Privatnost na društvenim mrežama

Seminarski rad u okviru kursa
Računarstvo i društvo
Matematički fakultet

Jovan Rumenić
mi17069@alas.matf.bg.ac.rs

1. september 2022.

Sažetak

Ovaj rad se bavi terminima privatnosti i bezbednosti na društvenim mrežama.Društvene mreže su postale deo ljudskog života. Počevši od deljenja informacija kao što su tekst, fotografije, poruke, mnogi su počeli da dele najnovije vesti i slike povezane sa vestima u domenu medija, upitnike, zadatke i radionice u domenu obrazovanja, onlajn ankete, marketing i ciljanje klijenata u domenu poslovanja, kao i šale, muziku i video zapise u domenu zabave. Dok uživamo u deljenju informacija na društvenim mrežama, to predstavlja veliki izazov za bezbednost i privatnost. Informacije korisnika koje treba da se čuvaju neotkrivene, treba da budu privatne. Ekspanzija društvenih mreža u poslednjoj deceniji donela je opravdan strah o količini privatnih podataka koji se izlažu na internet. Sistematične aktivnosti nadzora otkrivene od strane bivšeg obaveštajca Edward Snowdena samo su dodatno pojačale zabrinutost. Rad se bavi tehničkim, sociološkim i pravnim aspektima društvenih mreža s aspekta nekontrolisanog toka podataka.Opisani su scenariji u sklopu kojih je moguće dobiti privatne podatke na osnovu javno dostupnih. Pažnja je posvećena i pravnim aspektima sa stanovišta prikupljanja biometrijskih podataka. Ispitana je i spremnost subjekata da zaštite privatne podatke.

Sadržaj

1 Uvod

"Privatnost je pravo individue, grupe ili institucije da za sebe odrede kada, kako, i u kojoj meri se informacije o njima prosleđuju drugima."[1]
Prema procenama iz 2014. godine broj korisnika Facebook-a narastao je do cifre od 1.32 milijardi [9].Čak i pod grubom pretpostavkom da samo polovina korisničkih profila odgovara stvarnom fizičkom licu, i dalje je u pitanju značajan procenat svetske populacije. Podaci o skladišnim kapacitetima jedne ovakve mreže su neverovatni. Facebook-ova baza sredinom 2011. sadržavala je blizu 100 milijardi fotografija [10]. Korisnici na društvenim mrežama ostavljaju veliki broj podataka, direktno ili indirektno, koji se mogu iskoristiti da povežu korisnički profil sa stvarnom ličnošću iza profila.U radu će biti razmotreni tehnički detalji načina kontrole podataka te pravne i socijalne implikacije koji demonstriraju kako se online prisusvo i aktivnosti odražavaju na svet koji nije u domenu virtuelnog. U širem kontekstu istraživanja podataka, znatna mera produktivne analize kako bi se saznala napredna evidencija ljudskog ponašanja u međuljudskim organizacijama, može se odvijati bez narušavanja privatnosti korisnika. Stoga bi informacije trebalo da budu dostupne na način da privatnost bude sačuvana, a zaštita izuzetno ispitana. Sa druge strane, sumnja da je svaki nestručni korisnik zainteresovan da razbije informacije je malo verovatna, zbog njegovih drugih interesovanja koju upotreba svih informacija, uključujući prepoznate i delikatne, može da pruži. Zbog specifičnosti međuljudskih organizacija, najosnovnija mera koja se može primeniti jeste da se učini što kvalitetnijom zaštita privatnosti pojedinca.

2 Vrste podataka

U cilju generalnosti u nastavku će biti korišćen termin podatkovni subjekat koji predstavlja osobu ili organizaciju koja je vlasnik određenih podataka ili je njima opisana. Postoje dve vrste ovih podataka: primarni i sekundarni. Pod primarnim podacima podrazumevaju se oni koji direktno prikazuju određenu karateristiku podatkovnog subjekta. To može biti ime, mesto prebivališta, jedinstveni matični broj ili čak biometrijski podaci. Sekundarni podatak je onaj koji daje uvid u određenu preferencu i samostalno ne određuje primarnu karakteristiku osobe ili organizacije. Sa stanovišta društvenih mreža, privatni podatak korisnika može biti geografska lokacija, datum rođenja, političko ili versko opredeljenje. Sekundarni podatak mogu biti preference kao što su omiljeni sportski tim ili film. Ovakvi podaci su najčešće javno dostupni. Istraživanja su pokazala da nije potrebna velika količina truda da se zaključi primarna karateristika iz sekundarnih podataka, sa zadovoljavajućom tačnošću. Studija sprovedena na Cambridge Univerzitetu fokusirala se upravo na određivanju fizičkih ili karakternih osobina individue baziranih na analizi sekundarnih podataka [4]. Autori su na osnovu Facebook profila vršili dedukciju o karakteristikama osobe poput rase, intelekta, verskog i političkog uverenja. Među neobičajenim kategorijama našla se i informacija da li su se roditelji posmatrane osobe razveli pre nego je ista napunila 21 godinu. Svi ovi zaključci donošeni su na osnovu zapažanja obrazaca i korišćenjem istih u daljem radu. Svi prikupljeni podaci mogu se iskoristiti u svrhu ciljanog marketinga. Još jedan način koji je mnogo više zabrinjavajući jeste korišćenje biometrijskih osobina za prikupljanje podataka poput imena i prezimena te jedinstvenog matičnog broja. Istraživanje koje je sproveo Alessandro Acquisti demonstriralo je način na koji je moguće na osnovu fotografije nasumične, nepoznate osobe koja ima profil na društvenoj mreži saznati ime, prezime, u određenim slučajevima i jedinstveni matični broj [5].

3 Moguće pretnje i rizik po privatnost na društvenim mrežama

Sa stanovišta analitike privatnosti, determinante će nadgledati prednosti i predstavljati opasnosti koje utiču na izbor korisnika da otkrije određene akreditive. Takođe se primećuje da pojedinci neretko žele da se odreknu neke privatnosti radi adekvatne mogućnosti za nagradom. Korišćenjem društvenih mreža [8], ljudi se otvaraju različitim vrstama opasnosti koje za cilj imaju narušavanje privatnosti. Poznato je da privatnost može biti napadnuta na nekoliko načina ako se lične informacije ne koriste razumno i pouzdano. Privatnost implicira odgovarajući tok informacija koji je pod kontrolom subjekta podataka. Ova kontrola može se sprovoditi na više načina. Jedan je kroz podešavanje privatnosti unutar web aplikacije pri čemu subjekat podataka određuje koje podatke želi deliti sa javnošću, a koje želi da ostanu privatne. S tim u vezi, privatnost korisnika nije narušena ako isti postavi sliku na društvenoj mreži s postavkama da je ta ista slika dostupna javnosti. Medjutim, privatnost korisnika je narušena ako je tu istu sliku označi kao dostupnu uskom krugu ljudi, a treće lice dođe u posed te slike, bez znanja korisnika o ovoj mogućnosti. Drugi način je ugovor između subjekta podataka i davaoca usluge. Pri prijavljivanju na uslugu subjekat treba pristati na uslove davaoca koji mogu sadržavati i način na koji će podaci subjekta biti korišćeni. Ovi uslovi najčešće nisu podložni promenama. U oba slučaja radi se o vrsti ugovora čiji su učesnici subjekat i davalac usluge. U ugovoru se regulišu obaveze obe strane. Sa aspekta privatnosti, davalac usluge obično deklariše način na koji će privatni podaci korisnika biti korišćeni. Bitan izazov koji se nameće je koncept pristanka. Da li se pasivnost korisnika može smatrati kao prećutno odobravanje? U Evropi Facebook je vodio pravnu bitku upravo na navedenu temu. Sve do nedavno Facebook Photo Tag Suggest opcija bila je inicijalno uključena za sve korisnike. Za sliku postavljenu na ovu društvenu mrežu, ova opcija podrazumeva izvršavanje algoritma prepoznavanja lica nad bazom postojećih korisnika i predlaganje označavanja osoba koje su prepoznate na slikama. Ova opcija direktno je podrazumevala obradu osetljivih biometrijskih podataka (u sklopu

zakona o zašititi podataka u Evropskoj Uniji biometrijski podaci spadaju u zaštićenu kategoriju), bez direktnog pristanka subjekta čiji se podaci obrađuju. Da bi se subjekt zaštitio bila je potrebna aktivna participacija, na način da subjekat isključi ovu opciju, koja je inicijalno bila uključena. Nakon pravnih akcija pokrenutih od strane regulatornih tela za zaštitu privatnih podataka iz Nemačke i Irske, Facebook je promenio svoju politiku. Prepoznavanje lica bez inicijalnog pristanka subjekta je isključeno za korisnike unutar Evropske Unije. Ovaj slučaj naglasio je princip koji je Facebook kršio koji se može naći u sklopu člana 29 direktive o zašititi privatnih podataka koji je doneo Evropski parlament. "Pristanak dobijen kroz pasivnost ima unutrašnju neodređenost i samim tim ne prikazuje stvarnu volju subjekta"[7] Pristanak se treba dobiti aktivnim delovanjem u vidu potvrde od strane subjekta da se podaci koriste u određenu svrhu.

3.1 Otkrivanje privatnih informacija

Najveća prepreka u vezi sa privatnošću odnosi se na to da su akreditivi korisnika slični društvenom ugovoru gde korisnici trguju sopstvenim podacima u odnosu na finansijske ili nemonetarne nagrade. Vrlo je očigledno da će se razumni korisnici nastaviti interesovati za takav društveni ugovor sve dok količina prednosti nadmašuje sadašnje i buduće opasnosti izlaganja. Predlog je pouzdan sa hipotezom koja pretpostavlja da se ljudi odlučuju na odluke koje im omogućavaju da dožive najveće prednosti i minimizuju troškove. Postavljena je tako da koristi želje za otkrivanjem informacija korisnika datih na društvenim mrežama. S obzirom da se predloženi cilj odnosi na posmatranje uticaja unutrašnjih prednosti, cilj otkrivanja je deo dva konstrukta: jedan meri spremnost korisnika da se otkriju pre nagrade, dok drugi meri njihovu sposobnost da se otkriju podstaknutu nagradom. Nepojavljivanje unutrašnje-spoljašnjih kvalifikacija u ranijim radovima podrazumevala je da se cilj otkrivanja može posebno meriti iz važnih slobodnih razvoja.

4 Biometrijski podaci

Ranije spomenuti slučaj ukazuje na pitanja privatnosti kod korišćenja biometrijskih podataka. Tehnike prepoznavanja lica predstavljaju pouzdan alat za identifikovanje i praćenje osoba. Dodatno, lice je pouzdan alat za mapiranje online i offline identiteta. Ranije opisana Facebook opcija ima implikaciju da Facebook može prikupljati osetljive biometrijske podatake čak i za osobe koje nisu deo te društvene mreže. Zaista, ako se okači slika na kojoj je osoba koja nije član društvene mreže, ništa ne sprečava Facebook da biometrijske osobine osobe sačuva za buduću upotrebu. S tim u vezi, moraju postojati pravni mehanizmi koji će osigurati da društvene mreže ne smeju kreirati i održavati bazu podataka o subjektima koji nisu korisnici. Evropska komisija unutar regulative o zaštiti podataka definište princip transparentosti koji zahteva da svaka obrada privatnih podataka mora biti zakonita, korektna i transparentna u odnosu na subjekta.

4.1 Socijalne i pravne implikacije

Čak i pažljivim određivanjem podešavanja privatnosti, subjekt podataka nema potpunu kontrolu nad tokom informacija. Ako subjekt postavi fotografiju na društvenu mrežu koja je namenjena samo uskom krugu ljudi, isti mogu kroz deljenje značajno povećati publiku koja će to videti. Ovakve i slične situacije mogu rezultovati gubitkom ugleda subjekta u pitanju. Stranica facebookfired.com dokumentuje iskaze osoba koje su izgubile posao kao rezultat aktivnosti na društvenim mrežama. Dodatno je zabrinjavajuće istraživanje koje je pokazalo da osobe u okviru radnog okruženja donose privatne i profesionalne zaključke o kolegama bazirane isključivo na profilu na društvenim mrežama [11]. Postala je uobičajena praksa i za poslodavca da donosi zaključke o kandidatu koristeći isti izvor. S druge strane, čak se i potpuno odsustvo tih informacija uzima kao indikativan pokazatelj o introvertnosti osobe. Govor mržnje ili kleveta na društvenim mrežama može rezultovati pravnim akcijama protiv osobe koja to postavlja. Ovo je slučaj čak i ako se koristi pseudonim, ako se veštačenjem utvdi stvarni identitet korisnika.

5 Upravljanje poverenjem i problemi

Uzimajući u obzir značaj privatnih podataka i implikacije otkrivanja neželjenoj publici, bilo bi za očekivati da su subjekti generalno odgovorni spram svojih privatnih podataka, samim tim da ih nevoljno dele sa trećim stranama. Istraživanja su pokazala upravo suptrotno. Na primer izveštaj o e-komercu iz 2002. referencira istraživanje sprovedeno iste godine koje pokazuje da 82 % osoba koje obavljaju online kupovinu spremno dati svoje privatne podatke u zamenu za šansu da osvoje 100 dolara [3]. BBC spominje istraživanje sprovedeno u Londonu koje je pokazalo da su ljudi spremni otkriti svoje lozinke u zamenu za čokoladu [6]. S druge strane, samo 47 % ljudi spremno je platiti bili kakvu naknadu u cilju zaštite podataka [2]. Ovaj neočekivani nesklad u psihologiji i ekonomiji poznat je kao raskorak u spremnosti da se plati i spremnosti da se prihvati. Klasičan primer je eksperiment u kojem se svakoj osobi u sklopu jedne grupi osoba dodeli šolja, a drugoj grupi olovka. Zatim se svakoj osobi predstavi pitanje da li bi menjali svoj predmet za neki drugi alternativni predmet. Svakoj grupi osoba ponuđeni alternativni predmet je bio zapravo predmet koji ima druga grupa. Rezultati su pokazali da većina osoba koje imaju šolju bi radije zadržala šolju. S druge strane, većina osoba koja ima olovku bi radije zadržala olovku. Ovo je kontrainituitivno obzirom da je šolja u pitanju bila vrednija od olovke, što je bila i ocena subjekata pre početka eksperimenta. Nivo informatičke edukacije sigurno je presudan faktor u pristupima. Osoba koja poznaje rizike od otkrivanja privatnih informacija će biti manje spremna da ih otkrije od osobe koje nema taj nivo svesti.

5.1 Podešavanje privatnosti na društvenim mrežama

Kasnije istraživanje istraživalo je odnos između onlajn otkrivanja pojedinačnih podataka i zabrinutosti za privatnost i identifikovana je velika opasnost od online pukotina zaštite. Takođe je dobro predloženo da je privatnost termin koji je teško okarakterisati; legitimno, sa jedne strane aludira da je ne pominjemo, a opet može da uvrsti privilegiju da izabere stepen do kojeg se otkrivaju pojedinačni podaci, privilegiju da se fokusira na tačku kada,

kako i koji podaci mogu da se predoče drugima. Otkriće da su nečiji privatni podaci rasuti po internetu, uključujući ponižavajuće fotografije ili karakteristike koje se vraćaju putem fishing trikova ili nedovoljnih ograničenja zaštite, govori o stvarnoj opasnosti po mentalno zdravlje. Na Fejsbuku je postavka fluidna i slaba, što ima velike posledice u pogledu administracije privatnosti na Facebook-u. Često se malo razmišlja o utisku klijenata o njihovom okupljanju ljudi, u pogledu veličine i obima tog okupljanja, a postavke administracije zaštite su redovno zamršene, uzaludne i zahtevaju posebne procene. O opasnostima po privatnost se malo razmišlja, dok se društvene prednosti nastale iz otkrivanja pojedinačnih podataka često precenjuju. Društvene mreže rade na jačanju postavki privatnosti. Facebook i druge društvene mreže ograničavaju zaštitu kao glavni aspekt njihovih podrazumevanih postavki. Od suštinskog je značaja za klijente da uđu u podešavanja klijenta kako bi promenili svoje izbore zaštite. Mreže, kao što je Facebook, daju klijentima alternativu da ne prikazuju lične podatke, na primer, datum rođenja, e-poštu, broj telefona i poslovni status. Za pojedince koji odluče da uključe ove podatke, Facebook dozvoljava klijentima da ograniče pristup svom profilu na način da dozvole samo pojedincima koje priznaju kao "pratioce“ da vide njihov profil. Bilo kako bilo, čak ni ovaj nivo privatnosti ne može da spreči jednog od tih pratilaca da sačuva fotografiju na sopstvenom računaru i objavi je negde drugde.Trenutno je manje klijenata na društvenim mrežama ograničilo svoje profile. Na primeru ćemo prikazati način na koji korisnici ograničavaju vidljivost profila drugima na različitim društvenim mrežama :

- Facebook: Facebookova postavka privatnosti za nove korisnike postavljena je na "Friends only". Da biste ovo podesili, posetite Settings > Privacy > Who can see your future posts?
- Twitter: Settings > Security and privacy > Privacy > Tweet Privacy > Protect my Tweets.
- LinkedIn: Da biste promenili ovo: Settings > Account > Helpful Links > Edit your public profile.
- Google+: Da biste promenili ovu postavku, upišite ime kruga u polje “Za“ ispod vašeg posta pre nego što ga objavite.

Fejsbuk bi mogao jasno da izrazi da ne mogu da daju nikakve garancije u pogledu poštovanja privatnosti svojih informacija, kao i da, ako klijenti otvore svoje profile, sve podatke sadržane u tome mogu da vide svi korisnici društvene mreže(poslodavci, direktori...). Ne zaboravimo da većina neformalnih komunikacionih destinacija velikog dometa podstiče odustajanje od aplikacija, prikrivanje pada broja pratilaca i prikrivaje intriga. Međutim, veliki deo podataka je i dalje otvoren, što se podrazumeva. Od ključnog je značaja da klijenti svih društvenih mreža ograniče pristup svom profilu, a ne da postavljaju nezakonite ili omalovažavajuće sadržaje na svojim profilima, kao i da budu oprezni sa podacima koje čine pristupačnim.

6 Zaključak

Kreiranje korisničkih naloga na najvećim društvenim mrežama je besplatno. S tim u vidu, razumljivo je da ti servisi profit pronalaze u drugim vidovima aktivnosti, primarno kroz ciljano oglašavanje. Korisnici možda nisu proizvod, ali kada servis plaćaju drugi, sigurno nisu ni potrošač. Primećeno je da je zabrinutost za privatnost na društvenim mrežama veoma slaba i da korisnici ne nastoje da naprave odgovarajuće promene u pogledu privatnosti na društvenim mrežama, koje su znatno niže od drugih načina bezbednosnih operacija. Osim toga, mnogi korisnici društvenih mreža imaju manjak tehničkih znanja i tako se prepuštaju manjoj zabrinutosti za očuvanje privatnosti sopstvenog sadržaja. Čak su i spremni podeliti svoje privatne podatke, za vrlo malu naknadu ili mogućnost ostvarivanja iste. Pokazano je da nivo zaštite direktno proporcionalan informatičkoj pismenosti osobe. Ovo je indikacija da informiranost o načinu prikupljanja podataka i njihovo korišćenje, navodi na korake u zaštiti istih. Naizgled banalne aktivnosti na društvenim mrežama, kada se grupišu mogu otkriti iznenađujuće mnogo. Ako bismo išli na sprovođenje skupa dobro definisanih politika za društvene mreže, kao što su jaka lozinka, svest o čestoj promeni lozinke, svest o otkrivanju informacija, svrsi antivirusnog ili sličnog softvera, vlasničkog softvera itd, obezbedili bismo društvene mreže od daljih napada i ranjivosti.

Literatura

[1] Privacy and Freedom

[2] Rose, E., 2005. "Data Users versus Data Subjects: Are Consumers Willing to Pay for Property Rights to Personal Information?"

[3] B. Tedeschi, "Everybody talks about online privacy, but few do anything about it, New York Times, 03.06. 2002, str. 6

[4] M. Kosinskia, D. Stillwella, T. Graepelb, "Private traits and attributes are predictable from digital records of human behavior"

[5] A.Acquisti, R. Gross, F. Stutzman, "Privacy in the Age of Augmented Reality"

[6] "Passwords revealed by sweet deal"

[7] Direktiva 95/46 / EZ Evropskog parlamenta i Veća od 24. 10. 1995. o zaštiti pojedinaca s obzirom na obradu podataka i slobodnom toku takvih podataka"

[8] Patrick Van Eecke, Maarten Truyens, Privacy and social networks, Computer Law & Security Review;

[9] Facebook now has 1.32 billion users

[10] Facebook Photo Trends

[11] C. Robles, J. Golbeck, "Facebook Relationships in the workplace"

[12] *On Privacy and Security in Social Media – A Comprehensive Study*