil, vsaj še deset let hrani in obdeluje vaše osebne podatke?

- ☐ da in me to zelo moti
- ☐ da, vendar me to ne moti
- ☐ nisem vedel/-a
- ☐ vseeno mi je

17. Katere od spodaj naštetih nevarnosti, ki jih prinaša objavljanje osebnih podatkov na Facebooku, poznate?

- ☐ »Likeme« črvi
- ☐ kraja identitete
- ☐ ribarjenje podatkov ali »phishing«
- ☐ družbeni inženiring
- ☐ piškotki
- ☐ nezaželena elektronska pošta
- ☐ nič od naštetega

18. Ali veste, na koga se obrniti, ko je ogrožena vaša zasebnost?

- ☐ na Facebook
- ☐ na informacijskega pooblaščenca
- ☐ na razne organizacije, ki osveščajo o nevarnosti v spletu
- ☐ na Ministrstvo za javno upravo
- ☐ nič od naštetega
- ☐ ne vem

19. Ocenite, kako pomembni sta za vas varnost in zasebnost podatkov vašega profila na Facebooku?

- ☐ zelo pomembni
- ☐ precej pomembni
- ☐ manj pomembni
- ☐ nepomembni
- ☐ vseeno mi je

20. Želite izvedeti več o nevarnostih, ki jih prinaša uporaba Facebooka?

- ☐ da
- ☐ ne

PRILOGA B: Intervju z gospo Margerito Jurkovič, direktorico Pravnega centra za varstvo človekovih pravic (9. junij 2016)

Glede na to, da se vsakodnevno soočate s prijavi kršitev človekovih pravic – kako bi opredelili razumevanje pravice do zasebnosti in kaj ta pravica pravzaprav pomeni za posameznika?

Pravica do zasebnosti je elementarna človekova pravica, zaščiten z Ustavo, in varuje posameznika pred državno oblastjo, javnostjo in drugimi posamezniki. Gre za pravico »biti sam«, živeti svoje življenje samostojno, s čim manj vmešavanja. Navezuje se na družinsko življenje, na fizično in moralno integriteto ter čast in ugled. Ljudje ravnajo na določen način, vzdržujemo stike na podlagi lastnih želja in prepričanj, zato se moramo pred vdorom javnosti počutiti varne. Zasebnost je izredno pomembna dobrina in se lahko ogrozi na različne načine – včasih smo za to krivi sami, v drugih situacijah pa smo lahko ogroženi zaradi interesov drugih.

Kakšen je vaš pogled na varovanje pravice do zasebnosti v spletu? Ali menite, da nove tehnologije predstavljajo nevarnost za uporabnika in na kakšen način?

Razvoj tehnologije prinaša ogromno možnosti v smislu družbenega napredka, saj pred desetletji nismo mogli niti pomisliti, da bomo tako kmalu pričali določenim pozitivnim vidikom globalnega računalniškega omrežja, vendar pa ta ista tehnologija s seboj prinaša veliko nevarnosti – govorimo o ožanju pravice do zasebnosti. Z opazovanjem in sledenjem, katere strani posameznik obiskuje na internetu in kaj ga zanima, je mogoče izdelati psihološki profil osebe. S pomočjo piškotkov se shranjujejo profili posameznikov, kar postane problematično ob vdoru druge osebe v naš računalnik, bodisi, da do vdora pride fizično ali pa prek škodljive programske opreme. Področje zasebnosti na internetu v Sloveniji obravnava Zakon o varstvu osebnih podatkov, ki določa, kateri podatki se lahko zbirajo in na kakšen način, kako se morajo hraniti ter komu jih je dovoljeno posredovati. Načeloma je obdelava in uporaba osebnih podatkov dovoljena samo pod pogojem, da ima upravljalec zbirke podatkov pisno privoljenje posameznika. Zakon o varstvu osebnih podatkov je zelo strog in za osebe, ki zbirajo in shranjujejo podatke brez pooblastila predpisuje denarne kazni. Za najresnejše primere zlorab osebnih podatkov Kazenski zakonik določa tudi posebno kaznivo dejanje zloraba osebnih podatkov, za katerega je predpisana sankcija lahko zaporna kazen tudi do

treh let. Splet je torej, kolikor koristno, enako tudi nevarno orodje, predvsem za neosveščene posameznike in ranljive skupine, kot so otroci in mladoletniki. Nujno je treba obveščati javnost o samozaščitnih ukrepih v spletu, saj je v primeru zlorab velikokrat del krivde tudi na strani uporabnika.

Ali ste se v zadnjem času na Centru srečali s kakšnim primerom zlorabe osebnih podatkov prek spleta in ali lahko opišete okoliščine?

Pred kratkim smo na Centru obravnavali primer uporabnice, ki je članica ženskega nogometnega kluba, in je dva meseca njena soigralka zaradi medsebojnih nesoglasij iz maščevanja zlorabljala njen Facebook-profil. Prek zasebnih sporočil in objav nazidu je v njenem imenu virtualni javnosti sporočala, da je uporabnica istospolno usmerjena. Med drugim jo je v njenem imenu vpisovala in prek spletnih obrazcev včlanjevala v društva, ki se ukvarjajo z nediskriminacijo LGBT. Med drugim je osumljenka vdrla v njeno elektronsko pošto ter v njenem imenu pošiljala žaljiva elektronska sporočila njenim staršem, bratu in sestri. Podali smo kazensko ovadbo, državni tožilec je s pomočjo policije pridobil zadostno število dokazov in sprožil kazenski pregon zaradi suma kaznivega dejanja zlorabe osebnih podatkov. Uporabnica bo vložila tudi odškodninski zahtevek zaradi psihičnih bolečin, ki jih je doživela zaradi ravnanja obtožene.