

Maja Ružić-Baf\*  
Mirjana Radetić-Paić\*\*  
Saša Jovanović\*\*\*

## Jesu li društvene mreže sigurne?

UDK: 004.738.5:371  
Prethodno priopćenje

Primljeno: 9. 5. 2012.  
Prihvaćeno: 20. 8. 2012.

---

**Sažetak:** *Prijenosnici, ultraprijenosnici, „tableti”, pametni telefoni zadobili su puno povjerenje među studentima. Popularnost društvenih mreža, posebice Facebooka, postala je imperativom današnje generacije. No, postati i ostati korisnikom u sigurnosnim okvirima znajući se zaštititi od mogućih negativnih posljedica, većini mladih nije prioritet. Nedovoljno znanje i manjak vještina upozoravaju na negativne posljedice upotrebe društvenih mreža. Njihova sigurnost tema je ovog rada koji je podijeljen u dva dijela. U prvome se razmatraju teorijske postavke sigurnosti društvenih mreža te se prikazuju rezultati istraživanja nekoliko autora o toj temi. U drugom, empirijskom, dijelu rada prikazani su rezultati pilot-istraživanja studenata prvih godina studija o sigurnosti društvene mreže Facebook.*

**Ključne riječi:** *društvene mreže, pozitivne i negativne posljedice korištenja društvenih mreža, sigurnost, studenti.*

---

Maja Ruzic-Baf\*

Mirjana Radetic-Paic\*\*

Ana Jovanovic\*\*\*

## Are Social Networking Websites Safe?

UDC: 004.738.5:371

Preliminary communication

Accepted: 9<sup>th</sup> May 2012

Confirmed: 20<sup>th</sup> August 2012

**Summary:** *Laptops, ultra notebooks, tablets, smartphones have gained lots of confidence among students. The popularity of social networking websites, particularly Facebook, has become an imperative for today's generations. However, becoming a user and remaining as such within the security framework while knowing how to protect oneself from possible negative effects, is not a priority for most young people. Insufficient knowledge and a lack of skills indicate negative effects of using social networking websites. This scientific work, divided into two parts, deals with safety of social networking websites. The first part discusses theoretical foundations of safety on social networking websites and includes research-related results found by several authors. In the second, empirical, part of the article the results of a pilot research dealing with the safety of Facebook social networking website, conducted by first-year students, have been shown.*

**Keywords:** *social networking websites, positive and negative effects of using social networking websites, safety, students.*

### 1. Uvod

Integracija informacijskih i komunikacijskih tehnologija u obrazovne kurikulume neizostavan je dio kvalitetnog edukacijskog procesa. Uz mnogobrojne prednosti koje nam pruža, poput razvijanja pamćenja, metoda učenja, stjecanja vještina za rješavanje problema, razvijanja osjećaja vlastite sposobnosti i samopouzdanja (Radetić-Paić, Ružić-Baf i Zuliani, 2011.), moguće je izdvojiti i štetne posljedice koje se obično javljaju zbog neznanja i nekorištenja potrebnih tehnika kao što su: krađa identiteta, ukradena lozinka, lažno predstavljanje, širenje neistina, vršnjačko nasilje, vrijeđanje, uhođenje, uznemiravanje i slično.

Zaključci istraživanja provedenih u američkim školama navode da je internet pozitivno i vrlo korisno okruženje koje služi socijalizaciji, učenju i sudjelovanju u javnom životu. Uz navedene pozitivne mogućnosti korištenja internetom, postoje i one negativne, a to su najčešće opasnost od seksualnog uznemiravanja, maltretiranja, vršnjačkog nasilja te izloženost ilegalnim sadržajima (ISTFF, 2008.).

Dostupnost interneta, razvoj tehnologija *Web 2.0* te sve učestalija uporaba mobilnih telefona novijih generacija omogućuje mladim ljudima brz pristup željenim informacijama. Mladi ljudi sve češće zamjenjuju stolna računala ultraprijenosnicima, *tabletima*, pametnim telefonima i ostalim hitovima mobilnog računalstva. Dostupnost „u trenutku“ postala je imperativom, odnosno „ovisnošću“ današnjeg društva znanja. Stoga ne čudi podatak da broj korisnika (Pingdom, 2010.) interneta u Europi iznosi oko 475,1 milijun, a broj korisnika elektroničke pošte iznosio je do kraja 2010. godine **1,88 milijardi**. Krajem 2010. godine broj korisnika društvene mreže *Facebook* iznosio je šesto milijuna. Zanimljiv je podatak da je toj društvenoj mreži u 2010. godini pristupilo dvjesto pedeset milijuna korisnika. U Hrvatskoj je profil na društvenoj mreži *Facebook* otvorilo ukupno 1 506 860 korisnika (Socialbakers, 2011.).

Slobodno vrijeme mladih postalo je „(ne)vrijeme“ društvenih mreža. Hržica (2010.) navodi da mladi najčešće rabe društvene mreže kao što su *Webkinz* ili *Club Penguin*, a često i one namijenjene starijoj populaciji: *Windows Live Spaces*, *LinkedIn*, *Facebook*, *YouTube*, *MySpace*, *Flickr*, *Twitter*, *Delicious* i druge. Društvene mreže najčešće služe objavljivanju i pregledavanju fotografija ili videozapisa, pisanju poruka na zidovima, klikanju sviđalice, brbljanju, umreženom igranju igara, oglašavanju, pisanju *blogova*, objavljivanju mrežnih profila i dr.

Informacije koje korisnici objavljuju ili neke od informacija na njihovim stranicama (profilima) čine ih podložnijima krađi identiteta, virtualnom vršnjačkom nasilju i „grabežljivcima“ na internetu (Hržica, 2010.).

### **1.1. Ranija istraživanja**

Rezultati istraživanja koje su proveli Lenhart i Madden (2007.) pokazuju da su mnoga istraživanja usredotočena na internet u cjelini. Autori smatraju da su maloljetnici suočeni s različitim rizicima u različitim uvjetima na Mreži. Navode da se komunikacija na popularnim društvenim mrežama najčešće uspostavlja s prijateljima i s njihovim prijateljima, a rjeđe između potpunih stranaca. Treba napomenuti da se sve više mladih upušta u komunikaciju sa strancima koji se u većini slučajeva predstavljaju lažnim profilima. Ybarra i Mitchell (2008.) smatraju da su rizici društvenih mreža gotovo jednaki onima koji se odnose na uporabu interneta općenito.

Prikupljene podatke na društvenoj mreži *Facebook* moguće je iskoristiti radi: uzrokovanja štete ugledu osobe (ili neke druge neugodnosti, npr. zastrašivanja), ucjenjivanja korisnika, otkrivanja povjerljivih podataka, nanošenja fizičke boli, krađe identiteta, lažnog predstavljanja, uhođenja (čak i industrijske špijunaže), ciljanog (personaliziranog) oglašavanja, prepoznavanja lica (putem objavljenih fotografija) i dr. Prijetnje privatnosti uključuju: prikupljanje digitalnih zapisa o korisnicima, prikupljanje sporednih podataka, prepoznavanje lica korisnika, otkrivanje podataka pomoću fotografija, povezivanje podacima i oznakama u fotografijama, nemogućnost potpunog brisanja korisničkog računa. Sigurnosni rizici i opasnosti mogu se podijeliti na prijetnje mrežama i podacima, prijetnje identitetu i društvene prijetnje.

Prijetnje mrežama i podacima uključuju: neželjene poruke, *cross site scripting* (*xss*), viruse i crve te alate za grupiranje profila više društvenih mreža.

Prijetnje identitetu uključuju: *phishing* napade, otkrivanje podataka te lažni profil.

Društvene prijetnje uključuju: uhođenja, *cyber* nasilje te industrijsku špijunažu (CERT, 2010.).

Važno je napomenuti da se, primjerice, izbrisane fotografije i dalje nalaze na poslužiteljima.

Zlonamjerni korisnici provode razne oblike prijevара na *Facebooku*, uglavnom kako bi došli do financijske koristi (*phishing*, *hoax* i *scam*), tzv. *malveri*, *cross-site scripting* napadi (CERT, 2010.).

U rujnu 2011. godine Europska je komisija objavila skupinu rezultata (Fluckiger, Grehan i Donoso, 2011.) dobivenih neovisnom (drugom po redu) procjenom o provedbi „Načela za sigurnije društveno umrežavanje“ unutar EU-a. Procjena uključuje i rezultate testova provedenih na devet društvenih mreža. Prvi podatci objavljeni su u lipnju 2011. godine te uključuju rezultate testova provedenih na mrežnim stranicama: *Dailymotion*, *Flickr*, *Habbo Hotel*, *Stardoll*, *Skyrock*, *Windows Live*, *Yahoo Pulse*, *YouTube and Xbox Live*, *Arto*, *Bebo*, *Facebook*, *Giovani.it*, *Hyves*, *MySpace*, *Nasza-klaza.pl*, *Netlog*, *One.lt*, *Ratee*, *SchulerVZ*, *IRC Galleria (Sulake)*, *Tuenti and Zap.lu*.

Komisija je angažirala skupinu od četrnaest nacionalnih istraživača pod vodstvom koordinatora koji su imali prijašnja iskustva i saznanja iz područja uporabe i poznavanja interneta i novih tehnologija među mladima. Najprije su raščlanjena samoočitovanja svih potpisnika kako bi se objasnila njihova osobna sigurnosna pravila, zatim se počeo izrađivati standardizirani upitnik koji je služio kao osnova za testiranje mrežnih stranica. Istraživači su provodili ispitivanja na materinskom jeziku ispitanika (skupina stručnjaka provela je ispitivanje za društvenu mrežu *Tuenti* na španjolskom govornom području, stručnjaci zaduženi za *Facebook* proveli su ispitivanje na engleskom i francuskom govornom području,

*Netlog* je ispitivan na njemačkom i nizozemskom, *MySpace* na engleskom i španjolskom, a *Habbo Hotel* na engleskom i finskom jeziku).

Pridržavajući se anketnog upitnika, istraživači su pretraživali mrežne stranice, potom su se na iste registrirali kao maloljetnici i odgovarali na sljedeća pitanja:

1. Mogu li pronaći sigurnosne savjete/informacije za djecu?
2. Jesu li informacije koje se odnose na djecu lako razumljive i dostupne?
3. Mogu li blokirati prijatelja, tj. mogu li odbiti zahtjev za prijateljstvom?
4. Imam li mogućnosti uklanjanja/brisanja objava/slika s mog profila?
5. Kada sam prijavljen na svoj korisnički račun (profil), jesu li moji osobni podatci vidljivi samo mojim prijateljima ili svim drugim korisnicima?
6. Kada sam prijavljen na korisnički račun kao odrasli korisnik te upotrebljavam zajedničku tražilicu u potrazi za svojim nadimcima, uspijevam li pronaći korisničke račune (profile) koje sam napravio registrirajući se kao maloljetnik na toj mrežnoj stranici?

Mrežnim je stranicama također poslan izvještaj/zahtjev za pomoć te je analizirana brzina i kvaliteta odgovora.

Grehan i Donoso (2011.) istraživali su koliko se načela primjenjuje pri uporabi društvenih mreža. Analizirali su ukupno sedam načela:

1. povećanje pozornosti o porukama obrazovnog i sigurnosnog karaktera te prihvatljivim načinima ponašanja prema pravilima koja vrijede za korisnike, roditelje, učitelje i skrbnike, na istaknut, jasan i dobno prilagođen način
2. težnju za osiguravanjem dobno prilagođenih usluga namjernim posjetiteljima
3. poticanje korisnika da rabe alate i tehnologiju
4. omogućavanje mehanizama za prijavljivanje ponašanja ili sadržaja koji krše uvjete korištenja, koji su jednostavni za uporabu
5. mogućnost odgovora na obavijesti o ilegalnom sadržaju/ponašanju
6. omogućavanje i poticanje korisnika da upotrijebe zaštićen pristup osobnim informacijama
7. procjenu sredstava koja služe procjeni ilegalnog ili zabranjenog sadržaja/ponašanja.

Istraživanje *Facebooka* pokazalo je da je prvo načelo na vrlo zadovoljavajući način provedeno na njihovoj mrežnoj stranici, a ostala su načela prilično dobro provedena. Na toj društvenoj mreži posebnu pozornost treba obratiti na sljedeće komponente:

- izvješća o neprikladnom sadržaju/kontaktu ne zadovoljavaju
- profili (korisnički računi) maloljetnika nisu postavljeni kao privatni (prema

osnovnim postavkama), što upućuje na mogućnost pristupa ne samo prijateljima nego i prijateljima prijatelja

- pojedina se oglašavanja mogu smatrati neprikladnima za maloljetnike
- mehanizam kojim se onemogućuje ponovna registracija maloljetnih osoba nije djelotvoran
- postojeći mehanizmi namijenjeni roditeljskoj kontroli ne sadrže dovoljno informacija (*softver* namijenjen filtriranju pojedinih sadržaja)
- uvjeti korištenja nepotpuni su i nejasni mlađoj populaciji.

Budući da su informacijske i komunikacijske tehnologije postale nezamjenjivim dijelom učinkovitog odgojnog i obrazovnog procesa, a jedna od najčešće korištenih društvenih mreža današnjice jest *Facebook*, postavlja se pitanje koliko su korisnici društvenih mreža (studenti) upoznati sa smjernicama za uporabu podataka na društvenoj mreži *Facebook* i s postavkama privatnosti te koliko su sposobni procijeniti eventualne negativne učinke uporabe društvenih mreža.

## 2. Cilj istraživanja i metode rada

U ovom se istraživanju krenulo od pretpostavke da studenti nisu dovoljno upoznati sa smjernicama za uporabu podataka i postavljanje sigurnosnih postavki na društvenoj mreži *Facebook*. Ovim se pilot-istraživanjem pokušalo odgovoriti na pitanje postoji li razlika u poznavanju i uporabi sigurnosnih postavki na *Facebooku*.

Uzorak čini pedeset i osam studenata Odjela za odgojne i obrazovne znanosti Sveučilišta Jurja Dobrile u Puli. Podijeljeni su s obzirom na vrstu studija u dvije grupe (dvije nezavisne varijable): prva godina razredne nastave (N=30) i prva godina studija predškolskog odgoja (N=28). Primijenjen je upitnik koji sadrži ukupno 42 varijable, a za potrebe ovog pilot-istraživanja analizirane su sljedeće zavisne varijable:

1. dostupnost *e-mail* adrese korisnika
2. dostupnost broja mobilnog telefona korisnika
3. kontrola zadanih postavki privatnosti korisnika
4. postavljanje oznaka koje se odnose na profil korisnika
5. postavljanje oznaka (engl. *tag*)
6. postavljanje *tag* sugestija
7. mogućnost pisanja po zidu korisnika
8. mogućnost pregledavanja profila korisnika
9. mogućnost slanja poruka korisniku

10. mogućnost slanja zahtjeva za prijateljstvom
11. mogućnost oglašavanja trećih osoba
12. mogućnost društvenog oglašavanja
13. razumijevanje smjernica za korištenje podataka na društvenoj mreži *Facebook*.

Istraživanje je provedeno anonimno, a studenti su bili upoznati s činjenicom da u svakom trenutku mogu odustati od popunjavanja upitnika bez posljedica, što nitko nije učinio.

### 3. Rezultati istraživanja i rasprava

U Tablici 1 prikazana su mišljenja ispitanika o dostupnosti njihovih *e-mail* adresa javnosti. U prvoj skupini ispitanika (RN1) njih 67,9 posto objavilo je svoju adresu računalne pošte, a 43,3 posto studenata druge skupine (PO1) omogućuje uvid u e-adresu prijateljima s liste (hi-kvadrat=7,831; df=2; p=0,25). Može se zaključiti da studenti prve skupine ispitanika (dalje u tekstu RN1) smatraju kako *e-mail* adresa treba biti dostupna svima, a studenti druge skupine (dalje u tekstu: PO1) misle da bi adresa trebala biti vidljiva u većini slučajeva samo prijateljima. Vrijednost  $\chi^2$  testa (hi-kvadrat=7,831; df=2; p=0,05) veća je od granične vrijednosti na drugom stupnju slobode, što znači da se pokazatelji mogu smatrati značajnim, a ne slučajnim.

**Tablica 1** — *Mišljenja mladih o dostupnosti e-mail adresa<sup>1</sup>*

	javno	prijatelji	samo ja	označeni s liste	ukupno
<b>RN1</b>	67,9	14,3	17,9	0	100,0
<b>PO1</b>	33,3	43,3	23,3	0	100,0
<b>ukupno</b>	50,0	29,3	20,7	0	100,0

U Tablici 2 prikazana su mišljenja ispitanika o dostupnosti njihovih brojeva mobilnog telefona javnosti. Mišljenje obiju skupina ispitanika jest da brojevi mobilnog telefona ne bi trebali biti dostupni javnosti. Ispitanici prve skupine smatraju da bi u većini slučajeva brojevi mobilnih telefona trebali biti dostupni prijateljima (53,6%), a ispitanici druge skupine, ukupno njih 60 posto, smatraju da brojevi mobilnih telefona ne bi trebali biti vidljivi nikome. Vrijednost  $\chi^2$  testa iznosi (18,195; df=3; p=0,05). Može se zaključiti da su ispitanici druge skupine

<sup>1</sup> Dalje se u članku navode podatci u postotcima.

oprezniji pri davanju privatnih brojeva mobilnih telefona i omogućavanju njihove vidljivosti široj javnosti.

**Tablica 2** — *Mišljenja ispitanika o dostupnosti broja mobilnog telefona*

	javno	prijatelji	samo ja	označeni s liste	ukupno
<b>RN1</b>	28,6	53,6	14,3	3,6	100,0
<b>PO1</b>	0	40,0	60,0	0	100,0
<b>ukupno</b>	13,8	46,6	37,9	1,7	100,0

U Tablici 3 prikazane su izjave ispitanika o kontroli zadanih postavki privatnosti. Rezultati pokazuju da niti jedna skupina nije dovoljno upoznata s primjenjivanjem postavki privatnosti. Manje od polovine ispitanika iz objiju skupina (prva skupina: 7,1%, druga skupina: 23,3%) ne rabi opciju „prilagođeno“ među postavkama za privatnost. Vrijednost  $\chi^2$  testa veća je od granične vrijednosti na drugom stupnju slobode, što znači da se pokazatelji mogu smatrati značajnim, a ne slučajnim (hi-kvadrat=10,38; df=2; p=0,025).

**Tablica 3** — *Izjave ispitanika o kontroli zadanih postavki privatnosti*

	javno	prijatelji	prilagođeno	ukupno
<b>RN1</b>	14,3	78,6	7,1	100,0
<b>PO1</b>	40,0	36,7	23,3	100,0
<b>ukupno</b>	27,6	56,9	15,5	100,0

U Tablici 4 prikazane su izjave ispitanika o uključenosti oznaka. S obzirom na dobivene rezultate u Tablici 3, vidljivo je da su u većini slučajeva postavke koje se odnose na profil korisnika isključene (prva skupina: 64,3%, druga skupina: 86,7%; hi-kvadrat=3,962; df=1; p=0,05).



**Tablica 4** — *Izjave ispitanika o postavljanju oznaka koje se odnose na profil*

	uključene postavke	isključene postavke	ukupno
<b>RN1</b>	35,7	64,3	100,0
<b>PO1</b>	13,3	86,7	100,0
<b>ukupno</b>	24,1	75,9	100,0

U Tablici 5 prikazane su izjave ispitanika o uključenosti oznaka (*tag*). U objema skupinama postavke su ispitanika isključene. U prvoj skupini 35,7 posto ispitanika ima uključene postavke, a u drugoj skupini uključene postavke ima svega 10 posto ispitanika. Treba napomenuti da je *Facebook* uveo kontrolu objava fotografija i statusa tako da korisniku omogućava da u komentarima označi osobe s kojima, primjerice, nije prijatelj (hi-kvadrat=5,507; df=1; p=0,025).

**Tablica 5** — *Izjave ispitanika o postavljanju oznaka*

	Uključene postavke	Isključene postavke	Ukupno
<b>RN1</b>	35,7	64,3	100,0
<b>PO1</b>	10,0	90,0	100,0
<b>Ukupno</b>	22,4	77,6	100,0

U Tablici 6 prikazane su izjave ispitanika o postavljanju *tag* sugestija. Zanimljiv je i očekivan rezultat da niti jedna skupina ispitanika nema uključenu postavku *tag* sugestija iznad 50 posto. Vrijednost  $\chi^2$  testa veća je od granične vrijednosti na prvom stupnju slobode, što znači da se pokazatelji mogu smatrati značajnima (hi-kvadrat=7,447; df=1; p=0,005).

**Tablica 6** — *Izjave ispitanika o uključenosti opcije „tag“ sugestija*

	uključene postavke	isključene postavke	ukupno
<b>RN1</b>	35,7	64,3	100,0
<b>PO1</b>	6,7	93,3	100,0
<b>ukupno</b>	20,7	79,3	100,0

U Tablici 7 prikazane su izjave o mogućnostima pisanja po zidu, pregledavanja i slanja poruka te zahtjeva za prijateljstvom. U objema skupinama ispitanika vidljivo je da po zidu ispitanika pisati mogu samo prijatelji (prva skupina: 96,4%, druga skupina: 73,3%; hi-kvadrat=5,893; df=1; p=0,05). Pregledavanje profila u prvoj skupini (75%) omogućeno je samo prijateljima, a u drugoj je skupini (56,7%) uključena opcija javnog pregledavanja profila (hi-kvadrat=5,987; df=1; p=0,025). Nadalje, rezultati pokazuju da u prvoj skupini (92,9%) ispitanicima poruke mogu slati samo prijatelji, u drugoj također (60%) isključivo prijatelji. No, treba primijetiti da 40 posto ispitanika druge skupine omogućuje javno primanje poruka (hi-kvadrat=8,539; df=1; p=0,005). U objema skupinama ispitanika slanje zahtjeva za prijateljstvom omogućeno je svima, dakle ono je javno (hi-kvadrat=6,783; df=1; p=0,01).

**Tablica 7** — *Izjave ispitanika o raznim mogućnostima*

smjer	izjave ispitanika o mogućnosti pisanja po zidu		izjave ispitanika o mogućnosti pregleda		izjave ispitanika o mogućnosti slanja poruka		izjave ispitanika o mogućnosti slanja zahtjeva za prijateljstvom	
	RN1	PO1	RN1	PO1	RN1	PO1	RN1	PO1
javno	7,1	26,7	25,0	56,7	7,1	40,0	60,7	90
prijatelji	92,9	73,3	75,0	43,3	92,9	60,0	39,3	10
ukupno	100	100	100	100	100	100	100	100

Izjave ispitanika o mogućnosti oglašavanja trećih osoba pokazuju da ispitanici smatraju da bi takvo oglašavanje trebalo biti vidljivo i omogućeno od strane prijatelja, a ne javno (hi-kvadrat=6,953; df=2; p=0,025). Ispitanici isto smatraju pri izjavama o mogućnosti oglašavanja društvenih oznaka (hi-kvadrat=6,820; df=2; p=0,05).

Posljednja varijabla odnosila se na smjernice za korištenje podataka na *Facebooku*. Ispitanici obiju skupina odgovorili su da nisu pročitali smjernice koje se odnose na uporabu podataka na toj društvenoj mreži. Smatramo da je smjernice potrebno pročitati i razumjeti kako bi se ispitanici (studenti) mogli služiti društvenom mrežom ispravno, a jedan od važnih dijelova jest i način zaštite na društvenim mrežama.

Više od 50 posto ispitanika obiju skupina nije nikada pročitalo gore navedene smjernice, a zabrinjavajući je podatak da smjernice nije pročitalo 90 posto ispitanika druge skupine. Također, valja naglasiti da je 39,3 posto ispitanika prve skupine upoznato sa smjernicama za korištenje podataka na društvenoj mreži *Facebook* (hi-kvadrat=6,783; df=1; p=0,01).

#### 4. Zaključak

Na osnovi dobivenih rezultata možemo zaključiti da studenti prvih godina studija nisu dovoljno upoznati s pravilima korištenja podataka na *Facebooku* niti s općim uvjetima za korištenje te društvene mreže. Rezultati pokazuju da niti jedna grupa studenata nije dovoljno upoznata s postavkama privatnosti.

Zabrinjavajući je podatak da ispitanici druge skupine (PO1), njih 90 posto, i ispitanici prve skupine (RN1), njih 60,7 posto, pri otvaranju profila na *Facebooku* te pri daljnjoj uporabi te mreže, nisu nikada pročitali smjernice za korištenje podataka.

Budući da je pilot-istraživanje provedeno početkom akademske godine, važno je napomenuti da se u sklopu kolegija Informatika i Osnove informatike obrađuje nekoliko tema u vezi sa sigurnosti služenja internetom i s upoznavanjem studenata s pravilima uporabe podataka i uvjetima služenja društvenim mrežama. Nadalje, predlažemo da bi se upravo teme koje su vezane uz sigurnost društvenih mreža trebale obrađivati i u nižim razredima osnovne škole, jer se većina djece mlade od trinaest godina (uz znanje ili neznanje roditelja i učitelja) gotovo svakodnevno služi nekom od društvenih mreža. Stalna edukacija odgojitelja predškolske djece, učitelja razredne nastave, nastavnika, profesora i roditelja uvelike bi doprinijela kvalitetnijoj zaštiti mladih u mrežnom okruženju.

Društvene mreže nisu samo fenomen novoga, informacijskog i komunikacijskog doba (Šimović, 2010.) ili, pak, društveni fenomen koji je zaintrigirao pedagoge, sociologe, psihologe, nego pojava koja je uznemirila kreativne mozgove financijskih i marketinških stručnjaka.

## Literatura

1. Fluckiger, Cedric i sur. (2011.): *Facebook* 121(2): e 350 – e 357 (datum preuzimanja: 14. 1. 2012., dostupno na: <[http://ec.europa.eu/information\\_society/activities/social\\_networking/docs/individ\\_reports\\_11/facebook.pdf](http://ec.europa.eu/information_society/activities/social_networking/docs/individ_reports_11/facebook.pdf)>).
2. ISTFF (2008.): *Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking Of State Attorneys general of The United States*, Berkman.
3. Lenhart, Amanda; Madden, Mary (2007.): *Teens, Privacy, & Online Social Networks*.
4. Ybarra, Michele; Mitchell, Kimberly (2008.): How Risky Are Social Networking Sites? A Comparison of Places Online Where Youth Sexual Solicitation and Harassment Occurs. *Pediatrics*.
5. CERT (2010.): *Sigurnost društvene mreže Facebook* (dostupno na: <<http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-10-317.pdf>>).
6. Hržica, Viktorija (2010.): *Kako pomoći djeci u korištenju društvenih mreža na sigurniji način, Pogled* (datum preuzimanja: 31. 10. 2010., dostupno na: <<http://pogledkrozprozor.wordpress.com/2010/10/31/kako-pomoci-djeci-u-koritenju-drutvenih-mreza-na-sigurniji-nacin/>>).
7. Pingdom (2010.): *Internet 2010 in numbers* (datum preuzimanja: 12. 1. 2012., dostupno na: <[worldwide.http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/](http://worldwide.http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/)>).
8. Socialbakers (2011.): *Croatia Facebook Statistics* (dostupno na: <<http://www.socialbakers.com/facebook-statistics/croatia>>).
9. Radetić-Paić, Mirjana; Ružić-Baf, Maja; Zuliani, Đeni (2011.): *Poremećaji nedovoljno kontroliranog ponašanja sa psihološkog, socijalnopedagoškog te informacijskog i komunikacijskog aspekta*, Zagreb: Učiteljski fakultet Sveučilišta u Zagrebu. <[http://www.pewinternet.org/PPF/r/211/report\\_display.asp](http://www.pewinternet.org/PPF/r/211/report_display.asp)>.
10. Šimović, Vladimir (2010.): *Uvod u informacijske sustave*, Zagreb: Golden marketing – Tehnička knjiga, Učiteljski fakultet Sveučilišta u Zagrebu.

Maja Ružić-Baf\*

Mirjana Radetić-Paić\*\*

Saša Jovanović\*\*\*

## Sono sicure le reti sociali?

UDC: 004.738.5:371

Relazione al convegno

Ricevuto: 9. 5. 2012

Accettato per la stampa: 20. 8. 2012

**Riassunto:** *portatili, ultraportatili, tablet, smartphone godono presso gli studenti di una fiducia infinita. La popolarità delle reti sociali, soprattutto della social network Facebook, è uno degli imperativi delle generazioni d'oggi. Diventarne utente ed esserlo nei limiti di sicurezza, sapersi proteggere dalle possibili conseguenze negative spesso non rientra tra le prerogative dei giovani. La mancanza di conoscenze e le skills insufficienti sono il frutto negativo dell'uso delle reti sociali. Il tema dell'articolo riguarda la sicurezza delle reti sociali. Il lavoro è diviso in due parti. Nella prima parte vengono esaminate le premesse teoriche riguardanti la sicurezza delle reti sociali e vengono forniti i risultati delle ricerche di alcuni studiosi che hanno condotto ricerche sull'argomento. Nella seconda parte, la parte empirica, vengono offerti i risultati di una ricerca pilota condotta dagli studenti del primo anno sul tema della sicurezza della rete sociale Facebook.*

**Parole chiave:** *reti sociali, conseguenze positive e negative dell'uso delle reti sociali, sicurezza, studenti.*

\*dr. sc. Maja Ružić-Baf, doc.

\*\* dr. sc. Mirjana Radetić-Paić, doc.

\*\*\* Saša Jovanović,

studentica

Sveučilište Jurja Dobrila u Puli

Odjel za odgojne i obrazovne znanosti

mruzic@unipu.hr

\*Maja Ruzic-Baf, PhD,

Assistant Prof.

\*\* Mirjana Radetic-Paic, PhD, Assistant Prof.

\*\*\* Saša Jovanovic, student

University of „Juraj Dobrila“, Pula

Department of Pre-school and Primary School Teaching

mruzic@unipu.hr

\*dr. sc. Maja Ružić-Baf,

ricercatrice

\*\* dr. sc. Mirjana Radetic-Paic, ricercatrice

\*\*\* Saša Jovanovic, studente

Università degli Studi „Juraj Dobrila“, Pola

Dipartimento di Scienze della Formazione e dell'Educazione

mruzic@unipu.hr

