*XXVII Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – **PosTel 2009**, Beograd, 15. i 16. decembar 2009.*

DRUŠTVENO UMREŽAVANJE I ZAŠTITA PRIVATNOSTI KORISNIKA INTERNETA

Nataša Tomić, Dalibor Petrović
Saobraćajni fakultet Univerziteta u Beogradu

Sadržaj: *U radu se analizira problem zaštite privatnosti na Internetu, sa posebnim osvrtom na popularne sajtove za društveno umrežavanje (SDU). Nakon pregleda domaćeg i evropskog zakonodavstva u domenu zaštite privatnosti podataka i ličnosti, u centralnom delu rada ukazuje se na različite vidove zloupotrebe ličnih podataka koje korisnici, pretežno dobrovoljno, kreirajući lične profile ostavljaju na SDU. Nakon evidentiranih opasnosti ukazuje se na moguća rešenja i preporuke u oblasti zaštite privatnosti na Internetu.*

Ključne reči: *Privatnost, bezbednost, rizici, društveno umrežavanje, Internet.*

1. Uvod

Ako nisi siguran da ćeš učiniti stvarno dobro- gledaj bar da ne naneseš zlo. ***A. Haksli***

Jedna od najdiskutovanijih tema danas, kada je reč o društvenim posledicama upotrebe novih informaciono-komunikacionih tehnologija (IKT) a pre svega Interneta, jeste svakako problem zaštite privatnosti korisnika ovih tehnologija. Neslućena masovnost i brzina protoka informacija, koju su ove tehnologije omogućile, donele su sa sobom opasnost od različitih vidova zloupotrebe podataka koje se prenose putem IKT. Da ovde nije u pitanju samo jedan u nizu neosnovanih strahova, najbolje svedoči niz preporuka i vodiča za zaštitu privatnosti na Internetu koje su donela različita regulatorna tela širom sveta. O tome svedoče i brojni protesti javnosti, različite peticije pa čak i zvanične tužbe za ugrožavanje privatnosti korisnika najpopularnijih sajtova za društveno umrežavanje o čemu će detaljnije biti reči u nastavku ovog rada.

Na početku važno je naglasiti da je pravo privatnosti jedno od osnovnih ljudskih prava. "Pravo da se bude ostavljen na miru" podrazumeva čuvanje tajnosti nečijih podataka, osim, ukoliko postoji jasna potreba da se ovi podaci otkriju. Ovo pitanje zahteva oprezan pristup u mnogim oblastima (posebno u oblasti zdravlja i finansija, ali i prilikom korišćenja Interneta). Riley T. je ponudio predloge za zaštitu prava čoveka da bude ostavljen na miru [1]. Ovi predlozi su:

- interna upotreba informacione tehnologije, razvoj personalne politike, koja će štititi prava zaposlenih na privatnost, nasuprot pravu javnosti da sazna;
- donošenje zakona i vođenje politike koja će razjasniti pravo pristupa svake pojedine organizacije određenim informacijama o pojedincima;
- obezbeđenje mehanizama za uklanjanje ili izmenu netačne ili zastarele informacije i
- prihvatanje nove tehnologije, izgradnja sistema zaštite privatnosti odmah, a ne pošto se problem pojavi.

2. O pravnoj regulativi prava privatnosti

U Republici Srbiji se više zakonskih akata bavi zaštitom privatnosti pojedinaca i grupa, pa se može konstatovati da, makar formalno, postoji razgranat regulatorni okvir za borbu protiv ovakvih vidova zloupotreba.

Ustavom Republike Srbije[1] zajemčena je zaštita podataka o ličnosti, a prikupljanje, držanje, obrada i korišćenje podataka o ličnosti uređuju se zakonom. Zabranjena je i kažnjiva upotreba podataka o ličnosti izvan svrhe za koju su prikupljeni, u skladu sa zakonom, osim za potrebe vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije, na način predviđen zakonom. Svako ima pravo da bude obavešten o prikupljenim podacima o svojoj ličnosti, u skladu sa zakonom, i pravo na sudsku zaštitu zbog njihove zloupotrebe.

Zakonom o zaštiti podataka o ličnosti[2] 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. Zaštita podataka o ličnosti obezbeđuje se svakom fizičkom licu, bez obzira na državljanstvo i prebivalište, rasu, godine života, pol, jezik, veroispovest, političko i drugo uverenje, nacionalnu pripadnost, socijalno poreklo i status, imovinsko stanje, rođenje, obrazovanje, društveni položaj ili druga lična svojstva. Cilj ovog zakona je da, u vezi sa obradom podataka o ličnosti, svakom fizičkom licu obezbedi ostvarivanje i zaštitu prava na privatnost i ostalih prava i sloboda.

Pravom privatnosti i drugim pravima ličnosti bavi se i **Zakon o slobodnom pristupu informacijama od javnog značaja**[3] koji predviđa da organ vlasti neće tražiocu omogućiti ostvarivanje prava na pristup informacijama od javnog značaja ako bi time povredio pravo na privatnost, pravo na ugled ili koje drugo pravo lica na koje se tražena informacija lično odnosi, osim:
1) ako je lice na to pristalo; 2) ako se radi o ličnosti, pojavi ili događaju od interesa za javnost, a naročito ako se radi o nosiocu državne i političke funkcije i ako je informacija važna s obzirom na funkciju koju to lice vrši; 3) ako se radi o licu koje je svojim ponašanjem, naročito u vezi sa privatnim životom, dalo povoda za traženje informacije.

Zakon o telekomunikacijama Republike Srbije[4] predviđa da je javni telekomunikacioni operator dužan da preduzme odgovarajuće tehničke i organizacione mere kako bi obezbedio poverljivost i bezbednost svojih usluga i zabranjeno mu je da

[1] „Službeni glasnik Republike Srbije", broj 98/2006.
[2] "Službeni glasnik RS", br. 97/2008.
[3] „Službeni glasnik RS", broj 120/2004, 54/2007.
[4] „Službeni glasnik RS", broj 44/2003, 36/2006, 50/2009.

daje informacije o sadržaju, činjenicama i uslovima prenosa poruka, osim minimuma koji je neophodan za nuđenje usluga na tržištu ili u slučajevima predviđenim zakonom. Podatke o saobraćaju koji se odnose na pojedinačne korisnike i koji se obrađuju radi uspostavljanja veza, javni telekomunikacioni operator može čuvati i obrađivati samo u obimu koji je neophodan za ispostavljanje računa korisniku.[5] Zabranjene su 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 sudskim nalogom izdatim u skladu sa zakonom.

Strategija razvoja telekomunikacija u Republici Srbiji od 2006. do 2010. godine[6] predviđa da delovanje nacionalnih regulatornih tela obuhvata i zaštitu privatnosti, zaštitu korisničkog saobraćaja, podatke o lokaciji, kao i sprečavanje neželjene komunikacije. Korisnicima javnih telekomunikacionih usluga ili javnih telekomunikacionih mreža pored prava na nesmetano korišćenje i kvalitetnu javnu telekomunikacionu uslugu potrebno je obezbediti i pravo na privatnost i bezbednost informacija.

Vlada je donela **Strategiju razvoja informacionog društva u Republici Srbiji**[7] u kojoj se ukazuje da se elektronske mreže moraju osigurati od hakera i virusa i moraju biti dovoljno bezbedne da bi se izgradilo poverenje klijenata u elektronsko plaćanje, dok se pitanje bezbednosti mora uravnotežiti sa mogućom povredom privatnosti građana.

Kada je evropsko zakonodavstvo u pitanju, postoji nekoliko Direktiva koje se eksplicitno bave problematikom zaštite privatnosti lica i podataka, ali će ovom prilikom biti samo spomenute. Najopštija, direktiva koja reguliše ovu oblast i koja predstavlja osnovu za kasnije donete direktive jeste „Direktiva Evropskog Parlamenta i Saveta o zaštiti pojedinaca u vezi sa obradom podataka o ličnosti i slobodnom kretanju takvih podataka“, usvojena 1995. godine (**Directive 95/46/EC**)[8]. Usled intenzivnog razvoja telekomunikacija javila se potreba da se dalje produbе i preciziraju uslovi raspolaganja, čuvanja i distribucije ličnih podataka tako da je tokom 1997. godine usvojena Direktiva Evropskog Parlamenta i Saveta o obradi podataka o ličnosti i zaštita privatnosti u telekomunikacionom sektoru“ (**Directive 97/66/EC**)[9]. Ipak, ključna Direktiva koja je u potpunosti posvećena zaštiti privatnosti u domenu elektronskih komunikacija je takozvana *Direktiva o e-privatnosti* ili pod punim nazivom „Direktiva Evropskog Parlamenta i Saveta o obradi podataka o ličnosti i zaštiti privatnosti u sektoru elektronskih komunikacija, koja je usvojena 2002. godine (**Directive 2002/58/EC**)[10]. Ova direktiva direktno predstavlja dopunu direktive iz 1995. godine i nastala je sa ciljem da je dopuni u delu koji nije bio pokriven prvobitnim rešenjima a pre svega u oblasti prava na privatnost u sektoru elektronskih komunikacija i slobodnog prenosa podataka.

---

[5] Ipak javni telekomunikacioni operator je dužan da nadležnim državnim organima omogući pristup i analizu navedenih podataka, u skladu sa zakonom. (Član 54. Zakona o telekomunikacijama, „Službeni glasnik RS”, broj 44/2003, 36/2006, 50/2009.).

[6] „Službeni glasnik RS”, broj 99/2006.

[7] „Službeni glasnik RS”, broj 87/2006.

[8] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

[9] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML

[10] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

4. Društveno umrežavanje na Internetu

Samo do pre nekoliko godina pojam „društvena mreža“ bio je poznat jedino uskom krugu naučnika koji su se bavili evolucijom društvenih grupa. Međutim, nakon pojave specijalizovanih sajtova za društveno umrežavanje (SDU) kao što su Facebook, My Space, Hi5, itd., pojam društvena mreža ulazi u široku upotrebu i postaje neraskidivo vezan za Internet. Sociološki gledano, osnovno određenje društvenih mreža je da su one formirane od strane tačaka, odnosno pojedinaca i veza koje se među njima ostvaruju. Umesto nekadašnjih, tradicionalnih, zajednica u savremeno doba postaje sve opravdanije govoriti o društvenim mrežama. Služeći se definicijom Beri Velmana (Barry Wellman) možemo dodatno produbiti ovo shvatanje [2]. On zaključuje da su: «Zajednice - mreže interpesonalnih veza koje obezbeđuju društvenost, podršku, informacije, osećaj pripadnosti i društveni identitet». Znači, za razliku od nekadašnjih zajednica koje su bile zasnovane na deljenju vrednosti i društvene organizacije, mreže se grade u vezi sa izborom i strategijama socijalnih aktera, bilo da su u pitanju pojedinci, porodice ili organizacije. Ono što je takođe važno naglasiti, a tiče se kvaliteta veza koje se ostvaruju među socijlnim akterima, je to da „slabe“ veze često sa stanovišta aktera mogu imati veći značaj nego što ih imaju „jake“ veze. Upravo su one izvor informacija, radnih karakteristika, komunikacije, slobodnog vremena. [3]

Imajući ovakvo određenje društvenih mreža u vidu ne čudi zašto se Internet, kao mreža svih mreža, savršeno nadovezao na već uspostavljenu mrežnu logiku društvenih odnosa. Internet je pogodan kako za održavanje „jakih“ porodičnih, rođačkih ili drugih bliskih odnosa, tako i za sticanje i održavanje „slabih“ veza koje bi se njegovim nepostojanjem u manjem ili većem broju prekinule. Upravo u toj njegovoj karakteristici treba tražiti uslove za nastanak i ogromnu popularnost SDU.

5. Politika privatnosti na sajtovima za društveno umrežavanje

Problem zaštite privatnosti na SDU je predmet mnogobrojnih istraživanja, diskusija i preporuka kako šire javnosti tako i naučnika, vladinih i nevladinih organizacija. Razlog za ovako veliko interesovanje za ovu problematiku počiva na činjenici neslućene brzine povećanja broja ljudi koji, manje ili više, dobrovoljno dele informacije različitih nivoa poverljivosti kroz SDU[11]. Ono što zabrinjava je da informacije koje se čuvaju na SDU mogu zauvek ostati tamo i kao takve biti dostupne različitim pojedincima i zainteresovanim grupama i organizacijama. Pored toga, informacija, jednom puštena kroz mrežu, trenutno se kroz nju prenosi i postaje globalno dostupna svima.

Dodatni problem, na koji ukazuje većina analitičara koji se bave problemom zaštite privatnosti podataka na Internetu, predstavlja to što korisnici samoinicijativno i dobrovoljno pružaju informacije o sebi (ime i prezime, adrese, brojeve telefona, fotografije, itd) a da pri tom malo razmišljaju o posledicama takvog činjenja. Primera radi, Gros i Akuisti (Gross & Acquisti) u svom istraživanju pokazuju da čak 82% aktivnih korisnika Fejsbuka (Facebook) otkrivaju poverljive informacije o sebi kao što su, datum rođenja, broj mobilnog telefona, adresu, političku i seksualnu orijentaciju i ime

[11] Po najnovijem izveštaju Facebook ima preko 300 miliona aktivnih korisnika, http://www.facebook.com/press/info.php?statistics

partnera [4]. Do sličnih rezultata dolaze Jang i Kuan-Has (Young & Quan-Hasse) istražujući ponašanje studenata u Kanadi [5]. Rezultati pokazuju da neverovatnih 99,35% studenata koristi pravo ime u svojim profilima; 97,4% navodi ime škole koju su pohađali; 92,2% datum rođenja; 83,1% e-mail adresu; 80% ime grada u kome žive. Pored ovoga, gotovo svi studenti na profile postavljaju svoje slike (98,7%) i slike svojih prijatelja (96,1%). Ipak, studenti su nešto oprezniji kada je u pitanju davanje prave adrese (to čini samo 7,9%), ili broja mobilnog telefona (10,5%).

Ovako velika iskrenost korisnika SDU se podstiče i od strane pružalaca ovih usluga koji ohrabruju objavljivanje ličnih podataka stvarajući iluziju njihove potpune bezbednosti. Da situacija nije baš toliko bezazlena, kao što to verovatno misli većina korisnika SDU, svedoče brojne analize, vodiči i preporuke sa ciljem da se što bolje uredi ova oblast društvenog delovanja. Ali više od svega, o mogućnosti zloupotrebe podataka, svedoče i konkretne sumnje, peticije javnosti, pa čak i tužbe protiv najpopularnijeg SDU, Fejsbuka.

Prva velika rasprava na temu manipulacije ličnim podacima korisnika Fejsbuka, desila se nakon uvođenja kontraverznog sistema za reklamiranje pod nazivom „Beacon". Uvedena u novembru 2007, ova usluga bila je podešena tako da snima aktivnost svih Fejsbukovih korisnika na Internetu (kupovanje, prijavljivanje za različite usluge itd) i zatim te informacije prosleđuje listi prijatelja iz profila te osobe. Ideja je bila da se, preporučujući prijateljima usluge i proizvode koje koriste njihovi prijatelji, kompanije reklamiraju na jedan ličniji, personalizovan način. Nakon tužbe i pod pritiskom žalbi korisnika, samo dva meseca kasnije, Beacon usluga uz izvinjenje osnivača Marka Cukerberga (Mark Zuckerberg)[12] postaje opciona, da bi u septembru 2009. godine bilo objavljeno da će se u potpunosti ukinuti.[13]

Tokom 2009. godine Fejsbuk je još dva puta bio predmet široke diskusije i pritužbi javnosti. Novu kontroverzu (februar 2009. godine) izazvala je najava, od strane Fejsbuka, da će doći do izmene njihove politike vezane za privatnost podataka. Ono čime je ova najava posebno uzbudila javnost bio je jedan pasus čija se suština svodi na to da Fejsbuk zadržava pravo na posedovanje ličnih podatka korisnika čak i u slučaju da korisnik deaktivira svoj profil i obriše podatke sa njega. Međutim, nakon brojnih protesta i široke kampanje širom sveta i pretnje tužbom, kreatori Fejsbuka su još jednom bili primorani da odustanu od nameravanih promena.[14]

Mnogo ozbiljnije posledice po pitanje Fejsbukove politike privatnosti izazvala je tužba jedne kanadske nevladine organizacije koja se bavi politikom Interneta i javnim interesom (Canadian Internet Policy and Public Interest Clinic - CIPPIC) upućena „Kancelariji poverenika za privatnost informacija Kanade" (Office of the Privacy Commissioner-OPC). Ova organizacija iznela je pritužbe na politiku privatnosti podataka korisnika Fejsbuka na više nivoa [6]. Od pritužbe na neovlašćeno prikupljanje podataka o rođenju korisnika, do pritužbe na neovlašćeno davanje ličnih podataka korisnika trećim licima u svrhu reklamiranja. Kao odgovor na tužbu OPC je napravila više izveštaja i tokom marta 2009. godine dala je Fejsbuku 20 preporuka vezanih za uklanjanje uočenih nepravilnosti vezanih za politiku privatnosti njihovih korisnika [7]. Kao rezultat ovoga Fejsbuk koriguje jedan deo svoje politike privatnosti koji se odnosi na difoltno

[12] http://blog.facebook.com/blog.php?post=7584397130

[13] http://www.dailymail.co.uk/sciencetech/article-1215470/Facebook-turns-controversial-advertising-Beacon.html

[14] http://www.cnn.com/2009/TECH/02/18/facebook.reversal/index.html

(standardno) podešavanje sigurnosnih mehanizama na profilu, kao i u domenu oglašavanja, ali važan deo pritužbi koji se tiču aplikacija trećih lica, deaktivacije i brisanja profila, profila preminulih korisnika i ličnih informacija ne-korisnika, do danas je ostao nerešen.

6. Bezbedonosni rizici na sajtovima za društveno umrežavanje i preporuke za njihovo smanjivanje

Upravo su problemi poput do sada iznetih stvorili potrebu za usvajanjem određenih standarda kada je u pitanju privatnost podataka korisnika SDU. Jednu od najsadržajnijih analiza ove problematike sačinila je Evropska agencija za bezbednost mreže i informacija (*European Network and Information Security Agency* -ENISA). U svom izveštaju „Problemi bezbednosti i preporuke za online društvene mreže“ iz 2007. godine navode se sledeće pretnje, koje su podeljene u četiri kategorije [8]:

- *Pretnje po privatnost:*

1. Pravljenje digitalnih dosijea
2. Sekundarno prikupljanje podataka u marketinške svrhe
3. Programi za prepoznavanje lica na fotografijama korisnika
4. CBIR (*Content-based Image Retrieval*): Nova tehnologija koja se bazira na istraživanju sadržaja fotografije u cilju kreiranja ogromne baze podataka
5. Mogućnost povezivanja slike sa metapodacima (profil ili e-mail)
6. Poteškoće u brisanju profila

- *Tradicionalne opasnosti po mreže i bezbednost informacija*

7. Spamovanje
8. XSS (*Cross site scripting*): skriptovanje među sajtovima putem virusa i crva
9. SDU agregatori: posebni portali koji povezuju više SDU

- *Pretnje po identitet*

10. Ribolov kopljem (*spear fishing*) putem SDU
11. Infiltracija u mrežu
12. Useljavanje na profile i kaljanje reputacije putem krađe identiteta

- *Društvene pretnje*

13. Proganjanje
14. Zlostavljanje
15. Industrujska špijunaža

U skladu sa identifikovanim pretnjama ENISA daje sledeće preporuke i kontramere za povećanje nivoa bezbednosti lica i podataka:

- *Preporuke u oblasti vladinih regulatornih politika*

1. Ohrabriti podizanje svesti i edukativne kampanje
2. Ocentiti i ponovo analizirati regulativu
3. Povećati transparentnost u rukovanju podacima
4. Obeshrabriti zabranjivanje SDU u školama

- *Preporuke za provajdere i njihovu poslovnu politiku*

5. Uvesti strožiju identifikaciju i kontrolu pristupa tamo gde je moguće
6. Uvesti kontra mere protiv industrijske špijunaže
7. Maksimizirati mogućnosti izveštavanja korisnika o zloupotrebama, kao i za njihovo otkrivanje

8. Uspostaviti odgovarajuća (difoltna) podešavanja profila koja će zaista štiti privatnost korisnika
9. Pružaoci usluge SDU treba da ponude jednostavna sredstva za kompletno brisanje podataka
   - *Tehničke preporuke*
10. Ohrabriti upotrebu tehnika označavanje reputacije korisnika
11. Ugraditi automatizovane filtere
12. Tražiti saglasnost za tagovanje fotografija
13. Ograničiti spajderovanje i bulk daunlodovanje
14. Obezbediti bolju kontrolu privatnosti kod pretraživanja ličnih podataka
15. Regulisanje problema spamovanja na SDU
16. Regulisanje problema „pecanja“ na SDU
    - *Preporuke u oblasti istraživanja i standardizacije*
17. Promovisati i istražiti tehnike za anonimizaciju fotografija korisnika
18. Promovisati „prenosne“ mreže
19. Istražiti nove trendove u vezi sa SDU

Godinu dana kasnije (2008) “Međunarodna radna grupa za zaštitu podataka u telekomunikacijama”, takozvana Berlinska grupa, objavila je svoj izveštaj i vodič o zaštiti privatnosti, kako za kreatore SDU tako i za same korisnike ovih aplikacija [9]. U ovom izveštaju, poznatijem pod nazivom *Rimski memorandum*, posebno se ističu rizici po privatnost i bezbednost korisnika SDU sa posbnim naglaskom na sledeće pretnje:

1. *Na Internetu nema zaborava*-podaci ostaju zauvek sačuvani
2. *Obmanjujuće poimanje „zajednice“*- stvara lažnu sliku sigurnosti
3. *Besplatnost usluge*-koja se plaća time što se lični podaci kasnije koriste u marketinške svrhe
4. *Skupljanje podataka o kretanju na Internetu od strane provajdera usluga umrežavanja*
5. *Rastuće potrebe da se refinansiraju usluge i ostvari profit mogu dalje ohrabrivati prikupljanje, obradu i upotrebu podataka o korisnicima*
6. *„Odavanje“ više ličnih podataka nego što korisnik misli da je dao*
7. *Zloupotreba podataka iz ličnih profila od strane trećih lica*
8. *Rizik krađe identiteta i moguće „otmice“ profila od strane neautorizovanih trećih lica*
9. *Upotreba veoma nesigurne infrastrukture*
10. Uvođenje standarda interoperabilnosti i interfejsa za kreiranje aplikacija (API, Google 2007), u cilju tehničkog ujednačavanja različitih društvenih mreža.

U skladu sa identifikovanim rizicima, Radna grupa je napravila preporuke za one koji regulišu, pružaju i koriste usluge društvenog umrežavanja.

- *Za regulatorna tela:*

1. Omogućiti pravo na upotrebu pseudonima umesto pravih imena
2. Obezbediti da provajderi usluga budu iskreni i jasni u pogledu informacija koje su potrebne za osnovnu uslugu, tako da korisnici mogu da procene da li će dati te informacije, te mogućnost da korisnici mogu da ne dozvole bilo kakvu sekundarnu upotrebu njihovih podataka, posebno ne za ciljani marketing
3. Uvođenje obaveze obaveštavanja provali u podatake korisnika SDU
4. Revidirati postojeći regulatorni okvir u odnosu na upravljanje ličnim podacima koji se objavljuju na SDU

5. Integrisati pitanja privatnosti u obrazovni sistem
   - *Za pružaoce usluga društvenog umrežavnja*

1. Transparentno i otovoreno informisanje korisnika
2. Uvesti mogućnost kreiranja i korišćenja profila pod pseudonimom
3. Držanje obećanja koja su data korisnicima
4. Difolt podešavanja koja su usmerena na zaštitu privatnosti
5. Poboljšati kontrolu korisnika nad upotrebom njegovih podataka iz profila
6. Uvesti odgovarajuće mehanizme za upravljanje žalbama korisnika
7. Poboljšati i održavati sisteme za bezbednost informacija
8. Pronaći i/ili još više unaprediti mere protiv nelegalnih aktivnosti kao što su spamovanje i krađa identiteta
9. Ponuditi enkriptovane konekcije za održavanje profila
10. Pružaoci usluga društvenog umrežavanja koji deluju u različitim državama ili globalno, treba da poštuju standarde o zaštiti privatnosti tamo gde pružaju svoje usluge
    - *Za korisnike:*

1. Budite pažljivi, dva puta razmislite pre nego što objavite lične podatke u svom profilu
2. Dobro razmislite pre nego što upotrebite vaše stvarno ime. Koristite pseudonim.
3. Poštujte privatnost drugih
4. Budite informisani o pružaocu usluge
5. Koristite podešavanja koja vam omogućavaju zaštitu privatnosti
6. Koristite različite identifikacione podatke (*user name i password*) od onih koje koristite na drugim sajtovima
7. Koristite mogućnost da kontrolišete kako pružalac usluga koristi vaše lične podatke
8. Obratite pažnju na ponašanje dece na Internetu a posebno na SDU.

Kada je reč o preporukama ovde treba spomenuti i istraživanje ranije pomenute OPC koje sprovedeno tokom 2008 godine i koje nakon identifikovanja, manje više poznatih pretnji na SDU, daje čak 71 preporuku za poboljšanje zaštite privatnosti njihovih korisnika [10].

7. Iskustva Srbije

Kada je o Srbiji reč još u uvodnom delu je rečeno da određena zakonska regulativa, koja bi trebala da reguliše problem zaštite privatnosti lica i podataka na Internetu, postoji. Međutim i pored toga u našoj javnosti do sada se nije čulo za tužbe u ovoj oblasti. Kada je reč o upotrebi SDU Srbija je prva u regionu po broju registrovanih profila na Fjesbuku sa čak milion ovih profila. Ovaj broj ne bi trebalo mešati sa stvarnim brojem korisnika SDU koji je svakako manji ali ipak govori da je ovaj fenomen široko rasprostranjen među domaćim korisnicima Interneta. Sa druge strane, za razliku privrženosti fenomenu umrežavanja, Srbija je na dnu kada je reč o trgovini preko Interneta. Čak 87,4% korisnika Internet u Srbiji nikada nije kupovalo putem interneta [11], što ukazuje na to da se SDU ne shvataju kao potencijalno rizični po korisnike za razliku od trgovanja na Internetu.

Do danas su kod nas retka istraživanja koja se bave zaštitom privatnosti na Internetu. Svakako valjda spomenuti jedno od pionirskih istraživanja na ovu temu koje je sproveo Vlado Popović tokom 2001. godine na preko 1073 ispitanika [12]. Već u ovoj

ranoj fazi upotrebe Interneta u našoj zemlji, kako to pokazuju rezultati Popovićeve studije, tadašnji korisnici demonstriraju iznenađujuće veliku spremnost da ostave svoje lične podatke na Internetu. Ovde treba naglasiti da tada nisu postojali SDU te se njihova otvorenost ne može shvatiti kao izraz neke vrste pomodarstva, već pre kao nepostojanje izražene svesti o potencijalnim opasnostima koje vrebaju na Internetu. Pa tako, čak 75,7% ispitanika kaže da bi na Internetu ostavili podatke o godini svog rođenja, zanimanju (82,3%), polu (92,1%), itd. Polovina ispitanika je spremna da otkrije ime i prezime i e-mail, dok bi čak 22,4% otkrilo i kućnu adresu a nešto manje i broj telefona (15,2%). Na sve ovo treba dodati i 14% onih koji su spremni da na nekom od sajtova ostave tako poverljiv podatak kao što je to matični broj.

Skorije istraživanje koje se direktno bavilo SDU sprovela je tokom 2008. godine Svetlana Jovanović sa saradnicima, a ticalo se studentske populacije u Srbiji i njihove upotrebe Fejsbuka i My Space-a [13]. Istraživanje je sprovedeno na uzorku od 1664 ispitanika i rezultati do kojih se došlo su slični onima koji se odnose na njihove kolege na Zapadu. Najzanimljivi nalaz je da samo 5% korisnika drži svoj profil sakriven za sve korisnike, dok čak 56% studenata dozvoljavaja da njihov profil vide svi korisnici Fejsbuka bilo da su na listi njihovih prijatelja ili ne. Broj (35%) onih koji na svojim profilima otkrivaju puno ime i prezime, datum rođenja, e-mail adresu ili broj telefona nije mali.

Rezultati ovih studija pokazuju da je Srbija i kada je reč o ponašanju njenih Internet korisnika deo globalnog sveta. Iako se kod nas daleko manje kupuje putem Interneta, što pokazuje možda i neopravdano veliki strah od rizika ovakvog vida trgovanja, sa druge strane velika popularnost SDU kod naših korisnika i njihova nezabrinutost za mogućnost manipulacije ličnim podacima govori o tome da će u budućnosti biti veoma važno da se radi na podizanju svesti o rizicima koje nosi takvo ponašanje na SDU.

8. Zaključna razmatranja

Sajtovi za društveno umrežavanje, po našem mišljenju, paradigma su današnjeg rizičnog društva. Budući da se na Internet projektuje društvo u svom virtulenom obliku, razumljivo je da se po toj analogiji u virtuelni svet Interneta projektuju i rizici realnoga sveta. Ipak, kroz ovaj rad pokušali smo da pokažemo da se gore pomenuti rizici po privatnost lica i podataka mogu smanjiti na nekoliko nivoa.

Na zakonodavnom planu treba pružiti rešenja koja bi omogućila neometanu razmenu informacija i transakcije putem interneta. Neophodno je pokrenuti korišćenje elektronskog potpisa, dozvoliti identifikaciju i autorizaciju učesnika u transakciji, operacije s kreditnim karticama i uspostaviti nadležnost nad internet transakcijama. Uz to, neophodno je osigurati zaštitu ličnih podataka i privatnosti, prenos informacija kroz međunarodne sisteme, kriptografsku zaštitu i zaštitu korisnika od uvredljivog, nezakonitog i neželjenog internet sadržaja.

Provajderi usluga društvenog umrežavanja treba takođe, pored želje za sticanjem profita, da misle i na one koji im taj profit posredno donose, odnosno na svoje korisnike. Ukoliko se mehanizmi za zaštitu ličnih podataka ne podignu na nivo zaista bezbednog boravka na SDU, korisnici će početi da traže alternativne načine za njihovo umrežavanje.

I na kraju, ono što se već sada može uraditi je podizanje svesti korisnika SDU, ali ne kroz pozive na bojkot SDU, jer ti pozivi neće dati rezultata, već kroz stalno

promovisanje lične brige o podacima koji se daju drugima na raspolaganje u onoj meri u kojoj se pojedinac brine da ne izgubi ličnu kartu ili svoj mobilni telefon. Kada korisnici budu razumeli da su lični podaci koje ostavljaju u virtulenom prostoru Interneta vrlo realni i da se konsekvence njihove zloupotrebe mogu odraziti na njihove stvarne, a ne virtulene profile tada će biti daleko oprezniji po pitanju kome te podatke mogu poveriti na čuvanje, a kome ne.

Literatura

[1] Riley T, *Privacy in the digital age*, Washington, 1997.
[2] Wellman B, "Physical Place and CyberPlace: The Rise of Personalized Networking", *International Journal of Urban and Regional Research,*2001.
[3] Granovetter M,"The Strenght of Weak Ties: A Network Theory Revisited", *Sociological Theory*, USA,1983.
[4] Gross R. and Acquisti A, „Information revelation and Privacy in Online Social Networks", *ACM workshop on Privacy in the electronic society, Alexandria*, VA, USA, 2005
[5] Young A. L and Quan-Hasse A, „Information revelation and internet privacy concerns on social network sites: a case study of face book", *Fourth international conference on Communities and technologies*, University Park, Pa, USA, 2009.
[6] http://www.cippic.ca/uploads/CIPPICFacebookComplaint-29May08.pdf
[7] http://www.priv.gc.ca/cf-dc/2009/2009-008-0716-e.pdf
[8] http://www.ifap.ru/library/book227.pdf
[9] www.datenschutz-berlin.de/attachments/.../WP-social-network-services.pdf
[10] http://www.priv.gc.ca/information/pub/sub-comp-200901-e.pdf
[11] http://webrzs.statserb.sr.gov.yu/axd/dokumenti/ict/2009/ICT2009s.zip
[12] Popović V, „*Zaštita privatnosti na Internetu kao jednom od servisa multimedijalnih komunikacija*", Magistarski rad, Saobraćajni fakultet, Beograd, 2004.
[13] Jovanović S, Drakulić M. i Drakulić R, „Privatno -Javno?, Sumrak privatnosti u eri društvenih mreža", *56. Naučno-stručni skup psihologa Srbije – Sabor psihologa*, Kopaonik.

Abstract: *In this paper we have analyzed privacy protection on the Internet with special regards to the most popular social networking sites (SNS). After examining domestic and European privacy protection legal acts in central part of this paper we have highlighted different forms of personal data abuse. Additional problem represents that, by voluntary giving away of confidential personal data in theirs profiles, users became accomplices in these abuses. Finally, in this paper are emphasized different recommendations for prevention of personal data abuse.*

Keywords: *Privacy, safety, risk, social networking, Internet.*

SOCIAL NETWORKING AND INTERNET USERS PRIVACY PROTECTION

Nataša Tomić, Dalibor Petrović