

Redefiniranje pojma privatnosti u okviru modernih društvenih mreža

Račman, Anita

Master's thesis / Diplomski rad

2013

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Faculty of Humanities and Social Sciences / Sveučilište Josipa Jurja Strossmayera u Osijeku, Filozofski fakultet**

Permanent link / Trajna poveznica: <https://urn.nsk.hr/urn:nbn:hr:142:435864>

Rights / Prava: [In copyright](#)/[Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2024-11-26**



Repository / Repozitorij:

[FFOS-repository - Repository of the Faculty of Humanities and Social Sciences Osijek](#)



Sveučilište J.J. Strossmayera u Osijeku

Filozofski fakultet

Diplomski studij informatologije

**Redefiniranje pojma privatnosti u okviru modernih društvenih
mreža**

Anita Račman

Diplomski rad

Mentor: doc.dr.sc. Boris Badurina

Osijek, 2013.

Sadržaj

Sažetak.....	3
1. Uvod.....	4
2. Definiranje pojma društvena mreža	4
1.1. Funkcionalnost društvenih mreža	5
1.2. Klasifikacija društvenih mreža	7
4. Privatnost na internetu	10
4.1. Javnost informacija	12
4.2. Zaštita privatnosti i svijest korisnika	14
4.4. Krađa identiteta.....	16
4.3. Korištenje podataka u komercijalne svrhe	18
5. Istraživanje	23
5.1. Cilj i svrha istraživanja.....	23
5.2. Metodologija.....	24
5.3. Analiza rezultata	25
5.4. Rasprava	36
6. Zaključak	38
7. Literatura.....	40
8. Prilozi.....	42

Sažetak

Pojam društvena mreža postao je ljudska svakodnevnica i sve više je prisutan u današnjem društvu. Društvenim mrežama se koriste mnogi, neovisno o dobi, spolu ili nekim drugim socio-demografskim pitanjima. U ovom diplomskom radu, kako bismo što bolje razumjeli sam pojam privatnosti a nakon toga proveli kvalitetno istraživanje, na početku smo definirali sam pojam društvena mreža te ga prikazali ne kao skupinu ljudi umreženih putem neke platforme ili web-stranice za društveno umrežavanje nego upravo na način da na društvenu mrežu gledamo kao samu platformu ili web-stranicu. Obzirom da postoji više mogućih načina na koje je ugrožena privatnost korisnika na društvenim mrežama, prikazani su neki od najučestalijih te svijest samih korisnika o privatnost. U sklopu ovog rada provedeno je istraživanje o stavovima o privatnosti na Internetu. Sudionicima je podijeljen anketni upitnik od 9 pitanja gdje smo temeljem njihovih odgovora i nakon obrade rezultata dobili odgovore o njihovim stavovima o privatnosti koji pokazuju da ne postoji statistički značajna razlika u stavovima prema sigurnosti osim po pitanju privatnosti gdje se vidi da žene posvećuju više brige po tom pitanju. Razlika u stavovima ne postoji niti po pitanju dobi. Također istraživanje je pokazalo da osobe koje duže koriste društvenu mrežu Facebook pokazuju manji opći oprezu. Opći oprez i opći stav prema sigurnosti na internetu pokazali su se najizraženiji kod sudionika koji posjećuju Facebook račun najmanje jednom tjedno dok stavovi prema tehničkoj zaštiti najizraženiji su kod sudionika koji posjećuju Facebook najmanje jednom tjedno.

Ključne riječi: društvene mreže, privatnost, Facebook

1. Uvod

Pojam društvena mreža postao je ljudska svakodnevnica i sve više je prisutan u današnjem društvu. Društvenim mrežama se koriste mnogi, neovisno o dobi, spolu ili nekim drugim socio-demografskim pitanjima. U ovom diplomskom radu, kako bismo što bolje razumjeli sam pojam privatnosti a nakon toga proveli kvalitetno istraživanje, na početku ćemo definirati sam pojam društvena mreža, a zatim obraditi problem privatnosti. Obzirom da postoji više mogućih načina na koje je ugrožena privatnost korisnika na društvenim mrežama, bit će prikazani neki od najučestalijih na teorijskoj razini, a u zadnjem dijelu i provedeno istraživanje o stavovima o privatnosti na Internetu

2. Definiranje pojma društvena mreža

Prije nego definiramo sam pojam društvena mreža potrebno je napomenuti da u ovom radu na pojam društvena mreža nećemo gledati kao na skup ljudi umreženih putem internet servisa, nego upravo na taj internet servis putem kojega su oni umreženi.

Društvena mreža je vrsta internetskog servisa koji se najčešće javlja u obliku platforme, prozora ili web-stranice. To je platforma za izgradnju društvenih mreža ili društvenih odnosa među ljudima koji, primjerice, dijele interese, aktivnosti, pozadine, ili u stvarnom životu veze. Ukratko rečeno, to je internetski servis, koji služi za međusobno povezivanje korisnika. Također za društvene mreže možemo reći i da su besplatne online usluge koje korisnicima pružaju razne vrste komunikacije sa svijetom i mogućnost vlastite prezentacije. One predstavljaju pristupačne internet usluge koje kombiniraju tehnologiju i društvenu interakciju. Društvenim mrežama danas se koriste stotine milijuna ljudi, a osim onih generalnih, postoje i servisi s određenom namjenom glede sadržajnog fokusa i profila korisnika.¹ Uspjeh i popularnost neke društvene mreže ovise o prilagođavanju

¹ Usp. Vidipediija, slobodna tehno enciklopedija. Društvene mreže. URL: http://www.vidipediija.com/~vidipedi/index.php?title=Dru%C5%A1tvene_mre%C5%BEe. (2013-08-22)

potrebama korisnika, ali i o postavljanju novih tehnologija radi privlačenja novih korisnika i zadržavanja postojećih. Neke su društvene mreže postigle izniman uspjeh kada je u pitanju broj korisnika upravo zbog sposobnosti brze prilagodbe. Oni zbog svoje jednostavnosti, brzine i dosega, brzo mijenjaju javni diskurs u društvu i postavljaju trendove i podsjetnike na temama koje se kreću od okoline i politike prema tehnologiji i industriji zabave. Također, takva zajednice mogu se koristiti kako bi se radila kvantitativna predviđanja koja će nadmašiti ona o umjetnom tržištu.²

Sam pojam društvene mreže možemo definirati kao web stranice i usluge bazirane na webu koje (1) omogućuju pojedincima da izgrađuju javne ili polujavne profile unutar omeđenog sustava, (2) artikuliraju popis drugih korisnika s kojima dijele vezu, i (3) pregledavaju i zaobilaze njihov popis veza i onih izrađenih od strane drugih unutar sustava. Priroda i nomenklatura tih veza može varirati od stranice do stranice.³

To može rezultirati vezama između pojedinaca koje se inače ne bi dogodile, iako to često nije cilj. Na mnogim velikim stranicama društvenih mreža, sudionici nužno ne pretražuju internet ili nisu nužno u potrazi za upoznajem novih ljudi, umjesto toga, oni prvenstveno komuniciraju s ljudima koji su već dio njihove šire društvene mreže.⁴

1.1. Funkcionalnost društvenih mreža

Kako bismo lakše razumjeli samo pojam društvena mreža, pojasnit ćemo na kakvom principu ista funkcionira. Naime, društvena mreža kao usluga sastoji se od predstavljanja svakog korisnika (to često se naziva *Profil*), njegovim/njenim društvenim vezama, kao i nizom dodatnih usluga. Treba napomenuti da većina društvenih mreža

² Usp. Chen, Kay-Yut; Fine, Leslie R.; Huberman, Bernardo A. Predicting the Future. URL: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.2.3539&rep=rep1&type=pdf> (2013-09-04)

³ Usp. Danah M Boyd, Social Networking Sites: definition, history and scholarship, 2007. URL: <http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/pdf>. (2013-08-22)

⁴ Isto.

osiguravaju sredstva za interakciju korisnika preko interneta, kao što su e-mail i instant poruke. Društveno umrežavanje omogućuje korisnicima da dijele ideje, slike, postove, aktivnosti, događanja i interese s ljudima u njihovoj mreži.

Dok društvene mreže osiguravaju razne tehničke mogućnosti, njihova okosnica sastoji se od vidljivih profila koji prikazuju artikulirani popis *Prijatelja* koji su ujedno i korisnici sustava. Profili su jedinstvene stranice gdje se pojedinac može prijaviti. Nakon što se pridruži društvenoj mreži, pojedinac je zamoljen da ispuni obrasce koji sadrže niz pitanja. Profil se generira pomoću odgovora na ova pitanja, koja obično uključuju opise kao što su dob, mjesto, interese i odjeljak "O meni". Većina takvih društvenih mreža potiče korisnike da *uploadaju* sliku profila. Neke web stranice omogućuju korisnicima, da bi poboljšali svoje profile, dodavanje multimedijских sadržaja ili mijenjanje izgleda i dojma svom profilu. Druge, kao što su Facebook, omogućuju korisnicima da dodaju module ("aplikacije") koje poboljšavaju njihov profil.⁵

Vidljivost profila varira o mjestu i sukladan je diskreciji korisnika. Strukturne razlike oko vidljivosti i dostupnosti su jedan od osnovnih načina da se stranice društvenih mreža razlikuju jedne od drugih. Nakon uspješne prijave na društvenu mrežu, od korisnika se traži da se poveže s drugim korisnicima koje poznaje. Oznaka za te odnose razlikuje se ovisno o mjestu - popularni pojmovi su "Prijatelji", "Kontakti " i "Obožavatelji". Većina stranica društvenih mreža zahtijevaju dvosmjernu potvrdu za prijateljstvo, ali neke ne. Ove jednosmjerne veze su ponekad označene kao "Obožavatelji " ili "Sljedbenici", ali mnoge web stranice i njih zovu prijateljima. Izraz " Prijatelji " može biti pogrešan, jer veza ne znači nužno prijateljstvo u svakodnevnom kolokvijalnom smislu, a razlozi za povezivanje ljudi su različiti.⁶

Većina stranica društvenih mreža također osiguravaju mehanizam za korisnike da mogu ostaviti poruke na profilima svojih prijatelja profila. Ova značajka obično uključuje ostavljanje "komentara", iako stranice koriste razne etikete za ovu značajku. Osim toga, stranice društvenih mreža često imaju mogućnost slanja privatnih poruka sličnu *webmail-*

5 Isto.

6 Isto.

u. Iako su i privatne poruke i komentari popularni na većini glavnih stranica društvenih mreža, one nisu univerzalno dostupne. Iza profila, Prijatelja, komentara i privatnih poruka, stranice društvenih mreža uvelike se razlikuju u svojim značajkama i korisničkim bazama. Neki služe za razmjenu fotografija ili dijeljenje videa dok druge omogućuju bloganje i tehnologiju slanja instant poruka. Mnoge stranice društvenih mreža ciljaju na ljude iz određene zemljopisne regije ili jezičnih skupina, iako to ne mora uvijek određivati izbornu jedinicu za stranicu. Stranica Orkut, primjerice, je pokrenuta u Sjedinjenim Američkim Državama sa samo engleskim sučelje, ali Brazilci Portugalskog govornog područja su brzo postali dominantna skupina korisnika. Neke web stranice su dizajnirane za posebne etničke, vjerske, spolne orijentacije, političkih ili neku drugu kategoriju identiteta. Postoje čak stranice društvenih mreža za pse (Dogster) i mačke (Catster), iako njihovi vlasnici moraju upravljati njihovim profilima.

Dok su stranice društvenih mreža često dizajnirane kako bi bile široko dostupne, mnogi pokušavaju privući homogenu populaciju u početku, tako da nije neuobičajeno pronaći skupine društvenih mreža koje se razdvajaju po nacionalnosti, dobi, stupnju obrazovanja, ili drugim čimbenicima koji su uobičajeni segmenti društva, čak i ako to nije bila namjera dizajnera.⁷

1.2. Klasifikacija društvenih mreža

Osnovicu društvenih mreža predstavljaju društveni mediji koji uključuju tehnologije temeljene na Web-u i mobilne tehnologije koje se koriste kako bi se komunikacija preokrenula u interaktivni dijalog. Društvene mreže su definirane kao skupina internet aplikacija koje su izgrađene na ideološkim i tehnološkim osnovicama Web 2.0 tehnologije koje omogućavaju kreiranje i razmjenu korisnički generiranog sadržaja.⁸

⁷ Isto.

⁸ Usp. Kaplan, Andreas M.; Haenlein, Michael. Users of the world, unite! The challenges and opportunities of Social Media. URL: <http://www.sciencedirect.com/science/article/pii/S0007681309001232> (2013-08-24)

Društvene mreže su mediji za društvene interakcije te predstavljaju svojevrsan nadskup alata koji nadilaze same sfere društvene komunikacije. One su lako dostupne te su promijenile način na koji organizacije, društva i individualci komuniciraju. Također se odnose na mnogo oblika, uključujući časopise, internet forume, blogove, društvene blogove, mikroblog, wikije, podcastove, fotografije ili slike, video te stranice za društveno označavanje. Primjenjujući skup teorija u polju medijskog istraživanja (društvena prisutnost, bogatstvo medija) i društvene procese (samoprezentacije, samo otkrivanje) postoji šest tipova društvenih mreža. Oni se također mogu gledati kao izazovi i mogućnosti društvenih mreža, a to su:

- Kolabracijski projekti (ING. collabration projects) (Wikipedija),
- Blogovi i mikroblogovi (eng. blogs and microblogs) (Tumblr, Twitter),
- Društva sadržaja (eng Content Network) (Youtube),
- Stranice za društveno umrežavanje (eng. Social networking sites) (Facebook, Google Plus),
- Virtualni svijetovi (eng Virtual Worlds) (World Of Warcraft), te
- Virtualni društveni svjetovi (eng. Virtual Social Worlds) (Second Life)⁹

Prvo razvrstavanje može se temeljiti na bogatstvu medija i stupnju socijalne prisutnosti. Što je veća društvena prisutnost, veći je i društveni utjecaj koji komunikacijski partneri imaju jedni na druge. Usko povezana s idejom socijalne prisutnosti je koncept medijskog bogatstva. Teorija medijskog bogatstva temelji se na pretpostavci da je cilj bilo koje komunikacije rješavanje nejasnoća i smanjenje neizvjesnosti. On navodi da su mediji razlikuju u stupnju bogatstva koje posjeduju, odnosno, količina informacija koje omogućuju da se prenose u određenom vremenskom intervalu, te da su stoga neki mediji učinkovitiji od drugih u rješavanju nejasnoća i neizvjesnost.

⁹ Isto.

Obzirom na socijalnu dimenziju društvenih mreža, koncept samopredstavljanja tvrdi da u bilo kojoj vrsti socijalne interakcije ljudi imaju želju za kontroliranim impresioniranjem drugih ljudi. Navedeno čine s ciljem utjecanja na druge i to kako bi bili „nagrađeni“ (npr. napraviti pozitivan dojam), s druge strane, takvo ponašanje je potaknuto željom za stvaranje slike koje je sukladna s nečijim osobnim identitetom (npr. nošenje modernog odijela kako bi se osoba percipirala kao mlada i u trendu). Ključni razlog zašto se ljudi odlučuju za stvaranje osobne web stranice je želja da se pokažu u virtualnom prostoru. Samootkrivanje je ključan korak u razvoju bliskih odnosa ali također može pojaviti između potpunih stranaca. Obzirom na primijenjenu konteksta društvenih mreža, drugi dio klasifikacije može se izvršiti na temelju stupnja samo-otkrivanja što zahtijeva i vrstu samoprezentacije.¹⁰

Kombiniranje obje dimenzije dovodi do klasifikacije društvenih medija koje su vidljive u Tablici 1. Obzirom na društvenu prisutnost medija i bogatstvo, aplikacije kao što su zajednički projekti (npr. Wikipedia) i blogovi postižu najmanje, jer su često tekstualni i stoga dopuštaju samo relativno jednostavne razmjene. Na sljedećoj razini su zajednice baziranih na sadržaju (npr. YouTube) i stranica za društveno umrežavanje (npr. Facebook) koji, osim komunikacije bazirane na tekstu, omogućuje dijeljenje slika, videa i drugih oblika medija. Na najvišoj razini su virtualne igre i socijalni svjetovi (npr. World of Warcraft, Second Life), koje pokušavaju replicirati sve dimenzije samo u virtualnom okruženju. Što se tiče samopredstavljanja i samootkrivanja, najlakše će se to postići blogovima. Virtualni društveni svjetovi zahtijevaju višu razinu samootkrivanja od virtualnog svijeta igara obzirom da u njima vladaju stroge smjernice koje prisiljavaju korisnike da se ponašaju na određeni način.¹¹

¹⁰ Isto.

¹¹ Isto.

		Social presence/ Media richness		
		Low	Medium	High
Self-presentation/ Self-disclosure	High	Blogs	Social networking sites (e.g., Facebook)	Virtual social worlds (e.g., Second Life)
	Low	Collaborative projects (e.g., Wikipedia)	Content communities (e.g., YouTube)	Virtual game worlds (e.g., World of Warcraft)

Tablica 1.

4. Privatnost na internetu

U zadnjih nekoliko godina pitanje privatnosti na internetu se sve češće postavlja. Podaci o korisnicima se skupljaju različitim metodama, a najviše se upotrebljavaju u marketingu. Masovnom pojavom društvenih mreža, privatnost korisnika je dodatno narušena. Podignute su brojne sudske tužbe protiv organizacija i poslodavaca koji su prikupljali podatke dok je korisnik bezbrižno koristio internet.¹² O privatnosti na internetu se počelo više govoriti pojavom Web 2.0 servisa. Zbog velike količine osobnih podataka koje korisnici sami čine vidljivima, moguća je njihova zlouporaba.

Obzirom da je internet a s njim i društvene mreže postao nezaobilazni dio ljudskog života, a broj njegovih korisnika svakim danom sve više raste, samim tim rastom broja korisnika te njegovim nezaobilaznim razvojem, olakšava se i ubrzava protok informacija. No, to sa sobom kao posljedicu nosi i problem zaštite privatnosti. Kao što smo ranije naveli, postoje mnogi poznati slučajevi povrede privatnosti na internetu i društvenim mrežama koji upozoravaju kako to postaje sve veći problem u današnjem društvu. Problemom privatnosti na društvenim mrežama intenzivno se počelo baviti nakon popularizacije društvenih mreža na kojima korisnici ostavljaju mnogo privatnih

¹² Laboratorij za sustave i signale. Privatnost na Internetu. URL: <http://sigurnost.lss.hr/Novi-dokumenti/privatnost-na-internetu.html>

informacija, za koje žele da ostanu dostupne samo određenim osobama.¹³ Korisnici društvenih mreža žele privatnost barem u onoj mjeri u kojoj to imaju u stvarnom svijetu. No, privatnost na društvenim mrežama je vrlo teško postići zbog interaktivnosti korisnika i pružatelja internetskih usluga te njegovog besprekidnog razvoja. Privatne informacije koje korisnik ostavi na društvenim mrežama, svojom voljom ili ne, sve veća su vrijednost u današnjem društvu, pa su time i sve traženija roba. Ove informacije su vrlo korisne u oglašavanju koji je glavni izvor zarade većine današnjih web stranica, ali mogu biti korisne i zlonamjernim korisnicima kako bi im se olakšao napad. Pomoću tih informacija može se saznati mnogo o korisniku te se takve informacije mogu zloupotrijebiti. Korištenje osobnih informacija korisnika ne mora nužno biti loše, jer se one mogu iskoristiti i za poboljšanje korisničkog iskustva tijekom korištenja društvenih mreža (prilagođeni prikaz stranica, personalizirane ponude korisnicima i sl.).¹⁴

Također treba uzeti i u obzir da su društvene mreže medij kojeg nitko ne nadgleda. Sama regulacija se provodi na razini tvrtke koja pruža neki servis na internetu. Te tvrtke sastavljaju svoje uvjete korištenja koje korisnik mora prihvatiti ukoliko se želi služiti servisom. Rijetko koji korisnik pažljivo pročita te dugačke i složene uvjete. Upotreba informacija o korisniku koje on svjesno ili nesvjesno ostavlja dok koristi internet nije regulirana, što može dovesti do povrede privatnosti korisnika. Same informacije o korisniku se mogu sakupiti na nekoliko načina:

- preko računala korisnika (najčešće krađa cookie datoteka),
- praćenjem navika korisnika prilikom korištenja interneta (npr. praćenje Google pretraga),
- prikupljanjem s javnih servisa koje korisnik koristi.

¹³ Mučnjak, Dorja. Društvene mreže i knjižnice: etičko pitanje // Knjižničar/ka: časopis Knjižničarskog društva Rijeka 3 (2012), 3, str. 99. URL: <http://www.kdr.hr/drustvo/Casopis%20KDR%202012.pdf> (2013-09-10)

¹⁴ Usp. Laboratorij za sustave i signale. Privatnost na Internetu, 2010. URL: <http://sigurnost.lss.hr/images/dokumenti/lss-pubdoc-2010-10-002.pdf> (2013-09-10)

Ovo posljednje je specifično jer se s jedne strane od korisnika zahtjeva određeni broj osobnih podataka kako bi se servis mogao koristiti, a s druge strane mu se ne jamči zaštitu tih podataka. Ostali sigurnosni rizici uključuju web preglednike, pružatelje internetskih usluga te razne servise (poput Google street view) koje rade na principu *cloud computing-a*. Osnovno obilježje ovih servisa jest da se svi podaci (koji se inače nalaze na korisnikovom računalu) nalaze na udaljenim poslužiteljima te je njihova sigurnost, (a time i privatnost korisnika), u rukama pružatelja usluge.¹⁵

Zakonske regulative koje bi osiguravale korisnikovo pravo na privatnost uglavnom su nedovoljno razvijene dok u nekim državama uopće ne postoje čime se omogućuje njihovo zaobilaznje. Prilagodba različitim zakonima o privatnosti svake države povećava trošak razvoja proizvoda pa se javlja potreba za jedinstvenim propisima o privatnosti koji bi vrijedili za sve države svijeta. Na taj način bi i privatnost korisnika bila zaštićenija.¹⁶ Nažalost, zbog različitog shvaćanja prava na privatnost u različitim državama, teško je donijeti propis koji bi bio prihvaćen u svim državama. Upravo zbog izostanka „globalnih propisa“ jedino rješenje je odgovorno ponašanje korisnika. To znači da svaki korisnik mora biti svjestan koje i od kuda mu opasnosti prijete, te na temelju toga donijeti odluke o količini osobnih informacija koje će putem nekog servisa plasirati na internet.¹⁷

4.1. Javnost informacija

Kako bismo najbolje razumjeli kako se podaci koje ostavljamo na društvenim mrežama koriste i kako je time ugrožena naša privatnost, potrebno je razumjeti same informacije koje se mogu dobiti od pojedinca putem društvenih mreža. Postoje dvije vrste informacija

¹⁵ Usp. Laboratorij za sustave i signale. Privatnost na Internetu. URL: <http://sigurnost.lss.hr/Novi-dokumenti/privatnost-na-internetu.html> (2013-09-10)

¹⁶ Isto.

¹⁷ Isto.

koje se mogu sakupiti o korisniku i to upravo iz društvene mreže: informacije koje korisnik dijeli i podaci prikupljeni putem elektroničkog praćenja.

Informacije koje korisnik sam dijeli mogu uključivati:

- Fotografije i druge medije
- Dob i spol
- Biografski podaci (obrazovanje, povijest zapošljavanja, rodni grad, i sl.)
- Statusi (također poznat kao objave)
- Kontakti
- Zanimljivosti
- Zemljopisni položaj¹⁸

Sve ove informacije postaju javne na razne načine:

- Korisnik može odabrati da samu informaciju objavi za "javnosti" (bez ograničavanja pristupa putem dostupnih postavkama privatnosti).
- Određene informacije mogu biti javno vidljive prema zadanim postavkama. U nekim situacijama, korisnik će biti u mogućnosti promijeniti postavke privatnosti kako bi informacije učinio privatnima - tako da samo odobreni korisnici mogu vidjeti informacije. Ostali podaci moraju ostati javni, korisnik ne mora imati mogućnost da se ograniči pristup do njih.
- Društvena mreža može promijeniti svoju politiku privatnosti u bilo koje vrijeme bez dozvole korisnika. Sadržaj koji je objavljen pod ograničavajućim postavkama privatnosti može postati vidljiv kada se pravila o privatnosti izmijenjene.

¹⁸ Usp. Privacy rights clearinghouse. Social Networking Privacy: How to be Safe, Secure and Social, 2013. URL: <https://www.privacyrights.org/social-networking-privacy> (2013-09-04)

- Odobreni kontakti mogu kopirati i ponovno poslati informacije - uključujući fotografije - bez dozvole korisnika, potencijalno zaobilazeći postavke privatnosti.
- Dodatne aplikacije koje su dobile pristup profilu na društvenoj mreži mogu biti u mogućnosti vidjeti podatke koje korisnik privatno objavi.¹⁹

Društvene mreže i same nužno ne jamče sigurnost podataka koje su ustupili na profilu, čak i kad su te objavljene informacije bile postavljene kao privatne. To je pokazano u jednom incidentu u kojem su neovlašteni korisnici mogli vidjeti privatne *chat* poruke svojim kontaktima na Facebooku. Iako se ovakvi slučajevi, kao i druge slične greške obično brzo riješe, postoji velik potencijal za iskorištavanje *procurenih* informacija.²⁰

4.2. Zaštita privatnosti i svijest korisnika

Kada se govori o zaštiti privatnosti, tj. o svijesti korisnika društvenih mreža, treba naglasiti da je najviše takvih istraživanja svakako napravljeno u Sjedinjenim Američkim Državama i prema tim istraživanjima došlo je do podataka da više od 90% studenata koristi barem jednu društvenu mrežu, a 2007. godine (znači prije velikog proboja Facebooka) prema izvješću OCLC-a više od trećine stanovnika SAD-a je koristilo barem jednu društvenu mrežu.²¹ Ovakva istraživanja su nam važna jer nam omogućuju uvid u način shvaćanja privatnosti njene zaštite kod korisnika društvenih mreža. Što se tiče samih rezultata, oni pokazuju da postoji statistički značajna razlika u shvaćanju privatnosti između mladih i osoba srednje i starije životne dobi dok je zaključak tih istraživanja je da mlađi korisnici (do 30 godina) manje važnom smatraju privatnost od starijih. Nadalje, rezultati pokazuju da mladi jesu svjesni potrebe čuvanja privatnosti no vjeruju da im je privatnost na društvenim mrežama sama po sebi zaštićena, tj. da ih

¹⁹ Isto.

²⁰ Isto.

²¹ Usp. Mučnjak, Dorja. Društvene mreže i knjižnice: etičko pitanje // Knjižničar/ka: časopis Knjižničarskog društva Rijeka 3 (2012) , 3, str. 99. URL: <http://www.kdr.hr/drustvo/Casopis%20KDR%202012.pdf> (2013-09-10)

društvena mreža adekvatno štiti te da ne moraju ulagati posebne napore u daljnju zaštitu osobnih podataka.²²

Završno, na oprez upućuje podatak da u slučaju da moraju birati između zaštite privatnosti i društvene mreže, mladi bi se radije odrekli privatnosti nego društvene mreže. Ovakav podatak je zabrinjavajući i iz toga se može zaključiti i to da su mladi svjesni da je otkrivanje određene količine osobnih podataka esencijalno za funkcioniranje društvene mreže poput Facebooka (gdje se osobe predstavljaju svojim istinitim podacima) u smislu povezivanja osoba koje se i u stvarnom životu (ne samo u virtualnom) poznaju i družu.²³

napretkom tehnologija koje koriste društvene mreže će se pojaviti i novi sigurnosni propusti koje bi napadači mogli otkriti. Društvene će mreže postati neizostavno dio svakog dijela ljudskog života jer je komunikacija sa drugim pojedincima potrebna kako bi se ostvarili životni ili poslovni ciljevi. Društvene mreže su također i u poslovnom dijelu napravile velik pomak u komunikaciji, olakšavajući tvrtkama i poduzetnicima stabilno i održivo poslovanje. Otkrivanjem podataka, svaka tvrtka riskira sigurnost intelektualnog vlasništva i računalne infrastrukture. Primjerenom zaštitom svaka tvrtka može aktivno sudjelovati na profesionalnim društvenim mrežama. Trenutačni broj korisnika društvenih mreža nije poznat, ali kao što je vidljivo iz statistike, brojevi su reda veličine stotina milijuna za samo jednu društvenu mrežu. Broj novih korisnika koji postaju dijelom globalne zajednice neprestano raste, a s njime rastu mogućnosti koje društvena mreža nudi. Naravno, cilj svake tvrtke je ostvarivanje zarade, stoga redovito održavanje i ugrađivanje novih tehnologija u društvene mreže postaje svakodnevnica. Savjet korisnicima, u budućnosti, jednako kao i u današnje vrijeme zbog sigurnosti i zaštite privatnosti je primjena opreza pri korištenju društvenih mreža.²⁴

²² Isto.

²³ Isto.

²⁴ Usp. Miljak, Suzana. Uporaba društvenih mreža za upravljanje znanjem. URL: http://www.famns.edu.rs/skup1/radovi_pdf/miljak.pdf. (2013-08-31)

4.4. Krađa identiteta

Društvene mreže imaju milijune korisnika i svi rado dijele detalje o svojim životima s prijateljima i kontaktima. One su popularne s dobrim razlogom, pomažu ljudima da se povežu i zadržate kontakt s raznim ljudima iz svog života. No, zbog svoje popularnosti kradljivci identiteta koriste društvene mreže kao novi alat za krađu identiteta. Stoga pojedinci moraju biti svjesni opasnosti koja se pojavljuje u elektroničkom okruženju obzirom da su krađe identiteta u virtualnom obliku poznate otkada internet postoji, tako da ni društvene mreže nisu pošteđene tih opasnosti. Opasnost postoji uvijek, ali mogućnosti proporcionalno rastu s količinom osobnih podataka koje o sebi.

Društvene mreže pružaju novo mjesto za stare prijevare. Varijacije mnogih poznatih e-mail prijevare brzo su napravile svoj put na mrežnim stranicama. Stranice rade na tome da identificiraju i spriječe zlouporabu svojih sustava, ali krađe identiteta, zlonamjerni programi i krađe gotovine se događaju. Kao i kod drugih krađa identiteta, lopov koji napada na mrežnim stranicama također ima za cilj da prevari pojedina u pružanju osjetljivih informacije koje se mogu koristiti za krađu njegova identiteta. Trik može biti dostavljen umrežavanjem stranice sustavu za razmjenu poruka ili preko aplikacija dizajniranih da izgledaju kao bezopasan kviz, anketa ili besplatno slanje proizvoda. Isto tako, e-mailovi ili aplikacije mogu sadržavati zlonamjerni softver - kod dizajniran kako bi zarazio korisnikovo računalo ako ga korisnik *downloada*, obično s ciljem praćenja svih svojih budućih aktivnosti i daje pristup lopovu identifikacijskim podacima i lozinkama za financijske račune.²⁵

Lopovi se mogu predstavljati kao pojedini korisnik i ciljati na njegove prijatelje. Ova vrsta prijevare može biti jedan od najvažnijih uznemirujućih aspekata između društvenih mreža i krađe identiteta. Lopov se predstavlja kao korisnik da prevari njegove prijatelje a to može učiniti na već poznati način da hakira korisnikov račun i *spama* korisnikovu

²⁵ Usp. ProtectMyID. Facebook Fraud: Identity Theft through Social Networking.URL: http://www.protectmyid.com/images/education_center/pdf/050TypesofFraud/7_types%20of%20fraud_social%20networking.pdf (2013-11-09)

mrežu. Ali, na isti način na koji su neki lopovi financijskih identiteta uspostaviti nove kreditne račune u ime drugih pojedinaca, neki kradljivci društvenih identiteta mogu postaviti cijeli novi profil i lažno se predstavljati kao korisnik s ciljem pristupa osobama koje korisnik poznaje bez da korisnik zna o tome. Sigurnosni stručnjaci ističu da na društvenim i poslovnim mrežama mnogi od nas imaju objavljenih više nego dovoljno informacija o našim osobnim i poslovnim životima od kojih lopovi mogu lako stvoriti lažni profil koji izgleda autentično ljudima koji nas znaju. Ako netko objavi lažni profil na tuđe ime na društvenoj mreži koju pokradena osoba zapravo ne koristi, mogao bi izgraditi cijelu mrežu svojih prijatelja, obitelji i suradnika, a time dobiva pristup bogatstvu informacija o svakom od njih. I zato što ljudi često vjeruju da se dijele informacije i objave samo s ljudima koje već znaju, oni često objavljuju puno detalja koje hakeri mogu iskoristiti da se dođe do lozinki i probijanja sigurnosnih pitanja, poput datuma i mjesta rođenja, imena roditelja, pojedinosti o djeci ili kućnim ljubimcima i još mnogo toga.²⁶

Tako je kod pojedine osobe moguće doznati broj socijalnog osiguranja, koji se potom može koristiti kao dio krađe identiteta. Razne skupine korisnika su savjetovane da ili ne prikazati vlastiti datum rođenja na stranicama društvenih mreža, ili da ga sakriju od 'prijatelja' koje oni osobno ne poznaju.²⁷ Također su se pojavili slučajevi korisnika koji imaju fotografije koje su ukradene na društvenim mrežama, kako bi si na taj način pomogli u krađi identiteta. Malo je dokaza da većina korisnika društvenih mreža koristi pune mjere opreza kako bi se zaštitili od krađe identiteta.²⁸

²⁶ Isto.

²⁷ Usp. Wikipedia. Privacy concerns with social networking services. URL: http://en.wikipedia.org/wiki/Privacy_concerns_with_social_networking_services (2013-09-13)

²⁸ Isto.

4.3. Korištenje podataka u komercijalne svrhe

Internet i revolucija digitalne komunikacijske tehnologije dramatično su povećali tvrtkama mogućnost za ciljano oglašavanje za točno određene potrošače i za korištenje informacija o potrošačima za prilagodbu sadržaja oglašavanja. Međutim, kako online prikaz reklama postaje personaliziran, tvrtke riskiraju kako bi kupcima pronašle nametljive i osvajačke reklame.

Društvene mreže sada čine 23% online oglašavanja. One također uspoređuju veliku količinu osobnih podataka od svojih korisnika, a nude oglašivačima vlasničke oglasne mreže koje pomiču granice prilagođenog oglašavanja. Potrošači će možda vidjeti personaliziran sadržaj oglasa na takvim stranicama koji više apeliraju i više su povezani s njihovim interesima, ali također oni obratno mogu takvu situaciju vidjeti kao ne samo jezivom, nego i ugasiti stranicu ako osjete da je tvrtka je povrijedila njihovu privatnost.²⁹

Neka sučelja za socijalno umrežavanje kao što su Facebook eksperimentiraju s novim tehnologijama koje omogućuju potrošačima eksplicitnu kontrolu nad time koliko su informacije o njima javno dostupne. Teoretski, na taj način bi se mogla poboljšati učinkovitost online oglašavanja, jer su istraživanja ponašanja naglasila važnost potrošačke percepcije kontrole.³⁰

Facebook je najavio velik i dobro publiciran pomak u njihovim pravilima o privatnosti. Cilj je uvjeriti korisnike kako se njihovi podaci koriste, dajući im veću kontrolu nad svojim postavkama privatnosti i stupanj do kojega se njihove osobne identifikacijske podatke može pratiti ili koristiti od strane trećih osoba. Ova promjena nije utjecala na temeljni algoritam kojim su reklame prikazane, ciljano i personalizirano, budući da platforma za oglašavanje koristiti anonimne podatke. Postoje podaci o broju koliko je puta svaki oglas prikazan na pojedinačnom korisniku i koliki broj puta je korisnik kliknuo na svaki oglas u roku od pet tjedana od uvođenja nove kontrole privatnosti.

²⁹ Usp. Tucker, Catherine. Social Networks, Personalized Advertising, and Perceptions of Privacy Control, 2011. URL: http://www.twcresearchprogram.com/pdf/TWC_Tucker_v3a.pdf (2013-09-20)

³⁰ Isto.

Empirijska analiza sugerira da su personalizirane reklame dvostruko više učinkovite u privlačenju korisnika a Facebook stranica nakon smjene u Facebook politici koja je dala korisnicima više kontrole nad svojim osobnim informacijama ne daje značajne promjene u oglašavanju ali se koristi generička poruka tijekom razdoblja. To je i za očekivati, jer takvi oglasi ne bi jasno potrošačima pokazali jesu li njihovi osobni podaci ciljano korišteni.³¹

Treba napomenuti da je Facebook stvoren s osnovom idejom da spoji poznanike i stare prijatelje, no nije prošlo mnogo vremena do trenutka kada je prerastao u jednu od glavnih online oglašavačkih platformi upravo zbog mogućnosti okupljanja brojnih korisnika različitih demografskih skupina. Međutim, novija istraživanja pokazuju da je Facebookov udio u oglašavanju usporio i do 2014. godine neće zabilježiti veći pomak, dok je Google još uvijek prvak u tom području. Glavni razlog je upravo prefiks "društvena" koju ima Facebook.³²

Prema istraživanjima 66% Amerikanaca ne želi da marketing prilagodi reklame na njihovim interesima. Strah od takvog otpora dovela je do ograničenja krojenja oglasa oglašivača. Rana istraživanja o privatnosti jednostavno privatnost opisuju kao vođenje brige o davanju kontrole korisnicima nad svojim podacima. Međutim, više nedavnih istraživanja u informacijskim sustavima su pokazali kako pojedine razine kontrole mogu posredovati u zabrinutosti o privatnost. Literatura s područja psihologije pruža teorijsko obrazloženje tim nalazima. Kada potrošači osjećaju da je ponašanje tvrtke smeta njihovoj privatnost, to može dovesti do reaktancije. Odgovor na pitanje kako prevladati reaktanciju, koje je pojašnjeno i dokumentirano posebno u zdravstvenoj literaturi, je jačanje percepcije kontrole, čak i ako su te kontrole zapravo ne daju potpunu kontrolu nad domenom koja je pod prijetnjom. Dakle, tvrtke su u mogućnosti smanjiti reaktanciju

³¹ Isto.

³² Sok, Nikolina. Specijalizirane društvene mreže budućnost su interneta. URL: <http://www.planb.hr/specijalizirane-drustvene-mreze-buducnost-su-interneta/> (2013-09-04)

potencijalno nametljivim marketinškim aktivnostima na način da poboljšaju percipiranje kontrole potrošačima.³³

Prilikom svakog pristupa nekoj web stranici od strane korisnika, on nesvjesno otkriva dio informacija o sebi (poput vlastite IP adrese, datuma i vremena posjete web stranice, operacijskog sustava i web preglednika kojeg koristi itd). To su male količine informacija koje odvojeno ne daju puno saznanja o korisniku, ali ako se sve te male informacije o korisniku skupe i analiziraju, može se dobiti dosta dobra slika o njegovim navikama na internetu, interesima, trenutnim poslovima koje radi, a moguće je saznati i važne informacije poput imena i prezimena, mjesta stanovanja, zanimanja pa čak i broja bankovne kartice.³⁴ Upravo ovakve informacije se najčešće koriste u marketinške svrhe jer se na ovaj način mogu odrediti ciljane skupine za neki proizvod ili pojedinom korisniku prikazati točno određene reklame za koje je procijenjeno da bi korisnika najviše zanimalo (na temelju njegovih pretraživanja na internetu, trenutne stranice koje pregledava i sl). Ovakva upotreba privatnih informacija korisnika može zasmetati (npr. na mail adresu dolazi spam pošta), ali uglavnom mu neće izazvati veće neprilike.³⁵

Možemo reći da društvene mreže koje pružaju svoje usluge bez naknade korisnika mogu ostvariti profit od prodaje oglašavanja. To se ostvaruje kroz bihevioralno oglašavanje, također poznato kao ciljanje. Bihevioralno oglašavanje je pojam koji se koristi za krojenje reklama uzevši u obzir osobne interese pojedinca. Ova praksa je privlačna trgovcima jer ciljane reklame će vjerojatnije dovesti do kupnje od strane gledatelja za razliku od običnih, ne ciljanih reklama. Treba napomenuti da su ovakve reklame vrijedne

³³ Usp. Tucker, Catherine. Social Networks, Personalized Advertising, and Perceptions of Privacy Control, 2011. URL: http://www.twcresearchprogram.com/pdf/TWC_Tucker_v3a.pdf (2013-09-20)

³⁴ Usp. Laboratorij za sustave i signale. Privatnost na Internetu, 2010. URL: <http://sigurnost.lss.hr/images/dokumenti/lss-pubdoc-2010-10-002.pdf> (2013-09-10)

³⁵ Isto.

i na društvenim mrežama jer one mogu biti prodane po višoj cijeni od cijene redovnog oglasa.³⁶

Društvene mreže mogu prikupiti mnogo informacija o potencijalnim kupcima, a za koje su oglašivači vrlo zainteresirani. Na neki način, to može biti korisno za korisnika jer reklame on ili ona vidi može pojaviti više relevantne. Korisnike često ne smeta što im se prikazuju oglasi za ribičku opremu samo zato što je otvorio nekoliko web stranica s temama o ribolovu. Međutim, korisnika će itekako zasmetati ako internet servis zna njegovo ime, prezime i mjesto stanovanja, a on to nije nigdje upisao. Tada čovjek osjeća da mu je narušena privatnost. Još jedan slučaj u kojem je narušavanjem privatnosti korisniku učinjena šteta je krađa identiteta. Budući da se preko interneta može dobiti cijeli niz informacija o nekoj osobi, to može biti dovoljno da se neka druga osoba na osnovu prikupljenih informacija predstavlja identitetom žrtve.³⁷

Međutim ne postoje limiti za načine na koji oglašivači mogu prikupljati i koristiti informacije koje prikupe. Mogućnosti ponašanja reklamne industrije trenutno se uređuju. Tvrtke dobrovoljno slijede načela kao što načela koja su iznesena od strane Industry Group Interactive Advertising Bureau (IAB).³⁸

Ono što je svakako bitno napomenuti je da postoji zabrinutost u vezi takvog oglašavanja. U većini slučajeva potrošači ne mogu biti svjesni da su podaci povezani s njihovim profilima. Osim toga potrošači ne mogu vidjeti podatke povezane s njihovim profilima te nemaju mogućnosti ispraviti netočnosti. Također nema određenog maksimalnog razdoblja za zadržavanje podataka i nema sigurnosnih uvjeta za zadržavanje podataka, i na taj način ostavljaju ih podložne za moguće napade hakera kao i sigurnosne rizike.

³⁶ Usp. Privacy rights clearinghouse. Social Networking Privacy: How to be Safe, Secure and Social, 2013. URL: <https://www.privacyrights.org/social-networking-privacy> (2013-09-04)

³⁷ Usp. Laboratorij za sustave i signale. Privatnost na Internetu, 2010. URL: <http://sigurnost.lss.hr/images/dokumenti/lss-pubdoc-2010-10-002.pdf> (2013-09-10)

³⁸ Usp. Privacy rights clearinghouse. Social Networking Privacy: How to be Safe, Secure and Social, 2013. URL: <https://www.privacyrights.org/social-networking-privacy> (2013-09-04)

Ništa nije manje bitna i činjenica da se informacije o maloljetnicima mogu prikupljati i koristiti za bihevioralne reklame.³⁹

Što se Hrvatske tiče, prema Zakonu o zaštiti osobnih podataka⁴⁰ prikupljeni podaci se mogu koristiti isključivo u navedene svrhe i ukoliko je osoba čiji su predmetni podaci upoznata s njom. Isto tako, prema navedenom zakonu korisnik ima pravo usprotiviti se obradi osobnih podataka u svrhe marketinga (čl. 21.). No svemu navedenom ne ide u prilog činjenica da u čl. 7. Zakona o izmjeni i dopunama Zakona o zaštiti osobnih podataka⁴¹ osobni podaci, što podrazumijeva i fotografije, osobno ime, broj mobilnog telefona, tj. svaku informaciju koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati, se mogu koristiti ako je osoba sama objavila te podatke. Navedena činjenica je izuzetno bitna obzirom da su korisnici ti koji objavljuju veliku količinu podataka o sebi.

Ovaj problem je nešto o čemu se mnogo govorilo u medijima te je to glavni razlog zašto je Facebook postrožio pravila zaštite privatnosti a gore spomenuta istraživanja pokazuju nerazmjer između količine deklarativne brige o zaštiti privatnosti te količini podataka koje osobe svojevrijem ostavljaju na društvenoj mreži.⁴²

Ono što je najbitnije za zaključiti o korištenju podataka u komercijalne svrhe je to da su društvene mreže komercijalne i brinu se o svom prihodu. Tvrtke ih koriste za svoju promociju putem profila, a neke sponzoriraju diskusije i na taj način prikupljaju podatke o potrošačkim navikama te je ideja korištenja prikupljenih podataka u komercijalne svrhe sve bliža redovnoj praksi.

³⁹ Isto.

⁴⁰ Zakon o zaštiti osobnih podataka. // Narodne novine 103 (2003). URL: <http://narodne-novine.nn.hr/clanci/sluzbeni/305952.html> (2013-09-10)

⁴¹ Zakon izmjenama i dopunama Zakona o zaštiti osobnih podataka. // Narodne novine 41 (2008). URL: http://narodne-novine.nn.hr/clanci/sluzbeni/2008_04_41_1381.html (2013-09-10)

⁴² Usp. Mučnjak, Dorja. Društvene mreže i knjižnice: etičko pitanje // Knjižničar/ka: časopis Knjižničarskog društva Rijeka 3 (2012) , 3, str. 99. URL: <http://www.kdr.hr/drustvo/Casopis%20KDR%202012.pdf> (2013-09-10)

5. Istraživanje

5.1. Cilj i svrha istraživanja

Istraživanje je provedeno kako bi se dobio uvid o utjecaju dobi i spola na stavove prema privatnosti podataka na internetu. Ranija istraživanja pokazuju kako se mlađe osobe (18-29 godina starosti) osjećaju sigurnije na internetu nego starije osobe (50 + godina). Sukladno navedenom sjećaj sigurnosti može dovesti do veće spremnosti na djeljenje privatnih informacija na internetu (MacGibbon i Phair, 2012). Hoofnagle (2010) navodi da su mlađe osobe manje zabrinute i orijentirane na održavanje privatnosti svojih podataka, nego starije osobe. Osim toga istraživanja pokazuju da se žene osjećaju sigurnije na internetu nego muškarci, što može dovesti do njihove veće spremnosti na dijeljene podataka na internetu (MacGibbon i Phair, 2012)

Dakle, obzirom da je internet kao i društvene mreže sveprisutan u današnjici, zanimali su nas stavovi o privatnosti podataka na društvenim mrežama kao i razlike u stavovima obzirom na dob i spol. Pri tome smo koristili nezavisne varijable dob i spol dok je zavisna varijabla izraženost stava prema privatnosti podatka na internetu na pojedinoj subskali Upitnika privatnosti na internetu koji je priložen u ovom radu a same subskale su navedene u daljnjem tekstu. Veći rezultat ukazuje na veću brigu oko privatnosti vlastitih podaka.

Nadalje, istraživanje je krenulo od sljedeće hipoteze:

Postoji statistički značajna razlika u stavovima prema privatnosti podataka na internetu s obzirom na dob i spol. Mlađi sudionici i bit će spremnije dijeliti više podataka na internetu od starijih sudionika i muškaraca.

Nakon provedene obrade rezultata koja je uključila varijable dobi i spola provedene su dodatne provjere utjecaja varijabli kao što je mreža kojom se koriste sudionici i obzirom da se Facebook pokazao mrežom kojom se sudionici najčešće koriste u daljnju obradu rezultata uvrštene su 3 dodatne varijable a to su:

- dužina posjedovanja Facebook računa,

- prosječno posjećivanje Facebooka,
- vrijeme provedeno na Facebooku

Iz ovih dodatnih varijabli možemo postaviti i sljedeću hipotezu:

Smatramo da oni koji više vremena provode na internetu upoznati su s time kako mogu zaštititi svoju privatnost.

5.2. Metodologija

Istraživanje se provodilo tijekom listopada 2013. godine. Sudionici u istraživanju bili su korisnici interneta, od toga 138 ženskog i 87 muškog spola. Raspon godina sudionika kretao se od 13-85 godina. Istraživanje je provedeno putem online upitnika. Sudionicima je osigurana anonimnost, odnosno od njih se nije zahtjevalo da upišu ime i prezime. Sudionici su prvo upisali svoje socio-demografske podatke kao što su dob i spol a nakon toga bilo je potrebno odabrati koje društvene mreže koriste. Ukoliko su sudionici odabrali Facebook kao jednu od društvenih mreža koje koriste, ponuđena su im dodatna pitanja o tome koliko dugo imaju Facebook račun, koliko prosječno posjećuju Facebook te koliko vremenski gledano traje njihov prosječni posjet Facebooku. Nakon toga, sudionici su ispunjavali Upitnik privatnosti na internetu.

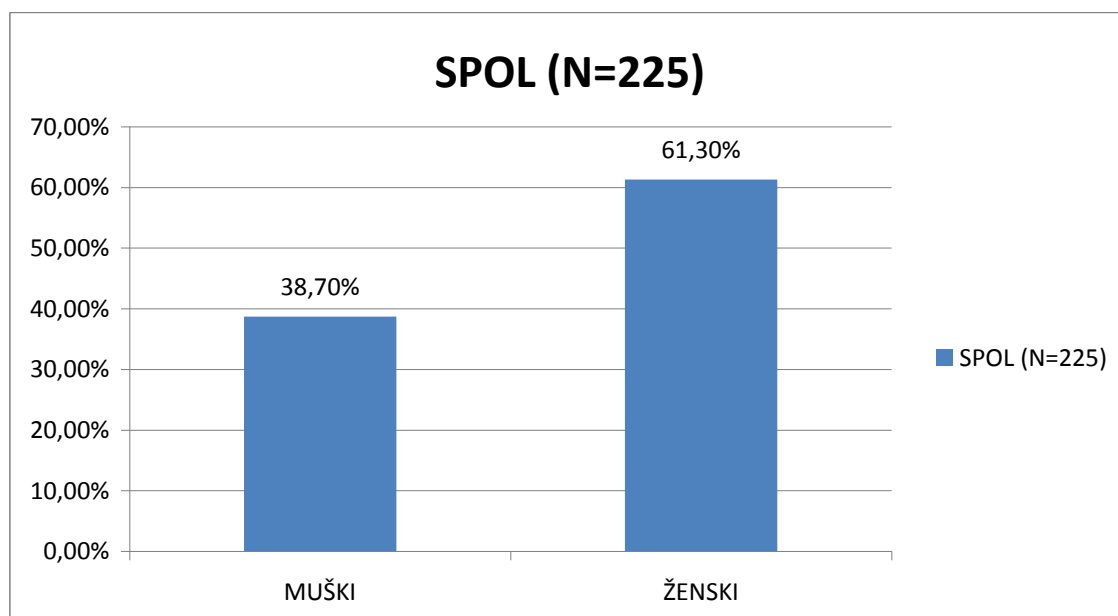
U istraživanju bi bila korištena prilagođena verzija Upitnika privatnosti na internetu (Internet Privacy Scales – IPS; Buchannan, 2006)⁴³. Anketni upitnik (Prilog 1.) sastoji se od 9 pitanja počevši od svojih socio-demografske podatke kao što su dob i spol. Upitnik se sastoji od tri subskale. Subskala „Briga o privatnosti“, koja sadrži 16 čestica, odražava afektivnu i kognitivnu komponentu stavova prema sigurnosti na internetu. Subskale „Opći oprez“, koja sadrži šest čestica, i „Tehnička zaštita“, koja sadrži šest čestica, odražavaju bihevioralnu komponentu stava prema sigurnosti na internetu. Odgovori sudionika bodovali se na skali Likertovog tipa od jedan (nikad) do pet (uvijek) na

⁴³ URL: http://personalwebpages.deusto.es/reips/pubs/papers/privacy_scalesJASIST.pdf (2013-09-10)

subskalama „Opći oprez“ i „Tehnička zaštita“, te od jedan (uopće se ne brinem) do pet (uvijek se brinem) na subskali „Briga o privatnosti“. Ukupni rezultat čini kompozit zbrojenih čestica te prosjek na pojedinim subskalama. Pri tome, veći rezultat predstavlja veću brigu o privatnosti vlastitih podataka.

5.3. Analiza rezultata

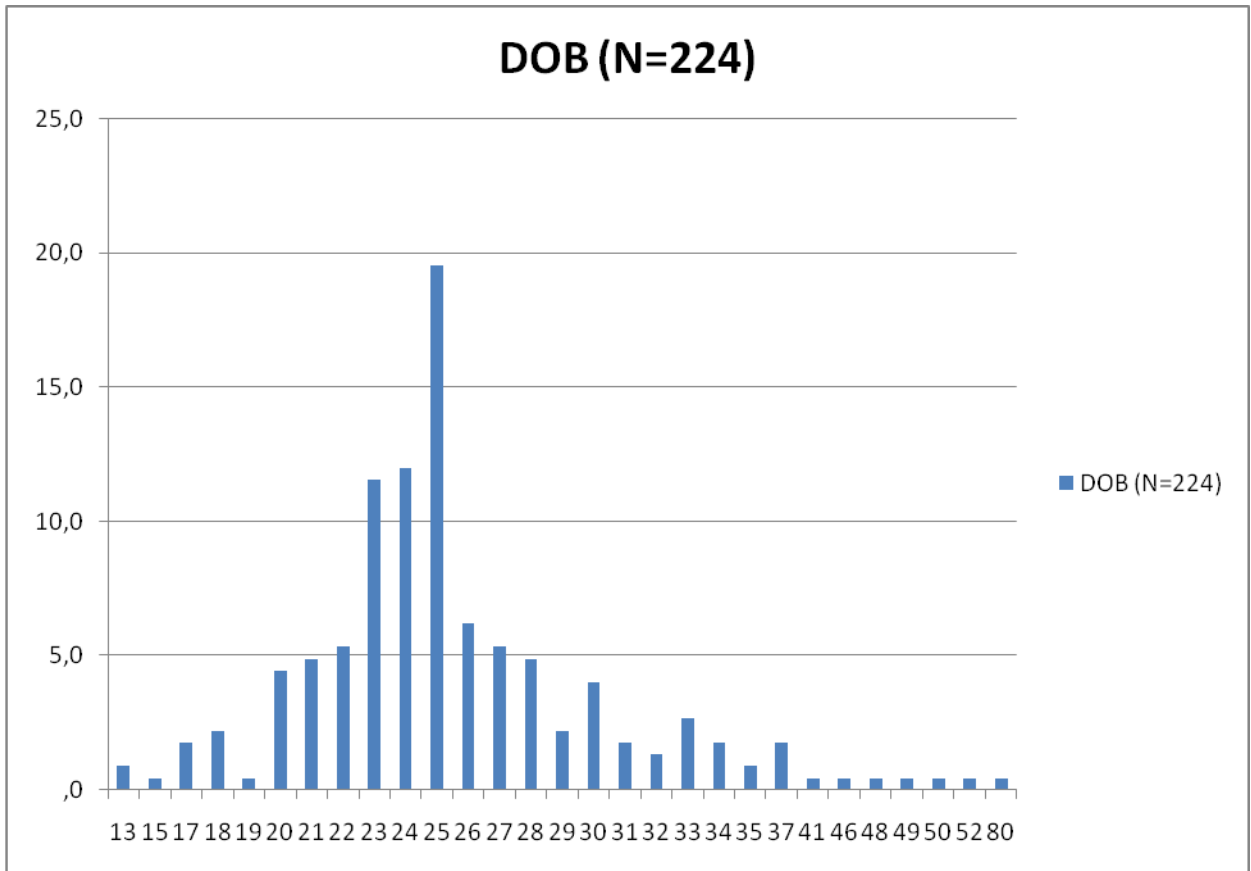
Kao što smo prethodno naveli, istraživanje smo započeli upitima socio-demografske prirode. Prvo pitanje našeg istraživanja odnosilo se na spol. Ukupan broj odgovora na ovo pitanje bilo je 225 od toga 138 ženskog i 87 muškog spola (Tablica 2).



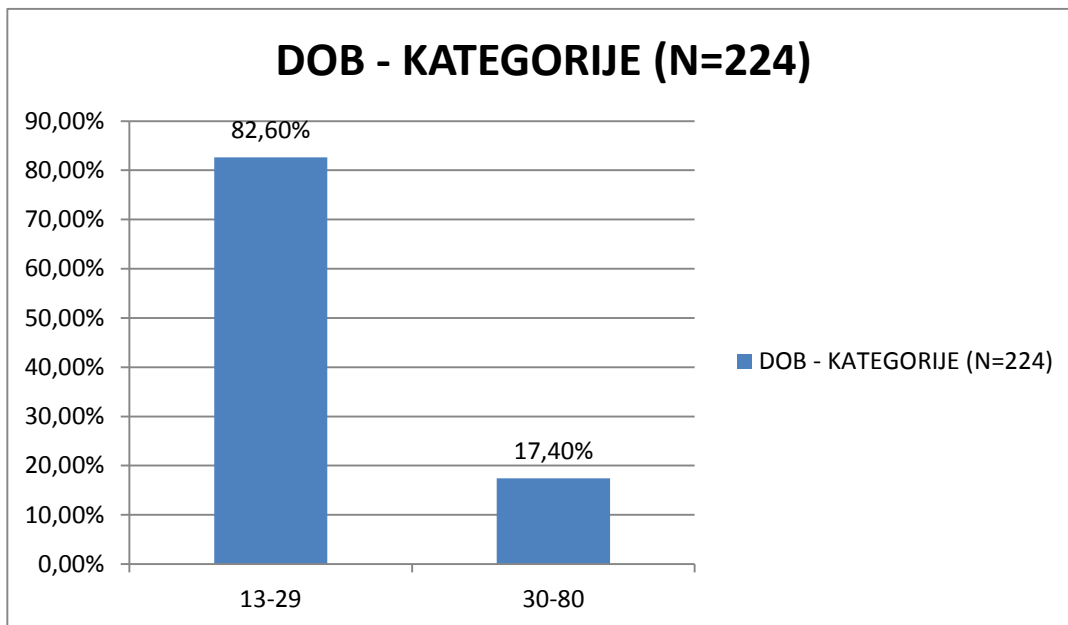
Tablica 2.

Sljedeće pitanje odnosilo se na dob ispitanika. Na ovo pitanje je odgovorilo 224 sudionika te se iz njihovih odgovora uviđa da se raspon godina sudionika kreće od 13-85 godina (Tablica 3). Iz navedenih rezultata lako možemo zaključiti kako je najviše sudionika starosti 25 godina. Najmlađi sudionici su starosti 13 godina dok je najstariji sudionik star 80 godina. Kako bismo lakše analizirali rezultate podjelili smo sudionike u dvije dobne skupine (Tablica 4). Prva dobna skupina odnosila se na sudionike u rasponu

od 13 do 29 godina dok se druga dobna skupina odnosila na sudionike u rasponu od 30 do 80 godina. Potrebno je naglasiti kako 185 sudionika, tj. 82,60% sudionika koji su odgovorili na ovo pitanje spada u prvu dobnu skupinu (od 13 do 29 godina) dok njih 39, tj. 17,40% spada u drugu dobnu skupinu (od 30 do 80 godina).



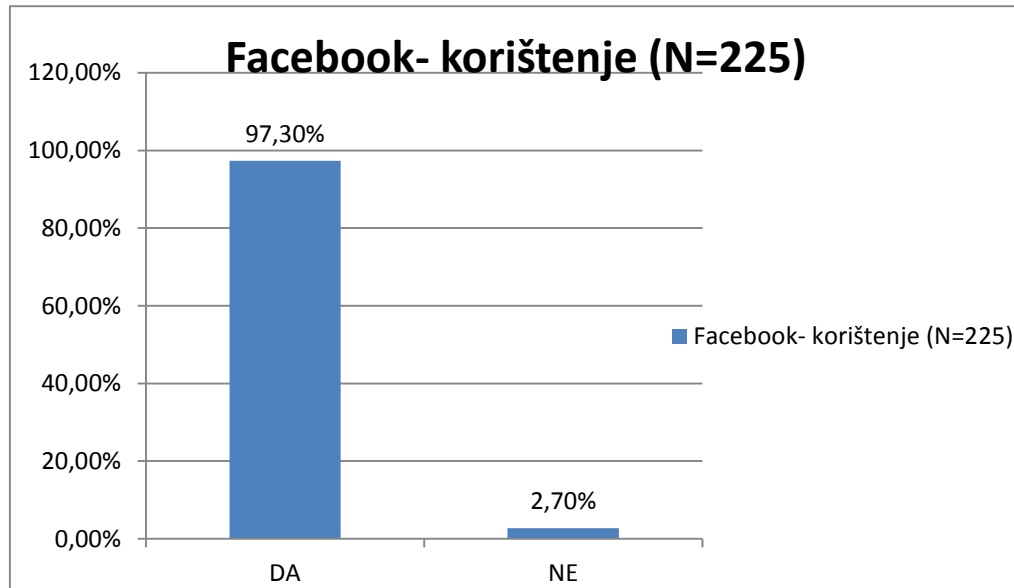
Tablica 3



Tablica 4

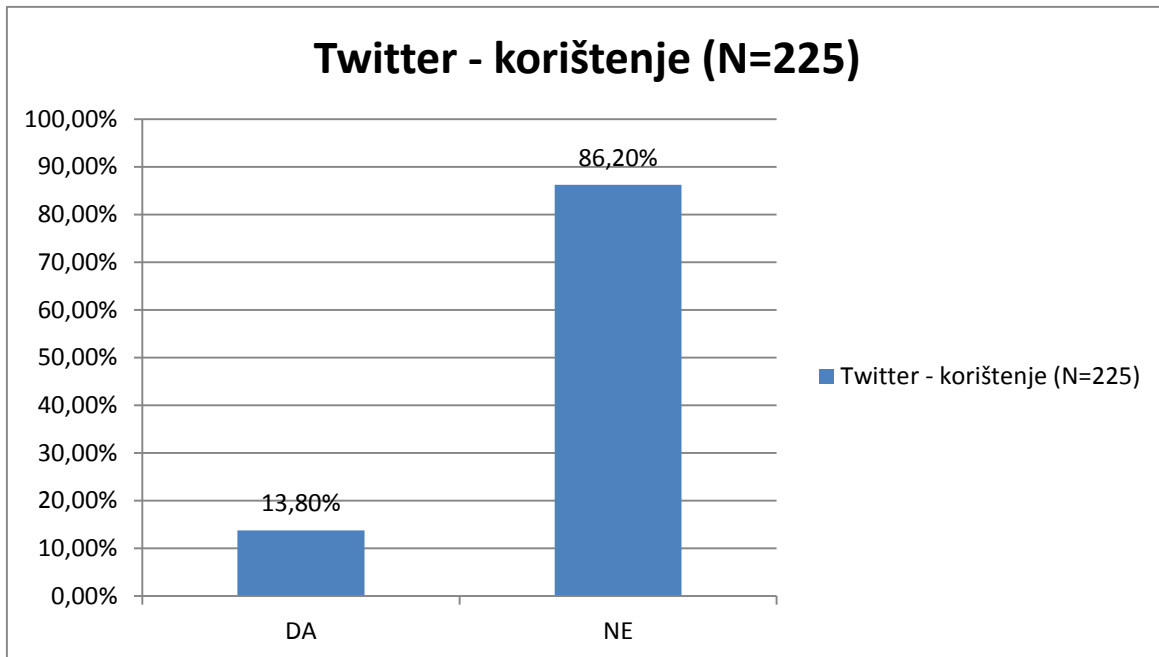
Nadalje nas je zanimalo koje od trenutno najpopularnijih društvenih mreža sudionici koriste. Ponuđene su društvene mreže Facebook, Twitter, Pinterest i LinkedIn gdje su se sudionici odabirom opcije “Da” ili “Ne” izjasnili koju mrežu koriste. U navedenim pitanjima o korištenju pojedine društvene mreže *missing values* tj. pitanja gdje sudionici nisu odgovorili gledano je kao da su odgovorili “Ne”.

Na pitanje o korištenju Facebooka (Tablica 5) odgovorilo je 225 sudionika i to na način da ih se 219, tj. 97,30 % izjasnilo da koristi Facebook dok ih se samo njih 6, tj. 2,70 % izjasnilo kako ga ne koriste. Ovaj podatak svjedoči o popularnosti Facebooka kao društvene mreže.



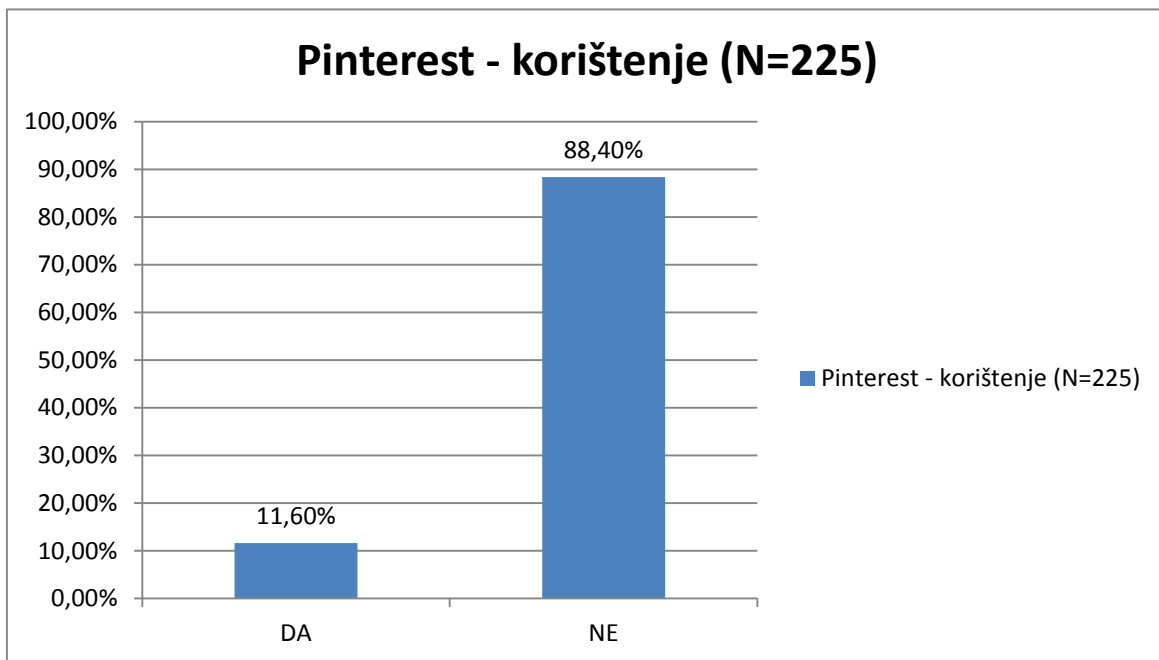
Tablica 5

Na pitanje o korištenju Twittera također se izjasnilo 225 sudionika (Tablica 6). Situacija je vidno drugačija nego s korisnicima Facebooka te se mnogo više sudionika izjasnilo da ne koriste Twitter nego da ga koriste. Nakon provedene analize utvrđeno je kako se 13,80 % sudionika izjasnilo da koriste mrežu Twitter dok se njih 86,20 % izjasnilo da koriste što bi značilo da ukupno njih 194 od 225 ne koristi ovu društvenu mrežu.



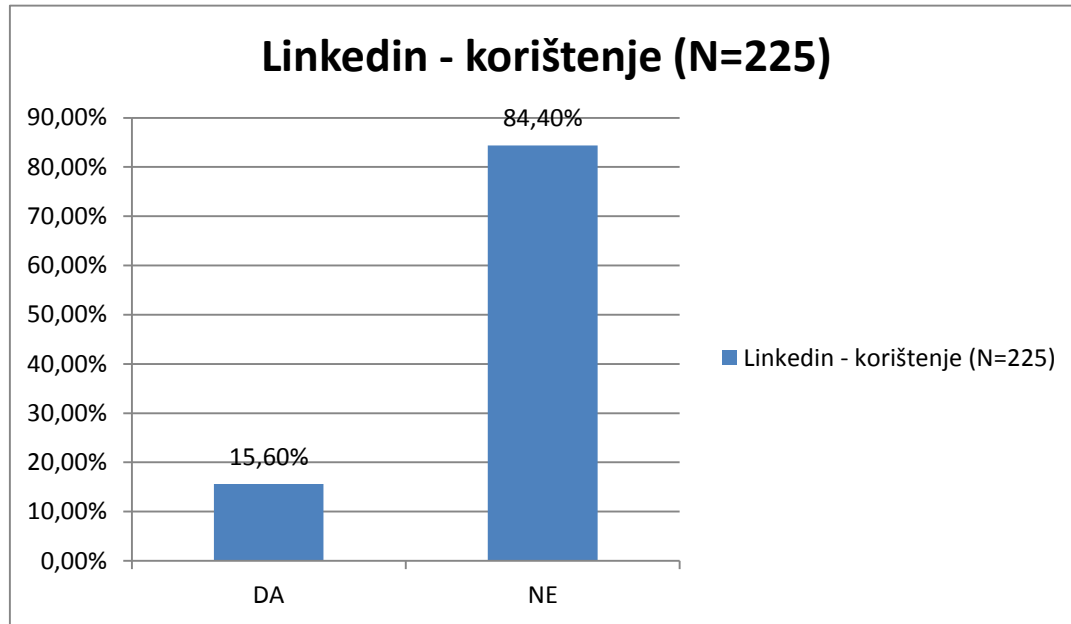
Tablica 6

Nadalje slijedi Pinterest (Tablica 7) gdje se također o pitanju o korištenju ove društvene mreže izjasnilo 225 sudionika i to na način da ih se njih 26, tj. 11,60 % izjasnilo da koriste ovu društvenu mrežu dok se njih čak 199, tj. 88,40 % izjasnilo da je ne koriste.



Tablica 7

Naposlijetku smo istražili korištenje društvene mreže LinkedIn (Tablica 8). I ovdje se izjasnilo 225 sudionika te su rezultati vrlo slični kao u slučaju korištenja Twittera i Pinteresta. Od 225 sudionika njih 35, tj. 15,60 % izjasnilo se da koriste ovu društvenu mrežu. Njih pak 190 izjasnilo se da je ne koriste što je 84,40% ispitanika.



Tablica 8

Nakon što smo obradili podatke, vrlo je lako zaključiti kako je Facebook daleko najzastupljenija mreža. Obzirom da je navedeno bilo očekivano, u daljnju obradu rezultata uvrštene su 3 dodatne varijable a to su dužina posjedovanja Facebook računa, prosječno posjećivanje Facebooka i vrijeme provedeno na Facebooku tako da se sljedeće tablice odnose se samo na korištenje Facebooka, manji broj odgovora sudionika na ovim pitanjama je rezultat što neki od sudionika ne koriste Facebook. Dakle, sudionici koji su pozitivno odgovorili na pitanje o tome koriste li Facebook dobili su mogućnost odgovaranja na 3 dodatna pitanja vezana za Facebook. Prilikom računanja ovdje su se morali uzeti u obzir samo oni koji su odgovorili na pitanje jer se pretpostavlja da oni koji nisu odgovorili nemaju Facebook. Upravo iz navedenog razloga na sljedećim upitima sudjelovalo je 219 sudionika.

Dakle, kao što smo ranije naveli, prvo pitanje se odnosilo na korištenje Facebooka (Tablica 9). Sudionicima je postavljen upit „Koliko dugo imate Facebook račun?“ te je 219 sudionika odgovorilo na sljedeći način, njih samo 0,9% koristi Facebook unazad 1 godinu dok najveći broj ispitanika, njih čak 67,6 % koristi Facebook 4 godine i duže. Iz navedenih rezultata može se jasno uočiti kako se s postotak povećavao s godinama korištenja Facebooka.

Facebook - korištenje	Postotak
Do 1 godine	0,9 %
Od 1 godine do 2 godine	2,7%
Od 2 godine do 3 godine	9,6%
Od 3 godine do 4 godine	19.2%
4 godine i duže	67,6%

Tablica 9

Što se tiče posjećivanja Facebooka (Tablica 10), na ovom pitanju je također sudjelovalo 219 sudionika. Sudionicima je postavljen upit „Koliko prosječno posjećujete svoj Facebook račun?“ a ponuđeni odgovori kretali su se od „Barem jednom tjedno“ do „Više od 5 puta tijekom dana“. Najveći postotak sudionika, čak njih 55 odgovorilo da posjećuje Facebook više od 5 puta tijekom dana.

Facebook - posjete	Postotak
Barem jednom tjedno	3,7 %
Više puta tjedno	2,7 %
Barem jednom dnevno	25,1 %
Do 5 puta tijekom dana	25,1 %
Više od 5 puta tijekom dana	43,4 %

Tablica 10.

Kao što smo ranije naveli, ispitali smo i koliko traje prosječni posjet Facebooku ispitanika (Tablica 11). I ovo pitanje odgovorilo je 219 sudionika od kojih se najveći broj, 89, tj. 40,6 % izjasnilo da koriste Facebook manje od 15 minuta dnevno. Najmanji broj sudionika izjasnio se da koristi Facebook od 1h do 2h dnevno, njih 16, tj. 7,3 %. Zanimljivo je da je više korisnika odovorilo da koriste Facebook više od 2 h dnevno, njih 23, tj. 10,5 % . Iz svega navedenoga možemo zaključiti da sudionici uglavnom imaju više kraćih posjeta dnevno.

Facebook - posjete	Postotak
Manje od 15 min	40,6 %
Od 15 min do 30 min	29,7 %
Od 30 min do 1 h	11,9 %
Od 1 h do 2 h	7,3 %
Više od 2 h	10,5 %

Tablica 11.

Nadalje smo ispitali mišljenja sudionika po pitanjima o općeg opreza, tehničke zaštite i brige o privatnosti te smo navedeno postavili kao subskele upitnika. Dobivena mišljenja sudionika usporedili smo s 5 već ranije spomenutih nezavisnih varijabli:

1. Dob
2. Spol
3. Koliko dugo imate Facebook račun?
4. Koliko prosječno posjećujete svoj Facebook račun?
5. Vremenski gledano, koliko traje Vaš prosječni posjet Facebooku?

Na taj način smo doznali postoji li značajnija razlika u stavovima sudionika po pitanjima nezavisnih varijabli.

Dakle, kako bi se provjerilo postoji li statistički značajna razlika u stavovima prema sigurnosti na internetu te pojedinim aspektima istih s obzirom na spol proveden je t-test.

Statistički značajna razlika u izraženosti stavova prema navedenoj varijabli dobivena je na subskali brige o privatnosti ($t=3,067$, $p=,002$). Navedeno je vidljivo u Tablici 12. Statistički značajna razlika u stavovima prema sigurnosti na internetu s obzirom spol potvrđena je samo na subskali brige o privatnosti, Na na ostalim subskalama primjećeno je kako ne postoji statistički značajna razlika kao niti u ukupnom rezultatu. Iz toga je jasno vidljivo da su se žene na subskali brige o privatnosti izjasnile kako više brinu o privatnosti od muškaraca dok po pitanjima općeg oprza kao i tehničkoj zaštiti nema razlike u stavovima.

	M		t	p
Opći oprez	M	16.1786	0,791	,430
	Ž	16.7704		
Tehnička zaštita	M	20,023	-1,366	,173
	Ž	19,022		
Briga o privatnosti	M	40,259	3,067	,002 p<0,01
	Ž	45,977		
UKUPNO	M	8,601	0,812	,418
	Ž	8,823		

Tablica 12.

Nadalje, kako bi se provjerilo postoji li statistički značajna razlika u stavovima prema sigurnosti na internetu te pojedinim aspektima istih s obzirom na dob sudionika proveden je t-test (Tablica 13). Rezultati t-test ukazali su kako ne postoji statistički značajna razlika u navedenim stavovima s obzirom na dob što je pokazalo da dob značajno ne utječe na stavove prema sigurnosti na internetu.

	M		t	p
Opći oprez	13-29	16,365	-1,074	,284
	29-30	17,395		
Tehnička zaštita	13-29	19,385	-0,106	,916
	29-30	19,487		
Briga o privatnosti	13-29	43,783	-,053	,958
	29-30	43,914		
UKUPNO	13-29	8,717	-0,383	,702
	29-30	8,852		

Tablica 13.

Kako je upitnik ukazao da velik broj sudionika koristi društvenu mrežu Facebook, provedene su daljnje analize koje su kao varijable uključile: dužinu posjedovanja Facebook računa, prosječno posjećivanje Facebooka i vremensko trajanje pojedinog posjeta. Prilikom provedbe navedenih analiza uočena je značajna razlika na varijabli dužine posjedovanja Facebooka računa na subskali općeg opreza. Najizraženije stavove u navedenoj subskali imali su sudionici koji koriste Facebook od 1-2 godine, dok su najmanje izražene stavove imali sudionici koji koriste Facebook 4 i duže godina iz čega se vrlo lako može zaključiti da što duže imaju Facebook manji je oprez. Navedeni rezultati vidljivi su u Tablici 14. Na ostalim subskalama te ukupnom rezultatu na upitniku nisu pronađene statistički značajne razlike.

		M	F	p
Opći oprez	do 1 godine	22,000	3,102	,017
	od 1 godine do 2 godine	23,167		
	od 2 godine do 3 godine	17,191		
	od 3 godine do 4 godine	16,585		
	4 godine i duže	16,224		
Tehnička zaštita	do 1 godine	23,000	0,425	,790
	od 1 godine do 2 godine	18,667		
	od 2 godine do 3 godine	20,476		
	od 3 godine do 4 godine	19,476		
	4 godine i duže	19,524		
Briga o privatnosti	do 1 godine	56,000	1,302	,271
	od 1 godine do 2 godine	50,667		
	od 2 godine do 3 godine	46,400		
	od 3 godine do 4 godine	41,500		
	4 godine i duže	43,750		
UKUPNO	do 1 godine	11,000	2,303	,060
	od 1 godine do 2 godine	10,139		
	od 2 godine do 3 godine	9,3333		
	od 3 godine do 4 godine	8,499		
	4 godine i duže	8,710		

Tablica 14.

Kada je uzeta u obzir varijabla prosječne posjećenosti Facebook računa dobivene su značajne razlike na subskalama općeg opreza ($F=7.191$, $p=,000$), tehničke zaštite

($F=6,454$, $p=,000$) te u ukupnom rezultatu ($F=7.132$, $p=,000$). Opći oprez najizraženiji je kod sudionika koji posjećuju facebook račun najmanje jednom tjedno ($M=21$), dok je najmanje izražen kod sudionika koji ga posjećuju više puta tjedno ($M=14,167$). Stavove prema tehničkoj zaštiti imaju najviše izraženi sudionici koji posjećuju facebook najmanje jednom tjedno ($M=23.25$), dok su najmanje izraženi kod onih koji ga posjećuju više puta tijekom dana ($M=18.426$). Opći stav prema sigurnosti na internetu najizraženije je također kod sudionika koji posjećuju facebook barem jedno tjedno ($M=10.461$), dok je najmanje izražen kod sudionika koji ga posjećuju više puta tijekom dana ($M=8.361$). Navedeni trend rezultata ukazuje na to da s porastom broja prosječnih posjeta na facebook stavovi prema sigurnosti na internetu postaju manje izraženi što znači da opći oprez, primjena tehničke zaštite i opća briga za privatnost opada.

		M	F	p
Opći oprez	Barem jednom tjedno	21,000	7,191	,000
	Više puta tjedno	14,167		
	Barem jednom dnevno	19,241		
	Do 5 puta tijekom dana	15,889		
	više od 5 puta tijekom dana	15,326		
Tehnička zaštita	Barem jednom tjedno	23,250	6,454	,000
	Više puta tjedno	19,668		
	Barem jednom dnevno	22,111		
	Do 5 puta tijekom dana	18,648		
	Više od 5 puta tijekom dana	18,426		
Briga o privatnosti	Barem jednom tjedno	49,375	1,315	,265
	Više puta tjedno	47,600		
	Barem jednom dnevno	46,039		
	Do 5 puta tijekom dana	41,245		
	Više od 5 puta tijekom dana	43,584		
UKUPNO	Barem jednom tjedno	10,461	7,132	,000
	Više puta tjedno	8,642		
	Barem jednom dnevno	9,705		
	Do 5 puta tijekom dana	8,410		
	Više od 5 puta tijekom dana	8,361		

Tablica 15

Kada je uzeto u obzir prosječno trajanje pojedinog posjeta facebooku, provedena analiza varijance nije ukazala da postoji značajna razlika u stavovima prema sigurnosti na internetu i njezinim aspektima. Navedeno je vidljivo u Tablici 16.

		M	F	p
Opći oprez	manje od 15 min	16,895	0,157	,960
	od 15 min do 30 min	16,302		
	od 30 min. do 1h	16,720		
	od 1h do 2h	17,000		
	više od 2 sata	16,261		
Tehnička zaštita	manje od 15 min	20,315	2,278	,062
	od 15 min do 30 min	19,270		
	od 30 min. do 1h	20,080		
	od 1h do 2h	20,313		
	više od 2 sata	16,870		
Briga o privatnosti	manje od 15 min	43,395	0,891	,471
	od 15 min do 30 min	43,742		
	od 30 min. do 1h	45,640		
	od 1h do 2h	48,929		
	više od 2 sata	40,842		
UKUPNO	manje od 15 min	8,919	1,452	,219
	od 15 min do 30 min	8,791		
	od 30 min. do 1h	8,909		
	od 1h do 2h	9,201		
	više od 2 sata	7,8860		

Tablica 16

5.4. Rasprava

Nakon dobivenih rezultata i njihove obrade, postavljena hipoteza prema kojoj se očekivalo da postoji statistički značajna razlika u stavovima prema sigurnosti na internetu s obzirom spol potvrđena je samo na subskali brige o privatnosti, dok na ostalim subskalama te ukupnom rezultatu ne postoji statistički značajna razlika. Žene na subskali

brige o privatnosti postižu značajno veće rezultate nego muškarci što ukazuje na to da više brige posvećuju pitanju privatnosti.

Postavljena hipoteza prema kojoj se očekivalo da postoji statistički značajna razlika u stavovima prema sigurnosti na internetu s obzirom na dob nije potvrđena.

Kako je upitnik ukazao da velik broj sudionika koristi društvenu mrežu Facebook, provedene su daljnje analize koje su kao varijable uključile: dužinu posjedovanja Facebook računa, prosječno posjećivanje Facebooka i vremensko trajanje pojedinog posjeta. Prilikom provedbe navedenih analiza uočena je značajna razlika na varijabli dužine posjedovanja Facebooka računa na subskali općeg opreza. Rezultati ukazuju na to da sudionici koji koriste Facebook od 1-2 godine izvještavaju o značajno manjem općem oprezu, nego sudionici koji koriste Facebook 4 i duže godina. Sukladno navedenom, može se zaključiti kako osobe koje duže koriste društvenu mrežu Facebook izvještavaju o manjem općem oprezu. Na ostalim subskalama te ukupnom rezultatu na upitniku nisu pronađene statistički značajne razlike.

Kada je uzeta u obzir varijabla prosječne posjećenosti Facebook računa dobivene su značajne razlike na subskalama općeg opreza, tehničke zaštite te u ukupnom rezultatu i to na način da je opći oprez najizraženiji kod sudionika koji posjećuju Facebook račun najmanje jednom tjedno, dok je najmanje izražen kod sudionika koji ga posjećuju više puta tjedno. Također je potrebno napomenuti da najviše izražene stavove prema tehničkoj zaštiti imaju sudionici koji posjećuju Facebook najmanje jednom tjedno a najmanje izraženi su kod onih koji ga posjećuju više puta tijekom dana. Opći stav prema sigurnosti na internetu najizraženiji je također kod sudionika koji posjećuju Facebook barem jedno tjedno, dok je najmanje izražen kod sudionika koji ga posjećuju više puta tijekom dana.

Rezultati ovog istraživanja ukazuju kako je potrebno razmotriti različite aspekte utjecaja koje varijable povezane sa samim korištenjem društvenih mreža imaju na razlike u stavovima prema sigurnosti na internetu. Također bi bilo potrebno sagledati je li spol dobra odrednica za provedbu ovog istraživanja obzirom da postoje različiti načini usvajanja stavova. Jedan od njih je npr. socijalizacija. Kada je riječ o privatnosti na internetu, i djevojke i muškarci se jednako socijaliziraju. S obzirom na to možemo

pretpostaviti da će razlike u stavovima prema sigurnosti kod muškaraca i žena biti raspoređene po slučaju tehničke zaštite i brige o privatnosti. Na aspektu općeg opreza, opet može biti socijalizacija jer se žene uči da budu opreznije, da kritički promatraju ponudene opcije i sl.

Također je potrebno napomenuti da je najveći broj sudionika u ovom istraživanju bio u rasponu od 13 do 29 godina, odnosno mlada životna dob. Sukladno navedenom, potrebna bi bila velika razlika u rezultatima s obzirom na dobne skupine da bi se ona proglasila značajnom, stoga možda ovo istraživanje nije bilo dovoljno osjetljivo. Navedeno bismo trebali poboljšati tako da bismo imali veći broj sudionika te podjednak i velik broj u svakoj dobnoj skupini. Tada bi i male razlike mogle biti značajne, a da se rizik od pogreške ne poveća. Navedeno možemo sagledati i kao potencijalne nedostatke provedenog istraživanja. Relativno homogen uzorak sudionika s obzirom na dobnu kategoriju kojoj pripadaju mogli su dovesti do rezultata koji ukazuju da ne postoji utjecaj spola i dobi na izraženost stavova prema sigurnosti na društvenim mrežama na svim aspektima stavova. Također postoji mogućnost da su neke druge varijable jače odrednice stavova prema sigurnosti na internetu ili se pak nalaze u podlozi djelovanja koje imaju spol i dob.

Svakako bi u daljnja istraživanja bilo potrebno uključiti ravnomjerniji broj sudionika različite dobi za što bi bio primjeren kvotni uzorak te bi se istraživanje moglo usmjeriti samo na korisnike Facebooka s obzirom da najveći broj sudionika koristi navedenu društvenu mrežu.

6. Zaključak

Sigurnost i privatnost na društvenim mrežama postaju zadnjih godina ozbiljne teme nerijetko prisutne u raznim medijima. Alati za društvene mreže uvelike slijede zahtjeve i pritiske korisnika te, u skladu s njima, unaprjeđuju i nadograđuju mogućnosti i opseg sigurnosnih postavki. Nadalje, korisnici postaju svjesni koje su informacije o njima dostupne javnosti i da ih mogu mijenjati informacije tako da odgovaraju njihovim

potrebama. Privatnost ne podrazumijeva samo da korisnici nešto drže daleko od očiju javnosti, već se radi o odabiru onoga što žele da javnost vidi. Prilikom korištenja društvenih mreža ljudi su izloženi brojnim napadima na svoju privatnost i od toga gotovo da se ne mogu zaštititi. Danas je mnogo lakše skupiti informacije o nečijim navikama posjećivanja određenih sadržaja i skinuti podatke unesene u različite online formulare.

Zbog zadovoljstva koje se postiže korištenjem Facebooka često se znaju zanemariti određene prijetnje prema privatnosti. S vremenom se stvorila navika korištenja, pa čak i ovisnost, tako da sada jednostavno više nema povratka. Informacije o krađi privatnih podataka vrlo teško da će bilo koga natjerati na prestanak korištenja društvenih mreža. Strategija za zaštitu privatnosti - mijenjanje vidljivosti profila tako da se pristup dozvoljava samo prijateljima - je jako slab mehanizam. Mnogi korisnici izgleda ni ne shvaćaju da ograničavanje pristupa svojim podacima nije dovoljna zaštitna mjera s obzirom na količinu, kvalitetu i konstantnost podataka koju objavljuju. Srećom, danas velike kompanije kao što su Google i Facebook moraju paziti na privatnost korisnika, pa se valja dobro upoznati s takvim servisima i vidjeti koje su opcije na raspolaganju. Dobar primjer je Facebook na kojem se i bazira ovaj rad, a koji omogućuje iznimno detaljno podešavanje sigurnosnih opcija, kao i onih vezanih uz privatnost. Korisnici ih često zanemaruju, pa ostavljaju svoj profil otvoren, možda ni ne znajući da svaki od 160 milijuna korisnika Facebooka može vidjeti njihove podatke. Zato je potrebno postati svjestan sigurnosnih rizika i opasnosti na društvenim mrežama. Treba znati da se korištenjem društvenih mreža, svaki korisnik se odriče dijela svoje privatnosti. Stoga je važno dobro procijeniti informacije koje planiramo objaviti i koje možda ostavljamo za sobom.

7. Literatura

1. Chen, Kay-Yut; Fine, Leslie R.; Huberman, Bernardo A. Predicting the Future. URL: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.2.3539&rep=rep1&type=pdf>
2. Danah M, Boyd, Social Networking Sites: definition, history and scholarship, 2007. URL: <http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/pdf>. (2013-08-22)
3. Kaplan, Andreas M.;Haenlein, Michael. Users of the world, unite! The challenges and opportunities of Social Media. URL: <http://www.sciencedirect.com/science/article/pii/S0007681309001232> (2013-08-24)
4. Miljak, Suzana. Uporaba društvenih mreža za upravljanje znanjem.URL: http://www.famns.edu.rs/skup1/radovi_pdf/miljak.pdf. (2013-08-31)
5. Mučnjak, Dorja. Društvene mreže i knjižnice: etičko pitanje // Knjižničar/ka: časopis Knjižničarskog društva Rijeka 3 (2012) , 3, str. 99. URL: <http://www.kdr.hr/drustvo/Casopis%20KDR%202012.pdf> (2013-09-10)
6. Privacy rights clearinghouse.Social Networking Privacy: How to be Safe, Secure and Social, 2013. URL: <https://www.privacyrights.org/social-networking-privacy>

7. ProtectMyID. Facebook Fraud: Identity Theft through Social Networking. URL: http://www.protectmyid.com/images/education_center/pdf/050TypesofFraud/7_types%20of%20fraud_social%20networking.pdf

8. Sok, Nikolina. Specijalizirane društvene mreže budućnost su interneta. URL: <http://www.planb.hr/specijalizirane-drustvene-mreze-buducnost-su-interneta/> (2013-09-04)

9. Tucker, Catherine. Social Networks, Personalized Advertising, and Perceptions of Privacy Control, 2011. URL: http://www.twcresearchprogram.com/pdf/TWC_Tucker_v3a.pdf (2013-09-20)

10. Vidipedija, slobodna tehno enciklopedija. Društvene mreže. URL: http://www.vidipedija.com/~vidipedi/index.php?title=Dru%C5%A1tvene_mre%C5%BEe. (2013-08-22)

11. Wikipedia. Privacy concerns with social networking services. URL: http://en.wikipedia.org/wiki/Privacy_concerns_with_social_networking_services

12. Zakon o zaštiti osobnih podataka. // Narodne novine 103 (2003). URL: <http://narodne-novine.nn.hr/clanci/sluzbeni/305952.html>

13. Zakon izmjenama i dopunama Zakona o zaštiti osobnih podataka. // Narodne novine 41 (2008). URL: http://narodne-novine.nn.hr/clanci/sluzbeni/2008_04_41_1381.html

8. Prilozi

Prilog 1. Anketni upitnik

Društveni mediji i privatnost

Poštovani,

Upitnik koji je pred Vama dio je istraživanja stavova o privatnosti na Internetu. Istraživanje se provodi kao dio diplomskog rada na Odsjeku za informacijske znanosti Filozofskog fakulteta u Osijeku. Svi prikupljeni podaci koristit će se jedino i isključivo u svrhu ovog istraživanja. Anketa je potpuno anonimna i ne bi trebala oduzeti više od 10 minuta Vašeg vremena. Molim Vas da anketu shvatite ozbiljno te da u odgovorima budete što iskreniji, jer o tome ovisi uspješnost istraživanja.

Unaprijed zahvaljujemo!

Postoji 9 pitanja u ovom upitniku.

1. Kojeg ste spola?

- ženskog muškog

2. Molimo navedite koliko imate godina?

3. Koristite li sljedeće društvene mreže?

	Da	Ne
Facebook	<input type="radio"/>	<input type="radio"/>
Twitter	<input type="radio"/>	<input type="radio"/>
Pinterest	<input type="radio"/>	<input type="radio"/>
LinkedIn	<input type="radio"/>	<input type="radio"/>

4. Koliko dugo imate Facebook račun?

- do 1 godine
- od 1 godine do 2 godine
- od 2 godine do 3 godine
- od 3 godine do 4 godine
- 4 godine i duže

5. Koliko prosječno posjećujete svoj Facebook račun?

- barem jednom tjedno
- više puta tjedno
- barem jednom dnevno
- do 5 puta tijekom dana
- više od 5 puta tijekom dana

6. Vremenski gledano, koliko traje Vaš prosječni posjet Facebooku?

- manje od 15 min
- od 15 min do 30 min

- od 30 min. do 1h
- od 1h do 2h
- više od 2 sata

7.

Pred Vama se nalaze pitanja koje se odnose na Vaše stavove prema sigurnosti općenito.

Molimo Vas da pažljivo pročitate sljedeća pitanja te odaberete odgovor koji se trenutno najviše odnosi na Vas.

1 – nikad

2 – vrlo rijetko

3 – ponekad

4 – vrlo često

5 – uvijek

Nakon što Vam osobni dokumenti isteknu uništavate li ih rezanjem ili nekim drugim načinom?	1	2	3	4	5
Skrivate li PIN broj svoje bankovne kartice kada koristite bankomat ili pri kupnji plaćate PIN-om?	1	2	3	4	5
Registrirate li se (osobnim podacima) samo na stranicama koje imaju istaknuta Pravila o privatnosti?	1	2	3	4	5
Čitate li Pravila privatnosti internet stranica prije nego li se registrirate Vašim osobnim podacima?	1	2	3	4	5
Tražite li pravila privatnosti na internet stranici prije nego li se registrirate Vašim osobnim podacima?	1	2	3	4	5
Pročitate li ugovore o korištenju u potpunosti prije nego li pristanete na njih?	1	2	3	4	5

8.

Pred Vama se nalaze pitanja koje se odnose na Vaše korištenje nekih tehničkih mogućnosti zaštite privatnosti na internetu.

Molimo Vas da pažljivo pročitate sljedeće tvrdnje te odaberete odgovor koji se trenutno najviše odnosi na Vas.

1 – nikad

2 – vrlo rijetko

3 – ponekad

4 – vrlo često

6– uvijek

Tražite li načine na koje možete kontrolirati što Vam ljudi šalju preko interneta (primjerice okvire u kojima možete označiti želite li prihvatiti ili odbiti određene ponude)?	1	2	3	4	5
Uklanjete li „poslužiteljske kolačiće“ (cookies) ?	1	2	3	4	5
Koristite li program za blokiranje prozorčića koji iskaču (<i>pop-up</i>)?	1	2	3	4	5
Provjeravati li svoje računalo u potrazi za malicioznim softverima („ <i>spyware</i> “)?	1	2	3	4	5
Brišete li povijest svog preglednika redovito?	1	2	3	4	5
Blokirate li poruke/elektroničke poruke od osoba s kojima ne želite komunicirati?	1	2	3	4	5

9.

Pred Vama se nalaze pitanja koje se na Vaše stavove odnosno brigu za pojedine aspekte sigurnosti na internetu.

Molimo Vas da pažljivo pročitate sljedeće tvrdnje te odaberete odgovor koji se trenutno najviše odnosi na Vas, pri čemu je značenje odgovora sljedeće:

1 – nikad

2 – vrlo rijetko

3 – ponekad

4 – vrlo često

6– uvijek

Općenito, koliko se brinete o Vašoj privatnosti dok se koristite internetom?	1	2	3	4	5
Brinete li se oko toga da organizacije prisutne na internetu nisu one kojima se predstavljaju?	1	2	3	4	5
Brinete li se oko toga da Vas se traži previše osobnih informacija kada se registrirate ili vršite kupovinu preko interneta?	1	2	3	4	5
Brinete li se o mogućnosti krađe identiteta putem interneta?	1	2	3	4	5
Brinete li se da osobe na internetu nisu one kojima se predstavljaju?	1	2	3	4	5
Brinete li se oko toga da bi se informacije o Vama mogle pronaći na starom računalu?	1	2	3	4	5
Brinete li se o tome tko bi mogao pristupiti Vašim medicinskim podacima preko interneta?	1	2	3	4	5
Brinete li se da bi osobe koje ne poznajete mogle doći do osobnih podataka o Vama putem Vaših aktivnosti na internetu?	1	2	3	4	5
Brinete li se da će prilikom korištenja Vaše kreditne kartice za kupovinu na internetu Vaš broj kreditne kartice netko drugi dobiti ili presresti?	1	2	3	4	5
Brinete li se da će se prilikom korištenja Vaše kreditne kartice za kupovinu na internetu Vaša kreditna kartica biti pogrešno terećena?	1	2	3	4	5
Brinete li se da će elektroničku poštu koju ste poslali pročitati još netko osim osobe kojoj ste ju poslali?	1	2	3	4	5

Brinete li se da će elektronička pošta koju ste poslali biti neprimjereno prosljeđena i drugim osobama?	1	2	3	4	5
Brinete li se da će elektronička pošta koju ste poslali biti isprintana i postavljena na mjesto gdje je drugi mogu vidjeti?	1	2	3	4	5
Brinete li se da računalni virus može poslati elektroničke pošte u Vaše ime?	1	2	3	4	5
Brinete li se da elektroničke pošte koje primete nisu od osoba za koje se predstavljaju?	1	2	3	4	5
Brinete li se da elektronička pošta koja sadrži naizgled legitimnu internet adresu može biti lažna?	1	2	3	4	5