

=Mateo Jurčić ♦ Andrea Miljko ♦ Lucija Mandić=

Filozofski fakultet Sveučilišta u Mostaru

mateo.jurcic@ff.sum.ba – andrea.miljko@ff.sum.ba – lucija.mandic@ff.sum.ba

UDK: 342.721:004.738.5

Prethodno priopćenje

SIGURNOSNA RAZMJENA PODATAKA DRUŠTVENIM MREŽAMA: PRAVO NA OSOBNOST I PRAVNA ZAŠTITA OSOBNIH PODATAKA

Sažetak

Društvene mreže, koje su postale globalni komunikacijski fenomen, danas su u uporabi na svim društvenim razinama. Svi aspekti globalizacije utjecali su na korisnike da stvaraju vlastite profile s osobnim podacima i objavljuju ih na mreži. Mnogi od tih korisnika društvenoga umrežavanja svakodnevno objavljuju ili daju osobne podatke. Promatrajući proces uvoza podataka iz društvenih mreža u raznorazne internetske aplikacije, postavlja se i pitanje je li to pravno utemeljeno. Koji su podatci obuhvaćeni? Jesu li pretežito osobne naravi i u koje se svrhe mogu koristiti takvi podatci? Jesu li ti podatci pouzdano zaštićeni? Ovo su važna pitanja na koja bi svaki korisnik trebao znati odgovor. Odgovori se odnose na privatnost i načela zaštite osobnih podataka. U ovom će se radu razmotriti pitanja društvenih mreža u kontekstu pravnoga okvira za zaštitu podataka, dat će se uvid u temeljne pojmove koji se odnose na osobne podatke, zaštitu podataka i opasnosti s kojima su korisnici svakodnevno suočeni. Bit će prezentirani rezultati istraživanja navika korisnika društvenih mreža u smislu otkrivanja osobnih podataka, rizicima s kojima su korisnici izloženi, zaštiti i zlouporabi njihovih podataka.

Ključne riječi: društvene mreže; podatci; sigurnost podataka; pravna zaštita

SAFETY EXCHANGE OF DATA THROUGH SOCIAL MEDIA: THE RIGHT TO IDENTITY AND LEGAL PROTECTION OF PERSONAL DATA

Abstract

Social media, which represent a global communication phenomenon, are used by all parts of the society today. All aspects of globalization have influenced users to create

profiles with personal data and to publish personal data online. Many of them publish or give out personal data daily. Watching the process of importing data from social media to various internet applications raises the question of the existence of legal foundation for those actions. Which data are included? Are they private in nature and for which purposes can such data be used? Are the data protected in a reliable way? These are important questions to which every user should know the answer. The answers refer to privacy and principles of personal data protection. This paper will examine the questions of social media in the context of data protection legal framework and an insight into basic term relating to personal data, data protection and dangers which users are facing daily will be given. The paper will also present a research about the habits of social media users in the sense of revealing personal data, the risks to which the users are exposed, protection and misuse of their data.

Keywords: social media; data; safety of data; legal protection

Uvod

S više od milijardu korisnika povezanih društvenim mrežama korisnikova privatnost postaje goruća tema mnogih rasprava u medijima te predmetom istraživanja unutar akademske zajednice. Društvene mreže, kao globalni komunikacijski fenomen, danas su u uporabi na svim društvenim razinama i neovisno o dobi i spolu premošćuju prostorna i vremenska ograničenja. Svi aspekti globalizacije utjecali su na korisnike da stvaraju vlastite profile s osobnim podacima, objavljuju ih i dijele s ostalim korisnicima na mreži. Iako profil na društvenim mrežama donosi određene prednosti, kao što su povezanost i upoznavanje s ostalim korisnicima, dijeljenje iskustava, ideja, interesa, postignuća, otkrića itd., ima i svoj rizik, čega možda nismo ni svjesni. Postojanjem rizika ne će se umanjiti prednosti društvenih mreža i njihova korist, nego je cilj korisnike društvenih mreža upozoriti na moguću zlorabu podataka i njezine posljedice. Promatrajući proces uvoza podataka iz društvenih mreža u raznorazne internetske aplikacije, postavlja se i pitanje je li to pravno utemeljeno. Koji su podatci obuhvaćeni? Jesu li pretežito osobne naravi i u koje se svrhe mogu koristiti takvi podatci? Jesu li ti podatci pouzdano zaštićeni? Gdje se pohranjuju te koliko će se dugo koristiti ili biti pohranjeni na nekom mjestu? Kroz ovaj rad pokušat ćemo odgovoriti na navedena pitanja te dati uvid u to kako studenti Sveučilišta u Mostaru gledaju na poimanje osobnih

podataka, kao i njihovu objavu na društvenim mrežama te kakvi su njihovi stavovi o privatnosti.

1. Privatnost i sigurnost društvenih mreža

Društvene mreže (engl. *social networks*) globalni su komunikacijski fenomen te su postale dio svakodnevnoga privatnoga i poslovnoga života. Kao što znamo, specifično obilježje društvenih mreža je u slobodi i jednostavnosti pristupa mrežama na načelu odabira neke specifične mreže prema potrebama i interesima.¹ Međutim, dijeljenje informacija s korisnicima društvenih mreža može dovesti do kršenja pravila privatnosti i sigurnosti.

Postoje mnogobrojne opasnosti koje mogu ugroziti sve korisnike na društvenim mrežama: ovisnost o društvenim mrežama, *cyberbullying*, zatim razni uznemiravajući sadržaji, nasilje, zlorabica informacija i slično. Većina korisnika na društvenim mrežama objavljuje svoje pravo ime i prezime, osobnu fotografiju, broj telefona te bez imalo oklijevanja ostale osobne podatke. Tako se svjesno odričemo dijela svoje privatnosti. Zapravo, na internetu se često otkrivaju mnogi osobni podatci jer se zaborave uključiti mogućnosti zaštite privatnosti ili se ustupa više podataka nego što je to potrebno.²

Naveli smo neke sigurnosne prijetnje društvenih mreža. Te je prijetnje moguće podijeliti u četiri skupine:

- *prijetnje privatnosti* koje se odnose na prikupljanje digitalnih zapisa o korisnicima, prikupljanje sporednih podataka poput IP adrese, vremena uspostavljanja i trajanje povezanosti s mrežom, poslane i primljene poruke itd., prepoznavanje lica korisnika na fotografijama i oznake na fotografijama te ujedno i otkrivanje podataka pomoću fotografija, otkivanje lokacija korisnika, otkivanje uređaja koji korisnik koristi, nemogućnost potpunog brisanja korisničkog računa i slično
- *prijetnje mrežama i podacima* neželjenim porukama ili tzv. popularnim spamovima, virusima i crvima, DoS napadima, krađom lozinki i povjerljivih podataka i slično.

¹ Usp. Anđelko MILARDOVIĆ, *Globalno selo: Sociologija informacijskog društva i cyber kulture*, Zagreb, 2010., str. 108.

² Usp. Parry AFTAB, *Kako prepoznati opasnosti interneta – vodič za škole i roditelje*, Zagreb, 2003., str. 76. – 77.

- *prijetnje identitetu* koje se ponajprije odnose na *phishing* napade, slučajno otkrivanje podataka, lažni profili
- *društvene prijetnje* kao što su uhođenje, *cyber* nasilje, industrijska špijunaža, što donosi gubitak intelektualnog vlasništva, pristup imovini ili pak ucjenjivanje zaposlenika tvrtki čije su žrtve.

Svaka od navedenih skupina prijetnji ima svoje rizike koji ne trebaju biti zanemareni kada koristimo društvene mreže ili pak ostale internetske usluge.³

Za sigurnost samih podataka važnu ulogu imaju informacijski sustavi, odnosno informacijska sigurnost koja mora biti usklađena s određenim ISO standardima. U kontekstu računalnih sustava imamo tri dimenzije informacijske sigurnosti (zaštita informacija kontrolnim pristupom):

- povjerljivost (zaštita od neovlaštenih informacija o čitanju)
- integritet (zaštita od neovlaštenog pisanja informacija)
- dostupnost (zaštita od djelovanja koja sprečavaju razuman pristup legitimnim korisnicima njihovim sustavima).⁴

U vezi s *online* privatnošću, razlikujemo tri vrste:

- informacijska privatnost (kontrola nad obrađivanjem i prijenosom osobnih podataka na mreži)
- socijalna privatnost (reguliranje blizine i udaljenosti prema drugima na mreži)
- osobna privatnost (percipirana kontrola preko emocionalnih i kognitivnih rezultata).

Trenutačna studija razmatra drugu vrstu. Usredotočimo se na postavke privatnosti u društvenim medijima jer imaju važnu ulogu u tom smislu pružajući mehanizam za socijalnu privatnost.

U suvremenom užurbanom svijetu ugrožavanje prava na privatnost ima za posljedicu ugrozu informacijske osobnosti koja se u najužem smislu riječi definira kao zahtjev pojedinaca, grupa ili institucija da samostalno odluče kada će, kako i koje informacije o sebi ustupiti drugima. U širem, općeprihvaćenom značenju, termin informacijske osobnosti zapravo se definira pojmom informacijska sigurnost pod kojim se podrazumijeva da pojedinac, u uvjetima informacijskog društva, odlučuje kada, kome, koliko i

³ Usp. CARNet CERT & LSS, *Sigurnosni rizici društvenih mreža*, Zagreb, 2009., str. 10. – 13.

⁴ Usp. FIPS, *Standards for Security Categorization of Federal Information and Information System*, Gaithersburg, 2004., str. 1. – 2.

kako će priopćiti osobne podatke, vodeći računa o svojim pravima i potrebama, ali i o pravima i potrebama zajednice u kojoj živi.⁵

1.1. Sigurnost podataka na društvenim mrežama: primjer Facebooka

Pravo na zaštitu osobnih podataka, jednako kao i pravo na osobnost i privatnost jedno je od temeljnih ljudskih prava. Zbog razvoja suvremenih informacijskih i komunikacijskih tehnologija ovo će pravo dobivati sve više na značaju jer se nerijetko može svjedočiti o njegovu izravnome kršenju, kao i zloporabi suvremenih medija, poput interneta, koji omogućuju da se praktički svaki podatak može objaviti i nakon toga nekontrolirano širiti.

Porastom društvenih mreža (Facebook, Instagram, Twitter i dr.) osobni podatci korisnika sve su više podložni nadzoru, ali i robnoj razmjeni. Postavljanjem svojih osobnih podataka na društvenim mrežama korisnici omogućuju trećoj strani lak pristup tim podacima. Tek u posljednje vrijeme, nakon višegodišnjih kritika upućenih Facebooku i drugim društvenim mrežama, raznih stručnjaka iz područja informacijskih i komunikacijskih znanosti te stručnjaka za zaštitu podataka, svijest o važnosti upravljanja osobnim podacima na društvenim mrežama lagano se budi i korisnici sve više daju pozornost postavkama privatnosti kao i pravilima o zaštiti podataka. Razlog tomu jest i činjenica da je Mark Zuckerberg u više navrata šokirao javnost svojim potezima dodavanjem novih funkcionalnosti svojoj društvenoj mreži te tako uvelike zadirao u privatnost svojih korisnika – od opcije za prepoznavanje lica preko uvođenja *Timelinea*, koji je ponovno otkrio neke zaboravljene detalje iz prošlosti, pa do nedavnog slučaja s Cambridge Analyticom.

Od ožujka 2018. ne stišava se bura upravo oko te afere vezane za društvenu mrežu Facebook kada je u javnost dospjela informacija o tome kako je analitičarska tvrtka Cambridge Analytica iskoristila ovu popularnu društvenu mrežu i zloupotrijebila gomilu korisničkih podataka bez saznanja samih korisnika. Godine 2014. prikupljeni podatci o više desetaka milijuna korisnika iskorišteni su u izgradnju informacijskoga sustava za profiliranje glasača kako

⁵ Marija BOBAN, „Pravo na privatnost i pravo na pristup informacijama u suvremenom informacijskom društvu“, *Zbornik radova Pravnog fakulteta u Splitu*, god. XLIX., 2012., str. 7. – 8.

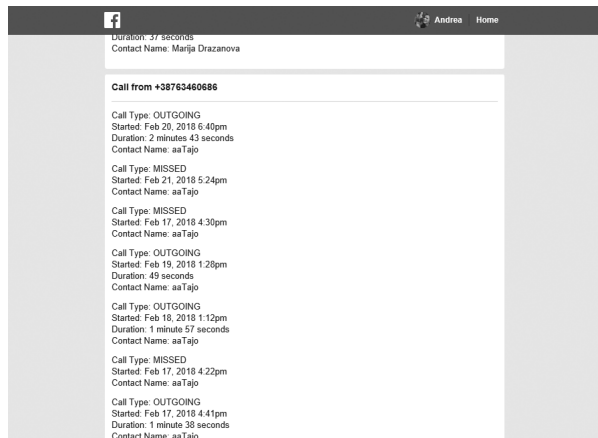
bi se personaliziranim oglašavanjem glasačima promijenilo političko mnijenje. Danas je poznato da je tvrtka Cambridge Analytica, između ostaloga, surađivala s voditeljem političke kampanje američkoga predsjednika Donalda Trumpa te je njihov sustav korišten i u pobjedničkoj Brexit kampanji.⁶ Prema navodima bivšega zaposlenika Cambridge Analytica Christophera Wylieja podatci su prikupljeni preko aplikacije Thisisyourdigitallife koju su napravili znanstveni suradnici Aleksandra Kogana sa Sveučilišta Cambridge. Kroz svoju tvrtku Global Science Research (GSR), u suradnji s Cambridge Analyticom, platio je stotinama tisuća korisnika sudjelovanje na testu osobnosti za navodno prikupljanje podataka u akademske svrhe. Međutim, nisu prikupljeni samo podatci korisnika aplikacije, nego i njihovih Facebook prijatelja, što je dovelo do baze podataka s osobnim podacima više od 87 milijuna korisnika Facebooka. Algoritam i baza podataka zajedno su činili snažan politički alat.

1.2. Niste na Facebooku? Nema veze, on vas svejedno prati

Pored same činjenice da je zlorabljena tolika količina osobnih podataka, iz dana u dan postaje jasnije da Facebook u svojim velikim data centrima sprema i one podatke koje nitko nije očekivao da će ih tamo pronaći. Korisnici društvenih mreža morali su više-manje znati da te iste društvene mreže mogu imati saznanja o njima kroz korisnikove klikove, navike surfanja, ali i kroz informacije koje su sami korisnici tamo postavili. Međutim, ono što iznenađuje jest činjenica da korisnici Facebooka, koji se odluče na preuzimanje svojih podataka iz arhive, pored vlastitih objava i podataka o prijateljima mogu pronaći i podatke o svojim dolaznim i odlaznim pozivima i SMS porukama (tzv. meta podatke), IP adrese s kojih su se spajali na tu društvenu mrežu, kao i oglašivačke preferencije i mnoge druge osjetljive podatke. Iako je Facebook dao službenu izjavu u kojoj navodi da neke podatke o kontaktima s telefona prikupljaju, ali samo prilikom instalacije same aplikacije na android pametni telefon i da se ti podatci ne ažuriraju i ne prodaju, ipak su mnogi korisnici

⁶ Usp. Carole CADWALLADR - Emma GRAHAM-HARRISON, „Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach“, *The Guardian*, 17. III. 2018., <<https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>>, (20. V. 2018.).

dokazali da je prikupljanje rađeno u više navrata i kroz duže vremensko razdoblje.



Slika 1.: Prikaz osobnih podataka korisnika (telefonskih poziva) preuzet iz arhive Facebooka

Dok je uporaba podataka i podatkovnih sustava omogućila svijetu uzbudljive novitete poput umjetne inteligencije, strojnog učenja i personalizirane digitalne trgovine, zbog nepostojećih regulacija bilo je samo pitanja vremena kada će se pojaviti i zlouporaba osobnih podataka prikupljenih preko raznoraznih sustava za upravljanje društvenim odnosima (Social CRM)⁷ koji organizacijama omogućuju učinkovitiji pristup klijentima.

Zbog sve češćih „curenja“ podataka od raznoraznih davatelja internetskih usluga, koje nije zaobišlo ni velike tvrtke kao što su Apple, Google, Ebay, Uber i druge, te naposljetku zbog posljednje afere s Facebookom, zaštita osobnih podataka postaje tema koja će definirati 2018. godinu.

1.2.1. Što je sve osobni podatak?

Kroz rad smo u više navrata spominjali pojmove podatka i osobnih podataka pa se postavlja i pitanje što su zapravo ti pojmovi?

Što se tiče samog pojma *podatak*, prema Zakonu o tajnosti podataka, Narodne novine br. 79/2007, „podatak je dokument, odnosno svaki napisani, umnoženi, nacrtani, slikovni, tiskani, snimljeni, fotografirani, magnetni, optički, elektronički ili bilo koji drugi zapis podatka, saznanje, mjera, postupak,

⁷ Social CRM (Content Relationship Menagement) – sustavi za upravljanje društvenim odnosima s klijentima.

predmet, usmeno priopćenje ili informacija, koja s obzirom na svoj sadržaj ima važnost povjerljivosti i cjelovitosti za svoga vlasnika.“⁸

Međutim, postavlja se i pitanje što je to osobni podatak koji je nama puno važniji.

Prema zakonu Europske unije, osobni podatci definirani su kao „bilo koji podaci vezani za fizičku osobu (dalje u tekstu: ‘subjekt obrade podataka’) kojoj je utvrđen identitet ili onu kojoj se može izravno ili neizravno utvrditi identitet, a posebno pozivanjem na identifikacijski broj ili na jedan ili više čimbenika karakterističnih za fizički, fiziološki, mentalni, ekonomski, kulturni ili socijalni identitet te osobe.”⁹

Ukratko možemo reći da su osobni podatci: ime i prezime, adresa stanovanja, e-adresa, IP i MAC adresa, GPS lokacija, RFID tagova i kolačića na web stranicama, telefonski broj, fotografija, videosnimke pojedinaca, OIB, biometrijski podatci (otisak prsta, snimka šarenice oka), genetski podatci, podatci o obrazovanju i stručnoj spremi, podatci o plaći, podatci o kreditnom zaduženju, podatci o računima u banci, podatci o zdravlju, seksualnom određenju, glas i mnogi drugi podatci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi.

1.2.2. Opća uredba o zaštiti podataka – GDPR

Važno je naglasiti da je potrebno primjenjivati niz tehničkih i pravnih pravila i smjernica kako bismo osigurali što veću sigurnost podataka. Jedan od načina kojim Europska unija želi regulirati zaštitu podataka jest *Opća uredba o zaštiti podataka – GDPR (General Data Protection Regulation)*, koja je stupila na snagu 25. svibnja 2019. nakon što su tvrtke prošle dvogodišnje razdoblje prilagodbe na novu regulativu. Cilj uredbe je izjednačiti sve zakone vezane za zaštitu osobnih podataka na cijelom prostoru Europske unije te vratiti potrošačima kontrolu nad njihovim podacima, što uključuje upravljanje i dijeljenje osobnih podataka s trećim stranama. GDPR se ne odnosi isključivo na davatelje internetskih usluga, nego i na banke, davatelje usluga zdravstvene zaštite, osiguravajuće kuće i druge tvrtke koje prikupljaju osjetljive podatke. Važno je napomenuti da se ova uredba primjenjuje i na poduzeća i organizacije (javne i

⁸ „Zakon o tajnosti podataka“, *Narodne novine-Službeni list Republike Hrvatske*, 2007., čl. 2.

⁹ „Poslovnik o obradi i zaštiti osobnih podataka u Eurojustu“, *Službeni list Europske unije*, 2005., C 68/01, čl. 1.(h).

privatne) koje imaju sjedište izvan Europske unije, no pružaju robu ili usluge u Europskoj uniji. Pritom nije važno u kojem su obliku podatci, pisanom ili elektroničkom. Isto tako, treba istaknuti koje to informacije štiti GDPR uredba:

- informacije o identitetu osobe:
 - ime
 - adresa
 - podatci osobne iskaznice
- Web podatke:
 - lokacija korisnika
 - *cookie* podatke
 - IP adresu
 - RFID (*radio frequency identification*)
- biometrijske podatke
- rasu, etničku pripadnost
- zdravstveno stanje i genetičke podatke
- spolnu orijentaciju
- političke stavove.¹⁰

2. Istraživanje

2.1. Ciljevi istraživanja, postupak i metode obrade podataka

Cilj je ovoga istraživanja ispitati upoznatost studenata Sveučilišta u Mostaru s dijeljenjem osobnih podataka na društvenim mrežama. Svjesni smo, naime, činjenice da mnogi dijele svoje podatke na društvenim mrežama i ostalim internetskim stranicama ili trgovinama bez imalo razmišljanja gdje će ti podatci završiti i tko će se njima služiti.

¹⁰ Usp. „Vodič kroz GDPR za početnike“, *GDPR informer*, <<https://gdprinformer.com/hr/vodic-kroz-gdpr>>, (30. V. 2018.).

Ispitivan je uzorak od 439 studenata različitih studijskih grupa na pred-diplomskoj i diplomskoj razini. Istraživanje je provedeno tijekom travnja i svibnja 2018. godine preko *online* anketnog upitnika od 20 pitanja, a odnosio se na osobne karakteristike ispitanika te na njihove navike korištenja i rada na društvenim mrežama. Za ispunjavanje anketnoga upitnika bilo je predviđeno vrijeme u trajanju od 15 minuta.

Radi ostvarivanja postavljenih ciljeva ovoga istraživanja koristile su se sljedeće statističke metode i analize: metode deskriptivne statistike (aritmetička sredina, standardna devijacija, frekvencije), hi-kvadrat test, t-test i analiza varijance (ANOVA), a podatci su prikazani u tablicama i grafikonima.

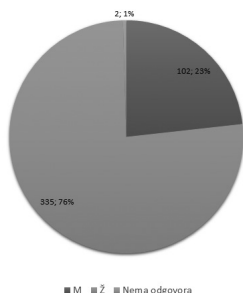
2.2. Hipoteze istraživanja

Cilj je istražiti kakva je upoznatost studenata Sveučilišta u Mostaru s dijeljenjem osobnih podataka na društvenim mrežama, odnosno istraživanje će biti vezano uz osobne stavove studenata o važnosti zaštite privatnosti na društvenim i/ili internetskim mrežama. Pretpostavlja se da su sve osobe koje će sudjelovati u istraživanju korisnici društvenih mreža ili pak interneta. U svome istraživanju postavili smo tri istraživačke hipoteze, od kojih je prva i temeljna hipoteza.

- H1: Pretpostavlja se da su studenti upoznati s pravilima i načinima dijeljenja osobnih podataka na internetskim i/ili društvenim mrežama.
- H2: Pretpostavlja se da će studenti koji su tijekom obrazovanja imali više kolegija koji su sadržajno uključivali informiranje o dijeljenju podataka na internetu i općenito upravljanje osobnim podacima (Pravni fakultet, Studij informatike s Fakulteta prirodoslovno-matematičkih i odgojnih znanosti, Studij informacijskih znanosti s Filozofskog fakulteta, Studij računarstva s Fakulteta strojarstva, računarstva i elektrotehnike) biti više upoznati u odnosu na ostale fakultete i studijske grupe pojedinih fakulteta.
- H3: Pretpostavlja se da će postojati razlika među studentima Pravno-ga fakulteta, Studija informatike s FPMOZ-a, Studija informacijskih znanosti s FF-a i Studija računarstva i da će studenti Informacijskih znanosti biti bolje upoznati s pravilima korištenja i upravljanja osobnim podacima.

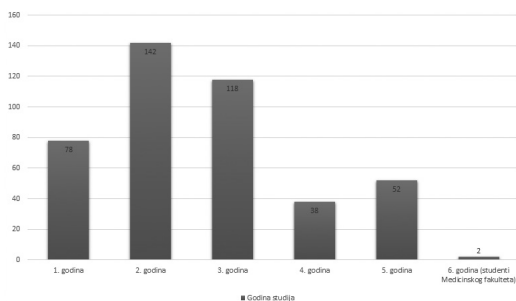
2.3. Uzorak istraživanja

Istraživanje je provedeno na prigodnom uzorku od 439 studenata Sveučilišta u Mostaru od čega 102 sudionika muškoga spola (23,2 %) i 335 sudionika ženskoga spola (76,31 %). Dvoje sudionika (0,49 %) nije odgovorilo na pitanje o spolu (*graf 1.*). Prosječna dob sudionika je 22 godine ($M = 21,73$; $Sd = 2,64$; min. = 18; maks. = 38). Od 439 ispitanika njih 99,1 % ima otvoren profil na društvenim mrežama, a samo 0,9 % nema.



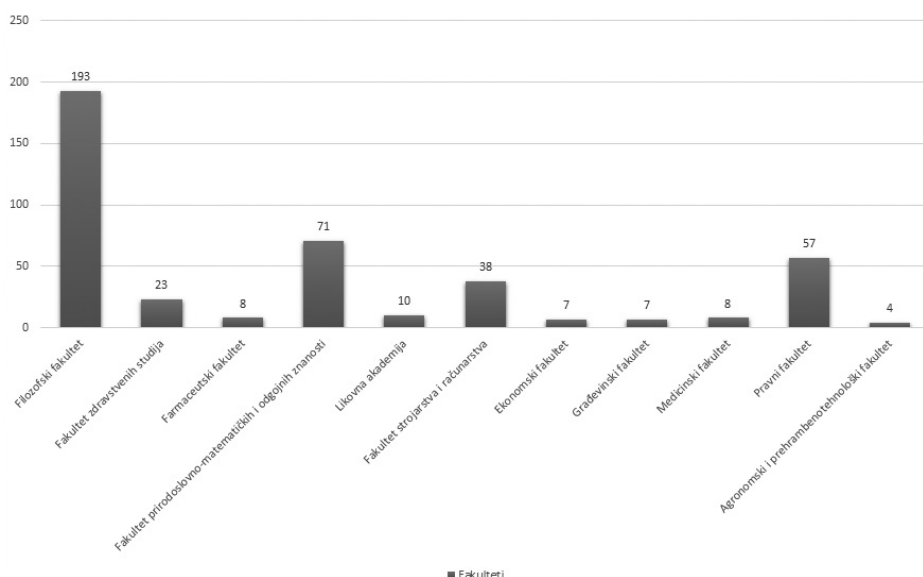
Graf 1.: Prikaz uzorka prema spolu (N = 439)

U ukupnom uzorku najviše su zastupljeni studenti druge godine studija (33 %), a najmanje studenti treće godine studija (8,8 %) i šeste godine studija (0,5 %), koja se u ovome slučaju odnosi samo na studente Medicinskoga fakulteta. Točnije, ukupno 430 sudionika odgovorilo je na pitanje o godini studija: 78 (18,1 %) – prva godina studija, 142 (33 %) – druga godina studija, 118 (27,5 %) – treća godina, 38 (8,8 %) – četvrta godina studija, 52 (12,1 %) – peta godina studija, 2 (0,5 %) – šesta godina studija (*graf 2.*).



Graf 2.: Prikaz raspodjele uzorka prema godini studiranja (N = 430)

Što se tiče zastupljenosti studenata po fakultetima, 426 sudionika odgovorilo je na ovo pitanje: Filozofski fakultet – 193 (44,3 %), Fakultet zdravstvenih studija – 23 (5,3 %), Farmaceutski fakultet – 8 (1,8 %), Fakultet prirodoslovno-matematičkih i odgojnih znanosti – 71 (16,3 %), Likovna akademija – 10 (2,3 %), Fakultet strojarstva i računarstva – 38 (8,5 %), Ekonomski fakultet – 7 (4,1 %), Građevinski fakultet – 7 (1,6 %), Medicinski fakultet – 8 (1,8 %), Pravni fakultet – 57 (13,1 %) i Agronomski i prehrambeno-tehnološki – 4 (0,9 %).

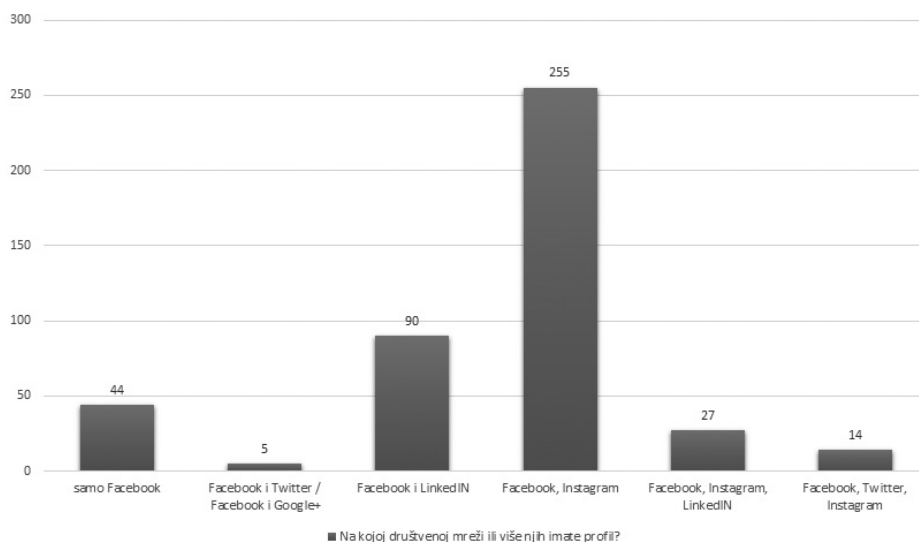


Graf 3.: Prikaz raspodjele uzorka prema fakultetima (N = 426)

2.4. Rezultati istraživanja

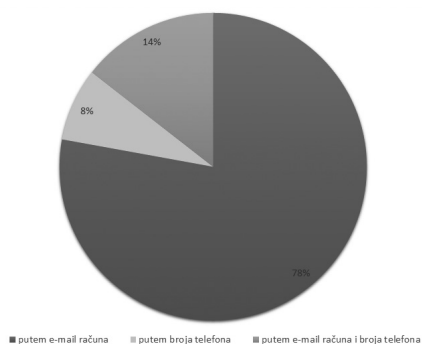
Sudionici, njih 435, odgovorilo je na pitanje na kojim društvenim mrežama ili više njih imaju profil. Kao što možemo i vidjeti na 4. grafu, društvene mreže koje su najviše zastupljene kod uzorka su Facebook i Instagram, s postotkom od 58,6, što je i bilo očekivano s obzirom na to da su to najpopularnije dvije mreže danas među mladima.

SIGURNOSNA RAZMJENA PODATAKA DRUŠTVENIM MREŽAMA: PRAVO NA OSOBNOST...



Graf 4.: Prikaz odgovora na pitanje „Na kojoj društvenoj mreži ili više njih imate profil?“ (N = 435)

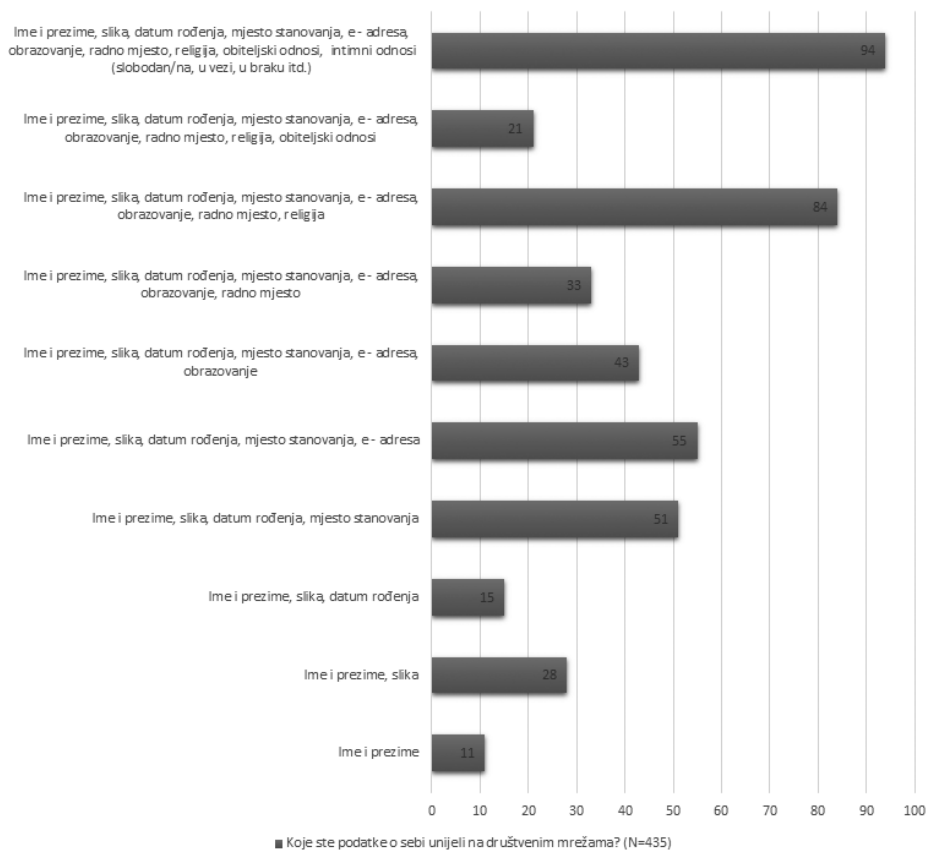
Osim podataka o tome na kojim društvenim mrežama studenti imaju svoje profile važan je i podatak o tome na koji način to čine, odnosno putem čega se prijavljuju na društvene mreže.



Graf 5.: Prikaz odgovora na pitanje „Na koji se način prijavljujete na društvene mreže?“ (N = 436)

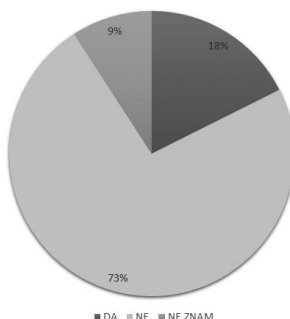
Na 6. grafu mogu se vidjeti podatci koje sudionici ankete unose prilikom prijave i dovršavanja profila na različitim društvenim mrežama i tako ih dijele s drugim korisnicima mreža. Vidljivo je da većina studenata (21,8 %) „otkriva“ svoje osobne podatke na društvenim mrežama uključujući ime i prezime, fotografiju, datum rođenja, mjesto stanovanja, e-adresu, obrazovanje, radno

mjesto, religiju, svoje obiteljske i intimne odnose. Samo 11 sudionika, odnosno 2,5 %, studenata otkriva samo svoje ime i prezime.



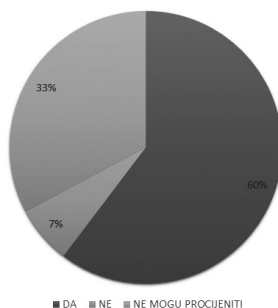
Graf 6.: Prikaz odgovora na pitanje „Koje ste podatke o sebi unijeli na društvenim mrežama?“ (N = 435)

Većina studenata, čak njih 320 (73,2 %) od 437 pristiglih odgovora, ne postavlja nepoznatim korisnicima svoje osobne podatke koje su naveli vidljivima, dok njih 77 (17,6 %) ipak te podatke dijele i s osobama koje ne poznaju (graf 7.).



Graf 7.: Prikaz odgovora na pitanje „Jesu li osobni podatci koje ste naveli na navedenoj društvenoj mreži ili više njih javni (vidljivi i osobama s kojima niste povezani preko društvene mreže)?“ (N = 437)

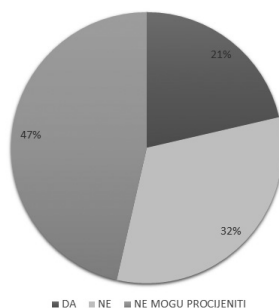
Što se tiče opasnosti koje se pojavljuju na društvenim mrežama, većina studenata (263, odnosno 60,3 %) smatra da je dovoljno informirana. Zanimljivo je da čak 143 studenta, odnosno 32,8 %, ne može procijeniti jesu li dovoljno informirani ili ne o opasnostima koje vrebaju na društvenim mrežama, što je neočekivano ako uzmemo u obzir da studenti mogu samostalno provjeriti i saznati više o internetskim opasnostima i barem se minimalno informirati kako bi bili sigurni (graf 8.).



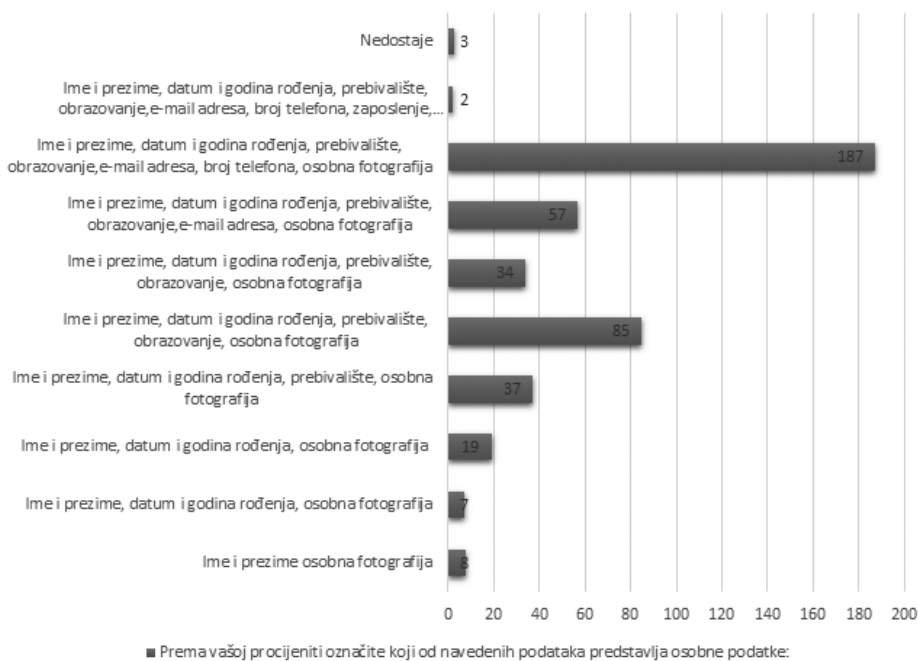
Graf 8.: Prikaz odgovora na pitanje „Jeste li dovoljno informirani o internetskim opasnostima na društvenim mrežama?“ (N = 436)

Većina studenata nije mogla procijeniti, čak 202 (46,4 %), jesu li osobni podatci koje su naveli na društvenim mrežama izloženi internetskim opasnostima (graf 9.). Postavlja se pitanje zašto je većina studenata dala takav odgovor. Je li možda razlog tomu što ne znaju što su zapravo osobni podatci ili pak ne znaju koje su to sve internetske opasnosti na društvenim mrežama? Možemo se referirati na postotke iz pitanja koje je također postavljeno studentima

o tome što su od navedenih podataka osobni podatci i time pokušati razmotriti razlog nemogućnosti samoprocjene iako razloga može biti više. Vidimo da većina studenata različito poima osobne podatke koje navode na društvenim mrežama, a tri studenta nisu dala nikakav odgovor (*graf 10.*).



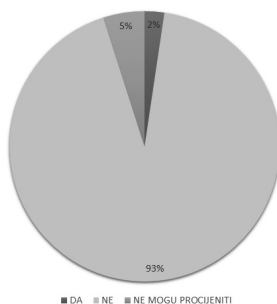
Graf 9.: Prikaz odgovora na pitanje „Jesu li osobni podatci koje ste naveli na navedenoj društvenoj mreži, ili više njih, izloženi internetskim opasnostima?“ (N = 435)



Graf 10.: Prikaz odgovora na pitanje „Prema vašoj procijeni označite koji od navedenih podataka predstavlja osobne podatke.“

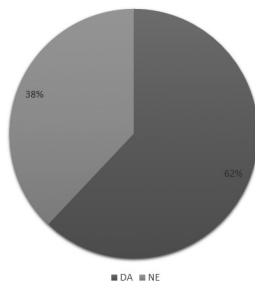
Na pitanje jesu li bili žrtve internetske opasnosti, većina studenata odgovorila je negativno, njih 394 (92,7 %), 10 studenata (2,4 %) dalo je potvrđan odgovor, a 21 student (4,9 %) nije mogao procijeniti jesu li bili žrtve internetske opasnosti (*graf 11.*).

Ako su studenti potvrdno odgovorili na prethodno pitanje, odnosno bili su žrtve internetske opasnosti, trebali su navesti o kojoj je vrsti internetske opasnosti riječ. Neki su odgovorili da su se suočili s krađom identiteta, s lažnim profilima na Facebooku, da su bili žrtve *cyber* nasilja i verbalnih napada, da su im zlorabljene fotografije i hakirani profili, da su im slani virusi preko poruka i slično.



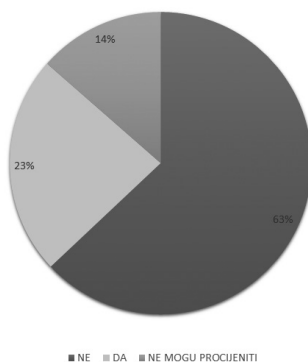
Graf 11.: Prikaz odgovora na pitanje „Jeste li na navedenoj društvenoj mreži ili više njih bili žrtva internetske opasnosti?“ (N = 425)

O tome provjeravaju li i prikupljaju li studenti podatke o određenim osobama ili događajima preko društvenih mreža ili više njih iako nemaju profil na društvenim mrežama, 270 studenata, odnosno 62,1 %, dalo je potvrđan odgovor, a 165 studenata, odnosno 37,9 %, nije prikupljalo podatke o osobama ili događajima (*graf 12.*).



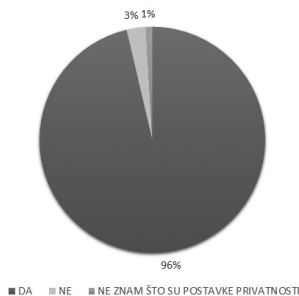
Graf 12.: Prikaz odgovora na pitanje „Jeste li preko navedene društvene mreže ili više njih prikupljali podatke o određenoj osobi ili događaju (čak i ako nemate profil na društvenim mrežama)?“ (N = 435)

Većina studenata, njih 274, odnosno 63 %, smatra da ne postoji privatnost na društvenim mrežama, 102 studenta (23,4 %) smatra da postoji privatnost na društvenim mrežama i njih 59 (13,6 %) ne može procijeniti navedenu tvrdnju (*graf 13.*).



Graf 13.: Prikaz odgovora na pitanje „Prema Vašem mišljenju postoji li privatnost na društvenim mrežama?“ (N = 435)

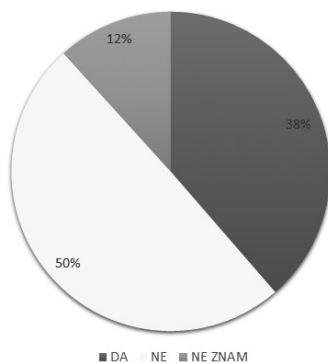
Prema dobivenim rezultatima, prikazanim u 14. grafu, 419 studenata, odnosno 96,3 %, koristi postavke privatnosti na društvenim mrežama, 2,8 % studenata ih ne koristi, a 0,9 % studenata uopće ne zna što su postavke privatnosti.



Graf 14.: Prikaz odgovora na pitanje „Koristite li postavke privatnosti na društvenim mrežama?“ (N = 435)

Danas je teško pronaći neku društvenu mrežu ili pak neki drugi društveni medij koji nema dodatnih uvjeta i pravila tako da korisnici preopterećeni dugačkim pravnim tekstovima redovito prihvaćaju uvjete a da im ne posvete potrebnu pozornost ili ih uopće ne čitaju i tako ne znaju na što pristaju. Prema dobivenim rezultatima (*graf 15.*) veći broj studenata, čak njih 216 (49,66 %)

studenata ne čita upute i uvjete o sigurnosti i privatnosti pri kreiranju profila na društvenim mrežama dok upute i uvjete o sigurnosti i privatnosti čita 168 studenata, odnosno 38,62 %.



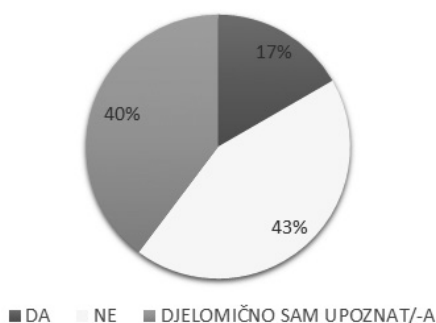
Graf 15.: Prikaz odgovora na pitanje „Jeste li prilikom kreiranja svojih profila pročitali upute i uvjete o sigurnosti i privatnosti?“ (N = 435)

Da objava osobnih podataka na društvenim mrežama može pridonijeti potencijalnoj krađi identiteta slaže se 66 % studenata dok njih 138, odnosno 31,6 %, nema izražen stav o toj tvrdnji. (graf 16.)



Graf 16.: Prikaz odgovora na pitanje „Procijenite svoje slaganje sa sljedećom tvrdnjom: Objava osobnih podataka na društvenim mrežama mogla bi pridonijeti potencijalnoj krađi identiteta.“ (N = 437)

Gotovo je jednak postotak onih studenata koji jesu ili ipak nisu upoznati sa zakonom o zaštiti osobnih podataka, koji je ove godine osobito popularan bio u Republici Hrvatskoj zbog primjene Opće uredbe o zaštiti osobnih podataka (GDPR) od svibnja 2018. (graf 17.).



Graf 17.: Prikaz odgovora na pitanje „Jeste li upoznati sa zakonom o zaštiti osobnih podataka?“ (N = 438)

Daljnijim istraživanjem htjeli smo ustanoviti kako studenti informacijskih znanosti, informatike, računarstva i prava u usporedbi s ostalim fakultetima i studijskim grupama pristupaju društvenim mrežama te dijeljenjem informacija na društvenim mrežama budući da su se tijekom studija susreli s nekim kolegijima koji su sadržajno uključivali informiranje o dijeljenju podataka na internetu i općenito upravljanje osobnim podacima.

Klaster je činio ukupno 149 sudionika. Detaljan broj prikazan je u tablici 1.

Tablica 1.: Broj sudionika ankete u klasteru po studijskim grupama u usporedbi s ostalim fakultetima/studijskim grupama

Studijska grupa	Broj sudionika (N)
Informacijske znanosti	59
Informatika	6
Računarstvo	27
Pravo	57
Ostali fakulteti i studijske grupe	277

Važno je napomenuti da su radi testiranja razlika u frekvenciji odgovora između klastera i drugih studijskih grupa/fakulteta primijenjeni hi-kvadrati. Testiranjem smo ustanovili da se razlike nisu pokazale statistički značajnima osim na pitanju koje podatke o sebi prikazuju na društvenim mrežama. Naime, studenti iz klastera, odnosno studenti prava, računarstva, informatike i informacijskih znanosti, unose manje informacija.

Tablica 2.: Prikaz statistički značajnih razlika u odgovorima na pitanje „Koje ste podatke o sebi unijeli na društvenim mrežama?“

9. Koje ste podatke o sebi unijeli na društvenim mrežama?											
Count											
1	9. Koje ste podatke o sebi unijeli na društvenim mrežama?										Total
	2	3	4	5	6	7	8	9	10		
Studij	3	17	7	34	42	36	24	58	14	55	290
Klaster	8	11	8	17	13	7	9	26	7	39	145
Total	11	28	15	51	55	43	33	84	21	94	435

$\chi^2 = 22.35$ df = 9, $p = .008$ Razlikuju se značajno*

Napomena: Brojevi od 1 do 10 u tablici predstavljaju sljedeće kategorije:

1. ime i prezime
2. ime i prezime, fotografija
3. ime i prezime, fotografija, datum rođenja
4. ime i prezime, fotografija, datum rođenja, mjesto stanovanja
5. ime i prezime, fotografija, datum rođenja, mjesto stanovanja, e-adresa
6. ime i prezime, fotografija, datum rođenja, mjesto stanovanja, e-adresa, obrazovanje
7. ime i prezime, fotografija, datum rođenja, mjesto stanovanja, e-adresa, obrazovanje, radno mjesto
8. ime i prezime, fotografija, datum rođenja, mjesto stanovanja, e-adresa, obrazovanje, radno mjesto, religija
9. ime i prezime, fotografija, datum rođenja, mjesto stanovanja, e-adresa, obrazovanje, radno mjesto, religija, obiteljski odnosi
10. ime i prezime, fotografija, datum rođenja, mjesto stanovanja, e-adresa, obrazovanje, radno mjesto, religija, obiteljski odnosi, intimni odnosi (slobodan/na, u vezi, u braku itd.)

Daljnijim istraživanjem napravili smo i usporedbu klastera međusobno. Broj sudionika u klasteru prikazan je u tablici 1.

Kruskal-Wallisovim testom ustanovili smo da razlike nisu značajne ($p = .620$) osobito u osobnoj procjeni koliko objava osobnih podataka na društvenim mrežama može pridonijeti potencijalnoj krađi identiteta.

Tablica 3.: Rezultati Kruskal-Wallisova testa

Ranks			
	grupa	N	Mean Rank
19. Procijenite svoje slaganje sa sljedećom tvrdnjom: <i>Objava osobnih podataka na društvenim mrežama mogla bi pridonijeti potencijalnoj krađi identiteta.</i>	1	59	77,16
	2	27	67,82
	3	6	63,50
	4	57	74,59
	Total	147	
Chi-Square	1,779		
df	3		
Asymp. Sig.	.620		
a. Kruskal-Wallisov test			
b. Grouping Variable: grupa			

Zaključak i rasprava

Slobodno možemo reći da je 2019. godinu obilježio Facebook skandal o kojem će se pričati i ubuduće i na neki način „uzdrmao“ mnoge postavljajući sebi, a i drugima, mnogobrojna pitanja o privatnosti i samoj njezinoj zaštiti i tako nas naveo na intenzivno razmišljanje o privatnosti koja je svakim danom sve više ugrožena na društvenim mrežama i na ostalim internetskim stranicama. Vrijednost informacija i podataka koje kruže internetskim prostorom iznimno je velika, a da toga nismo ni svjesni, što otkriva naše prekomjerno objavljivanje osobnih podataka iz privatnoga i poslovnoga života izlažući ih pritom mnogobrojnim opasnostima koje vrebaju i na društvenim mrežama i na internetu. Zbog svega što se događa na društvenim mrežama, počevši od onoga dobrog do lošega, što nas ujedno može i dovesti do sigurnog korištenja društvenih mreža, svakako bi bilo dobro poticati podizanje osviještenosti o opasnostima društvenih mreža u sklopu obrazovanja, osobito kod mladih ljudi, koji su najlakša meta u ovom lancu, kako bi barem na neki način pridonijeli boljoj zaštiti informacija i osobnih podataka na društvenim i internetskim stranicama.

U skladu s tim, provedeno je i istraživanje čiji su rezultati pokazali da 99,1 % studenata ima otvoren profil na društvenim mrežama, a samo 0,9 % studenata nema, što je očekivano budući da su danas društvene mreže sastavni dio

života svake mlade osobe, što pokazuje i broj društvenih mreža na kojima studenti imaju otvoren profil, odnosno većina njih ima otvoren profil na više od jedne društvene mreže. Danas je teško zamisliti dan bez korištenja barem jedne od društvenih mreža, a najviše su zastupljene Facebook i Instagram (58,6 %), što je i bilo očekivano s obzirom na to da su to najpopularnije dvije mreže danas među mladima, iako ne možemo zanemariti i ostale mreže kao što su LinkedIn, Google +, Twitter. Osim podataka o tome na kojim društvenim mrežama studenti imaju svoje profile, važan je i podatak o tome na koji način to čine, odnosno putem čega se prijavljuju na društvene mreže. Većina studenata prijavljuje se e-poštom, ali ima onih koji se prijavljuju telefonski dajući svoj broj i tako otkrivaju još jedan od važnih osobnih podataka.

Zaštita osobnih podataka vrlo je važna, a korištenjem društvenih mreža ona je sve ugroženija, a dobiveni podatci pokazuju da većina ispitanika drago-voljno ustupa svoje osobne podatke na društvenim mrežama pa tako možemo pretpostaviti da ih ustupaju i na ostalim internetskim stranicama i dijele ih s drugim korisnicima. Većina studenata, čak njih 73,2 % ne postavlja osobne podatke koje su naveli vidljivima nepoznatim korisnicima dok 17,6 % ipak te podatke dijele i s osobama koje ne poznaju. Vidljivo je da većina studenata (21,8 %) „otkriva“ svoje osobne podatke na društvenim mrežama uključujući ime i prezime, fotografiju, datum rođenja, mjesto stanovanja, e-adresu, obrazovanje, radno mjesto, religiju, svoje obiteljske i intimne odnose. Samo jedanaest sudionika, odnosno 2,5 % studenata, otkriva samo svoje ime i prezime.

Nadalje, postavlja se pitanje koliko smo svjesni opasnosti koje nam donosi internet i ostali društveni mediji. Što se tiče opasnosti koje se pojavljuju na društvenim mrežama, većina studenata smatra da je dovoljno informirana, njih 60,3 %. Zanimljivo je da 32,8 % studenata ne može procijeniti jesu li dovoljno informirani o opasnostima koje vrebaju na društvenim mrežama, što je neočekivano ako uzmemo u obzir da studenti mogu samostalno provjeriti i saznati više o internetskim opasnostima i barem se minimalno informirati kako bi bili sigurni. Na pitanje jesu li osobni podatci koje su naveli na društvenim mrežama ili više njih izloženi internetskim opasnostima, većina studenata opet nije mogla procijeniti, čak njih 46,4 %. Opet se postavlja pitanje zašto je većina studenata dala takav odgovor? Je li možda razlog tomu što ne znaju što su zapravo osobni podatci ili pak ne znaju koje su to sve internetske opa-

snosti na društvenim mrežama? Možemo se referirati na dobivene rezultate o tome što su od navedenih podataka osobni podatci i time pokušati razmotriti razloge nemogućnosti samoprocjene, iako razloga može biti više. Vidimo da većina studenata različito poima osobne podatke koje navode na društvenim mrežama, a tri studenta zapravo nisu ni dala nikakav odgovor. Na pitanje jesu li bili žrtve internetske opasnosti, većina studenata odgovorila je negativno, njih 92,7 %, iako ima onih studenata koji su ipak bili žrtve internetske opasnosti te su naveli neke sigurnosne prijetnje i rizike društvenih mreža kao što su lažni profili na Facebooku, cyber nasilje, hakirani profili, verbalni napadi, slanje virusa preko poruka, zloraba fotografija i slično.

Studenti, njih 66 %, izrazilo je svoje slaganje s tvrdnjom da objava osobnih podataka na društvenim mrežama može pridonijeti potencijalnoj krađi identiteta. Isto tako, vidimo da je gotovo jednak postotak onih studenata koji jesu ili nisu upoznati sa zakonom o zaštiti osobnih podataka, koji je ove godine osobito popularan bio u Republici Hrvatskoj zbog primjene Opće uredbe o zaštiti osobnih podataka (GDPR) od svibnja 2018.

Većina studenata smatra da ne postoji privatnost na društvenim mrežama, njih 63 %, a 96,3 % koristi postavke privatnosti na društvenim mrežama. Samo 2,8 % studenata ne koristi postavke privatnosti, a njih 0,9 % uopće ne zna što su postavke privatnosti. Danas je teško pronaći neku društvenu mrežu ili pak neki drugi društveni medij koji nema dodatnih uvjeta i pravila tako da korisnici preopterećeni dugačkim pravnim tekstovima redovito prihvaćaju uvjete a da im ne posvete potrebnu pozornost ili ih uopće ne pročitaju tako da ne znaju na što pristaju, što može biti riskantno. To nam potvrđuju i rezultati istraživanja koji pokazuju da veći broj studenata ipak ne čita upute i uvjete o sigurnosti i privatnosti pri kreiranju profila na društvenim mrežama, čak 49,66 % studenata, a njih 38,62 % čita upute i uvjete o sigurnosti i privatnosti.

Daljnijim istraživanjem htjeli smo ustanoviti kako studenti informacijskih znanosti, informatike, računarstva i prava u usporedbi s ostalim fakultetima i studijskim grupama pristupaju društvenim mrežama i dijeljenju informacija na društvenim mrežama budući da su se tijekom studija susreli s nekim kolegijima koji su sadržajno uključivali informiranje o dijeljenju podataka na internetu i općenito o upravljanju osobnim podacima. Klaster je činio 149 sudionika, a ostali fakulteti/studijske grupe činile su 277 sudionika, a u testi-

ranju su korišteni hi-kvadrati. Isto tako, napravljena je i usporedba klastera međusobno pa je Kruskal-Wallisovim testom ustanovljeno da nema značajnih razlika među klasterima.

Na početku istraživanja postavili smo tri hipoteze od kojih je ona prva temeljna. Treba utvrditi jesu li postavljene hipoteze potvrđene ili se trebaju odbaciti. Prema rezultatima istraživanja možemo zaključiti da korisnici društvenih mreža, odnosno studenti Sveučilišta u Mostaru, nisu dobro upoznati s pravilima i načinima dijeljenja osobnih podataka na društvenim mrežama i načinima na koje može biti ugrožena njihova privatnost unatoč tomu što koriste postavke privatnosti (njih 96%), jer većina te iste postavke privatnosti, odnosno upute i uvjete o sigurnosti pri kreiranju profila na društvenim mrežama ne čita (njih 50%), što je kontradiktorno.

Isto tako, rezultati istraživanja ukazuju na to da studenti informacijskih znanosti, informatike, računarstva i prava u usporedbi s ostalim fakultetima i studijskim grupama podjednako pristupaju društvenim mrežama i dijeljenju informacija na društvenim mrežama iako su se tijekom studija susreli s nekim kolegijima koji su sadržajno uključivali informiranje o dijeljenju podataka na internetu i općenito upravljanje osobnim podacima. Hipoteza se odbacuje djelomično jer su uočene razlike u unosu podataka na društvenim mrežama, koje studenti informacijskih znanosti, informatike, računarstva i prava u usporedbi s ostalim fakultetima i studijskim grupama unose manje.

Trećom hipotezom pretpostavljalo se da će postojati razlika među studentima informacijskih znanosti, informatike, računarstva i prava u objavi osobnih podataka na društvenim mrežama koji bi mogli doprinijeti krađi identiteta i da će studenti informacijskih znanosti u odnosu na druge studijske grupe objavljivati najmanje osobnih podataka koji mogu tome pridonijeti, što nije slučaj, jer nisu ustanovljene znatnije razlike.