# PRIVATNOST NA INTERNETU

**SEMINARSKI RAD**

**ALEKSANDAR KRSTIĆ 18717**

**19. AVG | 2025.**

## SADRŽAJ

# UVOD

U savremenom digitalnom dobu privatnost na internetu postaje jedna od najvažnijih tema vezanih za zaštitu ličnih podataka i bezbednost korisnika. Milioni ljudi svakodnevno koriste digitalne platforme kao što su Facebook, Instagram, TikTok, Twitter, LinkedIn, YouTube, pa čak i manje poznate servise, ostavljajući svoj digitalni trag. Taj trag uključuje lične podatke, navike, lokaciju, interesovanja, ali i informacije o kupovnim navikama, preferencijama i svakodnevnim aktivnostima. Kompanije te podatke koriste za kreiranje detaljnih profila korisnika, personalizovane reklame, analizu ponašanja i, u nekim slučajevima, za političke kampanje ili socijalna istraživanja.

**Privatnost** nije samo pitanje lične sigurnosti već i društvene odgovornosti. Svaka objavljena fotografija, status, komentar ili klik na reklamu predstavlja podatak koji može biti iskorišćen na različite načine, često bez potpune svesti korisnika. Shoshana Zuboff u svojoj knjizi *The Age of Surveillance Capitalism* opisuje koncept „ekonomije nadzora“, u kojem kompanije profitiraju na prikupljanju i analiziranju ličnih podataka korisnika, često na način koji korisnici ne mogu ni da predvide.

U ovom radu analiziraćemo pretnje privatnosti, metode praćenja korisnika, najpoznatije skandale u vezi sa curenjem podataka, rizike koje sami stvaramo, kao i savremene metode zaštite privatnosti. Posebno će biti istaknuta važnost zakonske regulative, ali i lične odgovornosti.

Kriterijumi za ocenu efikasnosti zaštite privatnosti uključuju: transparentnost kompanija u vezi sa prikupljanjem i obradom podataka, mogućnost korisnika da kontroliše i briše svoje podatke, kao i poštovanje zakonske i etičke regulative, poput evropskog **GDPR**-a i kalifornijskog **CCPA**. Ovi kriterijumi zasnivaju se na opšteprihvaćenim normama i ne odražavaju lični stav autora, već stručne standarde u oblasti informatike i prava.

# DIGITALNI TRAG

Svaki korisnik interneta ostavlja svoj digitalni trag, koji se može podeliti na pasivan i aktivan. **Pasivni trag** predstavlja informacije koje se beleže automatski, bez direktne interakcije ili svesti korisnika. Primeri uključuju IP adresu, lokaciju uređaja, trajanje posete web-stranici, klikove na reklame i istoriju pretraživača. **Aktivni trag** obuhvata podatke koje korisnik sam ostavlja – postove, komentare, fotografije i video snimke, informacije o lokaciji, podešavanja privatnosti, lajkovanje i deljenje sadržaja.

Ovi tragovi omogućavaju kompanijama da kreiraju detaljne profile korisnika, što im daje mogućnost da predviđaju ponašanje, personalizuju reklame i prodaju podatke trećim stranama. Na primer, Google beleži svaku pretragu i aktivnosti na YouTube-u, dok Facebook koristi algoritme za predlaganje prijatelja i sadržaja na osnovu interakcija korisnika.

Posledice digitalnog traga su dalekosežne. Osim komercijalne upotrebe, prikupljeni podaci mogu biti zloupotrebljeni u političke svrhe, manipulaciju mišljenjima, pa čak i u kriminalne svrhe. Mnogi korisnici nisu svesni obima podataka koji se prikupljaju i kako se oni mogu koristiti, što postavlja pitanje koliko zaista kontrolišemo sopstvenu privatnost i koliko je digitalni svet transparentan prema nama.

# KO UGROŽAVA PRIVATNOST I KAKO?

Privatnost korisnika interneta ugrožavaju različiti akteri. Tehnološke kompanije poput **Google**-a, **Meta**-e i **TikTok**-a svakodnevno prikupljaju ogromne količine podataka kako bi poboljšale svoje usluge, ostvarile profit kroz ciljani marketing i kreirale personalizovano iskustvo za korisnika. Međutim, obim i način prikupljanja podataka često prelazi granice transparentnosti.

Pored kompanija, postoje i tzv. **data brokers** – firme koje kupuju i prodaju podatke korisnika, uključujući informacije o finansijama, kupovnim navikama, obrazovanju i interesovanjima. Ove informacije se zatim koriste za ciljanje korisnika i kreiranje profila, često bez njihovog znanja ili saglasnosti.

**Hakeri** i **cyber kriminalci** predstavljaju treći nivo pretnje privatnosti. Oni koriste sofisticirane tehnike za krađu identiteta, pristup bankarskim podacima i osetljivim informacijama, a posledice ovih napada mogu biti katastrofalne za pojedince.

Na četvrtom nivou su **države** i **obaveštajne službe**, koje vrše masovno nadziranje građana pod izgovorom bezbednosti. Edward Snowden je otkrio aktivnosti NSA i Prism programa, pokazujući kako se ogromne količine ličnih podataka prikupljaju i analiziraju bez znanja građana.

Poznati skandali, poput Cambridge Analytica, Yahoo breach-a i curenja LinkedIn podataka, pokazuju da privatnost nije samo teorijski problem. Cambridge Analytica je zloupotrebila podatke miliona korisnika Facebook-a radi političkih kampanja, Yahoo breach 2013–2014 doveo je do curenja više od tri milijarde naloga, dok je 2021. procurelo više od 700 miliona LinkedIn profila. TikTok je takođe kritikovan zbog prikupljanja podataka o mladim korisnicima i njihovim interakcijama, što pokazuje koliko je digitalni svet kompleksan i koliko su korisnici ranjivi.

# TEHNIKE PRAĆENJA

Internet koristi različite metode praćenja aktivnosti korisnika, koje se stalno razvijaju i postaju sofisticiranije. **Kolačići (cookies)** i **third-party cookies** beleže aktivnosti korisnika na web-stranicama i omogućavaju praćenje preko više platformi. **Browser fingerprinting** omogućava identifikaciju uređaja prema podešavanjima pregledača, instaliranim fontovima, veličini ekrana i drugim parametrima, bez potrebe za kolačićima.

Praćenje lokacije putem **GPS**-a, **Wi-Fi** mreža i mobilnih antena omogućava precizno lociranje korisnika u realnom vremenu. Algoritmi veštačke inteligencije analiziraju obrasce ponašanja i predviđaju buduće aktivnosti, dok socijalni inženjering koristi psihološke metode kako bi korisnike naveo da otkriju lične podatke ili preduzmu akcije koje nisu planirali.

Sve ove tehnike omogućavaju prikupljanje ogromnih količina informacija bez direktne saglasnosti korisnika, što znači da očuvanje privatnosti postaje izuzetno zahtevno. U savremenom digitalnom okruženju, skoro svaka interakcija sa internetom može biti zabeležena, analizirana i iskorišćena.

# KAKO SAMI UGROŽAVAMO PRIVATNOST?

U mnogim slučajevima korisnici interneta sami doprinose ugrožavanju svoje privatnosti, često ne shvatajući stvarni rizik svojih online aktivnosti. Jedan od najčešćih načina ugrožavanja privatnosti je preterano deljenje ličnih informacija na društvenim mrežama. Objavljivanje fotografija sa geotagom, statusa o lokaciji ili planovima putovanja omogućava trećim licima da prate kretanje korisnika, ali i da prikupljaju podatke o njihovim navikama, interesovanjima i svakodnevnim aktivnostima. Ove informacije mogu biti zloupotrebljene u reklamne, kriminalne, pa čak i političke svrhe.

**Korišćenje javnog Wi-Fi-ja** bez zaštite predstavlja dodatni rizik. Javne mreže su često nezaštićene i lako dostupne hakerima, koji mogu presretati nešifrovane podatke, uključujući lozinke, e-mailove i informacije o bankovnim transakcijama. Čak i prividno bezopasne aktivnosti, poput pregledavanja društvenih mreža ili slanja poruka, mogu omogućiti neovlašćen pristup osjetljivim informacijama.

**Prihvatanje opcije „Accept All Cookies“** bez promišljanja takođe olakšava praćenje korisnika. Kolačići prikupljaju podatke o pretragama, klikovima, lokaciji i interesovanjima, a mnogi korisnici ne shvataju da time praktično omogućavaju kompanijama da kreiraju detaljan digitalni profil koji se može koristiti za ciljane reklame ili čak manipulaciju ponašanjem.

Još jedan čest problem je **korišćenje istih lozinki za više naloga**. Ukoliko dođe do kompromitovanja jednog naloga, haker može pristupiti i svim ostalim servisima koji koriste istu lozinku. Ovo predstavlja ozbiljan bezbednosni rizik, jer može dovesti do krađe identiteta, finansijskih gubitaka ili kompromitovanja poslovnih i privatnih podataka.

**Instaliranje softvera sa nepouzdanih izvora** ili **klikanje na nepoznate linkove** povećava rizik od malware-a, spyware-a i virusa koji mogu špijunirati aktivnosti korisnika, krasti podatke ili čak šifrovati fajlove i tražiti otkupninu (ransomware). Ovakvi napadi nisu retkost i pogađaju kako privatne korisnike, tako i kompanije, dovodeći do ozbiljnih finansijskih i pravnih posledica.

Pored tehničkih grešaka, ugrožavanje privatnosti često nastaje zbog **nedovoljne digitalne pismenosti**. Mnogi korisnici ne razumeju kako funkcionišu algoritmi za praćenje, kako se prikupljaju podaci i koje posledice može imati njihovo deljenje. Zbog toga se preporučuje stalno obrazovanje i razvijanje svesti o opasnostima na internetu. Digitalna pismenost omogućava korisnicima da razumeju rizike, prepoznaju sumnjive situacije i preduzmu odgovarajuće mere zaštite, što je jednako važno kao i tehnička zaštita.

Primeri iz prakse pokazuju koliko male greške mogu imati velike posledice. Na primer, mnogi korisnici ne znaju da njihovi podaci sa mobilnih aplikacija za fitnes i lokaciju mogu biti prodati trećim stranama, dok objavljivanje fotografija sa detetom ili adresom u potpunosti otkriva privatne informacije koje mogu biti zloupotrebljene.

U suštini, očuvanje privatnosti nije samo pitanje tehnologije – to je i **pitanje ponašanja**, **navika** i **svesti**. Samo kombinacijom odgovornog deljenja informacija, pažljivog korišćenja tehnologije i stalnog obrazovanja korisnici mogu efikasno smanjiti rizik od ugrožavanja svoje privatnosti na internetu.

# MERE ZAŠTITE PRIVATNOSTI

Efikasna zaštita privatnosti na internetu zahteva kombinaciju **tehnoloških rešenja**, **lične discipline** i **stalne edukacije**. Samo tehnička rešenja bez svesti korisnika ili, s druge strane, lična disciplina bez savremenih alata, nisu dovoljni da bi se podaci zaštitili.

Jedan od osnovnih koraka u očuvanju privatnosti je korišćenje **jakih** i **jedinstvenih lozinki** za svaki nalog, u kombinaciji sa **dvofaktorskom autentifikacijom (2FA)**. Dvofaktorska autentifikacija dodaje dodatni sloj zaštite, jer čak i ako neko dođe do lozinke, ne može pristupiti nalogu bez dodatnog koda koji korisnik dobija na mobilni uređaj ili putem aplikacije za autentifikaciju. Na primer, Google i Facebook nude ovu opciju i njeno korišćenje značajno smanjuje rizik od hakovanja.

**VPN (Virtual Private Network)** i **Tor** omogućavaju anonimno surfovanje internetom, skrivajući stvarnu IP adresu korisnika i šifrujući podatke koji putuju internetom. Ovo je posebno važno kada se koristi javni Wi-Fi, koji je čest izvor napada i krađe podataka. Korišćenje VPN-a može takođe sprečiti da internet provajderi ili treće strane prate aktivnosti korisnika na mreži.

**Enkriptovani servisi za komunikaciju**, poput **Signal-a** i **ProtonMail-a**, štite sadržaj poruka, email-ova i poziva od prisluškivanja i neovlašćenog pristupa. Za razliku od običnih servisa, kod enkriptovanih servisa samo korisnici imaju ključeve za dešifrovanje poruka, što znači da čak ni provajder ne može pristupiti sadržaju komunikacije.

**Kontrola privatnosti** na društvenim mrežama je još jedan ključni element zaštite. Postavljanje privatnog profila, ograničavanje vidljivosti objava samo na odabrane osobe,

deaktiviranje geolokacije kod objava i pažljivo biranje ko može da vidi informacije na nalogu, značajno smanjuje rizik od zloupotrebe podataka. Takođe, redovno pregledanje aplikacija koje imaju pristup ličnim informacijama i brisanje onih koje nisu neophodne je efikasan način da se minimizira digitalni trag.

**Edukacija i stalno praćenje novih tehnologija i rizika** su neophodni jer se metode praćenja i zloupotrebe stalno razvijaju. Korisnici treba da budu upoznati sa opasnostima phishing napada, lažnih linkova, malicioznih softvera i socijalnog inženjeringa. Poznavanje osnovnih pravila digitalne higijene, poput neotvaranja sumnjivih linkova i neinstaliranja nepouzdanog softvera, može sprečiti mnoge bezbednosne incidente.

Takođe, sve veći broj korisnika koristi alate za blokiranje reklama **(ad blockers)** i skripti **(script blockers)** kako bi sprečili praćenje putem kolačića i browser fingerprinting-a. Iako ovo ne garantuje potpunu anonimnost, značajno otežava praćenje i prikupljanje podataka od strane trećih strana.

Bez primene ovih mera, privatnost u digitalnom dobu postaje praktično **nedostižna**. Lična odgovornost, svesnost i edukacija korisnika jednako su važni kao i tehnička zaštita. Samo kombinacijom svih ovih elemenata moguće je očuvati kontrolu nad ličnim podacima i smanjiti rizik od zloupotrebe, krađe identiteta i neovlašćenog nadzora.

# BUDUĆNOST PRIVATNOSTI

Digitalno okruženje postaje sve složenije i dinamičnije, a sa njim i pitanje zaštite ličnih podataka. Razvoj veštačke inteligencije i analiza velikih podataka (Big Data) omogućavaju kreiranje veoma preciznih i detaljnih profila korisnika. Kompanije, vlade i različite organizacije mogu pratiti ponašanje ljudi na internetu, njihove navike, interesovanja i čak emocionalna stanja. Istovremeno, Internet of Things (IoT) uređaji, koji su sve prisutniji u svakodnevnom životu – od pametnih satova i telefona, do kućnih aparata i automobila – neprekidno prikupljaju podatke. Ovi podaci se često čuvaju i analiziraju bez punog znanja korisnika, što otvara dodatna pitanja o bezbednosti i transparentnosti.

Pored ovih aspekata, pojavljivanje **deepfake** tehnologija i naprednih **AI manipulacija** donosi nove rizike. Danas je moguće kreirati uverljive **lažne fotografije**, **audio snimke** i **video sadržaje** koji mogu biti zloupotrebljeni za dezinformacije, ucene ili kompromitovanje reputacije pojedinaca i institucija. Granica između stvarnog i digitalno generisanog

sadržaja postaje sve tanja, što dodatno komplikuje zaštitu privatnosti i autentičnosti podataka.

Sa druge strane, pravni okvir pokušava da prati ove promene. Regulative poput Opšte uredbe o zaštiti podataka (GDPR) u Evropskoj uniji ili California Consumer Privacy Act (CCPA) u Sjedinjenim Američkim Državama postavljaju standarde i definišu prava korisnika. Međutim, njihova primena u praksi i dalje zavisi od toga koliko su kompanije spremne da budu transparentne i koliko su sami korisnici svesni svojih prava i odgovornosti. Čak i kada postoje zakonske garancije, njihova efikasnost je ograničena ukoliko korisnici ne razumeju na koji način se njihovi podaci koriste ili ih olako dele.

U tom kontekstu, postavlja se pitanje budućnosti privatnosti: **da li će ona postati luksuz** dostupan samo onima koji mogu sebi da priušte dodatne alate i zaštitu, ili će se tretirati kao osnovno ljudsko pravo koje mora biti jednako zagarantovano svima? Razvoj tehnologije sugeriše da će zaštita privatnosti postajati sve izazovnija, dok društvena odgovornost i regulative moraju raditi u pravcu očuvanja prava pojedinca. Budućnost će verovatno doneti balans između koristi od novih tehnologija i potrebe da se očuva lična sigurnost, ali taj balans će zahtevati stalnu borbu, svest i prilagođavanje i na nivou pojedinaca i na nivou društva u celini.

# ZAKLJUČAK

Privatnost na internetu predstavlja jedan od najkritičnijih problema savremenog društva. Kombinacija lične odgovornosti, svesti o digitalnom tragu, primene tehnoloških rešenja i poštovanja zakonske regulative ključna je za očuvanje privatnosti. Svaki korisnik mora biti svestan posledica svojih online aktivnosti i važnosti zaštite ličnih podataka.

Osnovna poruka je jednostavna, ali važna:

***Ako je usluga besplatna – ti si proizvod.*** Svesnost, obrazovanje i pažljivo korišćenje tehnologije jedini su način da očuvamo privatnost u digitalnom dobu.

# LITERATURA


1. **FTC – zaštita ličnih podataka**: https://consumer.ftc.gov/articles/protect-your-personal-information-hackers-and-scammers
2. **Google – sigurnost i privatnost**: https://safety.google/security-privacy/
3. **StaySafeOnline – upravljanje identitetom i privatnošću**: https://www.staysafeonline.org/articles/7-tips-to-manage-your-identity-and-protect-your-privacy-online
4. **Akademski rad – rizici na društvenim mrežama**: https://arxiv.org/abs/1303.3764
5. **Akademski rad – privatnost po dizajnu (Privacy by Design)**: https://arxiv.org/abs/1501.03726
6. **Vesti – sajber prevare u Australiji**: https://www.news.com.au/technology/online/hacking/nearly-half-of-aussie-internet-users-smashed-by-scammers-last-year/news-story/1788d7d0139389a8ebd5c25b1ea7facd
7. **TechRadar – verifikacija starosti i rizici privatnosti**: https://www.techradar.com/vpn/what-happens-to-your-data-when-you-verify-your-age