Zbornik
Instituta za kriminološka i
sociološka istraživanja
2013 / Vol. XXXII / 1 / 49-60

Originalni naučni rad
UDK: 342.738:004.378.5;
004.738.5:316.472.4

SOCIJALNO UMREŽAVANJE PRIVATNOSTI*

Vesna Žunić-Pavlović*
Marina Kovačević-Lepojević*
Univerzitet u Beogradu, Fakultet za specijalnu edukaciju i rehabilitaciju

Borko Lepojević*
Ministarstvo odbrane Republika Srbija

Još od kraja devedesetih godina kada dolazi do oživljavanja kocepta socijalnog umrežavanja na internetu, pažnju javnosti zaokupljuje proučavanje negativnih aspekata funkcionisanja sajtova za socijalno umrežavanje, posebno primedbi koje se odnose na zloupotrebu privatnosti. Rezultati istraživanja ponašanja korisnika na socijalnim mrežama sugerišu da se više od polovine korisnika opredeljuje da privatne podatke učini javno dostupnim. Sa druge strane, obezbeđenost platformi za socijalno umrežavanje korisnika nije zadovoljavajuća. Poseban problem predstavlja neovlašćeno prikupljanje podataka o komunikaciji građana od strane bezbednosnih agencija razvijenih država sveta u sklopu aktivnosti koje se odnose na prevenciju terorizma i kriminala.

Cilj ovog rada je sagledavanje negativnih posledica socijalnog umrežavanja u kontekstu zloupotrebe privatnosti. Posebna pažnja ukazuje se analizi međunarodne i domaće legislative u pravcu obezbeđivanja privatnosti korisnika na internetu i izdvajanju preporuka za postupanje regulatornih tela i korisnika.

KLJUČNE REČI: socijalne mreže / privatnost / internet / zaštita

* Ovaj tekst je nastao kao rezultat na projektu "Kriminal u Srbiji: fenomenologija, rizici i mogućnosti socijalne intervencije" (broj 47011) koji finansira Ministarstvo prosvete, nauke i tehnološkog razvoja RS.
* E-mail: ziniceva@ eunet.rs
* E-mail: marina.lepojevic@gmail.com
* E-mail: borko.lepojevic@evision.rs

UVOD

Sve popularnija tema u laičkoj i stručnoj javnosti jeste bezbednost sadržaja komunikacije građana koja se odvija na internetu, posebno posredstvom sajtova za socijalno umrežavanje. Postavlja se pitanje koliko je u koncept socijalnog umrežavanja na internetu "umrežena" privatnost i u kom pravcu.

Podaci koje prikupljaju internet pretraživači, sajtovi za socijalno umrežavanje i komunikaciju smatraju se vrlo aktuelnim za državne službe. Edward Snowden izneo je podatke o američkom programu za masovni nadzor elektronskih komunikacija građana pod nazivom "Prizma" i obelodanio da su NSA i FBI tim putem imali direktan pristup centralnim serverima devet vodećih američkih internet kompanija (Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube i Apple) i pritom stekli uvid u audio i video razgovore, fotografije, emailove i dokumenta miliona korisnika servisa ovih kompanija[1]. Prema podacima kompanije *Google* od jula do decembra 2012. godine trideset jedna zemlja je uputila 21.389 zahteva za otkrivanje privatnih podataka o korisnicima, među kojima najviše SAD (8.438), Indija (2.431), Francuska (1.693), Nemačka (1.550) i Velika Britanija (1.458) (Google Transparency Report, 2013). Tokom prve polovine 2013. godine (od januara do jula), zahteve za pristup podacima 38000 korisnika Facebook kompanije uputile su 74 države. Podaci koje su vlasti tražile od kompanije su imena korisnika, IP adrese, ali i uvid u sadržaj profila korisnika. Američke vlasti ozbiljno prednjače u odnosu na ostatak sveta, sa 11000 zahteva za pristup nalozima 20000 korisnika kompanije Facebook. U 79% slučajeva na ove zahteve odgovorilo se pozitivno. Posle američkih vlasti, podaci Facebook korisnika najviše su zanimali vlast u Velikoj Britaniji iz koje je na adresu kompanije stiglo 1975 zahteva za podacima o 2337 naloga, na koje je Facebook u 68% slučajeva odgovorio pozitivno. Među zemljama koje predvode podnosioce zahteva su i Francuska, Nemačka i Indija. Ove zemlje su i jedine koje su uputile zahteve za informacijama o više od 1000 korisničkih naloga. Republika Srbija tražila je informacije o jednom korisniku, a na zahtev nije odgovoreno pozitivno (Facebook, 2013).

[1] http://www.informacija.rs/Ostalo/Skandal-u-Vasingtonu-Kako-je-Obamina-administracija-pratila-milione-korisnika-interneta.html, pristupljeno 10. septembra 2013. godine

POJAM SOCIJALNOG UMREŽAVANJA

Popularno mišljenje o nastanku i održavanju koncepta socijalnog umrežavanja na internetu zasniva se na društvenim promenama koje se ogledaju u transformaciji zajednice od funkcionisanja po principu solidarnih grupa, domaćinstava, do organizacije u mrežama pojedinaca (Welman 2001; Castells, 2009). Pojedinac u tom kontekstu čini osnovnu jedinicu virtuelne zajednice na prvi pogled lišene konteksta, fizičkog prostora čije je mesto danas i svuda i nigde konkretno, u središtu tzv. umreženog individualizma. Nove veze između pojedinaca su uglavnom slabe i površne, ali kao takve neophodne za socijalno funkcionisanje. Autori smatraju da tako formirane slabe veze (poznanici) omogućavaju bolju pristupačnost informacijama i resursima u odnosu na jake veze (rođaci, prijatelji) (Granovetter, 1983). Sa druge strane autori smatraju da internet povoljno deluje na održavanje i slabih i jakih veza (Wellman, 2001). U skladu sa prethodno prikazanim teorijskim opredeljenjem, izdvaja se definicija socijalnih mreža koja oslikava savremeno viđenje društvene zajednice lišene konteksta (komšiluk, selo, opština) kao sistema interpesonalnih veza koje pojedincima obezbeđuju društvenost, podršku, informisanost, osećaj pripadnosti i socijalni identitet (Wellman, 2001:228). Ono što je zajedničko za sve sajtove za socijalno umrežavanje je da omogućavaju korisnicima formiranje javnog ili polujavnog profila, kreiranje mreže ličnih kontakata i konstantan uvid u sopstvena kretanja i putanje drugih osoba na mreži (Boyd, Ellison, 2007:210). Priroda međusobne povezanosti članova na mreži generalno varira od sajta do sajta. Kako će jedna virtuelna zajednica izgledati zavisi od tehnološke opremljenosti, interfejsa, sadržajnosti, koji treba da odgovori na zahteve korisnika i kulturnog konteksta (teme, pravila, obrasci interakcija).

Sa jedne strane, autori ističu da socijalno umrežavanje doprinosi kvalitetu socijalnih interakcija, upotpunjva i ohrabruje komunikaciju u fizičkom svetu, podstiče razvoj tolerancije na različitosti, prevazilaženje klasnih, verskih, uzrasnih, kulturnih, političkih razlika, podstiče kreativnost, akademske sposobnosti, socijalne veštine, sazrevanje i razvoj identiteta kod adolescenata, samopouzdanje, pa čak i duhovni razvoj (Pempek i drugi, 2009; Van den Berg, Leenes, 2011). Međutim, nisu zanemarljive primedbe poput povreda privatnosti, produbljivanja razlika između bogatih i siromašnih, socijalne isključenosti, porasta komercijalnih i političkih zloupotreba, širenja nedozvoljenih sadržaja, lažnog predstavljanja, krađe identiteta, proganjanja, osramoćivanja, diskriminaciju, ucene i drugo (Whitte, Mannon, 2010; Gross, Acquisti, 2005).

KONCEPTUALIZACIJA PRIVATNOSTI

Jedna od ključnih karakteristika sajtova za socijalno umrežavanje je deljenje ličnih sadržaja i informacija sa drugim korisnicima (Van den Berg, Leenes, 2011). Korisnici se trude da posredstvom teksta, slika, video zapisa prenesu što više informacija o sebi i tako ostavljaju veliku količinu ličnih podataka koja može naknadno biti zloupotrebljena.

Privatnosti podrazumeva mogućnost lične kontrole nad sopstvenim krugom intimnosti u četiri dimenzije: fizička, psihološka, socijalna (interaktivna) i informaciona dimenzija (Leino-Kilpia i drugi, 2001, prema Debatin, 2011). Kako su pitanja zloupotrebe privatnosti u tehnološkom kontekstu, domenu socijalnih mreža pretežno vezana za informacionu komponentu privatnosti, razlikujemo pretnje poput prikupljanja podataka o ličnosti, praćenja podataka, analize i sekundarne upotrebe podataka radi ucene, korišćenje podataka u komercijalne, političke i druge svrhe.

Istraživanja (Acquisti, Gross, 2006) pokazuju da zabrinutost osoba u vezi sa pitanjima zloupotrebe privatnosti na sajtovima za socijalno umrežavanje ne utiče na odluku o pristupanju određenoj mreži, niti je ona praćena restriktivnijom politikom pri ostavljanju ličnih podataka na profilu. Podaci pokazuju da se obrasci socijalnog umrežavanja i politika privatnosti s tim u vezi razlikuju u odnosu na pol. Korisnice su spremnije da ostavljaju fotografije, a korisnici brojeve telefona, kućne adrese, puno ime i prezime, kao i lažne podatke na profilima (Lenhart, Madden, 2007). Rezultati istraživanja preko 4000 profila studenata Carnegie Mellon Univerziteta u Pittsburgu pokazuju da 90,8% studenata na profilima na fejsbuku ostavlja fotografije, 87,8 % datum rođenja, 39,9% broj telefona, od kojih 28% fiksnog telefona, 50,8% adresu stanovanja. U 89% korisnici daju istinite informacije o svom imenu i prezimenu, dok su u 61% fotografije koje korisnici imaju na profilima na fejsbuku dovoljno prepoznatljive da mogu poslužiti za identifikaciju korisnika. Samo 1,2 % studenata izvršilo je podešavanja u vezi sa ograničenjem vidljivosti profila za pretraživače. Na osnovu prikupljenih informacija o regulisanju privatnosti, autori su izvršili analizu očekivanih rizika i tako prepoznali 35,9% vlasnika profila koji su u riziku da budu progonjeni u fizičkom svetu, 77,7% u i/ili virtuelnom (sajber proganjanje) (Gross, Acquisti, 2005).

Prema Evropskoj agenciji za bezbednost mreže i informacija izdvajaju se specifični načini ugrožavanja privatnosti putem socijalnih mreža (ENISA, 2007): pravljenje digitalnih dosijea (prikupljanje podataka sa profila na socijalnim mrežama od strane treće osobe i korišćenje u svrhu ucene ili slično); sekundarno prikupljanje podataka (prikupljanje podataka o

korisnicima u marketinške, komercijalne svrhe na primer radi formiranja cene pri kupovini preko internetu ili ustupanja podataka nekoj trećoj strani); program za prepoznavanje lica na fotografijama korisnika (povezivanje fizičkih karakteristika korisnika sa podacima); program za prepoznavanje objekata na fotografijama (povezivanje sadržaja fotografija korisnika sa podacima uz opasnost od zloupotrebe u svrhu ucene, proganjanja, neželjenog marketinga); mogućnost povezivanja slike sa metapodacima (tagovanje fotografija koje upućuju na profile ili i-mejlove drugih korisnika); i teškoće u brisanju profila (gubljenje kontrole korisnika nad sopstvenim podacima pa čak i u slučaju deaktiviranja profila, podaci ostaju u bazi podataka sajta).

ZAKONODAVNI OKVIR

Evropski okviri očuvanja privatnosti na sajtovima za socijalno umrežavanje počivaju na dokumentima: *Evropska konvencija za ljudska prava i Evropska konvencija o zaštiti pojedinaca u vezi sa automatskim procesuiranjem ličnih podataka Saveta Evrope*, kao i *Direktiva o zaštiti podataka* (95/46/EC) *Evropske unije*, *Direktiva o obradi podataka o ličnosti i zaštiti privatnosti u telekomunikacionom sektoru* (97/66/EC) i *Direktiva o obradi podataka o ličnosti i zaštiti privatnosti u sektoru elektronskih komunikacija* (2002/58/EC).

U sklopu nacionalne legislative posrednu regulaciju privatnosti pružaju: Zakon o zaštiti podataka o ličnosti RS, Zakon o telekomunikacijama RS i Zakon o elektronskim komunikacijama RS. *Zakonom o zaštiti podataka o ličnosti Republike Srbije* uređuju se uslovi za prikupljanje i obradu podataka o ličnosti, prava lica i zaštita prava lica čiji se podaci prikupljaju i obrađuju, ograničenja zaštite podataka o ličnosti, postupak pred nadležnim organom za zaštitu podataka o ličnosti, obezbeđenje podataka, evidencija, iznošenje podataka iz Republike Srbije i nadzor nad izvršavanjem ovog Zakona. *Zakonom o elektronskim komunikacijama Republike Srbije* uređuju se bezbednost i integritet elektronskih komunikacionih mreža i usluga, tajnost elektronskih komunikacija, zakonito presretanje i zadržavanje podataka, nadzor nad primenom ovog zakona, mere za postupanje suprotno odredbama ovog zakona. Na inicijativu Poverenika i Ombudsmana odredbe Zakona o elektronskim komunikacijama Republike Srbije kojima je propisano da mimo odluke suda nadležne službe mogu pristupati zadržanim podacima, proglašene su od strane Ustavnog suda RS neustavnim. Na sednici održanoj 13. juna 2013. godine, utvrđeno je da odredbe člana 128. stav 1. i stav 5. i člana 129. stav 4. Zakona o elektronskim komunikacijama nisu u saglasnosti sa Ustavom (Odluka broj IVz - 1245/2010). Nadležni državni

organ koji ostvaruje pristup, odnosno kome se dostavljaju zadržani podaci, dužan je da vodi evidenciju o pristupu, odnosno dostavljanju zadržanih podataka, koja naročito sadrži: određenje akta koji predstavlja pravni osnov za pristup, odnosno dostavljanje zadržanih podataka, datum i vreme pristupanja, odnosno dostavljanja zadržanih podataka, kao i da ovu evidenciju čuva kao tajnu, u skladu sa zakonom kojim se uređuje tajnost podataka (član 28). *Zakonom o telekomunikacijama Republike Srbije* predviđene su obaveze telekomunikacionog operatora u smislu preduzimanja odgovarajućih tehničkih i organizacionih mera kako bi obezbedio poverljivost i bezbednost svojih usluga. Odredba iz člana 55, stav 1 Zakona o telekomunikacijama Republike Srbije je prema odluci Ustavnog suda od 28. maja 2009. godine (Odluka broj IVz -149/2008) proglašena neustavnom. Prema tome, stav 1. člana 55. upućuje da su zabranjene sve aktivnosti ili korišćenje uređaja kojima se ugrožava ili narušava privatnost i poverljivost poruka koje se prenose telekomunikacionim mrežama, osim kada postoji saglasnost korisnika ili ako se ove aktivnosti vrše u skladu sa zakonom ili sudskim nalogom izdatim u skladu sa zakonom.

Zakon o krivičnom postupku Republike Srbije (član 161) predviđa da se posebne dokazne radnje, između ostalih i nadzor nad eletronskom komunikacijom, mogu odrediti prema licu za koje postoje osnovi sumnje da je učinilo krivično delo iz člana 162, a da se na drugi način ne mogu prikupiti dokazi za gonjenje ili bi njihovo prikupljanje bilo znatno otežano (stav 1), izuzetno i prema licu za koje postoje osnovi sumnje da priprema neko krivično delo (stav 2), a da okolnosti ukazuju da se ono na drugi način ne bi moglo otkriti, sprečiti ili dokazati ili bi to izazvalo nesrazmerne teškoće ili opasnost i uz ocenu da se isti rezultat ne bi mogao postići na način na koji se manje ograničavaju prava građana. Krivična dela u vezi sa kojima se nadzor i snimanje komunikacije mogu izreći su: ona za koje je posebnim zakonom određeno da su u nadležnosti javnog tužilaštva posebne nadležnosti; od teškog ubistva, otmice, pranja, falsifikovanja novca, neovlašćene proizvodnje i stavljanja u promet opojnih droga, preko krivičnog dela ugrožavanja nezavisnosti, teritorijalne celine, napada na ustavno uređenje, diverzije, sabotaže, špijunaže, izazivanje nacionalne, rasne i verske mržnje i netrpeljivosti, povrede teritorijalnog suvereniteta, nedozvoljenog prelaza državne granice i krijumčarenja ljudi, trgovine ljudima do zloupotrebe službenog položaja, primanja i davanja mita; i sprečavanja i ometanja dokazivanja (član 162). Prema članu 178 na obrazloženi predlog javnog tužioca sud može odrediti računarsko pretraživanje već obrađenih ličnih i drugih podataka i njihovo poređenje sa podacima koji se odnose na osumnjičenog i krivično delo. Naredbu iz člana 179. stav 1. ovog zakonika izvršava policija, Bezbednosno-informativna agencija, Vojno-bezbednosna

agencija, carinske, poreske i druge službe ili drugi državni organ. Po završetku računarskog pretraživanja podataka državni organ dostavlja sudiji za prethodni postupak izveštaj koji sadrži: podatke o vremenu početka i završetka računarskog pretraživanja podataka, podatke koji su pretraženi i obrađeni, podatke o službenom licu koje je sprovelo posebnu dokaznu radnju, opis primenjenih tehničkih sredstava, podatke o obuhvaćenim licima i rezultatima primenjenog računarskog pretraživanja podataka (član 180). Drugi način za tajno prikupljanje podataka definisan je zakonima kojima je regulisan rad službi bezbednosti (Bezbednosno-informativna agencija, Vojnoobaveštajna agencija i Vojnobezbednosna agencija). U ovom pravnom režimu službe bezbednosti mogu tajno prikupljati podatke radi prevencije, ali ne i radi krivičnog gonjenja počinilaca zločina. Prema članu 14 *Zakona o Bezbednosno-informativnoj agenciji Republike Srbije* odstupanje od načela nepovredivosti tajnosti pisama i drugih sredstava opštenja, na predlog direktora Agencije odobrava odlukom predsednik Vrhovnog kasacionog suda, odnosno sudija tog suda koji je određen da po ovim predlozima odlučuje u slučaju odsustva predsednika tog suda, u roku od 72 sata od podnošenja predloga. Prema članu 13. *Zakona o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji* operativni prodor u organizacije, grupe i institucije; tajno pribavljanje i otkup dokumenata I predmeta; tajni uvid u evidencije podataka i tajno praćenje i nadzor lica na otvorenom prostoru i javnim mestima uz korišćenje tehničkih sredstava preduzimaju se na osnovu pisanog i obrazloženog naloga direktora VBA ili lica koje ovlasti, dok se tajni elektronski nadzor telekomunikacija i informacionih sistema radi prikupljanja zadržanih podataka o telekomunikacionom saobraćaju bez uvida u njihov sadržaj preduzima na osnovu odluke nadležnog višeg suda (član 13a).

PREPORUKE ZA UNAPREĐIVANJE PRIVATNOSTI

Evropska komisija je 2009. godine formulisala principe (European Commission, 2009) za unapređivanje sigurnosne politike sajtova za socijalno umrežavanje i tim putem podržala inicijativu za podizanje nivoa bezbednosti koja je podneta od strane 21 sajta za socijalno umrežavanje, i to su: Podizanje svesti o upućivanju i pristupačnosti sigurnosnih poruka i polisa korisnicima, roditeljima, nastavnicima i drugim zainteresovanim stranama, koje treba da su uočljive, jasne i uzrastno prilagođene; servisi koje nude sajtovi za socijalno umrežavanje treba da budu uzrastno prilagođeni populaciji kojoj su namenjeni; tehnološka opremljenost sajtova za socijalno umrežavanje i upućivanje korisnika u oruđa koja su im dostupna; predviđanje mehanizama putem kojih se jednostavno mogu prijaviti

ponašanja ili sadržaji koji su u suprotnosti sa uslovima korišćenja servisa; pravovremeni odgovor na žalbe korisnika o neprikladnim sadržajima ili ponašanjima; omogućiti korisnicima i ohrabriti ih da vode računa o sopstvenoj privatnosti i imaju punu kontrolu nad informacijama koje postavljaju; I identifikovanje potencijalnih pretnji putem pregleda nedozvoljenih sadržaja i ponašanja.

Analizom 14 sajtova za socijalno umrežavanje (Arto, Bebo, Facebook, Giovani, Hyves, IRC-Galleria, Myspace, Nasza-Klasa, Netlog, One, Rate, SchuelerVZ (Vznet Netzwerke), Tuenti i Zap) o sprovođenju prethodno opisanih principa od strane Evropske komisije, utvrđeno je da iako 11 sajtova predviđa minimalnu starosnu granicu za pristupanje sajtu za socijalno umrežavanje, samo dva omogućavaju da po difoltu lične informacije maloletnika mogu biti vidljive samo njihovim prijateljima, pa ih mogu kontaktirati samo oni koje su prethodno označili kao prijatelje (ograničenje važi i za prijatelje prijatelja) (Bebo, MySpace); takođe na dve socijalne mreže potrebno je da osoba prethodno dobije poziv od nekog ko je aktuelni korisnik; profili maloletnika sa 12 sajtova ne mogu se pronaći putem eksternih pretraživača kao što su Google, Bing, Yahoo; svi sajtovi imaju bar jedan mehanizam putem koga se mogu prijaviti neprikladni sadržaji ili ponašanja; 13 sajtova ima vrlo pristupačna podešavanja privatnosti na profilima; 11 sajtova ima dodatnu tehničku podršku i drugo (Donoso, 2011).

Nužno je da korisnici budu dobro informisani o svojim pravima na privatnost i efektivnim strategijama za njihovo obezbeđivanje. Međunarodna radna grupa za zaštitu podataka u oblasti telekomunikacija (2008) objavila je izveštaj i vodič o zaštiti privatnosti na sajtovima za socijalno umrežavanje poznat kao Rimski memorandum. Korisnici socijalnih mreža bi trebalo da imaju u vidu da: jednom puštena informacija na mreži ostaje u začaranom krugu; da se virtuelna zajednica u mnogome razlikuje od zajednice u fizičkoj stvarnosti i da ne treba upadati u zamku intimnosti; da ništa nije besplatno, odnosno njihovi podaci mogu biti sekundarno iskorišćeni za druge svrhe; da podaci mogu biti izmanipulisani od strane provajdera i na primer ustupljeni nekom trećem licu; da mogu biti suočeni sa promenom pravila koja se tiču privatnosti usled porasta broja korisnika i potrebe kompanija koje su vlasnici socijalnih mreža u usponu da ostvare profit; da svojim postupcima odaju mnogo više informacija nego što su predvideli (na primer program za prepoznavanje sadržaja fotografija i na taj način utvrđivanje lokacije korisnika); zloupotrebe podataka sa profila od strane treće osobe; krađu identiteta; upotrebu vrlo nesigurne infrastrukture; postojanje nerešenih sigurnosnih problema internet provajdera koji se samo dodaju na postojeće

probleme prisutne kod socijalnog umrežavanja i trend tehničkog spajanja različitih sajtova za socijalno umrežavanje koji nosi nove rizike. Radna grupa dalje pruža izvesne smernice za unapređivanje bezbednosti regulatornim telima, sajtovima za socijalno umrežavanje i neposrednim korisnicima.

UMESTO ZAKLJUČKA

Rezultati istraživanja ukazuju da su sajtovi za socijalno umrežavanje nedovoljno usmereni prema očuvanju privatnosti korisnika, nadležne institucije za očuvanje privatnosti i ljudskih prava nespremne I nezainteresovane, a korisnici slabo obavešteni o svojim pravima na privatnost i načinima za njeno obezbeđivanje. Integrisanje i personalizacija različitih internet servisa, olakšavanje komunikacije i veća dostupnost sadržaja i usluga, povećava opasnost od kompromitovanja veće količine privatnih podataka u budućnosti. Neophodno je obezbediti koordinisanu aktivnost stručnjaka, korisnika i regulatornih tela u cilju kontrole pristupa i upravljanja osetljivim, privatnim podacima radi adekvatnog obezbeđivanja zaštite privatnosti.

REFERENCE

(1) Acquisti, A., Gross, R. (2006) Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In G. Danezis, P. Golle (Eds.), *Proceedings of 6th Workshop on privacy Enhancing Technologies* (pp. 36–58). Cambridge, UK: Robinson College.
(2) Boyd, D., Ellison, N. (2007) Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 13 (1), 210-230.
(3) Castells, M. (2009) *Comunication power*. NewYork: Oxford University Press
(4) Council of Europe (1981) *Convention for the protection of individuals with regard to automatic processing of personal data.* Strasbourg: Council of Europe.
(5) Debatin, B. (2011) Ethics, Privacy, and Self-Restraint in Social Networking. In S. Trepte, L. Reinecke (Eds.), *Privacy on-line: Perspectives on Privacy and Self-Disclosure in the Social Web*. Hamburg: Springer.
(6) Donoso, V. (2011) *Assessment of the implementation of the Safer Social Networking Principles for the EU on 14 websites: Summary Report.* Luxembourg: European Commission, Safer Internet Programme

(7) ECHR (2010) *European convention for the protection of human rights and fundamental freedoms.* Strasbourg: Council of Europe.
(8) ENISA (2007) *Security Issues and Recommendations for Online Social Networks*. Crete: European Network and Information Security Agency. Retrived November 19. 2013. from http://www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks
(9) EU (1995) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal, L* 281, 23/11/1995, 0031-0050.
(10) European Commission (2009) *Safer Social Networking Principles for the EU*. Brussels: EU.
(11) Retrived December 2. 2013. from http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf, on
(12) Facebook (2013) *Global Government Request Report.* Retrieved September 10., 2013.
(13) from https://www.facebook.com/about/government_requests
(14) Directive 97/66/EC, *Official Journal L 024*, 30/01/1998 P. 0001 – 0008. Retrived November 20 from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML
(15) Granovetter, M. (1983) *The strength of the weak ties: a network theory revisited*. NewYork: Stony Brook University.
(16) Google Transparency Report (2013) *Google Transparency Report – User Data Requsts.* Retrieved December 4., 2013. from http://www.google.com/transparencyreport/userdatarequests/?p=2012-06
(17) Gross, R., Acquisti, A. (2005) *Information Revelation and Privacy in Online Social Networks.*Workshop on Privacy in the Electronic Society (WPES), November 5, Alexandria.
(18) International Working Group on Data Protection in Telecommunications (2008) *Report and Guidance on Privacy in* Social Network *Services – Roma memorandum*. 43rd meeting, 3-4 March, Rome (Italy). Retrived November 22. 2013. from www.datenschutzberlin.de/attachments/.../WP_social_network_services.pdf.
(19) Lenhart, A., Madden, M. (2007) *Teens, privacy and on-line social networks.*Washington: Pew research center (Pew internet and American life project). Retrived December 2 2013. from

http://www.pewinternet.org/~/media//Files/Reports/2007/PIP_Teens_Privacy_SNS_Report_Final.pdf.pdf.

(20) Odluka broj IVz - 1245/2010 (2013) Odluka Ustavnog suda Republike Srbije o ustavnosti odredbi Zakona o elektronskim komunikacijama. Pristupljeno 10. septembra sa http://www.poverenik.rs/images/stories/praksazastita/Odluke-Ustavnog-suda/IUz12452010.pdf

(21) Pempek, A., Yermolayeva, Y., Calvert, S. (2009) College students' social networking experiences on Facebook. *Journal of Applied Developmental Psychology,* 30 (3), 227–238.

(22) Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti Republike Srbije (2013) *Izveštaj o sprovođenju Zakona o slobodnom pristupu informacijama od javnog značaja i Zakona o zaštiti podataka o ličnosti za 2012. godinu.* Beograd: Poverenik.

(23) Zakon o bezbednosno-informativnoj agenciji Republike Srbije. *Službeni glasnik RS,* br. 42/2002 I 111/2009.

(24) Zakon o zaštiti podataka o ličnosti Republike Srbije. *Službeni glasnik*, 97/08.

(25) Zakon o elektronskim komunikacijama Republike Srbije. *Službeni glasnik* , 44/10.

(26) Zakon o telekomunikacijama Republike Srbije. *Službeni glasnik* , 44/03.

(27) Zakon o krivičnom postupku Republike Srbije. *Službeni glasnik RS,* br. 72/2011, 101/2011 i 121/2012.

(28) Zakonom o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji Republike Srbije, *Službeni glasnik RS,* br. 88/2009, 55/2012-odluka US I 17/2013.

(29) Van den Berg, B., Leenes, R. (2011) Keeping Up Appearances: Audience Segregation in Social

(30) Network Sites. In S. Gutwirth, Y. Poullet, P. De Hert (Eds.), *Computer Privacy and Data Protection: an Element of Choice* (pp. 211-233). Dordecht: Springer.

(31) Wellman, B. (2001) Physical Place and Cyberplace: the Rise of Personalized Networking. *International Journal of Urban and Regional Research*, 25 (2), 227-253.

(32) Whitte, J., Mannon, S. (2010) *The Internet and Social Inequalities.* NewYork and London: Routledge.

Zbornik IKSI, 1/2013 – V. Žunić-Pavlović, M. Kovačević-Lepojević, B. Lepojević
„Socijalno umrežavanje privatnosti”, (str. 49-60)

SOCIAL NETWORKING OF PRIVACY

Since the late nineties when there was a revival of the multiplier concept of social networking on the Internet, public attention to preoccupy the study of the negative aspects of the functioning of social networking sites, especially complaints relating to abuse of privacy. The results of the researches on the routine activities of the social networking sites users show that more than half of users live their personal information. At the other side, safety platforms of social networking sites are week. A particular problem is the unauthorized collection of data on citizens' communications by the security agencies of the developed countries of the world as part of the activities related to the prevention of terrorism and crime.
The aim of this article is to access the negative consequences of social networking in the context of privacy issues. Besides the review of the international and domestic laws on social networking sites, some safety instructions for users and social networking sites will be given.

KEYWORDS: social networking / privacy / internet / protection